COSIC

Publications

Search in our publications database

Filters

Authors

Select...

Leave empty to select all

Type of Publication

Select...

Leave empty to select all

Years

2026 ×
2025 ×
2024 ×
2023 ×
2022 ×
2021 ×
2020 ×
2019 ×

Press x to select all

Status

Published

Press x to select all

□ Limit to international □ Limit to peer-reviewed □ Limit to author

By Year | By Category | By Author

2026

1 [Journal article] S. Manasidis, Q. Norga, S. Kundu and I. Verbauwhede, "MPSpeed: Implementing and Optimizing MPC-in-the-Head Digital Signatures in Hardware", IACR Cryptology ePrint Archive 2026(206), 24 pages, 2026. BibTex LaTex

2 [Journal article] R. Geelen and F. Vercauteren, "Better GBFV Bootstrapping and Faster Encrypted Edit Distance Computation", IACR Cryptology ePrint Archive 2025(1104), 22 pages, 2026. BibTex LaTex

3 [Journal article] E. Desmet, S. Kundu and I. Verbauwhede, "Masking Out of Order: Side-Channel Leaks from Software-Masked Cryptography on Out-of-Order Processors", IACR Cryptology ePrint Archive 2026(123), 19 pages, 2026. BibTex LaTex

4 [Journal article] J. Bos, J. Renes, F. Vercauteren and P. Wang, "Structured Module Lattice-based Cryptography", IACR Cryptology ePrint Archive 2026(98), 23 pages, 2026. BibTex LaTex

5 [Journal article] Y. Chen, Y. Hiraga, N. Mouha, Y. Naito, Y. Sasaki and T. Sugawara, "Beyond-Birthday-Bound Security with HCTR2: Cascaded Construction and Tweak-based Key Derivation", IACR Cryptology ePrint Archive 2026(85), 61 pages, 2026. BibTex LaTex

6 [Journal article] A. Ovchinnikov, A. Rezaei Shahmirzadi and S. Dhooghe, "Uniform Sharing in Multiple Stages: BibTex

NullFresh for Arbitrary Functions", IACR Cryptology ePrint Archive 2026(79), pp. 1-34, 2026. LaTex

7 [Journal article] T. Kitazawa, L. Wouters, B. Gierlichs, D. Fujimoto, I. Verbauwhede and Y. Hayashi, "Active Electromagnetic Side-Channel Analysis: Crossing Physical Security Boundaries through Impedance Variations", IACR Transactions on Cryptographic Hardware and Embedded Systems 2026(1), 26 pages, 2026. BibTex LaTex

8 [Journal article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "Combined Stability: Protecting against Combined Attacks", IACR Transactions on Cryptographic Hardware and Embedded Systems 2026(1), 32 pages, 2026. BibTex LaTex

9 [Journal article] M. Chen and J. Meers, "Timed Commitments and Timed Encryption: Generic Constructions and Instantiations from Isogenies", IACR Cryptology ePrint Archive 2026(57), 26 pages, 2026. BibTex LaTex

10 [Journal article] T. Decru and S. Kunzweiler, "Abelian surfaces in Hesse form and explicit isogeny formulas", IACR Cryptology ePrint Archive 2026(39), 26 pages, 2026. BibTex LaTex

11 [Journal article] K. Baghery and H. Moghaddas, "Fully Secure DKG Protocols for Discrete Logarithm Revisited", IACR Cryptology ePrint Archive , , 2026. BibTex LaTex

12 [Journal article] M. Van Kenhove, E. Pohle, L. Schild, M. Zbudila, M. Sebrechts, F. De Turck, B. Volckaert and A. Abidin, "MOZAIK: A Privacy-Preserving Analytics Platform for IoT Data Using MPC and FHE", arXiv 2601(2245), 49 pages, 2026. BibTex LaTex

13 [Journal article] K. Reijnders, "The Cokernel Pairing", IACR Cryptology ePrint Archive 2026(1), 23 pages, 2026. BibTex LaTex

14 [Journal article] R. Gesteira Minarro, T. Yoshizawa, R. Palacios and G. Lopez, "Highway to Hack – Security Gaps in ETSI ITS Standards", Computer Standards & Interfaces 97, 10 pages, 2026. BibTex LaTex

15 [Journal article] R. Geelen and F. Vercauteren, "Better GBFV Bootstrapping and Faster Encrypted Edit Distance Computation", IACR Communications in Cryptology 2(4), 23 pages, 2026. BibTex LaTex

16 [Journal article] T. Yoshizawa, H. Agarwal, D. Singelée and B. Preneel, "Certificate Revocation - Search for A Way Forward", Computers & Security 163, 17 pages, 2026. BibTex LaTex

17 [Journal article] L. Pirker, Q. Norga, S. Kundu, A. Ganguly, B. Van Leeuwen, A. Karmakar and I. Verbauwhede, "HYPERSHIELD: Protecting the Hypercube MPC-in-the-Head Framework Against Differential Probing Adversaries without Masking", IACR Cryptology ePrint Archive 2026(81), 24 pages, 2026. BibTex LaTex

18 [Thesis] A. Janssens van der Maelen, R. Geelen, J. Kang and J. Spiessens, "Private information retrieval with GBFV: analysis and implementation", Master thesis, KU Leuven, F. Vercauteren, 49 pages, 2026. BibTex LaTex

19 [Thesis] R. Geelen, "Towards Practical Bootstrapping in Fully Homomorphic Encryption", Phd thesis, KU Leuven, I. Verbauwhede and F. Vercauteren, 282 pages, 2026. BibTex LaTex

20 [Thesis] D. Toprakhisar, "On the Gaps in Fault and Combined Attack Security and Efficient Countermeasure Design", Phd thesis, KU Leuven, V. Rijmen and S. Petkova-Nikova, 332 pages, 2026. BibTex LaTex

21 [Thesis] S. Duttagupta, "Analysis and Design of Cryptographic Protocols for IoT Devices", Phd thesis, KU Leuven, B. Preneel and D. Singelée, 256 pages, 2026. BibTex LaTex

22 [Book] T. Yoshizawa, "Security and Privacy of ITS Standards and Their Research Challenges", S. de Luca (Ed.), IntechOpen, 20 pages, 2026. BibTex LaTex

23 [Talk] Q. Norga, "Hardware Cost Evaluation in Microarchitecture Security", 2nd Microarchitecture Security Conference (uASC '26), Leuven, BE, 2026. BibTex LaTex

2025

1 [Conf article] G. Borin, M. Corte-Real Santos, J. Komada Eriksen, R. Invernizzi, M. Mula, S. Schaeffler and F. Vercauteren, "Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies" In Advances in Cryptology - ASIACRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, , 2025. BibTex LaTex

2 [Conf article] S. Dhooghe, A. Ovchinnikov and D. Toprakhisar, "StaMAC: Fault Protection via Stable-MAC Tags " In Advances in Cryptology - ASIACRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, 37 pages, 2025. BibTex LaTex

3 [Conf article] N. El Kassem, W. Hellemans, I. Siachos, E. Dushku, S. Vasileiadis, D. S. Karas, L. Chen, C. Patsakis and T. Giannetsos, "PRIVÉ: Towards Privacy-Preserving Swarm Attestation" In Proceedings of the $E International Conference on Security and Cryptography SECRYPT, SCITEPRESS, pp. 247-262, 2025. BibTex LaTex

4 [Conf article] R. Sarenche, A. Aghabagherloo, S. Petkova-Nikova and B. Preneel, "Bitcoin under Volatile Block Rewards: How Mempool Statistics Can Influence Bitcoin Mining" In Proceedings of ACM CCS 2025, Association for Computing Machinery (ACM), ACM, pp. 903-917, 2025. BibTex LaTex

5 [Conf article] S. Kundu, Q. Norga, A. Karmakar, U. Ojha, A. Ganguly and I. Verbauwhede, "mUOV: Masking the Unbalanced Oil and Vinegar Digital Signature Scheme at First- and Higher-Order" In Proceedings of ACM CCS 2025, Association for Computing Machinery (ACM), ACM, pp. 1994-2008, 2025. BibTex LaTex

6 [Conf article] A. Bhati, E. Andreeva, S. Müller and D. Vizár, "Sonikku: Gotta Speed, Keed! A Family of Fast and Secure MACs" In Cryptology and Network Security , Lecture Notes in Computer Science, Springer-Verlag, 32 pages, 2025. BibTex LaTex

7 [Conf article] P. Schwarz, E. Pohle, A. Abidin and B. Preneel, "Evaluating Ascon in Secure Multi-Party Computation using Reverse Multiplication-Friendly Embeddings" In Proceedings of the 24 annual ACM workshop on Privacy in the electronic society, Association for Computing Machinery (ACM), ACM, pp. 60-74, 2025. BibTex LaTex

8 [Conf article] J. De Meulemeester, Q. Norga, F. Piessens, I. Verbauwhede and M. Bognar, "Hardware Cost Evaluation in Systems Security" In ACM REP 2025: Proceedings of the 3 ACM Conference on Reproducibility and Replicability, Association for Computing Machinery, pp. 229-233, 2025. BibTex LaTex

9 [Conf article] P. Sluys, L. Wouters, B. Gierlichs and I. Verbauwhede, "Partial Key Overwrite Attacks in Microcontrollers: a Survey" In CASCADE 2025, Lecture Notes in Computer Science 15952, Springer-Verlag, pp. 429-447, 2025. BibTex LaTex

10 [Conf article] Q. Norga, J. D'Anvers, S. Kundu and I. Verbauwhede, "X2X: Low-Randomness and High-Throughput A2B and B2A Conversions for d+1 shares in Hardware" In CASCADE 2025, Lecture Notes in Computer Science 15952, Springer-Verlag, pp. 119-158, 2025. BibTex LaTex

11 [Conf article] K. Kluczniak and L. Schild, "FDFB2: Full-Domain Functional Bootstrapping with Function Amortization" In Workshop on Encrypted Computing and Applied Homomorphic Cryptography 2025, Association for Computing Machinery (ACM), pp. 13-25, 2025. BibTex LaTex

12 [Conf article] W. Castryck, R. Invernizzi, G. Lorenzon, J. Meers and F. Vercauteren, "Orient Express: Using Frobenius to Express Oriented Isogenies" In Progress in Cryptology - LATINCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 145-173, 2025. BibTex LaTex

13 [Conf article] K. Reijnders, "The Tate Profile" In Progress in Cryptology - LATINCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 209-233, 2025. BibTex LaTex

14 [Conf article] K. Bogner, A. Abidin and D. Singelée, "Continuous Variable Quantum Distance Bounding" In IEEE INFOCOM 2025 Workshop, IEEE, 6 pages, 2025. BibTex LaTex

15 [Conf article] X. Limani, A. Troch, M. Van Kenhove, A. Papageorgiou, F. De Turck, E. Pohle, L. Schild, M. Zbudila, A. Abidin, B. Volckaert, M. Camelo Botero, J. Marquez-Barja and N. Slamnik-Kriještorac, "End-to-End Network Slicing: Securing Sensitive Data Across the Network" In COMMUNICATIONS IN CHINA. IEEE/CIC INTERNATIONAL CONFERENCE. 2025, IEEE Computer Society, IEEE, 6 pages, 2025. BibTex LaTex

16 [Conf article] D. Chaum, R. Carback, J. Clark, C. Liu, M. Nejadgholi, B. Preneel, A. Sherman, M. Yaksetig, Z. Yin, F. Zagórski and B. Zhang, "Revisiting Silent Coercion" In International Joint Conference on Electronic Voting 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 38-54, 2025. BibTex LaTex

17 [Conf article] W. Hellemans, N. El Kassem, M. Rabbani, E. Dushku, L. Chen, A. Braeken, B. Preneel and N. Mentens, "SPARK: Secure Privacy-Preserving Anonymous Swarm Attestation for In-Vehicle Networks" In 10 IEEE European Symposium on Security and Privacy (Euro S&P 2025), IEEE, 20 pages, 2025. BibTex LaTex

18 [Conf article] R. Sarenche, E. Tas, B. Monnot, C. Schwarz-Schilling and B. Preneel, "Commitment Attacks on Ethereum's Reward Mechanism" In 10 IEEE European Symposium on Security and Privacy (Euro S&P 2025), IEEE, pp. 504-526, 2025. BibTex LaTex

19 [Conf article] A. Bhati and E. Andreeva, "Breaking the IEEE Encryption Standard -- XCB-AES in Two Queries" In Advances in Cryptology - CRYPTO 2025, Lecture Notes in Computer Science 16003, Y. Kalai and S. Kamara (Eds.), Springer-Verlag, pp. 172-199, 2025. BibTex LaTex

20 [Conf article] K. Cong, E. Orsini, E. Pohle and O. Zajonc, "Row Reduction Techniques for n-Party Garbling" In Advances in Cryptology - CRYPTO 2025, Lecture Notes in Computer Science 16003, Y. Kalai and S. Kamara (Eds.), Springer-Verlag, pp. 522-555, 2025. BibTex LaTex

21 [Conf article] A. Robinson, S. Arpin, J. Lau, A. Mesnard, R. Perlner, J. Tillich and V. Vasseur, "Error Floor Prediction with Markov Models for QC-MDPC Codes" In Advances in Cryptology - CRYPTO 2025, Lecture Notes in Computer Science 16003, Y. Kalai and S. Kamara (Eds.), Springer-Verlag, pp. 221-252, 2025. BibTex LaTex

22 [Conf article] P. Dartois, J. Komada Eriksen, T. Fouotsa, A. Herledan le Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren and B. Wesolowski, "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies" In Advances in Cryptology - CRYPTO 2025, Lecture Notes in Computer Science 16003, Y. Kalai and S. Kamara (Eds.), Springer-Verlag, pp. 67-99, 2025. BibTex LaTex

23 [Conf article] W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit and Y. Bo Ti, "KLPT²: Algebraic Pathfinding in Dimension Two and Applications" In Advances in Cryptology - CRYPTO 2025, Lecture Notes in Computer Science 16003, Y. Kalai and S. Kamara (Eds.), Springer-Verlag, pp. 167-200, 2025. BibTex LaTex

24 [Conf article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "Picking up the Fallen Mask: Breaking and Fixing the RS-Mask Countermeasure" In Selected Areas in Cryptography, 40 Annual International Workshop, SAC 2025, Lecture Notes in Computer Science, Springer-Verlag, 22 pages, 2025. BibTex LaTex

25 [Conf article] H. Morita, E. Pohle, K. Sadakane, P. Scholl, K. Tozawa and D. Tschudi, "MAESTRO: Multi-Party AES Using Lookup Tables" In 34 USENIX Security Symposium 2025, L. Bauer and G. Pellegrino (Eds.), Usenix, pp. 1965-1984, 2025. BibTex LaTex

26 [Conf article] W. Legiest, J. D'Anvers, B. Spasic, N. Tran and I. Verbauwhede, "Leuvenshtein: Efficient FHE-based Edit Distance Computation with Single Bootstrap per Cell" In 34 USENIX Security Symposium 2025, L. Bauer and G. Pellegrino (Eds.), Usenix, 18 pages, 2025. BibTex LaTex

27 [Conf article] A. Mertens, G. Nicolas and S. Rovira Cisterna, "Convolution-Friendly Image Compression with FHE" In Progress in Cryptology - AFRICACRYPT 2025, Lecture Notes in Computer Science, V. Rijmen, S. Petkova-Nikova and A. Nitaj (Eds.), Springer-Verlag, pp. 3-24, 2025. BibTex LaTex

28 [Conf article] N. Antonijević, S. Duttagupta, D. Singelée, E. Argones Rúa and B. Preneel, "ZeroTouch: Reinforcing RSS for Secure Geofencing" In 30 ACM Symposium on Access Control Models and Technologies , Association for Computing Machinery (ACM), ACM, 13 pages, 2025. BibTex LaTex

29 [Conf article] A. Bhati, E. Andreeva, S. Müller and D. Vizár, "Sonikku: Gotta Speed, Keed! A Family of Fast and Secure MACs" In ArcticCrypt 2025, 32 pages, 2025. BibTex LaTex

30 [Conf article] M. Mahdavi, E. Meamari, E. Heydari Beni and M. Sheikhi, "Leveled Homomorphic Encryption over Composite Groups" In Progress in Cryptology - AFRICACRYPT 2025, Lecture Notes in Computer Science, V. Rijmen, S. Petkova-Nikova and A. Nitaj (Eds.), Springer-Verlag, pp. 25-50, 2025. BibTex LaTex

31	[Conf article] T. Vlummens and G. Acar, "Formguard: Continuous Privacy Testing for Websites Using Automated Interaction Replay" In Proceedings of IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), L. O'Conner (Ed.), IEEE, pp. 260-268, 2025.	BibTex LaTex
32	[Conf article] I. Siros, D. Singelée and B. Preneel, "CovFUZZ: Coverage-based fuzzer for 4G&5G protocols" In 10 IEEE European Symposium on Security and Privacy (Euro S&P 2025), IEEE, pp. 737-754, 2025.	BibTex LaTex
33	[Conf article] M. Alea, M. Rosa, S. Farfalha, K. Myny and G. Gielen, "DERMIS: Toward a Fully-Integrated Large-Area High-Resolution Tactile Slip Sensing Solution" In IEEE International Symposium on Circuits and Systems (ISCAS 2025), IEEE, 5 pages, 2025.	BibTex LaTex
34	[Conf article] M. Velazquez Lopez, S. Olafusi, F. Berghmans, N. Papadopoulos and K. Myny, "In pixel VCO-based 5V 58.5µW Capacitance Sensing for Large Area Electrowetting Arrays" In IEEE International Symposium on Circuits and Systems (ISCAS 2025), IEEE, 5 pages, 2025.	BibTex LaTex
35	[Conf article] M. Rahimi, "PARSAN-Mix: Packet-Aware Routing and Shuffling with Additional Noise for Latency Optimization in Mix Networks" In Applied Cryptography and Network Security - ACNS 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 159-188, 2025.	BibTex LaTex
36	[Conf article] K. Baghery, N. Knapen, G. Nicolas and M. Rahimi, "Pre-Constructed Publicly Verifiable Secret Sharing and Applications" In Applied Cryptography and Network Security - ACNS 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 89-119, 2025.	BibTex LaTex
37	[Conf article] M. Zbudila, A. Abidin and B. Preneel, "Exploring Adversarial Attacks on the MaSTer Truncation Protocol" In IH&MMSEC 2025: ACM Workshop on Information Hiding and Multimedia Security Proceedings, Association for Computing Machinery (ACM), ACM, pp. 86-97, 2025.	BibTex LaTex
38	[Conf article] D. Bouakaz, M. Dandekar, J. Biesmans, W. Dehaene and K. Myny, "1kb IGZO TFT Based Flexible SRAM for IoT Applications" In IMW2025_proceeding, ISBN, IEEE, 4 pages, 2025.	BibTex LaTex
39	[Conf article] C. Ozkan and D. Singelée, "A Novel Evidence-Based Threat Enumeration Methodology for ICS" In (WNDSS) International Workshop on Network and Distributed Systems Security 2025 , Lecture Notes in Computer Science, Springer-Verlag, pp. 175-188, 2025.	BibTex LaTex
40	[Conf article] A. Aghabagherloo, A. Abadi, S. Sarkar, V. Asutosh Dasu and B. Preneel, "Impact of Data Duplication on Deep Neural Network-Based Image Classifiers: Robust vs. Standard Models" In 2025 DLSP - IEEE Symposium on Security and Privacy Workshop (SP), IEEE, 8 pages, 2025.	BibTex LaTex
41	[Conf article] A. Aghabagherloo, R. Sarenche, M. Zarezadeh, B. Preneel and S. Kopsell, "Priv-PFL: A Privacy-Preserving and Efficient Personalized Federated Learning Approach" In 2025 DLSP - IEEE Symposium on Security and Privacy Workshop (SP), IEEE, 6 pages, 2025.	BibTex LaTex
42	[Conf article] Y. Guo, R. Degraeve, P. Saraza-Canflanca, B. Kaczer, E. Bury and I. Verbauwhede, "Effects of Temperature and Device-to-Device Variability in pFET-Based Bias Temperature Instability Reservoir Computing" In IEEE International Reliability Physics Symposium 2017, IEEE, 7 pages, 2025.	BibTex LaTex
43	[Conf article] J. De Meulemeester, L. Wilke, D. Oswald, T. Eisenbarth, I. Verbauwhede and J. Van Bulck, "BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments" In IEEE Symposium on Security and Privacy 2025, IEEE Computer Society, IEEE, pp. 4117-4135, 2025.	BibTex LaTex
44	[Conf article] D. Monaco, N. Antonijević, S. Duttagupta, D. Singelée, A. Sacco, E. Marín Fàbregas and B. Preneel, "PathSafe: Secure Path Verification in Software-Defined Networks" In IEEE/IFIP Network Operations and Management Symposium 2025, IEEE/IFIP, 9 pages, 2025.	BibTex LaTex
45	[Conf article] A. Basso, G. Borin, W. Castryck, M. Corte-Real Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren and B. Wesolowski, "PRISM: Simple And Compact Identification and Signatures From Large Prime Degree Isogenies" In Public Key Cryptography, 28 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 300-332, 2025.	BibTex LaTex

46 [Conf article] S. Duttagupta and D. Singelée, "PISA: Privacy-Preserving Smart Parking" In 2025 22 IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE Xplore, 4 pages, 2025. BibTex LaTex

47 [Conf article] B. Allombert, J. Biasse, J. Komada Eriksen, P. Kutas, C. Leonardi, A. Page, R. Scheidler and M. Tot Bagi, "Faster SCALLOP from non-prime conductor suborders in medium sized quadratic fields" In Public Key Cryptography, 5 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2002, Lecture Notes in Computer Science 2274, D. Naccache and P. Paillier (Eds.), Springer-Verlag, 30 pages, 2025. BibTex LaTex

48 [Conf article] A. Flórez-Gutiérrez, E. Lambooij, G. Leurent, H. Raddum, T. Tiessen and M. Verbauwhede, "Cryptanalysis of Full SCARF" In Advances in Cryptology - EUROCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2025. BibTex LaTex

49 [Conf article] Y. Chen, A. Dutta, A. Jha and M. Nandi, "Towards Optimally Secure Deterministic Authenticated Encryption Schemes" In Advances in Cryptology - EUROCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, 39 pages, 2025. BibTex LaTex

50 [Conf article] S. Hou, M. Li, K. Hu, S. Wang and B. Preneel, "Revisiting Truncated Differential Attack from the Perspective of Equivalent Propagation Equations" In Information Security and Cryptology - Inscrypt 2024, Lecture Notes in Computer Science, D. Lin, M. Wang and M. Yung (Eds.), Springer-Verlag, pp. 361-381, 2025. BibTex LaTex

51 [Conf article] K. Baghery, "Π: A Unified Framework for Computational Verifiable Secret Sharing" In Public Key Cryptography, 28 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2025, Lecture Notes in Computer Science, Springer-Verlag, 35 pages, 2025. BibTex LaTex

52 [Conf article] R. Geelen and F. Vercauteren, "Fully Homomorphic Encryption for Cyclotomic Prime Moduli" In Advances in Cryptology - EUROCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 366-397, 2025. BibTex LaTex

53 [Conf article] M. Chen and C. Petit, "Computing the Endomorphism Ring of a Supersingular Elliptic Curve from a Full Rank Suborder" In Advances in Cryptology - EUROCRYPT 2025, Lecture Notes in Computer Science, Springer-Verlag, pp. 446-474, 2025. BibTex LaTex

54 [Conf article] M. Hassan, J. Vliegen, S. Picek and N. Mentens, "Designing Hardware-Friendly Hash Functions for Network Security Using Cartesian Genetic Programming" In Applications of Evolutionary Computation, Lecture Notes in Computer Science, Springer-Verlag, pp. 221-237, 2025. BibTex LaTex

55 [Conf article] R. Sarenche, S. Petkova-Nikova and B. Preneel, "Mining Power Destruction Attacks in the Presence of Petty-Compliant Mining Pools" In International Conference on Financial Cryptography and Data Security - FC 2025, Lecture Notes in Computer Science, Springer-Verlag, , 2025. BibTex LaTex

56 [Conf article] A. Sateesan, J. Vliegen and N. Mentens, "FLARE: An FPGA-Based Universal Large Flow Detection Engine" In Proceedings of the 21 International Symposium on Applied Reconfigurable Computing (ARC 2025), Springer LNCS 15594, R. Giorgi, M. Stojilović, D. Stroobandt, P. Brox Jiménez and Á. Barriga Barros (Eds.), Springer, Cham, pp. 106-120, 2025. BibTex LaTex

57 [Conf article] Q. Norga, S. Kundu, U. Ojha, A. Ganguly, A. Karmakar and I. Verbauwhede, "Masking Gaussian Elimination at Arbitrary Order, with Application to Multivariate- and Code-Based PQC" In Topics in Cryptology - CT-RSA 2025, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 15598, A. Patra (Ed.), Springer-Verlag, pp. 249-272, 2025. BibTex LaTex

58 [Conf article] K. Cong, R. Geelen, J. Kang and J. Park, "Revisiting Oblivious Top-k Selection with Applications to Secure k-NN Classification" In Selected Areas in Cryptography, 39 Annual International Workshop, SAC 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 3-25, 2025. BibTex LaTex

59 [Conf article] V. Mishra, A. Abidin and B. Preneel, "The Accountability Strikes Back: Decentralizing the Key BibTex

Generation in CL-PKC with Traceable Ring Signatures" In Charting the Intelligence Frontiers – Edge AI Systems Nexus 2024, pp. 379-398, 2025. LaTex

60 [Conf article] S. Arpin, W. Castryck, J. Komada Eriksen, G. Lorenzon and F. Vercauteren, "Generalized class group actions on oriented elliptic curves with level structure" In International Workshop on the Arithmetic of Finite Fields (WAIFI 2024), Lecture Notes in Computer Science, Springer-Verlag, pp. 171-190, 2025. BibTex LaTex

61 [Conf article] M. Rahimi, P. Kumar and C. Diaz, "LAMP: Lightweight Approaches for Latency Minimization in Mixnets with Practical Deployment Considerations" In Network and Distributed System Security Symposium (NDSS 2025), Internet Society, 19 pages, 2025. BibTex LaTex

62 [Conf article] S. Cai, M. Chen and C. Petit, "Faster Algorithms for Isogeny Computations over Extensions of Finite Fields" In Number Theoretic Methods in Cryptology - Proceedings, Lecture Notes in Computer Science 14966, A. Dąbrowski, J. Pieprzyk and J. Pomykała (Eds.), Springer-Verlag, pp. 136-155, 2025. BibTex LaTex

63 [Conf article] N. Vander Meeren, S. Van Beek, M. Monteiro, F. Garcia-Redondo, J. Chatterjee, A. Kumar, K. Wostyn, S. Couet and I. Verbauwhede, "Magnetic immunity of STT-MRAM: external magnetic field orientation impact on writing reliability" In IEEE International Electron Devices Meeting 2024, IEEE , 4 pages, 2025. BibTex LaTex

64 [Journal article] Q. Norga, S. Kundu and I. Verbauwhede, "ML-DSA-OSH: An Efficient, Open-Source Hardware Implementation of ML-DSA", IACR Cryptology ePrint Archive 2025(2337), 7 pages, 2025. BibTex LaTex

65 [Journal article] B. Askin Ozdemir and V. Rijmen, "Analysis of Diffusion Properties in Generalized Feistel Ciphers under Multidimensional Linear Cryptanalysis", IACR Cryptology ePrint Archive 2025(2337), 33 pages, 2025. BibTex LaTex

66 [Journal article] R. Sarenche, S. Duttagupta, F. Milizia, K. Bogner and V. Mishra, "Distributed Symmetric Key Establishment with Forward Secrecy for Implantable Medical Devices", IACR Cryptology ePrint Archive 2025(2322), 19 pages, 2025. BibTex LaTex

67 [Journal article] H. Cui, G. Luo, J. Lau, J. Bao, J. Balasch and I. Verbauwhede, "Extending and Accelerating Inner Product Masking with Fault Detection via Instruction Set Extension", IACR Cryptology ePrint Archive 2025(2165), 8 pages, 2025. BibTex LaTex

68 [Journal article] J. Bobolz, E. Heydari Beni, A. Lehmann, O. Mirzamohammadi, C. Özbay and S. Sedaghat, "Multi-Verifier Keyed-Verification Anonymous Credentials", IACR Cryptology ePrint Archive 2025(2156), 64 pages, 2025. BibTex LaTex

69 [Journal article] I. Siros, J. Heirwegh, D. Singelée and B. Preneel, "ThreadFuzzer: Fuzzing Framework for Thread Protocol", arXiv , 15 pages, 2025. BibTex LaTex

70 [Journal article] D. Shanmugasundaram Veeraraghavan, B. Gierlichs and I. Verbauwhede, "A Graph-Theoretic Framework for Randomness Optimization in First-Order Masked Circuits", IACR Cryptology ePrint Archive 2025(2102), 7 pages, 2025. BibTex LaTex

71 [Journal article] S. Das, R. Invernizzi, P. Kutas and J. Meers, "Leveled Isogeny Problems with Hints", IACR Cryptology ePrint Archive 2025(2075), 26 pages, 2025. BibTex LaTex

72 [Journal article] S. Banerjee and S. Duttagupta, "TreeCast: Multi-Party Key Establishment Protocol for IoT Devices", IACR Cryptology ePrint Archive 2025(2021), 8 pages, 2025. BibTex LaTex

73 [Journal article] S. Atapoor, K. Baghery, G. Nicolas, R. Pedersen and J. Spiessens, "Batched and Packed (Publicly) Verifiable Secret Sharing: A Unified Framework and Applications", IACR Cryptology ePrint Archive 2025(2018), 45 pages, 2025. BibTex LaTex

74 [Journal article] P. Dartois, J. Komada Eriksen, R. Invernizzi and F. Vercauteren, "qt-Pegasis: Simpler and Faster Effective Class Group Actions", IACR Cryptology ePrint Archive 2025(1859), 38 pages, 2025. BibTex LaTex

75 [Journal article] J. Bertels and I. Verbauwhede, "A High Throughput Kyber NTT", IACR Cryptology ePrint BibTex

Archive 2025(1763), 5 pages, 2025. PDF 🔗 LaTex

76 [Journal article] A. Neyt and T. Beyne, "Improved Differential Cryptanalysis of SPEEDY", IACR Transactions on Symmetric Cryptology 2025(3), pp. 444-474, 2025. PDF BibTex LaTex

77 [Journal article] T. Morrison, J. Lau, E. Orvis, G. Scullard and L. Zobernig, "Zeta functions of abstract isogeny graphs and modular curves", arXiv , 39 pages, 2025. PDF 🔗 BibTex LaTex

78 [Journal article] M. Zbudila, A. Suresh, H. Yalame, O. Mirzamohammadi, A. Abidin and B. Preneel, "SoK: Connecting the Dots in Privacy-Preserving ML - Systematization of MPC Protocols and Conversions Between Secret Sharing Schemes", IACR Cryptology ePrint Archive 2025(1679), 46 pages, 2025. PDF 🔗 BibTex LaTex

79 [Journal article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "Combined Stability: Protecting against Combined Attacks", IACR Cryptology ePrint Archive 2025(1692), 32 pages, 2025. PDF 🔗 BibTex LaTex

80 [Journal article] Y. Dang, M. Grujic, B. Yang, W. Zhu, M. Zhu, I. Verbauwhede and L. Liu, "Entropy extractor based high-throughput post-processings for True Random Number Generators", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(4), pp. 145-171, 2025. PDF 🔗 BibTex LaTex

81 [Journal article] E. Lambooij, P. Neumann, M. Verbauwhede, S. Wang and T. Zhang, "Meet-in-the-Middle Attacks on Full ChiLow-32", IACR Cryptology ePrint Archive 2025(1601), 17 pages, 2025. PDF 🔗 BibTex LaTex

82 [Journal article] A. Anarjan, C. Ozkan, H. Ergun, D. Hertem and D. Singelée, "An advanced cybersecurity risk assessment framework: Integrating vulnerabilities and exploitation techniques for systematic attack path analysis in multilayered power system networks", Sustainable Energy, Grids and Networks , 21 pages, 2025. 🔗 BibTex LaTex

83 [Journal article] C. Beierle and T. Beyne, "A degree bound for planar functions", Combinatorial Theory 5(3), 26 pages, 2025. PDF 🔗 BibTex LaTex

84 [Journal article] E. Andreeva, A. Bhati and A. Weninger, "Multiforked Iterated Even-Mansour and a Note on the Tightness of IEM Proofs", IACR Cryptology ePrint Archive 2025(1543), 24 pages, 2025. PDF 🔗 BibTex LaTex

85 [Journal article] S. Duttagupta, D. Singelée, X. Carpent, V. Guler, T. Yoshizawa, S. Aghili, A. Abidin and B. Preneel, "CARPOOL: Secure And Reliable Proof of Location", IACR Cryptology ePrint Archive 2025(1502), 15 pages, 2025. 🔗 BibTex LaTex

86 [Journal article] T. Beyne, G. Leander and I. Schütt, "Pairwise independence of AES-like block ciphers", IACR Cryptology ePrint Archive 2025(1495), 33 pages, 2025. PDF 🔗 BibTex LaTex

87 [Journal article] C. Bonte, G. Nicolas and N. Smart, "Complex Elections via Threshold (Fully) Homomorphic Encryption", IACR Cryptology ePrint Archive 2025(1482), 30 pages, 2025. PDF 🔗 BibTex LaTex

88 [Journal article] A. Ali, J. Choi, B. Gipson, S. Gorantala, J. Kun, W. Legiest, L. Lim, A. Viand, M. Zerihun Demissie and H. Zheng, "HEIR: A Universal Compiler for Homomorphic Encryption", arXiv , 31 pages, 2025. PDF 🔗 BibTex LaTex

89 [Journal article] A. Basso, J. Bos, J. D'Anvers, A. Karmakar, J. Bermudo Mera, J. Renes, S. Sinha Roy, F. Vercauteren, P. Wang, Y. Wang, S. Zhang and C. Zhong, "Using Learning with Rounding to Instantiate Post-Quantum Cryptographic Algorithms", IACR Cryptology ePrint Archive 2025(1382), 35 pages, 2025. PDF 🔗 BibTex LaTex

90 [Journal article] W. Hellemans, L. Le Jeune, M. Rabbani, B. Preneel and N. Mentens, "Toward a Real-Time Intrusion Detection System for Modern In-Vehicle Networks", IEEE Transactions on Intelligent Transportation Systems , pp. 1-15, 2025. 🔗 BibTex LaTex

91 [Journal article] X. Pottier, J. D'Anvers, T. de Ruijter and I. Verbauwhede, "SMOOTHIE: (Multi-)Scalar Multiplication Optimizations On TFHE", IACR Cryptology ePrint Archive , 28 pages, 2025. PDF 🔗 BibTex LaTex

92 [Journal article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "Picking up the Fallen Mask: Breaking and Fixing the RS-Mask Countermeasure", IACR Cryptology ePrint Archive 2025(1320), 22 pages, 2025. ▶ 🔗 BibTex LaTex

93

[Journal article] H. Xu, M. Gama, E. Heydari Beni and J. Kang, "FRIttata: Distributed Proof Generation of FRI-based SNARKs", IACR Cryptology ePrint Archive 2025(1285), 30 pages, 2025. BibTex LaTex

94 [Journal article] G. Avoine, X. Carpent and D. Leblanc-Albarel, "In the Vault, But Not Safe: Exploring the Threat of Covert Password Manager Providers", IACR Cryptology ePrint Archive 2025(1278), 12 pages, 2025. BibTex LaTex

95 [Journal article] S. Duttagupta, A. Kolozyan, G. Nicolas, B. Preneel and D. Singelée, "What's the Matter? An In-Depth Security Analysis of the Matter Protocol", IACR Cryptology ePrint Archive 2025(1268), 33 pages, 2025. BibTex LaTex

96 [Journal article] G. Pope, K. Reijnders, D. Robert and B. Smith, "Simpler and Faster Pairings from the Montgomery Ladder", IACR Communications in Cryptology -12(2), 29 pages, 2025. BibTex LaTex

97 [Journal article] K. Baghery, N. Ghaedi Bardeh, S. Khazaei and M. Rahimi, "On Round-Optimal Computational VSS", IACR Communications in Cryptology 2(2), pp. 1-22, 2025. BibTex LaTex

98 [Journal article] M. Corte-Real Santos, J. Komada Eriksen, A. Leroux, M. Meyer and L. Panny, "Evaluation of Modular Polynomials from Supersingular Elliptic Curves.", IACR Cryptology ePrint Archive 2025(1154), 30 pages, 2025. BibTex LaTex

99 [Journal article] M. Corte-Real Santos, J. Komada Eriksen, A. Leroux, M. Meyer and L. Panny, "Evaluation of Modular Polynomials from Supersingular Elliptic Curves", IACR Cryptology ePrint Archive 2025(1154), 30 pages, 2025. BibTex LaTex

100 [Journal article] K. Miteloudi, L. Batina and N. Mentens, "A5/3 make or break: A massively parallel FPGA architecture for exhaustive key search", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(3), pp. 361-388, 2025. BibTex LaTex

101 [Journal article] W. Castryck, R. Invernizzi, G. Lorenzon, J. Meers and F. Vercauteren, "Orient Express: Using Frobenius to Express Oriented Isogenies", IACR Cryptology ePrint Archive 2025(1047), 30 pages, 2025. BibTex LaTex

102 [Journal article] S. Petkova-Nikova, S. Andreoli, P. Stănică, L. Budaghyan and E. Piccione, "On Decompositions of Permutations in Quadratic Functions", Journal of Cryptology 38, 22 pages, 2025. BibTex LaTex

103 [Journal article] R. Jadoul, B. Van Leeuwen and O. Zajonc, "Multiparty FHE Redefined: A Framework for Unlimited Participants", IACR Cryptology ePrint Archive 2025(965), 30 pages, 2025. BibTex LaTex

104 [Journal article] R. Jadoul, B. Van Leeuwen and O. Zajonc, "An Efficient Framework for Collusion Resistant Multiparty FHE", IACR Cryptology ePrint Archive 2025(965), 28 pages, 2025. BibTex LaTex

105 [Journal article] U. Banerjee, C. Juvekar, Y. Lee, L. Liu, S. Mathew, T. Poppelmann, S. Sen, T. Sugawara, I. Verbauwhede and R. Tugce Yazicigil, "Writing a Good Security Paper for ISSCC (2025)", arXiv , 4 pages, 2025. BibTex LaTex

106 [Journal article] A. Raisiardali, K. Iordanou, J. Kufel, K. Gudimetla, K. Myny and E. Ozer, "Flexing RISC-V Instruction Subset Processors to Extreme Edge", arXiv , 18 pages, 2025. BibTex LaTex

107 [Journal article] A. Raisiardali, K. Iordanou, J. Kufel, K. Gudimetla, K. Myny and E. Ozer, "Flexing RISC-V Instruction Subset Processors to Extreme Edge", arXiv , 18 pages, 2025. BibTex LaTex

108 [Journal article] T. de Ruijter, J. D'Anvers and I. Verbauwhede, "Don't be mean: Reducing Approximation Noise in TFHE through Mean Compensation", IACR Cryptology ePrint Archive 2025(809), 23 pages, 2025. BibTex LaTex

109 [Journal article] M. Zbudila, A. Abidin and B. Preneel, "Exploring Adversarial Attacks on the MaSTer Truncation Protocol", IACR Cryptology ePrint Archive 2025(773), 15 pages, 2025. BibTex LaTex

110 [Journal article] A. Huszak, T. Yoshizawa, A. Aghabagherloo, D. Singelée and B. Preneel, "On Performance Improvement of Reinforcement Learning for Collision Avoidance in Autonomous Intersections", IEEE Access 13, pp. 189225-189241, 2025. BibTex LaTex

111 [Journal article] C. Bootland, K. Cong, D. Demmler, T. Frederiksen, B. Libert, J. Orfila, D. Rotaru, N. Smart, T. Tanguy, S. Tap and M. Walter, "Threshold (Fully) Homomorphic Encryption", IACR Cryptology ePrint Archive 2025(699), 259 pages, 2025. BibTex LaTex

112 [Journal article] J. Kang and L. Schild, "Pirouette: Query Efficient Single-Server PIR", IACR Cryptology ePrint Archive 2025(680), 13 pages, 2025. BibTex LaTex

113 [Journal article] P. Sluys, L. Wouters, B. Gierlichs and I. Verbauwhede, "An in-depth security evaluation of the Nintendo DSi gaming console", IACR Cryptology ePrint Archive 2025(568), 20 pages, 2025. BibTex LaTex

114 [Journal article] K. Reijnders, "A Note on the Advanced Use of the Tate Pairing", IACR Cryptology ePrint Archive 2025(477), 11 pages, 2025. BibTex LaTex

115 [Journal article] S. Dhooghe, A. Ovchinnikov and D. Toprakhisar, "StaMAC: Fault Protection via Stable-MAC Tags", IACR Cryptology ePrint Archive 2025(455), 37 pages, 2025. BibTex LaTex

116 [Journal article] P. Dartois, J. Komada Eriksen, T. Fouotsa, A. Herledan le Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren and B. Wesolowski, "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies", IACR Cryptology ePrint Archive 2025(401), 62 pages, 2025. BibTex LaTex

117 [Journal article] W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit and Y. Bo Ti, "KLPT^2: Algebraic Pathfinding in Dimension Two and Applications", IACR Cryptology ePrint Archive 2025(372), 54 pages, 2025. BibTex LaTex

118 [Journal article] K. Baghery, E. Ebrahimi, O. Mirzamohammadi and S. Sedaghat, "Traceable Verifiable Secret Sharing and Applications", IACR Cryptology ePrint Archive 2025(318), 44 pages, 2025. BibTex LaTex

119 [Journal article] R. Siyadatzadeh, F. Mehrafrooz, N. Mentens and T. Stefanov, "P2W: From Power Traces to Weights Matrix -- An Unconventional Transfer Learning Approach", arXiv , 26 pages, 2025. BibTex LaTex

120 [Journal article] S. Taylor, P. Melas, M. Jaatun, A. Omerovic, R. Seidl, N. Goetze, J. Kuhr, D. Prosvirin, M. Leone, P. De Lutiis, A. Kuznetsov, A. Gritskevich, G. Triantafyllou,, A. Mpantis, O. Garcia Perales, B. Wenning and S. Duttagupta, "Toward Cybersecurity Testing and Monitoring of IoT Ecosystems", arXiv , 28 pages, 2025. BibTex LaTex

121 [Journal article] J. Alich, A. Askeland, S. Banik, T. Beyne, A. Canteaut, P. Felke, G. Leander, W. Meier and L. Stennes, "Observations on TETRA Encryption Algorithm TEA-3", IACR Cryptology ePrint Archive 2024(2045), 33 pages, 2025. BibTex LaTex

122 [Journal article] T. Beyne, Y. Chen and M. Verbauwhede, "A Robust Variant of ChaCha20-Poly1305", IACR Cryptology ePrint Archive 2025(222), 46 pages, 2025. BibTex LaTex

123 [Journal article] T. Beyne and M. Verbauwhede, "Cryptanalysis of a nonlinear filter-based stream cipher", IACR Cryptology ePrint Archive 2025(197), 8 pages, 2025. BibTex LaTex

124 [Journal article] J. Bertels, H. Lima Pereira and I. Verbauwhede, "FINAL bootstrap acceleration on FPGA using DSP-free constant-multiplier NTTs", IACR Cryptology ePrint Archive 2025(137), 23 pages, 2025. BibTex LaTex

125 [Journal article] A. Basso, G. Borin, W. Castryck, M. Corte-Real Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren and B. Wesolowski, "PRISM: Simple And Compact Identification and Signatures From Large Prime Degree Isogenies", IACR Cryptology ePrint Archive 2025(135), 36 pages, 2025. BibTex LaTex

126 [Journal article] I. Thakur, A. Karmakar, C. Li and B. Preneel, "A Survey on Transciphering and Symmetric Ciphers for Homomorphic Encryption", IACR Cryptology ePrint Archive 2025(93), 35 pages, 2025. BibTex LaTex

127 [Journal article] R. Sarenche, A. Aghabagherloo, S. Petkova-Nikova and B. Preneel, "Bitcoin Under Volatile Block Rewards: How Mempool Statistics Can Influence Bitcoin Mining", arXiv , 21 pages, 2025. BibTex LaTex

128 [Journal article] O. Mirzamohammadi, J. Bobolz, S. Sedaghat, E. Heydari Beni, A. Abidin, D. Singelée and B. Preneel, "Keyed-Verification Anonymous Credentials with Highly Efficient Partial Disclosure", IACR Communications in Cryptology 2(3), 50 pages, 2025. BibTex LaTex

129 [Journal article] W. Legiest, J. D'Anvers, B. Spasic, N. Tran and I. Verbauwhede, "Leuvenshtein: Efficient FHE-based Edit Distance Computation with Single Bootstrap per Cell", IACR Cryptology ePrint Archive 2025(12), 30 pages, 2025. BibTex LaTex

130 [Journal article] X. Pottier, T. de Ruijter, J. Bertels, W. Legiest, M. Van Beirendonck and I. Verbauwhede, "OPTIMSM: FPGA hardware accelerator for Zero-Knowledge MSM", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(12055), 22 pages, 2025. BibTex LaTex

131 [Journal article] M. Gama, E. Heydari Beni, J. Kang, J. Spiessens and F. Vercauteren, "Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data", IACR Communications in Cryptology 2(3), 58 pages, 2025. BibTex LaTex

132 [Journal article] J. Gaspoz and S. Dhooghe, "Code-based Masking: From Fields to Bits Bitsliced Higher-Order Masked SKINNY", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(3), 23 pages, 2025. BibTex LaTex

133 [Journal article] S. Kundu, A. Ghosh, A. Karmakar, S. Sen and I. Verbauwhede, "Rudraksh: A compact and lightweight post-quantum key-encapsulation mechanism", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(2), 34 pages, 2025. BibTex LaTex

134 [Journal article] K. Baghery, "\Pi: A Unified Framework for Computational Verifiable Secret Sharing", IACR Cryptology ePrint Archive 2023(1669), 35 pages, 2025. BibTex LaTex

135 [Journal article] A. Aghabagherloo, R. Galvez, D. Preuveneers and B. Preneel, "Unveiling Illusionary Robust Features: A Novel Approach for Adversarial Defenses in Deep Neural Networks", IEEE Access 13, pp. 154678-154694, 2025. BibTex LaTex

136 [Journal article] D. Shanmugasundaram Veeraraghavan, J. Balasch, B. Gierlichs and I. Verbauwhede, "Low-Cost First-Order Secure Boolean Masking in Glitchy Hardware - full version", IEEE Transactions on Information Forensics and Security 20, pp. 2437-2449, 2025. BibTex LaTex

137 [Journal article] T. Sacchetti, M. Bognar, J. De Meulemeester, B. Gierlichs, F. Piessens, V. Bezsmertnyi, M. Molteni, S. Cristalli, A. Gringiani, O. Thomas and D. Antonioli, "AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling", ACM Transactions on Embedded Computing Systems 24(5), 34 pages, 2025. BibTex LaTex

138 [Journal article] D. Shanmugasundaram Veeraraghavan, S. Dhooghe, J. Balasch, B. Gierlichs and I. Verbauwhede, "Higher-Order Time Sharing Masking", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(2), pp. 235-267, 2025. BibTex LaTex

139 [Journal article] L. Oldenburg, M. Juarez Miro, E. Argones Rúa and C. Diaz, "Shift Your Shape: Correlating and Defending Mixnet Flows Based on Their Shapes", IEEE Transactions on Dependable and Secure Computing , 18 pages, 2025. BibTex LaTex

140 [Journal article] T. Beyne and M. Verbauwhede, "Integral cryptanalysis in characteristic p", IACR Cryptology ePrint Archive , 38 pages, 2025. BibTex LaTex

141 [Book chapter] L. Wouters, B. Gierlichs and B. Preneel, "Security of Automotive Systems" In Embedded Cryptography 3, Wiley, pp. 225-243, 2025. BibTex LaTex

142 [Thesis] J. Kang, "Optimisations and Applications of Fully Homomorphic Encryption", Phd thesis, KU Leuven, F. Vercauteren, N. Smart and I. Iliashenko, 330 pages, 2025. BibTex LaTex

143 [Thesis] J. Gaspoz, "Secure Software Masking Schemes Against Power Analysis Attacks", Phd thesis, KU Leuven, V. Rijmen and S. Petkova-Nikova, 218 pages, 2025. BibTex LaTex

144 [Thesis] A. Bhati, "Advanced Cryptography for Modern Data Security: Provably Secure and Efficient Symmetric-Key Modes from Expanding Primitives", Phd thesis, KU Leuven, B. Preneel and E. Andreeva, 370 pages, 2025. BibTex LaTex

🔗

145 [Thesis] M. Hassan, "Evolutionary Computation for the Design and Evaluation of Hardware-Efficient Non-Cryptographic Hash Functions", Phd thesis, KU Leuven, N. Mentens, 228 pages, 2025. 🔗 BibTex LaTex

146 [Thesis] S. Kundu, "Post-quantum Cryptography: NIST Standardization and beyond", Phd thesis, KU Leuven, I. Verbauwhede and A. Karmakar, 228 pages, 2025. PDF BibTex LaTex

147 [Thesis] R. Sarenche, "Incentive Analysis in Permissionless Blockchains", Phd thesis, KU Leuven, B. Preneel and S. Petkova-Nikova, 406 pages, 2025. 🔗 BibTex LaTex

148 [Thesis] D. Shanmugasundaram Veeraraghavan, "Efficient Hardware Masking Using Heuristic and Formal Methods", Phd thesis, KU Leuven, I. Verbauwhede and B. Gierlichs, 236 pages, 2025. PDF 🔗 BibTex LaTex

149 [Thesis] E. Pohle, "On Multi-Party Thresholdized Block Ciphers and Applications", Phd thesis, KU Leuven, B. Preneel and A. Abidin, 304 pages, 2025. PDF 🔗 BibTex LaTex

150 [Thesis] Z. Zhang, "Low-Latency Hardware Secure Masking for Symmetric Key Cryptography", Phd thesis, KU Leuven, V. Rijmen and S. Petkova-Nikova, 220 pages, 2025. 🔗 BibTex LaTex

151 [Thesis] A. Dewever, "Differential cryptanalysis in the fixed-key model of block ciphers GIFT-64 and BAKSHEESH", Master thesis, KU Leuven, V. Rijmen, 90 pages, 2025. PDF 🔗 BibTex LaTex

152 [Thesis] S. Banerjee and S. Duttagupta, "Multi-party Key Establishment for Resource-Constrained Devices", Master thesis, Indian Statistical Institute, B. Preneel and M. Nandi, 60 pages, 2025. PDF BibTex LaTex

153 [Thesis] S. Nanthakumar and I. Siros, "Fuzzing the Digital Audio Broadcasting Protocol", Master thesis, KU Leuven, B. Preneel, 51 pages, 2025. PDF 🔗 BibTex LaTex

154 [Thesis] Z. Zihang, "A Three-Stage Hierarchical Framework for Protecting Children from Harmful Video Content", Master thesis, KU Leuven, B. Preneel and V. Rijmen, 96 pages, 2025. PDF 🔗 BibTex LaTex

155 [Thesis] Z. Miao, "Accelerating Arithmetic on AMD Versal FPGA Architecture", Master thesis, KU Leuven, F. Vercauteren and I. Verbauwhede, 125 pages, 2025. PDF BibTex LaTex

156 [Thesis] M. Boscardin, "Evaluating the Effectiveness and Privacy Implications of Parental Control Apps: Technical Capabilities, Limitations, and Children's Bypassing Tactics", Master thesis, KU Leuven, B. Preneel, 94 pages, 2025. PDF 🔗 BibTex LaTex

157 [Thesis] Y. Thijs, "Privacy Preserving Systems using FHE-friendly Ciphers", Master thesis, KU Leuven, V. Rijmen, 76 pages, 2025. PDF 🔗 BibTex LaTex

158 [Thesis] C. De Paepe, "Protecting AES-128 Against First-Order Side-Channel Analysis in Micro-Architectures by Enforcing Threshold Implementation Principles", Master thesis, KU Leuven, V. Rijmen, 96 pages, 2025. PDF 🔗 BibTex LaTex

159 [Thesis] J. Willemen, "Design and Optimization of an FPGA Accelerator for Hybrid Homomorphic Encryption Operations", Master thesis, KU Leuven, I. Verbauwhede, 79 pages, 2025. PDF 🔗 BibTex LaTex

160 [Thesis] L. van Baren, "Towards First-Order Masked Hawk Digital Signatures", Master thesis, KU Leuven, I. Verbauwhede, 53 pages, 2025. PDF 🔗 BibTex LaTex

161 [Thesis] Q. Govaerts, "Let's Get Physical: Exploiting Electromagnetic Emanations as Covert Channels in Spectre Attacks", Master thesis, KU Leuven, I. Verbauwhede, 101 pages, 2025. PDF 🔗 BibTex LaTex

162 [Thesis] H. Vermeersch, "Accelerating Number Theoretic Transforms on AMD's AI Engine Architecture", Master thesis, KU Leuven, I. Verbauwhede, 145 pages, 2025. PDF 🔗 BibTex LaTex

163 [Thesis] X. Su, "Efficient Implementation of Galois Extension of $\mathbb{Z}_{2^k}$ and its Applications in MPC-in-the-Head Zero-Knowledge Proofs", Master thesis, KU Leuven, N. Smart, 114 pages, 2025. PDF 🔗 BibTex LaTex

164 [Thesis] H. Xu, "Distributed Proof Generation of FRI-based SNARKs", Master thesis, KU Leuven, N. Smart, 71 pages, 2025. BibTex LaTex

165 [Thesis] L. Oldenburg, "Traffic Analysis Attacks and Defenses on Anonymizing Networks", Phd thesis, KU Leuven, C. Diaz, 284 pages, 2025. BibTex LaTex

166 [Thesis] M. Meylaerts, "Side channel analysis on complementary flexible thin-film transistor technologies", Master thesis, UHasselt & KU Leuven, N. Mentens and K. Myny, 50 pages, 2025. BibTex LaTex

167 [Thesis] D. Ruttens, "Side channel power analysis on unipolar flexible thin-film transistor technologies for SRAM", Master thesis, UHasselt & KU Leuven, N. Mentens and K. Myny, 92 pages, 2025. BibTex LaTex

168 [Thesis] S. Scevenels, "Onderzoek naar RISC-V-architecturen op flexibele technologieën", Master thesis, UHasselt & KU Leuven, K. Myny, 41 pages, 2025. BibTex LaTex

169 [Thesis] E. Tsampanis, "Low-power Dynamic logic circuits for flexible electronics", Master thesis, UHasselt & KU Leuven, K. Myny, 69 pages, 2025. BibTex LaTex

170 [Thesis] M. Vranckx, "Designing an amplifier for biomedical signals in IGZO", Master thesis, UHasselt & KU Leuven, K. Myny, 98 pages, 2025. BibTex LaTex

171 [Thesis] B. Spauwen, "The Development of an Analog Front End in LTPO Technology", Master thesis, UHasselt & KU Leuven, K. Myny, 70 pages, 2025. BibTex LaTex

172 [Thesis] M. Kerkhofs, "Supersingular Isogeny Graphs and Applications", Master thesis, KU Leuven, F. Vercauteren, 87 pages, 2025. BibTex LaTex

173 [Thesis] B. Biesbrouck, "10 Secure Computations for the Price of 1: A Study of Reverse Multiplication-friendly Embeddings and its Implementation in Magma", Master thesis, KU Leuven, F. Vercauteren, 49 pages, 2025. BibTex LaTex

174 [Thesis] S. Chentouf, "Lattice-Based Zero-Knowledge Proofs for Privacy-Preserving Federated Learning", Master thesis, KU Leuven, F. Vercauteren, 52 pages, 2025. BibTex LaTex

175 [Thesis] H. Cattoire, "Enhancing privacy in the Solid protocol through Attribute-Based Encryption", Master thesis, KU Leuven, B. Preneel, 57 pages, 2025. BibTex LaTex

176 [Thesis] A. Mertens, "Making Privacy Technologies More Efficient", Phd thesis, KU Leuven, N. Smart, 207 pages, 2025. BibTex LaTex

177 [Thesis] M. Gama, "MPC in the Real World: Practical Aspects of Multi-Party Computation", Phd thesis, KU Leuven, N. Smart and S. Petkova-Nikova, 268 pages, 2025. BibTex LaTex

178 [Thesis] L. Wouters, "Security Evaluation of Connected Embedded Devices", Phd thesis, KU Leuven, B. Preneel and B. Gierlichs, 230 pages, 2025. BibTex LaTex

179 [Thesis] R. Jadoul, "Secure Multiparty Computation, Inside and Out of the Head", Phd thesis, KU Leuven, N. Smart, 290 pages, 2025. BibTex LaTex

180 [Proceeding] "Progress in Cryptology - AFRICACRYPT 2025", Lecture Notes in Computer Science, V. Rijmen, S. Petkova-Nikova and A. Nitaj (Eds.), Springer-Verlag, 2025. BibTex LaTex

181 [Proceeding] "International Workshop on the Arithmetic of Finite Fields (WAIFI 2024)", Lecture Notes in Computer Science 15176, S. Petkova-Nikova and D. Panario (Eds.), Springer, 2025. BibTex LaTex

182 [Proceeding] "Information Security and Cryptology - Inscrypt 2025", Lecture Notes in Computer Science, D. Lin, M. Wang and M. Yung (Eds.), Springer-Verlag, 2025. BibTex LaTex

183 [Book] T. Beyne and V. Rijmen, "Linear cryptanalysis", Cambridge University Press, 209 pages, 2025. BibTex LaTex

184 [Report] C. Ozkan, X. Zou and D. Singelée, "SBOMs also need Security. Can you fully trust SBOMs? An in-depth analysis of malicious developer attacks against SBOM tools.", Whitepaper - COOCK project IIoT-SBOM, 12 pages, 2025. BibTex LaTex

185 [Report] T. Beyne, "Ultrametric integral cryptanalysis", Lecture notes, Ruhr University Bochum, 57 pages, 2025. BibTex LaTex

186 [Talk] J. De Meulemeester and J. Van Bulck, "Fifty Dollars To Root The Cloud: Low-Cost Memory Interposer Attacks On Confidential Computing", Black Hat Europe 2025, London, GB, 2025. BibTex LaTex

187 [Talk] T. Yoshizawa, "Security and privacy gaps in V2X standards", The ULTIMO Frontier: Let's Talk Automated Mobility - Cybersecurity and Privacy in Autonomous Mobility, online, On, 2025. BibTex LaTex

188 [Talk] A. Herlédan Le Merdy, "Unconditional foundations for supersingular isogeny-based cryptography", Theory of Cryptography (TCC 2025) , Aarhus, DK, 2025. BibTex LaTex

189 [Talk] T. Yoshizawa, "PQC Impacts on V2X", null, Frankfurt, DE, 2025. BibTex LaTex

190 [Talk] Q. Norga, "mUOV: Masking the Unbalanced Oil and Vinegar Digital Signature Scheme at First- and Higher-Order", NIST Sixth PQC Standardization Conference, Gaithersbrug (Maryland), US, 2025. BibTex LaTex

191 [Talk] R. Geelen, "Revisiting the Slot-to-Coefficient Transformation for BGV and BFV", ArcticCrypt, Longyearbyen, NO, 2025. BibTex LaTex

192 [Talk] I. Verbauwhede, "Hardware Security: state of the art: Keynote", CF '25: 22nd ACM International Conference on Computing Frontiers, Cagliari , IT, 2025. BibTex LaTex

193 [Talk] B. Preneel, "Crypto Wars Revisited", ACNS 2025, Munich, DE, 2025. BibTex LaTex

194 [Talk] S. Kundu, "Implementation aspects of lattice-based post-quantum schemes", PQCSA summer school, Albena, Albena, BG, 2025. BibTex LaTex

195 [Talk] P. Sluys, "A Peek Behind the Curtain: Debug Interfaces and How to Misuse Them", DistriNet LLVM Workshop 2025, Gent, BE, 2025. BibTex LaTex

196 [Talk] A. Bhati, "MPC-Friendly Modes of Authenticated Encryption", Invited Talk, MOZAIK Winter School, Heverlee, BE, 2025. BibTex LaTex

197 [Talk] E. Heydari Beni, "QRYPT: End-to-End Encrypted Audio Calls via Blind Audio Mixing", Real World Crypto Symposium, Sofia, BG, 2025. BibTex LaTex

198 [Talk] J. Kang, "Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data", The 4th Annual FHE.org Conference on Fully Homomorphic Encryption, Sofia, Bulgaria, 2025, Sofia, BG, 2025. BibTex LaTex

199 [Talk] R. Geelen, "Fully Homomorphic Encryption for Cyclotomic Prime Moduli", 4th Annual FHE.org Conference on Fully Homomorphic Encryption, Sofia, BG, 2025. BibTex LaTex

200 [Talk] R. Geelen, "Fully Homomorphic Encryption for Cyclotomic Prime Moduli", London-ish Lattice Coding & Crypto Meeting, Egham, GB, 2025. BibTex LaTex

201 [Talk] V. Rijmen, "Challenges in Symmetric-Key Cryptography", DRDO Seminar, New Delhi, IN, 2025. BibTex LaTex

202 [Talk] A. Bhati, "Generalized Indifferentiable Sponge and its Application to Polygon Miden VM", Invited Talk, ALPSY Workshop, Obergurgl, AT, 2025. BibTex LaTex

203 [Patent] X. Carpent, B. Gierlichs, B. Preneel and I. Vlasceanu, "Secure boot device for increased cryptographic and ownership resilience", Patent number WO2025002541A1 WIPO (PCT), HUAWEI TECHNOLOGIES CO., LTD, 2025. BibTex LaTex

2024

1. [Conf article] R. Sarenche, S. Petkova-Nikova and B. Preneel, "Deep Selfish Proposing in Longest-Chain Proof-of-Stake Protocols" In Financial Cryptography and Data Security - International Conference, FC 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 24-40, 2024. BibTex LaTex

2. [Conf article] E. Argones Rúa, E. Maiorana and P. Campisi, "Strengthened Fuzzy Extractors using Turbo-codes: Case Study on Finger Vein Authentication" In $E IEEE International Workshop on Information Forensics and Security (WIFS 2024), IEEE, 6 pages, 2024. BibTex LaTex

3. [Conf article] M. Sel, H. Reefat, N. Karimi and K. Mersinas, "Evaluation of Entity Trustworthiness Based on Public and Private Data" In IFIPTM 2023: IFIP International Conference on Trust Management , Springer, pp. 136-145, 2024. BibTex LaTex

4. [Conf article] J. Blindenbach, J. Cheon, G. Gürsoy and J. Kang, "On the overflow and p-adic theory applied to homomorphic encryption" In The 8th International Symposium on Cyber Security, Cryptology and Machine Learning, Lecture Notes in Computer Science, M. Elhadad, M. Kutyłowski and G. Persiano (Eds.), Springer-Verlag, pp. 268-279, 2024. BibTex LaTex

5. [Conf article] K. Nakagawa, H. Onuki, W. Castryck, M. Chen, R. Invernizzi, G. Lorenzon and F. Vercauteren, "SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies" In Advances in Cryptology - ASIACRYPT 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 272-303, 2024. BibTex LaTex

6. [Conf article] T. Beyne and M. Verbauwhede, "Ultrametric integral cryptanalysis" In Advances in Cryptology - ASIACRYPT 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 392-423, 2024. BibTex LaTex

7. [Conf article] S. Sedaghat, F. Baldimtsi, K. Kryptos Chalkias, Y. Ji, J. Lindstrøm, D. Maram, B. Riva, A. Roy, S. Sedaghat and J. Wang, "zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials" In Proceedings of ACM CCS 2025, Association for Computing Machinery (ACM), ACM, 20 pages, 2024. BibTex LaTex

8. [Conf article] P. Mondal, S. Adhikary, S. Kundu and A. Karmakar, "ZKFault: Fault attack analysis on zero-knowledge based post-quantum digital signature schemes" In Advances in Cryptology - ASIACRYPT 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 132-167, 2024. BibTex LaTex

9. [Conf article] A. Sajadi, N. Zidaric, T. Stefanov and N. Mentens, "A Systematic Comparison of Side-channel Countermeasures for RISC-V-based SoCs" In 2024 IEEE Nordic Circuits and Systems Conference (NorCAS), IEEE, 7 pages, 2024. BibTex LaTex

10. [Conf article] M. Rahimi, "MALARIA: Management of Low-Latency Routing Impact on Mix Network Anonymity" In NCA, IEEE Computer Society 22, IEEE, 10 pages, 2024. BibTex LaTex

11. [Conf article] T. Yoshizawa and B. Preneel, "Intersections Are Not Good for Your Privacy" In IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2024), IEEE, pp. 166-171, 2024. BibTex LaTex

12. [Conf article] Z. Zhang, S. Petkova-Nikova and V. Nikov, "Glitch-Stopping Circuits: Hardware Secure Masking without Registers" In Proceedings of ACM CCS 2025, Association for Computing Machinery (ACM), ACM, pp. 3406-3420, 2024. BibTex LaTex

13. [Conf article] R. Zhang, K. Wu, Y. Sun and M. Mustafa, "Privacy-Preserving Load-Shaping Strategies for Smart Meters using Deep Reinforcement Learning" In IEEE PES Innovative Smart Grid Technologies (ISGT Europe 2016), IEEE, 5 pages, 2024. BibTex LaTex

14. [Conf article] M. Zbudila, E. Pohle, A. Abidin and B. Preneel, "MaSTer: Maliciously Secure Truncation for Replicated Secret Sharing without Pre-Processing" In Cryptology and Network Security , Lecture Notes in Computer Science, M. Kohlweiss and R. Di Pietro (Eds.), Springer-Verlag, pp. 49-73, 2024. BibTex LaTex

15. [Conf article] M. Rahimi, "LARMix++: Latency-Aware Routing in Mix Networks with Free Routes Topology" In International Conference on Cryptology and Network Security, CANS 2024, Lecture Notes in Computer Science, BibTex LaTex

Springer-Verlag, pp. 187-211, 2024.

16 [Conf article] M. Rahimi, "Poster: Effect of mixing process on end-to-end latency in mix networks" In International Conference on Cryptology and Network Security, CANS 2024, Lecture Notes in Computer Science, Springer-Verlag, 2 pages, 2024. BibTex LaTex

17 [Conf article] D. Das, S. Meiser, E. Mohammadi and A. Kate, "Divide and Funnel: A Scaling Technique for Mix-Networks" In 37 IEEE Computer Security Foundations Symposium 2024, IEEE Computer Society, IEEE, pp. 468-483, 2024. BibTex LaTex

18 [Conf article] I. Bulut and E. Argones Rúa, "Machine Learning-Based Secure Malware Detection with Feature Extraction from Binary Executable Headers" In European Symposium on Research in Computer Security - ESORICS 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 193-203, 2024. BibTex LaTex

19 [Conf article] Y. Guo, R. Degraeve, P. Roussel, B. Kaczer, E. Bury and I. Verbauwhede, "Reducing Reservoir Dimensionality with Phase Space Construction for Simplified Hardware Implementation" In Artificial Neural Networks and Machine Learning – ICANN 2024, Springer-Verlag, pp. 156-167, 2024. BibTex LaTex

20 [Conf article] R. Zhang, Y. Sun and M. Mustafa, "Proactive Load-Shaping Strategies with Privacy-Cost Trade-offs in Residential Households based on Deep Reinforcement Learning" In IEEE International Conference on Smart Grid Communications (SmartGridComm 2024), IEEE, 7 pages, 2024. BibTex LaTex

21 [Conf article] A. Bhati, E. Andreeva and D. Vizár, "OAE-RUP: A Strong Online AEAD Security Notion and its Application to SAEF" In The 14th International Conference on Security and Cryptography for Networks (SCN 2024), Lecture Notes in Computer Science, Springer-Verlag, pp. 117-139, 2024. BibTex LaTex

22 [Conf article] K. Cong, J. Kang, G. Nicolas and J. Park, "Faster Private Decision Tree Evaluation for Batched Input from Homomorphic Encryption" In Security in Communication Networks, 14 International Conference, SCN 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 3-23, 2024. BibTex LaTex

23 [Conf article] J. Bertels, Q. Norga and I. Verbauwhede, "A Better Kyber Butterfly for FPGAs" In International Conference on Field Programmable Logic and Applications (FPL 2024), IEEE Computer Society, IEEE, pp. 171-177, 2024. BibTex LaTex

24 [Conf article] A. Abidin, K. Eldefrawy and D. Singelée, "Entanglement-based Mutual Quantum Distance Bounding" In The 8th International Symposium on Cyber Security, Cryptology and Machine Learning, Lecture Notes in Computer Science, M. Elhadad, M. Kutyłowski and G. Persiano (Eds.), Springer-Verlag, pp. 219-235, 2024. BibTex LaTex

25 [Conf article] T. Claverie, D. Leblanc-Albarel, G. Avoine and X. Carpent, "Time-memory Trade-offs Sound the Death Knell for GPRS and GSM" In Advances in Cryptology - CRYPTO 1983, Lecture Notes in Computer Science, D. Chaum (Ed.), Springer-Verlag, pp. 206-240, 2024. BibTex LaTex

26 [Conf article] K. Cong, D. Das, G. Nicolas and J. Park, "Panacea: Non-Interactive and Stateless Oblivious RAM" In 9 IEEE European Symposium on Security and Privacy (Euro S&P 2024), IEEE, 20 pages, 2024. BibTex LaTex

27 [Conf article] T. Beyne and Y. Chen, "Information-theoretic security with asymmetries" In Advances in Cryptology - CRYPTO 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 463-494, 2024. BibTex LaTex

28 [Conf article] T. Decru, "Radical $\root N \of {\mathrm {\acute{e}lu}}$ Isogeny Formulae" In Advances in Cryptology - CRYPTO 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 107-128, 2024. BibTex LaTex

29 [Conf article] F. Abacha, S. Teo, L. Cordeiro and M. Mustafa, "Synthetic Data Aided Federated Learning Using Foundation Models" In International Workshop on Federated Learning in the Age of Foundation Models In Conjunction with IJCAI 2024 (FL@FM-IJCAI 2024), Lecture Notes in Artificial Intelligence, Springer-Verlag, 8 pages, 2024. BibTex LaTex

30 [Conf article] R. Jadoul, A. Mertens, J. Park and H. Lima Pereira, "NTRU-based FHE for Larger Key and Message Space" In Information Security and Privacy - 2024 Australasian Conference, ACISP 2024, Lecture Notes in BibTex LaTex

Computer Science 14895, T. Zhu and Y. Li (Eds.), Springer-Verlag, pp. 141-160, 2024.

31 [Conf article] M. Hassan, J. Vliegen, S. Picek and N. Mentens, "A Systematic Exploration of Evolutionary Computation for the Design of Hardware-oriented Non-cryptographic Hash Functions" In GECCO '24: Proceedings of the Genetic and Evolutionary Computation Conference, Association for Computing Machinery (ACM), J. Handl (Ed.), ACM, pp. 1255-1263, 2024. BibTex LaTex

32 [Conf article] E. Alqahtani, S. Teo, L. Cordeiro and M. Mustafa, "Improved Federated Learning with Non-IID Data Using Foundation Models" In Proceedings of the 2024 Poster Session of the 8 IEEE European Symposium on Security and Privacy (IEEE EuroS&P-PS 2024), IEEE Computer Society, IEEE, 3 pages, 2024. BibTex LaTex

33 [Conf article] E. Alqahtani and M. Mustafa, "Poster: Privacy-Preserving Billing for Local Energy Markets" In Proceedings of the 2024 Poster Session of the 8 IEEE European Symposium on Security and Privacy (IEEE EuroS&P-PS 2024), IEEE Computer Society, IEEE, 3 pages, 2024. BibTex LaTex

34 [Conf article] D. Du Pont, J. Bertels, F. Turan, M. Van Beirendonck and I. Verbauwhede, "Hardware Acceleration of the Prime-Factor and Rader NTT for BGV Fully Homomorphic Encryption" In IEEE Symposium on Computer Arithmetic, IEEE, pp. 1-8, 2024. BibTex LaTex

35 [Conf article] A. Bhati, A. Dufka, E. Andreeva, A. Roy and B. Preneel, "Skye: An Expanding PRF based Fast KDF and its Applications" In Proceedings of the 19 ACM Asia Conference on Computer and Communications Security (ASIACCS 2024), Association for Computing Machinery (ACM), ACM, 17 pages, 2024. BibTex LaTex

36 [Conf article] B. Bozdemir, M. Onen and B. Askin Ozdemir, "PRIDA: PRIvacy-preserving Data Aggregation with multiple data customers" In 39th International Conference on ICT Systems Security and Privacy Protection (SEC 2024), IFIP Conference Proceedings, Kluwer, pp. 46-60, 2024. BibTex LaTex

37 [Conf article] M. Garcia-Constantino, A. Konios, I. Ekerete, M. Mustafa, I. Hussein Lopez-Nava and Y. Altamirano-Flores, "Using Thermal and Contact Sensors for Mood Detection in Smart Living Environments" In International Conference on PErvasive Technologies Related to Assistive Environments (PETRA), Association for Computing Machinery (ACM), ACM, pp. 351-358, 2024. BibTex LaTex

38 [Conf article] A. Baron, L. Le Jeune, W. Hellemans, M. Rabbani and N. Mentens, "Evaluation of Lightweight Machine Learning-Based NIDS Techniques for Industrial IoT" In Applied Cryptography and Network Security - ACNS 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 246-264, 2024. BibTex LaTex

39 [Conf article] L. Wu, Y. Fan, B. Preneel, W. Wang and M. Wang, "Automated Generation of Masked Nonlinear Components: From Lookup Tables to Private Circuits" In Applied Cryptography and Network Security - ACNS 2003, Lecture Notes in Computer Science 2846, J. Zhou, M. Yung and Y. Han (Eds.), Springer-Verlag, pp. 319-339, 2024. BibTex LaTex

40 [Conf article] M. Rahimi, "CLAM: Client-Aware Routing in Mix Networks" In 2025 ACM Workshop on Information Hiding and Multimedia Security, Association for Computing Machinery (ACM), ACM, pp. 199-209, 2024. BibTex LaTex

41 [Conf article] Z. Moti, A. Senol, H. Bostani, F. Borgesius, V. Moonsamy, A. Mathur and G. Acar, "Targeted and Troublesome: Tracking and Advertising on Children's Websites" In IEEE Symposium on Security and Privacy 2024, IEEE Computer Society, IEEE, pp. 1517-1535, 2024. BibTex LaTex

42 [Conf article] K. Bogner, D. Singelée and A. Abidin, "Entangled States and Bell's Inequality: A New Approach to Quantum Distance Bounding" In Workshop on Quantum-Secure Networks and Systems, Lecture Notes in Computer Science, Springer-Verlag, pp. 1-6, 2024. BibTex LaTex

43 [Conf article] T. Yoshizawa, A. Braeken and B. Preneel, "Toward Viable Security Solution for VRUs in V2X Communication" In IEEE Vehicular Networking Conference, pp. 33-40, 2024. BibTex LaTex

44 [Conf article] T. Yoshizawa, A. Aghabagherloo, A. Huszak, C. Ujvarosi, D. Singelée and B. Preneel, "Security-Focused Training Model of Reinforcement Learning in Autonomous Vehicles" In IEEE Vehicular Networking Conference, pp. 215-218, 2024. BibTex LaTex

45 [Conf article] Y. Guo, R. Degraeve, M. Vandemaele, P. Saraza-Canflanca, J. Franco, B. Kaczer, E. Bury and I. Verbauwhede, "Exploiting Bias Temperature Instability for Reservoir Computing in Edge Artificial Intelligence Applications" In IEEE International Reliability Physics Symposium 2024, IEEE, pp. 1-7, 2024.

BibTex LaTex

46 [Conf article] A. Senol, A. Ukani, D. Cutler and I. Bilogrevic, "The Double Edged Sword: Identifying Authentication Pages and their Fingerprinting Behavior" In Proceedings of the The Web (WWW) Conference, ACM, pp. 1690-1701, 2024.

BibTex LaTex

47 [Conf article] J. Vliegen, M. Rabbani, W. Hellemans and N. Mentens, "HAGAR: Hashgraph-based Aggregated Communication and Remote Attestation" In Malicious Software and Hardware in Internet of Things, 7 pages, 2024.

BibTex LaTex

48 [Conf article] H. Saurabh, A. Golder, S. Titti, S. Kundu, C. Li, A. Karmakar and D. Das, "SNOW-SCA: ML-assisted Side-Channel Attack on SNOW-V" In IEEE International Symposium on Hardware-Oriented Security and Trust - HOST 2024, ISBN, IEEE, pp. 139-149, 2024.

BibTex LaTex

49 [Conf article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "SoK: Parameterization of Fault Adversary Models - Connecting Theory and Practice" In Topics in Cryptology - CT-RSA 2024, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science, Springer-Verlag, pp. 433-459, 2024.

BibTex LaTex

50 [Conf article] M. Xu, L. Dennis and M. Mustafa, "Safeguard Privacy for Minimal Data Collection with Trustworthy Autonomous Agents" In International Conference on Autonomous Agents and Multiagent Systems (AAMAS), Association for Computing Machinery (ACM), ACM, pp. 1966-1974, 2024.

BibTex LaTex

51 [Conf article] M. Namazi Rizi, N. Zidaric, L. Batina and N. Mentens, "Optimised AES with RISC-V Vector Extensions" In 27 IEEE Workshop on Design and Diagnostics of Electronic Circuits & Systems (DDECS 2024), IEEE, 4 pages, 2024.

BibTex LaTex

52 [Conf article] C. Delpech de Saint Guilhem and R. Pedersen, "New Proof Systems and an OPRF from CSIDH" In Public Key Cryptography, 27 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 217-251, 2024.

BibTex LaTex

53 [Conf article] B. Ege, B. Swinkels, D. Toprakhisar and P. Vadnala, "Practical Improvements to Statistical Ineffective Fault Attacks" In Workshop on Constructive Side-Channel Analysis and Secure Design 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 59-75, 2024.

BibTex LaTex

54 [Conf article] D. Toprakhisar, S. Petkova-Nikova and V. Nikov, "CAPABARA: A Combined Attack on CAPA" In Workshop on Constructive Side-Channel Analysis and Secure Design 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 76-89, 2024.

BibTex LaTex

55 [Conf article] A. Mitrokotsa, S. Mukherjee, S. Sedaghat, D. Slamanig and J. Tomy, "Threshold Structure-Preserving Signatures: Strong and Adaptive Security under Standard Assumptions" In Public Key Cryptography, 27 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 1-24, 2024.

BibTex LaTex

56 [Conf article] A. Braeken, B. Da Silva, L. Segers, J. Knödtel, M. Reichenbach, C. Wulf, S. Pertuz, D. Göhringer, J. Vliegen, M. Rabbani and N. Mentens, "Trusted Computing Architectures for IoT Devices" In Proceedings of the 20 International Symposium on Applied Reconfigurable Computing (ARC 2024), Springer LNCS, Springer, Cham, pp. 241-254, 2024.

BibTex LaTex

57 [Conf article] T. Yoshizawa and B. Preneel, "Open Questions in VRU Standards from Security and Privacy Perspectives" In IEEE Conference on Standards for Communications and Networking, pp. 278-283, 2024.

BibTex LaTex

58 [Conf article] P. Mondal, S. Kundu, S. Bhattacharya, A. Karmakar and I. Verbauwhede, "A practical key-recovery attack on LWE-based key-encapsulation mechanism schemes using Rowhammer" In Applied Cryptography and Network Security - ACNS 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 271-300, 2024.

BibTex LaTex

59 [Conf article] K. Cong, K. Eldefrawy, N. Smart and B. Terner, "The Key Lattice Framework for Concurrent Group Messaging" In Applied Cryptography and Network Security - ACNS 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 133-162, 2024. BibTex LaTex

60 [Conf article] M. Rahimi, P. Kumar and C. Diaz, "LARMix: Latency-Aware Routing in Mix Networks" In Network and Distributed System Security Symposium (NDSS 2024), Internet Society, 18 pages, 2024. BibTex LaTex

61 [Conf article] P. Sluys, L. Wouters, B. Gierlichs and I. Verbauwhede, "An in-depth security evaluation of the Nintendo DSi gaming console" In Smart Card Research and Advanced Applications - CARDIS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 23-42, 2024. BibTex LaTex

62 [Conf article] T. Behdadnia, C. Ozkan, D. Singelée and G. Deconinck, "Encrypted Traffic Classification for Early-Stage Anomaly Detection in Power Grid Communication Network" In IEEE PES Innovative Smart Grid Technologies (ISGT Europe 2023), IEEE, pp. 1-6, 2024. BibTex LaTex

63 [Conf article] F. Baldimtsi, K. Kryptos Chalkias, F. Garillot, J. Lindstrøm, B. Riva, A. Roy, S. Sedaghat, A. Sonnino, P. Waiwitlikhit and J. Wang, "Subset-optimized BLS Multi-signature with Key Aggregation" In International Conference on Financial Cryptography and Data Security - FC 2024, Lecture Notes in Computer Science, Springer-Verlag, pp. 188-205, 2024. BibTex LaTex

64 [Conf article] S. Kundu, A. Karmakar and I. Verbauwhede, "On the masking-friendly designs for post-quantum cryptography" In International Conference on Security, Privacy and Applied Cryptography Engineering, Lecture Notes in Computer Science, Springer-Verlag, pp. 162-184, 2024. BibTex LaTex

65 [Journal article] J. Blindenbach, J. Kang, S. Hong, C. Karam, T. Lehner and G. Gürsoy, "Ultra-secure storage and analysis of genetic data for the advancement of precision medicine", Genome Biology , 27 pages, 2024. BibTex LaTex

66 [Journal article] R. Sarenche, R. Zhang, S. Petkova-Nikova and B. Preneel, "Selfish Mining Time-Averaged Analysis in Bitcoin: Is Orphan Reporting an Effective Countermeasure?", IEEE Transactions on Information Forensics and Security 20, pp. 449-464, 2024. BibTex LaTex

67 [Journal article] L. Wu, Y. Fan, W. Wang, B. Preneel and M. Wang, "Extending Randomness-Free First-Order Masking Schemes and Applications to Masking-Friendly S-boxes", IACR Transactions on Cryptographic Hardware and Embedded Systems 2025(1), pp. 340-366, 2024. BibTex LaTex

68 [Journal article] H. Hart, P. Mondal, S. Kundu, S. Adhikary, A. Karmakar and C. Li, "LightCROSS: A Secure and Memory Optimized Post-Quantum Digital Signature CROSS", IACR Cryptology ePrint Archive 2025(1929), 28 pages, 2024. BibTex LaTex

69 [Journal article] S. Kundu, Q. Norga, U. Ojha, A. Ganguly, A. Karmakar and I. Verbauwhede, "mUOV: Masking the Unbalanced Oil and Vinegar Digital Sigital Signature Scheme at First- and Higher-Order", IACR Cryptology ePrint Archive 2024(1875), 13 pages, 2024. BibTex LaTex

70 [Journal article] D. Leblanc-Albarel and B. Preneel, "Black-box Collision Attacks on the NeuralHash Perceptual Hash Function", IACR Cryptology ePrint Archive 2024(1869), 14 pages, 2024. BibTex LaTex

71 [Journal article] S. Singh, C. Marin, Y. Liang, Y. Chen, N. Mentens and R. Nijssen, "Introduction to the Special Issue on FPGA-based Embedded Systems for Industrial and IoT Applications", ACM Transactions on Reconfigurable Technology and Systems 17(4), pp. 1-2, 2024. BibTex LaTex

72 [Journal article] D. Leblanc-Albarel and B. Preneel, "Black-box Collision Attacks on Widely Deployed Perceptual Hash Functions", IACR Cryptology ePrint Archive 2024(1869), 38 pages, 2024. BibTex LaTex

73 [Journal article] M. Hassan, A. Sateesan, J. Vliegen, S. Picek and N. Mentens, "A Genetic Programming approach for hardware-oriented hash functions for network security applications", Applied Soft Computing 165, 12 pages, 2024. BibTex LaTex

74 [Journal article] Q. Norga, S. Kundu, U. Ojha, A. Ganguly, A. Karmakar and I. Verbauwhede, "Masking Gaussian Elimination at Arbitrary Order, with Application to Multivariate- and Code-Based PQC", IACR Cryptology ePrint BibTex LaTex

Archive 2024(1777), 30 pages, 2024.

75 [Journal article] H. Saurabh, S. Kundu, S. Titti, A. Golder, C. Li, A. Karmakar and D. Das, "Full Key Extraction of SNOW-V Using ML-assisted Power SCA", IEEE Design & Test , 7 pages, 2024. BibTex LaTex

76 [Journal article] T. Beyne and C. Bouvier, "Exponential sums in linear cryptanalysis", IACR Cryptology ePrint Archive 2024(1755), 28 pages, 2024. BibTex LaTex

77 [Journal article] I. Siros, D. Singelée and B. Preneel, "CovFUZZ: Coverage-based fuzzer for 4G&5G protocols", arXiv , 17 pages, 2024. BibTex LaTex

78 [Journal article] S. Duttagupta and D. Singelée, "PISA: Privacy-Preserving Smart Parking", IACR Cryptology ePrint Archive 2024(1725), 10 pages, 2024. BibTex LaTex

79 [Journal article] M. Gama, E. Heydari Beni, J. Kang, J. Spiessens and F. Vercauteren, "Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data", IACR Cryptology ePrint Archive 2024(1684), 66 pages, 2024. BibTex LaTex

80 [Journal article] J. Park, B. Van Leeuwen and O. Zajonc, "FINALLY: A Multi-Key FHE Scheme Based on NTRU and LWE", IACR Cryptology ePrint Archive 2024(1505), 26 pages, 2024. BibTex LaTex

81 [Journal article] A. Bhati, M. Verbauwhede and E. Andreeva, "Breaking, Repairing and Enhancing XCBv2 into the Tweakable Enciphering Mode GEM", IACR Cryptology ePrint Archive , 39 pages, 2024. BibTex LaTex

82 [Journal article] J. Park, B. Van Leeuwen and O. Zajonc, "FINALLY: A Multi-Key FHE Scheme Based on NTRU and LWE", IACR Communications in Cryptology 1(3), pp. 1-26, 2024. BibTex LaTex

83 [Journal article] T. Decru, T. Fouotsa, P. Frixons, V. Gilchrist and C. Petit, "Attacking trapdoors from matrix products", IACR Communications in Cryptology 1(3), 43 pages, 2024. BibTex LaTex

84 [Journal article] T. Beyne and M. Verbauwhede, "Ultrametric integral cryptanalysis", IACR Cryptology ePrint Archive 2024(722), 49 pages, 2024. BibTex LaTex

85 [Journal article] S. Atapoor, C. Delpech de Saint Guilhem and A. Kindi, "STARK-based Signatures from the RPO Permutation", IACR Cryptology ePrint Archive 2024(1553), 32 pages, 2024. BibTex LaTex

86 [Journal article] A. Bhati and E. Andreeva, "Breaking the IEEE Encryption Standard – XCB-AES in Two Queries", IACR Cryptology ePrint Archive 2024(1554), 29 pages, 2024. BibTex LaTex

87 [Journal article] T. Beyne and C. Bouvier, "Linear approximations of the Flystel construction", IACR Cryptology ePrint Archive 2024(1465), 3 pages, 2024. BibTex LaTex

88 [Journal article] T. Van hamme, G. Garofalo, E. Argones Rúa, D. Preuveneers and W. Joosen, "A Novel Evaluation Framework for Biometric Security: Assessing Guessing Difficulty as a Metric", IEEE Transactions on Information Forensics and Security 19, pp. 8369-8384, 2024. BibTex LaTex

89 [Journal article] A. Peetermans and I. Verbauwhede, "TRNG Entropy Model in the Presence of Flicker FM Noise", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(4), pp. 285-306, 2024. BibTex LaTex

90 [Journal article] K. Kluczniak and L. Schild, "FDFB2: Functional Bootstrapping via Sparse Polynomial Multiplication", IACR Cryptology ePrint Archive 2024(1376), 21 pages, 2024. BibTex LaTex

91 [Journal article] D. Chaum, R. Carback, M. Yaksetig, J. Clark, M. Nejadgholi, B. Preneel, A. Sherman, F. Zagórski, B. Zhang and Z. Yin, "Votexx: Extreme Coercion Resistance", IACR Cryptology ePrint Archive 2024(1354), 39 pages, 2024. BibTex LaTex

92 [Journal article] A. Sateesan, J. Vliegen, S. Scherrer, H. Hsiao, A. Perrig and N. Mentens, "SPArch: A Hardware-oriented Sketch-based Architecture for High-speed Network Flow Measurements", ACM Transactions on Privacy and Security , 35 pages, 2024. BibTex LaTex

93 [Journal article] R. Sarenche, E. Tas, B. Monnot, C. Schwarz-Schilling and B. Preneel, "Commitment Attacks on Ethereum's Reward Mechanism", arXiv , 34 pages, 2024. BibTex LaTex

94 [Journal article] R. Sarenche, E. Tas, B. Monnot, C. Schwarz-Schilling and B. Preneel, "Commitment Attacks on Ethereum's Reward Mechanism", arXiv , 23 pages, 2024. BibTex LaTex

95 [Journal article] K. Erdayandi and M. Mustafa, "PP-LEM: Efficient and Privacy-Preserving Clearance Mechanism for Local Energy Markets", Sustainable Energy, Grids and Networks 39(101477), 26 pages, 2024. BibTex LaTex

96 [Journal article] I. Ben Guirat, D. Das and C. Diaz, "Blending Different Latency Traffic With Beta Mixing", Proceedings on Privacy Enhancing Technologies 2024(2), pp. 464-478, 2024. BibTex LaTex

97 [Journal article] L. Oldenburg, M. Juarez Miro, E. Argones Rúa and C. Diaz, "MixMatch: Flow Matching for Mixnet Traffic", Proceedings on Privacy Enhancing Technologies 2024(2), pp. 276-294, 2024. BibTex LaTex

98 [Journal article] A. Bhati and T. Ashur, "Generalized Indifferentiable Sponge and its Application to Polygon Miden VM", IACR Cryptology ePrint Archive , 19 pages, 2024. BibTex LaTex

99 [Journal article] X. Huang, W. Ruan, W. Huang, G. Jin, Y. Dong, C. Wu, S. Bensalem, R. Mu, Y. Qi, X. Zhao, K. Cai, Y. Zhang, S. Wu, P. Xu, D. Wu, A. Freitas and M. Mustafa, "A survey of safety and trustworthiness of large language models through the lens of verification and validation", Artificial Intelligence Review 57(175), 53 pages, 2024. BibTex LaTex

100 [Journal article] M. Corte-Real Santos and K. Reijnders, "Return of the Kummer: a Toolbox for Genus-2 Cryptography", IACR Cryptology ePrint Archive 2025(948), 44 pages, 2024. BibTex LaTex

101 [Journal article] G. Qu, D. Mukhopadhyay, N. Mentens and W. Liu, "Special Section on Emerging Topics in Hardware Computing Systems Security", IEEE Transactions on Emerging Topics in Computing 12(2), pp. 482-482, 2024. BibTex LaTex

102 [Journal article] C. Diaz and H. Halpin, "Decentralized Reliability Estimation for Mixnets", arXiv , 20 pages, 2024. BibTex LaTex

103 [Journal article] N. Mentens, "Hardware Security in the Era of Emerging Device and System Technologies", IEEE Security & Privacy 22(3), pp. 4-6, 2024. BibTex LaTex

104 [Journal article] V. Rijmen, "Cryptanalytic Audit of the XHash Sponge Function and its Components", IACR Cryptology ePrint Archive 2024(656), 9 pages, 2024. BibTex LaTex

105 [Journal article] A. Mertens, G. Nicolas and S. Rovira, "Convolution-friendly Image Compression in FHE", IACR Cryptology ePrint Archive 2024(559), 7 pages, 2024. BibTex LaTex

106 [Journal article] C. Mujdei, L. Wouters, A. Karmakar, A. Beckers, J. Bermudo Mera and I. Verbauwhede, "Side-channel Analysis of Lattice-based Post-quantum Cryptography: Exploiting Polynomial Multiplication", ACM Transactions on Embedded Computing Systems 23(2), pp. 1-23, 2024. BibTex LaTex

107 [Journal article] P. Ravi, A. Chattopadhyay, J. D'Anvers and A. Baksi, "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results", ACM Transactions on Embedded Computing Systems 23(2), pp. 1-54, 2024. BibTex LaTex

108 [Journal article] P. Ravi, T. Paiva, D. Jap and J. D'Anvers, "Defeating Low-Cost Countermeasures against Side-Channel Attacks in Lattice-based Encryption", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(2), pp. 795-818, 2024. BibTex LaTex

109 [Journal article] K. Jastaniah, N. Zhang and M. Mustafa, "Efficient User-Centric Privacy-Friendly and Flexible Wearable Data Aggregation and Sharing", Transactions on Cloud Computing 12(4), pp. 967-982, 2024. BibTex LaTex

110 [Journal article] R. Sarenche, R. Zhang, S. Petkova-Nikova and B. Preneel, "Selfish Mining Time-Averaged Analysis in Bitcoin: Is Orphan Reporting an Effective Countermeasure?", IACR Cryptology ePrint Archive , 26 BibTex LaTex

pages, 2024.

111 [Journal article] I. Chillotti, E. Orsini, P. Scholl and B. Van Leeuwen, "Scooby: Improved multi-party homomorphic secret sharing based on FHE", Information and Computation 297, 18 pages, 2024. BibTex LaTex

112 [Journal article] D. Almani, T. Muller, X. Carpent, T. Yoshizawa and S. Furnell, "Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments", Future Internet 16(3), 25 pages, 2024. BibTex LaTex

113 [Journal article] R. Sarenche, R. Zhang, S. Petkova-Nikova and B. Preneel, "Selfish Mining Time-Averaged Analysis in Bitcoin: Is Orphan Reporting an Effective Countermeasure?", IACR Cryptology ePrint Archive 2024(363), 28 pages, 2024. BibTex LaTex

114 [Journal article] P. Saraza-Canflanca, F. Fodor, J. Diaz Fortuny, B. Gierlichs, R. Degraeve, B. Kaczer and I. Verbauwhede, "Unveiling the Vulnerability of Oxide-Breakdown-Based PUF", IEEE Electron Device Letters 45(5), pp. 750-753, 2024. BibTex LaTex

115 [Journal article] T. Beyne and A. Neyt, "Note on the cryptanalysis of Speedy", IACR Cryptology ePrint Archive 2024(262), 2 pages, 2024. BibTex LaTex

116 [Journal article] K. Jastaniah, N. Zhang and M. Mustafa, "Efficient Privacy-Friendly and Flexible Wearable Data Processing with User-Centric Access Control", IEEE Access 12, pp. 37012-37029, 2024. BibTex LaTex

117 [Journal article] M. Calderini, R. Civino and R. Invernizzi, "Differential experiments using parallel alternative operations", Journal of Mathematical Cryptology 18(1), 9 pages, 2024. BibTex LaTex

118 [Journal article] R. Geelen, "Revisiting the Slot-to-Coefficient Transformation for BGV and BFV", IACR Communications in Cryptology 1(3), 24 pages, 2024. BibTex LaTex

119 [Journal article] Y. Dong, Y. Wang, M. Gama, M. Mustafa, G. Deconinck and X. Huang, "Privacy-Preserving Distributed Learning for Residential Short-Term Load Forecasting", IEEE Internet of Things Journal 11(9), pp. 16817-16828, 2024. BibTex LaTex

120 [Journal article] Q. Norga, J. D'Anvers, S. Kundu and I. Verbauwhede, "X2X: Low-Randomness and High-Throughput A2B and B2A Conversions for d+1 shares in Hardware", IACR Cryptology ePrint Archive 2024(114), 40 pages, 2024. BibTex LaTex

121 [Journal article] S. Atapoor, K. Baghery, H. Lima Pereira and J. Spiessens, "Verifiable FHE via Lattice-based SNARKs", IACR Communications in Cryptology 1(1), 27 pages, 2024. BibTex LaTex

122 [Journal article] O. Amine, K. Baghery, Z. Pindado and C. Ràfols, "Simulation extractable versions of Groth's zk-SNARK revisited", International Journal of Information Security 23, pp. 431-445, 2024. BibTex LaTex

123 [Journal article] D. Das, C. Diaz, A. Kiayias and T. Zacharias, "Are continuous stop-and-go mixnets provably secure?", Proceedings on Privacy Enhancing Technologies 2024(4), pp. 665-683, 2024. BibTex LaTex

124 [Journal article] D. Shanmugasundaram Veeraraghavan, S. Dhooghe, J. Balasch, B. Gierlichs and I. Verbauwhede, "Time Sharing - A Novel Approach to Low-Latency Masking", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(3), pp. 249-272, 2024. BibTex LaTex

125 [Journal article] S. Kundu, S. Saha, A. Karmakar, D. Mukhopadhyay, S. Chowdhury and I. Verbauwhede, "Carry Your Fault: A Fault Propagation Attack on Side-Channel Protected LWE-based KEM", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(3), pp. 844-869, 2024. BibTex LaTex

126 [Journal article] C. Badertscher, S. Sedaghat and H. Waldner, "Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments", Proceedings on Privacy Enhancing Technologies 2024(4), pp. 1-76, 2024. BibTex LaTex

127 [Journal article] M. Aljafar, Z. Ul Abideen, A. Peetermans, B. Gierlichs and S. Pagliarini, "SCALLER: Standard Cell BibTex

Assembled and Local Layout Effect-based Ring Oscillators", IEEE Embedded Systems Letters 2023(6), pp. 493-496, 2024. LaTex

128 [Journal article] E. Pohle, A. Abidin and B. Preneel, "Fast Evaluation of S-boxes with Garbled Circuits", IEEE Transactions on Information Forensics and Security 19, pp. 5530-5544, 2024. BibTex LaTex

129 [Journal article] F. Zobiri, M. Gama, S. Petkova-Nikova and G. Deconinck, "Residential Flexibility Characterization and Trading Using Secure Multiparty Computation", International Journal of Electrical Power & Energy Systems 155, 13 pages, 2024. BibTex LaTex

130 [Journal article] A. Peetermans and I. Verbauwhede, "Characterization of Oscillator Phase Noise Arising from Multiple Sources for ASIC True Random Number Generation", IEEE Transactions on Circuits and Systems I: Regular Papers 71(3), pp. 1144-1157, 2024. BibTex LaTex

131 [Journal article] L. Schild, A. Abidin and B. Preneel, "Fast Transciphering Via Batched And Reconfigurable LUT Evaluation", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(4), pp. 205-230, 2024. BibTex LaTex

132 [Journal article] H. Morita, E. Pohle, K. Sadakane, P. Scholl, K. Tozawa and D. Tschudi, "MAESTRO: Multi-party AES using Lookup Tables", IACR Cryptology ePrint Archive 2024(1317), 24 pages, 2024. BibTex LaTex

133 [Journal article] J. Gaspoz and S. Dhooghe, "Bit t-SNI Secure Multiplication Gadget for Inner Product Masking", IACR Transactions on Cryptographic Hardware and Embedded Systems 1(2025), pp. 104-127, 2024. BibTex LaTex

134 [Journal article] S. Kundu, Q. Norga, A. Karmakar, S. Gangopadhyay, J. Bermudo Mera and I. Verbauwhede, "Scabbard: An Exploratory Study on Hardware Aware Design Choices of Learning with Rounding-based Key Encapsulation Mechanisms", ACM Transactions on Embedded Computing Systems 24(1), pp. 1-40, 2024. BibTex LaTex

135 [Journal article] W. Castryck, M. Chen, R. Invernizzi, G. Lorenzon and F. Vercauteren, "Breaking and Repairing SQIsign2D-East", IACR Cryptology ePrint Archive 2024(1453), 23 pages, 2024. BibTex LaTex

136 [Thesis] B. Van Leeuwen, "Mathematical Aspects of Secure Computation", Phd thesis, KU Leuven, N. Smart, 302 pages, 2024. BibTex LaTex

137 [Thesis] A. Peetermans, "Robust Randomness Generation on Embedded Devices", Phd thesis, KU Leuven, I. Verbauwhede, 234 pages, 2024. BibTex LaTex

138 [Thesis] S. Sedaghat, "Privacy-Enhancing Techniques in Distributed Systems", Phd thesis, KU Leuven, B. Preneel, 241 pages, 2024. BibTex LaTex

139 [Thesis] P. Pal, E. Heydari Beni, M. Gama and J. Kang, "From zero to HEro: zkSNARKs proof construction with HE", Master thesis, Indian Statistical Institute, F. Vercauteren and B. Roy, 57 pages, 2024. BibTex LaTex

140 [Thesis] J. Heirwegh, I. Siros and D. Singelée, "Fuzzing of Thread & Matter devices", Master thesis, KU Leuven, B. Preneel, 56 pages, 2024. BibTex LaTex

141 [Thesis] N. Vander Meeren, "Magnetic immunity of STT-MRAM", Master thesis, KU Leuven, I. Verbauwhede, 168 pages, 2024. BibTex LaTex

142 [Thesis] D. Toebat, "Implementing new NIST standards on Hardware Security Modules", Master thesis, KU Leuven, V. Rijmen, 62 pages, 2024. BibTex LaTex

143 [Thesis] E. Desmet, "Exploring Laser Fault Injection on a Modern Intel FinFET Processor", Master thesis, KU Leuven, I. Verbauwhede, 79 pages, 2024. BibTex LaTex

144 [Thesis] G. Ooghe, "Let's Get Physical: Exploiting Voltage Fault Injection Vulnerabilities in Intel SGX Enclaves", Master thesis, KU Leuven, I. Verbauwhede, 50 pages, 2024. BibTex LaTex

145 [Thesis] J. Weyn, "Isogeny interpolation: More efficient meet-in-the-middle approach", Master thesis, KU Leuven, F. Vercauteren, 84 pages, 2024. BibTex LaTex

146 [Thesis] I. Van de Weyer, "Emulsifier map for MAYO", Master thesis, KU Leuven, F. Vercauteren, 73 pages, 2024. BibTex LaTex

147 [Thesis] M. Yousif, "A new isogeny-based key exchange protocol ", Master thesis, KU Leuven, F. Vercauteren, 102 pages, 2024. BibTex LaTex

148 [Thesis] A. Slabbinck, "Error Correction for Linear Secret Sharing Schemes with Q3-structures", Master thesis, KU Leuven, N. Smart, 57 pages, 2024. BibTex LaTex

149 [Thesis] K. Sauwens, "Exploration of Polyadic Tensor Decomposition as a Tool for Public Key Cryptography", Master thesis, KU Leuven, V. Rijmen, 61 pages, 2024. BibTex LaTex

150 [Thesis] N. Knapen, "On Publicly Verifiable Secret Sharing Schemes and Applications", Master thesis, KU Leuven, N. Smart, 56 pages, 2024. BibTex LaTex

151 [Thesis] T. Van Eetvelde, "Blockchain Mining Games with Multiple Mining Pools", Master thesis, KU Leuven, B. Preneel, 51 pages, 2024. BibTex LaTex

152 [Thesis] A. Madhusudan, "Design of Scalable and Secure Decentralized Applications", Phd thesis, KU Leuven, B. Preneel and S. Petkova-Nikova, 231 pages, 2024. BibTex LaTex

153 [Thesis] M. Grujic, "Design Methodologies and Security Evaluations for True Random Number Generators", Phd thesis, KU Leuven, I. Verbauwhede and V. Rozic, 202 pages, 2024. BibTex LaTex

154 [Thesis] I. Ben Guirat, "Evaluation Techniques for Mix Networks", Phd thesis, KU Leuven, C. Diaz, 181 pages, 2024. BibTex LaTex

155 [Thesis] A. Senol, "Online Tracking Technologies and Protection Mechanisms", Phd thesis, KU Leuven, C. Diaz and G. Acar, 235 pages, 2024. BibTex LaTex

156 [Thesis] R. Daels, "Influence of WDDL Gate Architecture in A SESYM Masked Asynchronous Circuit", Master thesis, KU Leuven, V. Rijmen, S. Petkova-Nikova, S. Dhooghe and Z. Zhang, 42 pages, 2024. BibTex LaTex

157 [Thesis] S. Atapoor, "On Practical Threshold Protocols and Verifiable Secret Sharing", Phd thesis, KU Leuven, N. Smart, pp. 1-319, 2024. BibTex LaTex

158 [Thesis] R. Pedersen, "Distributed Protocols from Isogenies", Phd thesis, KU Leuven, F. Vercauteren and E. Orsini, 319 pages, 2024. BibTex LaTex

159 [Thesis] A. Sateesan, "FPGA design for large flow detection in high-speed networks", Phd thesis, KU Leuven, N. Mentens and J. Vliegen, 262 pages, 2024. BibTex LaTex

160 [Thesis] O. Perez Castillo, "Evaluating a Mixnet Based on Threshold Cryptography Regarding its Resilience-Cost Trade-Off", Master thesis, KU Leuven, I. Ben Guirat, D. Das, L. Oldenburg and C. Diaz, 50 pages, 2024. BibTex LaTex

161 [Proceeding] "Cryptology and Network Security ", Lecture Notes in Computer Science, M. Kohlweiss and R. Di Pietro (Eds.), Springer-Verlag, 2024. BibTex LaTex

162 [Report] I. Siros, D. Singelée and B. Preneel, "GitHub Copilot: the perfect Code compLeeter?", arXiv paper, 10 pages, 2024. BibTex LaTex

163 [Report] T. Yoshizawa, D. Balenson, C. Bösch, K. Han, M. Hoffmann, S. Pape, N. Trkulja and T. Yoshizawa, "Automotive Privacy Engineering", Sec.4.3 of Privacy Protection of Automated and Self-Driving Vehicles (Dagstuhl Seminar 23242), 41 pages, 2024. BibTex LaTex

164 [Talk] V. Rijmen, "Challenges in symmetric-key cryptography ", 444, Chennai, IN, 2024. BibTex LaTex

165 [Talk] R. Invernizzi, "PRISM: PRime degree ISogeny Mechanism", Isogeny Club, Online, On, 2024. ▶ BibTex LaTex

166 [Talk] I. Verbauwhede, "Hardware Security: State of the Art", ASHES '24, Salt Lake City, US, 2024. 🔗 BibTex LaTex

167 [Talk] B. Preneel, "Quantum safe crypto: time to prepare. Bart Preneel", Cybersecurity Research Consortium Industry Day, Mechelen, BE, 2024. BibTex LaTex

168 [Talk] B. Preneel, "Cybersecurity and AI: A Match Made in Heaven?", Cybersec Netherlands, Utrecht, NL, 2024. BibTex LaTex

169 [Talk] G. Lorenzon, "Generalized class group actions on oriented elliptic curves with level structure", The Isogeny Club, Online, On, 2024. PDF ▶ BibTex LaTex

170 [Talk] V. Mishra, "The Accountability Strikes Back: Decentralizing the Key Generation in CL-PKC with Traceable Ring Signatures", European Conference on EDGE AI Technologies and Applications - EEAI, Cagliari, IT, 2024. BibTex LaTex

171 [Talk] B. Preneel, "Crypto evoluties en quantum computing en hun impact op beveiliging", Privacy Cafe Hasselt, Hasselt, BE, 2024. BibTex LaTex

172 [Talk] M. Rahimi, "Poster : "CLAM: Client-Aware Routing in Mix Networks"", PETS 2024 - Privacy Enhancing Technologies Symposium, Bristol, GB, 2024. PDF BibTex LaTex

173 [Talk] B. Preneel, "The Encryption Debate: An Enduring Struggle", CODASPY '24, Porto, PT, 2024. 🔗 BibTex LaTex

174 [Talk] B. Preneel, "Location Privacy in the IoT", Cybersecurity and Privacy (CySeP) Summer School, Stockholm, SE, 2024. BibTex LaTex

175 [Talk] G. Lorenzon, "Generalized class group actions on oriented elliptic curves with level structure", 275, Ottawa, CA, 2024. PDF BibTex LaTex

176 [Talk] B. Preneel, "The many faces of the crypto wars", 1-day event on Security in Times of Surveillance, Eindhoven, NL, 2024. BibTex LaTex

177 [Talk] R. Geelen, "BGV and BFV Bootstrapping: History, State-of-the-Art, and Future Perspectives", Fully Homomorphic Encryption: Interesting Directions and Emerging Applications, Zürich, CH, 2024. PDF BibTex LaTex

178 [Talk] R. Geelen, "Poster: BGV and BFV Bootstrapping: History, State-of-the-Art, and Future Perspectives", Hardware Summit for Computing on Encrypted Data, Leuven, BE, 2024. PDF BibTex LaTex

179 [Talk] B. Preneel, "Global supply chain risks in software and hardware", REMIT Conference New Perspectives For Technology And Multilateralism, Leuven, BE, 2024. BibTex LaTex

180 [Talk] P. Sluys, "smol, the Shoddy Minsize-Oriented Linker. Or: Everything You Never Wanted To Know About ld.so", DistriNet LLVM Meetup 2024, Gent, BE, 2024. 🔗 BibTex LaTex

181 [Talk] G. Nicolas, " Why formal methods remain inaccessible for most cryptographers", 707, Dresden, DE, 2024. ▶ BibTex LaTex

182 [Talk] R. Geelen, "Revisiting Oblivious Top-k Selection with Applications to Secure k-NN Classification", 3rd Annual FHE.org Conference on Fully Homomorphic Encryption, Toronto, CA, 2024. ▶ BibTex LaTex

183 [Talk] D. Archer, "BASALISC: Programmable Hardware Accelerator for BGV and CKKS FHE - An Interim Design Update", 3rd Annual FHE.org Conference on Fully Homomorphic Encryption, Toronto, CA, 2024. ▶ BibTex LaTex

184 [Talk] N. Smart, "Cat or Dog? What PETS Are and How to Choose Them", Privacy-Enhancing Technology Summit Europe, London, GB, 2024. BibTex LaTex

2023

1 [Conf article] W. Castryck and F. Vercauteren, "A polynomial time attack on instances of M-SIDH and FESTA" In Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 127-156, 2023. BibTex LaTex

2 [Conf article] E. Crites, M. Kohlweiss, B. Preneel, S. Sedaghat and D. Slamanig, "Threshold Structure-Preserving Signatures" In Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 348-382, 2023. BibTex LaTex

3 [Conf article] S. Atapoor, K. Baghery, D. Cozzo and R. Pedersen, "VSS from Distributed ZK Proofs and Applications" In Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 405-440, 2023. BibTex LaTex

4 [Conf article] W. Castryck and F. Vercauteren, "A polynomial-time attack on instances of M-SIDH and FESTA" In Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 127-156, 2023. BibTex LaTex

5 [Conf article] M. Gama, E. Heydari Beni, E. Orsini, N. Smart and O. Zajonc, "MPC With Delayed Parties Over Star-Like Networks" In Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 1-56, 2023. BibTex LaTex

6 [Conf article] L. Braun, C. Delpech de Saint Guilhem, R. Jadoul, E. Orsini, N. Smart and T. Tanguy, "ZK-for-Z2K: MPC-in-the-Head Zero-Knowledge Proofs for $mathbb{Z}_{2^k}$" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 137-157, 2023. BibTex LaTex

7 [Conf article] C. Delpech de Saint Guilhem, E. Ebrahimi and B. Van Leeuwen, "Zero-Knowledge Systems from MPC-in-the-Head and Oblivious Transfer" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 120-136, 2023. BibTex LaTex

8 [Conf article] S. Atapoor, "Identity-Based Threshold Signatures from Isogenies" In Cryptography and Coding, 5 IMA International Conference, Lecture Notes in Computer Science 1025, C. Boyd (Ed.), Springer-Verlag, pp. 220-240, 2023. BibTex LaTex

9 [Conf article] A. Senol and G. Acar, "Unveiling the Impact of User-Agent Reduction and Client Hints: A Measurement Study" In Proceedings of the 23 annual ACM workshop on Privacy in the electronic society, Association for Computing Machinery (ACM), ACM, pp. 91-106, 2023. BibTex LaTex

10 [Conf article] A. Bhati, E. Pohle, A. Abidin, E. Andreeva and B. Preneel, "Let's Go Eevee! A Friendly and Suitable Family of AEAD Modes for IoT-to-Cloud Secure Computation" In ACM Conference on Computer and Communications Security - CCS 2023, ACM, pp. 2546-2560, 2023. BibTex LaTex

11 [Conf article] M. Van Beirendonck, J. D'Anvers, I. Verbauwhede and F. Turan, "FPT: a Fixed-Point Accelerator for Torus Fully Homomorphic Encryption" In Proceedings of the 22nd ACM Conference on Computer and Communications Security, Association for Computing Machinery (ACM) 2023, ACM, pp. 741-755, 2023. BibTex LaTex

12 [Conf article] J. Park, K. Cong, D. Das and G. Nicolas, "Poster: Panacea---Stateless and Non-Interactive Oblivious RAM" In Proceedings of the 22nd ACM Conference on Computer and Communications Security, Association for Computing Machinery (ACM) 2023, ACM, pp. 3585-3587, 2023. BibTex LaTex

13 [Conf article] X. Song, Y. Sun, M. Mustafa and L. Cordeiro, "QNNREPAIR: Scalable Quantized Neural Network Repair" In International Conference on Software Engineering and Formal Methods (SEFM 2023), Lecture Notes in Computer Science, Springer-Verlag, 18 pages, 2023. BibTex LaTex

14 [Conf article] A. Hutu and M. Mustafa, "Privacy Preserving Billing in Local Energy Markets with Imperfect Bid-Offer Fulfillment" In IEEE International Conference on Smart Grid Communications (SmartGridComm 2023), IEEE, 9 pages, 2023. BibTex LaTex

15 [Conf article] E. Alqahtani and M. Mustafa, "Zone-Based Privacy-Preserving Billing for Local Energy Market BibTex

Based on Multiparty Computation" In IEEE International Conference on Smart Grid Communications (SmartGridComm 2023), IEEE, 6 pages, 2023. LaTex

16 [Conf article] Z. Umayya, D. Malik, D. Gosain and P. Kumar, "PTPerf: On the performance evaluation of Tor Pluggable Transports" In Proceedings of the ACM on Internet Measurement Conference, ACM, pp. 501-525, 2023. BibTex LaTex

17 [Conf article] M. Gama, J. Chiang, B. David and C. Lebeda, "Correlated-Output-Differential-Privacy and Applications to Dark Pools" In Advances in Financial Technologies 2023, LIPIcs, 27 pages, 2023. BibTex LaTex

18 [Conf article] D. Almani, T. Muller, X. Carpent, S. Furnell and T. Yoshizawa, "Pre-Signature Scheme for Trustworthy Offline V2V Communication" In IFIPTM 2023: IFIP International Conference on Trust Management , Springer, 16 pages, 2023. BibTex LaTex

19 [Conf article] T. Decru, L. Maino and A. Sanso, "Towards a Quantum-resistant Weak Verifiable Delay Function" In Progress in Cryptology - LATINCRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 149-168, 2023. BibTex LaTex

20 [Conf article] K. Baghery, A. Mertens and S. Sedaghat, "Benchmarking the Setup of Updatable zk-SNARKs" In Progress in Cryptology - LATINCRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 375-396, 2023. BibTex LaTex

21 [Conf article] S. Jeon, H. Lee and J. Park, "Practical Randomized Lattice Gadget Decomposition With Application to FHE" In European Symposium on Research in Computer Security - ESORICS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 353-371, 2023. BibTex LaTex

22 [Conf article] I. Ben Guirat, C. Diaz, K. Eldefrawy and H. Zeilberger, "Mixnet Traffic Analysis by Adversaries with Partial Visibility" In European Symposium on Research in Computer Security - ESORICS 2023, Lecture Notes in Computer Science, Springer-Verlag, 20 pages, 2023. BibTex LaTex

23 [Conf article] A. Abidin, E. Pohle and B. Preneel, "Arithmetic Circuit Implementations of S-boxes for SKINNY and PHOTON in MPC" In European Symposium on Research in Computer Security - ESORICS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 86-105, 2023. BibTex LaTex

24 [Conf article] S. Scherrer, J. Vliegen, A. Sateesan, H. Hsiao, N. Mentens and A. Perrig, "ALBUS: a Probabilistic Monitoring Algorithm to Counter Burst-Flood Attacks" In International Symposium on Reliable Distributed Systems, IEEE, 14 pages, 2023. BibTex LaTex

25 [Conf article] D. Preuveneers, I. Bulut, E. Argones Rúa and W. Joosen, "On the Use of AutoML for Combating Alert Fatigue in Security Operations Centers" In European Symposium on Research in Computer Security - ESORICS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 609-627, 2023. BibTex LaTex

26 [Conf article] S. Dhooghe and S. Petkova-Nikova, "The Random Fault Model" In Selected Areas in Cryptography, 39 Annual International Workshop, SAC 2023, Lecture Notes in Computer Science, C. Carlet, K. Mandal and V. Rijmen (Eds.), Springer-Verlag, pp. 1-23, 2023. BibTex LaTex

27 [Conf article] S. Dhooghe and A. Ovchinnikov, "Threshold Implementations with Non-Uniform Inputs" In Selected Areas in Cryptography, 39 Annual International Workshop, SAC 2023, Lecture Notes in Computer Science, C. Carlet, K. Mandal and V. Rijmen (Eds.), Springer-Verlag, 29 pages, 2023. BibTex LaTex

28 [Conf article] K. Monta, M. Nagata, J. Balasch and I. Verbauwhede, "On the Unpredictability of SPICE Simulations for Side-Channel Leakage Verification of Masked Cryptographic Circuits" In 60 Design Automation Conference (DAC 2023), IEEE, 6 pages, 2023. BibTex LaTex

29 [Conf article] K. Erdayandi, M. Mustafa and L. Cordeiro, "A Privacy-Preserving and Accountable Billing Protocol for Peer-to-Peer Energy Trading Markets" In International Conference on Smart Energy Systems and Technologies - SEST 2023, IEEE, 6 pages, 2023. BibTex LaTex

30 [Conf article] W. Castryck, M. Houben, S. Merz, M. Mula, S. van Buuren and F. Vercauteren, "Weak instances of BibTex

class group action based cryptography via self-pairings" In Advances in Cryptology - CRYPTO 2023, Lecture Notes in Computer Science, H. Handschuh and A. Lysyanskaya (Eds.), Springer-Verlag, pp. 762-792, 2023. LaTex

31 [Conf article] Y. Chen, W. Choi and C. Lee, "Improved Multi-User Security Using the Squared-Ratio Method" In Advances in Cryptology - CRYPTO 2023, Lecture Notes in Computer Science, H. Handschuh and A. Lysyanskaya (Eds.), Springer-Verlag, pp. 694-724, 2023. BibTex LaTex

32 [Conf article] C. Baum, L. Braun, C. Delpech de Saint Guilhem, M. Klooß, E. Orsini, L. Roy and P. Scholl, "Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head" In Advances in Cryptology - CRYPTO 2023, Lecture Notes in Computer Science, H. Handschuh and A. Lysyanskaya (Eds.), Springer-Verlag, pp. 581-615, 2023. BibTex LaTex

33 [Conf article] J. De Meulemeester, A. Purnal, L. Wouters, A. Beckers and I. Verbauwhede, "SpectrEM: Exploiting Electromagnetic Emanations During Transient Execution" In 32 USENIX Security Symposium 2023, Usenix, pp. 6293-6310, 2023. BibTex LaTex

34 [Conf article] T. Yadav, D. Gosain and K. Seamons, "Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations" In 32 USENIX Security Symposium 2023, Usenix, pp. 3637-3654, 2023. BibTex LaTex

35 [Conf article] M. Dandekar, K. Myny and W. Dehaene, "An Active-Pixel Readout Circuit Technique towards all LTPS-TFT-on-foil Large-Area Imagers with Inherent Nonlinearity Compensation" In IEEE International Symposium on Circuits and Systems (ISCAS 2023), IEEE, 5 pages, 2023. BibTex LaTex

36 [Conf article] T. Decru and S. Kunzweiler, "Efficient computation of (3^n,3^n)-isogenies" In Progress in Cryptology - AFRICACRYPT 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 53-78, 2023. BibTex LaTex

37 [Conf article] E. Manino, B. Magri, M. Mustafa and L. Cordeiro, "Certified Private Inference on Neural Networks via Lipschitz-Guided Abstraction Refinement" In Workshop on Formal Methods for ML-Enabled Autonomous Systems - FoMLAS 2023, EPTCS, 13 pages, 2023. BibTex LaTex

38 [Conf article] A. Purnal, M. Bognar, F. Piessens and I. Verbauwhede, "ShowTime: Amplifying Arbitrary CPU Timing Side Channels" In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (ASIACCS 2023), Association for Computing Machinery (ACM), ACM, pp. 205-217, 2023. BibTex LaTex

39 [Conf article] K. Satoshi, T. Kondo, N. Karimi, K. Mersinas, M. Sel, R. Yus and S. Tezuka, "International Mutual Recognition: A Description of Trust Services in US, UK, EU and JP and the Testbed “Hakoniwa”" In Proceedings of the 20 International Conference on Security and Cryptography SECRYPT, S. De Capitani di Vimercati and P. Samarati (Eds.), SCITEPRESS, pp. 764-771, 2023. BibTex LaTex

40 [Conf article] S. Atapoor, K. Baghery, D. Cozzo and R. Pedersen, "CSI-SharK: CSI-FiSh with Sharing-friendly Keys" In Information Security and Privacy - 2023 Australasian Conference, ACISP 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 471-502, 2023. BibTex LaTex

41 [Conf article] A. Madhusudan, S. Sedaghat, S. Tiwari, K. Cong and B. Preneel, "Reusable, Instant and Private Payment Guarantees for Cryptocurrencies" In Information Security and Privacy - 2023 Australasian Conference, ACISP 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 580-605, 2023. BibTex LaTex

42 [Conf article] W. Legiest, J. D'Anvers, F. Turan, M. Van Beirendonck and I. Verbauwhede, "Neural Network Quantisation for Faster Homomorphic Encryption" In The 22nd IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS 2023), IEEE, 4 pages, 2023. BibTex LaTex

43 [Conf article] E. Marquet, J. Moeyersons, E. Pohle, M. Van Kenhove, A. Abidin and B. Volckaert, "Secure Key Management for Multi-Party Computation in MOZAIK" In Proceedings of IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, pp. 133-140, 2023. BibTex LaTex

44 [Conf article] E. Pohle, M. Zbudila, A. Abidin and B. Preneel, "Poster: MaSTer: (Practically) Maliciously Secure Truncation for Replicated Secret Sharing" In 8 IEEE European Symposium on Security and Privacy (Euro S&P 2023), IEEE, 4 pages, 2023. BibTex LaTex

45 [Conf article] J. Biesmans, K. Myny and N. Mentens, "Evaluation of Secure Circuit Styles Using Unipolar Logic Gates" In IEEE Northeast Workshop on Circuits and Systems 21, IEEE, 5 pages, 2023. BibTex LaTex

46 [Conf article] T. Yoshizawa and B. Preneel, "Post-Quantum Impacts on V2X Certificates – Already at The End of The Road" In IEEE Vehicular Technology Conference, 6 pages, 2023. BibTex LaTex

47 [Conf article] K. Cong, Y. Lai and S. Levin, "Efficient Isogeny Proofs Using Generic Techniques" In Applied Cryptography and Network Security - ACNS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 248-275, 2023. BibTex LaTex

48 [Conf article] S. Atapoor, K. Baghery, D. Cozzo and R. Pedersen, "Practical Robust DKG Protocols for CSIDH" In Applied Cryptography and Network Security - ACNS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 219-247, 2023. BibTex LaTex

49 [Conf article] A. Acharya, T. Ashur, E. Cohen, C. Hazay and A. Yanai, "A New Approach to Garbled Circuits" In Applied Cryptography and Network Security - ACNS 2023, Lecture Notes in Computer Science, Springer-Verlag, pp. 611-641, 2023. BibTex LaTex

50 [Conf article] A. Abidin, X. Limani, E. Marquet, J. Moeyersons, E. Pohle, M. Van Kenhove, J. Marquez-Barja, N. Slamnik-Kriještorac and B. Volckaert, "MOZAIK: An End-to-End Secure Data Sharing Platform" In Proceedings of the 2 International Workshop on Data Economy, ACM, pp. 34-40, 2023. BibTex LaTex

51 [Conf article] S. Cui and J. Balasch, "Efficient Software Masking of AES through Instruction Set Extensions" In Design, Automation and Test in Europe, IEEE, 6 pages, 2023. BibTex LaTex

52 [Conf article] A. Aghabagherloo, R. Galvez, D. Preuveneers and B. Preneel, "On the Brittleness of Robust Features: An Exploratory Analysis of Model Robustness and Illusionary Robust Features" In 2025 DLSP - IEEE Symposium on Security and Privacy Workshop (SP), IEEE, 7 pages, 2023. BibTex LaTex

53 [Conf article] L. Giner, S. Steinegger, A. Purnal, M. Eichlseder, D. Gruss, S. Mangard and T. Unterluggauer, "Scatter and Split Securely: Defeating Cache Contention and Occupancy Attacks" In IEEE Symposium on Security and Privacy (SP 2023), IEEE, pp. 2273-2287, 2023. BibTex LaTex

54 [Conf article] J. Biesmans, F. Regazzoni and N. Mentens, "Application-Specific FPGAs: Cryptographic Agility Through Customized Reconfigurable Architectures" In Proceedings of the 30 Reconfigurable Architectures Workshop (RAW 2023), pp. 121-124, 2023. BibTex LaTex

55 [Conf article] X. Song, Y. Sun, M. Mustafa and L. Cordeiro, "AIREPAIR: A Repair Platform for Neural Networks" In International Conference on Software Engineering - ICSE 2023, IEEE/ACM, pp. 98-101, 2023. BibTex LaTex

56 [Conf article] W. Hellemans, M. Rabbani, N. Mentens and B. Preneel, "Yes we CAN! Towards bringing security to legacy-restricted Controller Area Networks. A review" In Malicious Software and Hardware in Internet of Things, pp. 352-357, 2023. BibTex LaTex

57 [Conf article] J. Bertels, F. Turan, M. Van Beirendonck and I. Verbauwhede, "Hardware Acceleration of FHEW" In 2023 IEEE Workshop on Design and Diagnostics of Electronic Circuits & Systems (DDECS 2023), IEEE, 4 pages, 2023. BibTex LaTex

58 [Conf article] T. Yoshizawa and B. Preneel, "A New Approach To Pseudonym Certificate Management in V2X Communication" In IEEE Vehicular Networking Conference, pp. 25-32, 2023. BibTex LaTex

59 [Conf article] S. Duttagupta, E. Marín Fàbregas, D. Singelée and B. Preneel, "HAT: Secure and Practical Key Establishment for Implantable Medical Devices" In ACM Conference on Data and Application Security and Privacy (CODASPY), ACM, pp. 213-224, 2023. BibTex LaTex

60 [Conf article] J. D'Anvers, "One-Hot Conversion: Towards Faster Table-based A2B Conversion" In Advances in Cryptology - EUROCRYPT 2023, Lecture Notes in Computer Science 14006, C. Hazay and M. Stam (Eds.), Springer-Verlag, pp. 628-657, 2023. BibTex LaTex

61 [Conf article] D. Shanmugasundaram Veeraraghavan, J. Balasch, B. Gierlichs and I. Verbauwhede, "Low-Cost First-Order Secure Boolean Masking in Glitchy Hardware" In Design, Automation and Test in Europe, IEEE, 2 pages, 2023. BibTex LaTex

62 [Conf article] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH" In Advances in Cryptology - EUROCRYPT 2023, Lecture Notes in Computer Science 14006, C. Hazay and M. Stam (Eds.), Springer-Verlag, pp. 1-15, 2023. BibTex LaTex

63 [Conf article] R. Geelen, I. Iliashenko, J. Kang and F. Vercauteren, "On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption" In Advances in Cryptology - EUROCRYPT 2023, Lecture Notes in Computer Science 14006, C. Hazay and M. Stam (Eds.), Springer-Verlag, pp. 257-286, 2023. BibTex LaTex

64 [Conf article] Y. Altamirano-Flores, A. Konios, I. Hussein Lopez-Nava, M. Garcia-Constantino, I. Ekerete and M. Mustafa, "Analysis of Accelerometer Data for Personalised Mood Detection in Activities of Daily Living" In 7th Workshop on emotion awareness for pervasive computing beyond traditional approaches (EmotionAware 2023), in conjunction with IEEE International Conference on Pervasive Computing and Communications (PerCom 2023), IEEE, 6 pages, 2023. BibTex LaTex

65 [Conf article] A. Rasaii, S. Singh, D. Gosain and O. Gasser, "Exploring the Cookieverse: A Multi-Perspective Analysis of Web Cookies" In PAM 2023: International Conference on Passive and Active Network Measurement, Springer, pp. 623-651, 2023. BibTex LaTex

66 [Conf article] A. Askeland, S. Dhooghe, S. Petkova-Nikova, V. Rijmen and Z. Zhang, "Guarding the First Order: The Rise of AES Maskings" In Smart Card Research and Advanced Applications - CARDIS 2022, Lecture Notes in Computer Science 13820, I. Buhan and T. Schneider (Eds.), Springer-Verlag, pp. 103-122, 2023. BibTex LaTex

67 [Conf article] P. Kumar, D. Gosain and C. Diaz, "On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies" In Network and Distributed System Security Symposium (NDSS 2023), Internet Society, 18 pages, 2023. BibTex LaTex

68 [Conf article] M. Hassan, A. Sateesan, J. Vliegen, S. Picek and N. Mentens, "Evolving Non-cryptographic Hash Functions Using Genetic Programming for High-speed Lookups in Network Security Applications" In Applications of Evolutionary Computation, Lecture Notes in Computer Science 13989, Springer-Verlag, pp. 302-318, 2023. BibTex LaTex

69 [Journal article] Y. Chen, A. Flórez-Gutiérrez, A. Inoue, R. Ito, T. Iwata, K. Minematsu, N. Mouha, Y. Naito, F. Sibleyras and Y. Todo, "Key Committing Security of AEZ and More", IACR Transactions on Symmetric Cryptology 2023(4), 37 pages, 2023. BibTex LaTex

70 [Journal article] B. Askin Ozdemir, T. Beyne and V. Rijmen, "Multidimensional Linear Cryptanalysis of Feistel Ciphers", IACR Transactions on Symmetric Cryptology 2023(4), 25 pages, 2023. BibTex LaTex

71 [Journal article] Y. Wang, M. Mustafa, F. Zobiri, J. Nightingale and G. Deconinck, "Consumption Prediction with Privacy Concern: Application and Evaluation of Federated Learning", Sustainable Energy, Grids and Networks 38(101248), 12 pages, 2023. BibTex LaTex

72 [Journal article] H. Çeliker, F. De Roose, M. Willegems, S. Smout, W. Dehaene and K. Myny, "Analysis and Comparison of Logic Architectures for Digital Circuits in a-IGZO Thin-Film Transistor Technologies", IEEE Journal of Solid-State Circuits 59(6), pp. 1858-1870, 2023. BibTex LaTex

73 [Journal article] S. Dhooghe, D. Toprakhisar and A. Ovchinnikov, "StaTI: Protecting against Fault Attacks Using Stable Threshold Implementations", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(1), pp. 229-263, 2023. BibTex LaTex

74 [Journal article] T. Beyne and M. Verbauwhede, "Integral Cryptanalysis Using Algebraic Transition Matrices", IACR Transactions on Symmetric Cryptology 2023(4), pp. 244-269, 2023. BibTex LaTex

75 [Journal article] T. Poppelmann, S. Sinha Roy and I. Verbauwhede, "Secure and Efficient Post-Quantum Cryptography in Hardware and Software", Dagstuhl Reports 13(4), pp. 24-39, 2023. BibTex LaTex

76 [Journal article] S. Andreoli, E. Piccione, L. Budaghyan, P. Stănică and S. Petkova-Nikova, "On Decompositions of Permutations in Quadratic Functions", IACR Cryptology ePrint Archive , 20 pages, 2023. BibTex LaTex

77 [Journal article] O. Mirzamohammadi, K. Jannes, L. Sion, D. Van Landuyt, A. Abidin and D. Singelée, "Security and Privacy Threat Analysis for Solid", IEEE Software, Special Issue on Software Protection 1(1), pp. 1-11, 2023. BibTex LaTex

78 [Journal article] J. Park and S. Rovira, "Efficient TFHE Bootstrapping in the Multiparty Setting", IEEE Access 11, pp. 118625-118638, 2023. BibTex LaTex

79 [Journal article] R. Pedersen and C. Delpech de Saint Guilhem, "New proof systems and an OPRF from CSIDH", IACR Cryptology ePrint Archive 2023(1614), pp. 1-41, 2023. BibTex LaTex

80 [Journal article] P. Méaux, J. Park and H. Lima Pereira, "Towards Practical Transciphering for FHE with Setup Independent of the Plaintext Space", IACR Cryptology ePrint Archive , 24 pages, 2023. BibTex LaTex

81 [Journal article] A. Lebanov, M. Velazquez Lopez, F. De Roose, N. Papadopoulos, G. Indiveri, A. Rubino, M. Payvand, S. Smout, M. Willegems, F. Catthoor, J. Genoe, P. Heremans and K. Myny, "Flexible Unipolar IGZO Transistor-Based Integrate and Fire Neurons for Spiking Neuromorphic Applications", IEEE Transactions on Biomedical Circuits and Systems 18(1), pp. 200-214, 2023. BibTex LaTex

82 [Journal article] M. Montakhabi, A. Madhusudan, M. Mustafa, W. Vanhaverbeke, E. Almirall and S. Van der Graaf, "Leveraging Blockchain for Energy Transition in Urban Contexts", Journal of Big Data & Society (BD&S) -(-), 13 pages, 2023. BibTex LaTex

83 [Journal article] Q. Liu, B. Preneel, Z. Zhao and M. Wang, "Improved Quantum Circuits for AES: Reducing the Depth and the Number of Qubits", IACR Cryptology ePrint Archive 2023(1417), 39 pages, 2023. BibTex LaTex

84 [Journal article] J. Pelgrims, K. Myny and W. Dehaene, "An Ultrasonic Driver Array in Metal-Oxide Thin-Film Technology Using a Hybrid TFT-Si DLL Locking Architecture", IEEE Journal of Solid-State Circuits 59(2), 12 pages, 2023. BibTex LaTex

85 [Journal article] R. Geelen, M. Van Beirendonck, H. Lima Pereira, B. Huffman, T. McAuley, B. Selfridge, D. Wagner, G. Dimou, I. Verbauwhede, F. Vercauteren and D. Archer, "BASALISC: Programmable Hardware Accelerator for BGV Fully Homomorphic Encryption", IACR Transactions on Cryptographic Hardware and Embedded Systems 2023(4), pp. 32-57, 2023. BibTex LaTex

86 [Journal article] S. Dhooghe and J. Luis Imana, "Domain-oriented masked bit-parallel finite-field multiplier against side-channel attacks", Information Processing Letters 182(1), 7 pages, 2023. BibTex LaTex

87 [Journal article] M. Remmerswaal, L. Wu, S. Tiran and N. Mentens, "AutoPOI: automated points of interest selection for side-channel analysis", Journal of Cryptographic Engineering 14, pp. 463-474, 2023. BibTex LaTex

88 [Journal article] P. Kumar, R. Sharma, S. Chakravarty, M. Maity and K. Singh, "Dolphin: A Cellular Voice Based Internet Shutdown Resistance System", Proceedings on Privacy Enhancing Technologies 2023(1), pp. 589-607, 2023. BibTex LaTex

89 [Journal article] T. Ashur, A. Bhati, A. Kindi, M. Mahzoun and L. Perrin, "XHash: Efficient STARK-friendly Hash Function", IACR Cryptology ePrint Archive , 14 pages, 2023. BibTex LaTex

90 [Journal article] T. Ashur, A. Kindi and M. Mahzoun, "XHash8 and XHash12: efficient stark-friendly hash functions", IACR Cryptology ePrint Archive 2023(1045), 15 pages, 2023. BibTex LaTex

91 [Journal article] A. Kumar, R. Degraeve, A. Beckers, A. Fantini, I. Verbauwhede, D. Linten and G. Kar, "Fault Attack Investigation on TaO<sub>x</sub> Resistive-RAM for Cyber Secure Application", IEEE Transactions on BibTex LaTex

Electron Devices 70(8), pp. 4170-4177, 2023.

92 [Journal article] I. Fernandez-Hernandez, R. Hirokawa, V. Rijmen and Y. Aikawa, "PPP/PPP-RTK Message Authentication", NAVIGATION: Journal of the Institute of Navigation 70(2), 21 pages, 2023.
BibTex LaTex

93 [Journal article] V. Tulceanu, S. Muys and B. Preneel, "Small data: fuzzy emotional memory brainwave authentication", Special Issue of the Journal of Intelligent and Fuzzy Systems 45(1), in print, 2023.
BibTex LaTex

94 [Journal article] V. Tulceanu, L. De Greve and B. Preneel, "Brainwave authentication: from motor to cognitive and emotional tasks", Special Issue of the Journal of Intelligent and Fuzzy Systems 45(1), 12 pages, 2023.
BibTex LaTex

95 [Journal article] R. Attarian and A. Keshavarz-Haddad, "Effective website fingerprinting attack based on the first packet direction only", Computer Networks 231, 12 pages, 2023.
BibTex LaTex

96 [Journal article] N. Smart, "Practical and Efficient FHE-based MPC", IACR Cryptology ePrint Archive 2023(981), pp. 1-39, 2023.
BibTex LaTex

97 [Journal article] T. Balenbois, J. Orfila and N. Smart, "Trivial Transciphering With Trivium and TFHE", IACR Cryptology ePrint Archive 2023(980), pp. 1-18, 2023.
BibTex LaTex

98 [Journal article] T. Beyne, "An invariant of the round function of QARMAv2-64", IACR Cryptology ePrint Archive 2023(963), 1 pages, 2023.
BibTex LaTex

99 [Journal article] S. Sadati Faramarzi, B. Luo, J. Poortmans, J. Genoe and K. Myny, "Thin-Film Transistor-Based Sensor Interface Circuits Enabling Distributed Local In-Module Solar Cell Temperature Monitoring", IEEE Journal of Solid-State Circuits 59(1), pp. 307-315, 2023.
BibTex LaTex

100 [Journal article] A. Abidin, K. Eldefrawy and D. Singelée, "Entanglement-based Mutual Quantum Distance Bounding", arXiv null(2305.09905v1), 22 pages, 2023.
BibTex LaTex

101 [Journal article] A. Bhati, A. Dufka, E. Andreeva, A. Roy and B. Preneel, "Skye: An Expanding PRF based Fast KDF and its Applications", IACR Cryptology ePrint Archive 2023(781), 17 pages, 2023.
BibTex LaTex

102 [Journal article] L. Wu, Y. Fan, B. Preneel, W. Wang and M. Wang, "An automated generation tool of hardware masked S-box: AGEMA+", IACR Cryptology ePrint Archive 2023(831), 24 pages, 2023.
BibTex LaTex

103 [Journal article] L. Wu, Y. Fan, B. Preneel, W. Wang and M. Wang, "Automated Generation of Masked Nonlinear Components: From Lookup Tables to Private Circuits", IACR Cryptology ePrint Archive 2023(831), pp. 1-23, 2023.
BibTex LaTex

104 [Journal article] R. Sarenche, S. Aghili, D. Singelée and T. Yoshizawa, "DASLog: Decentralized Auditable Secure Logging for UAV Ecosystems", IEEE Internet of Things Journal 10(23), pp. 20264-20284, 2023.
BibTex LaTex

105 [Journal article] C. Carlet, E. Piccione, S. Andreoli, L. Budaghyan, S. Dhooghe, S. Petkova-Nikova, G. Petrides and V. Rijmen, "An Optimal Universal Construction for the Threshold Implementation of Bijective S-boxes", IEEE Transactions on Information Theory 70(1), 16 pages, 2023.
BibTex LaTex

106 [Journal article] J. Wang, C. Niu, Q. Liu, M. Li, B. Preneel and M. Wang, "Cryptanalysis of SPEEDY", IACR Cryptology ePrint Archive 2023(612), 33 pages, 2023.
BibTex LaTex

107 [Journal article] T. Ashur, M. Mahzoun and D. Toprakhisar, "How Not To Design An Efficient FHE-Friendly Block Cipher: Seljuk", The Computer Journal 66(6), pp. 1312-1319, 2023.
BibTex LaTex

108 [Journal article] E. Dushku, M. Rabbani, J. Vliegen, A. Braeken and N. Mentens, "PROVE: Provable remote attestation for public verifiability", Journal of Information Security and Applications null(75), 13 pages, 2023.
BibTex LaTex

109 [Journal article] L. Zhang, H. Kan, F. Qiu and F. Hao, "A Publicly Verifiable Optimistic Fair Exchange Protocol Using Decentralized CP-ABE", The Computer Journal , 13 pages, 2023.
BibTex LaTex

110 [Journal article] T. Ashur, T. Buschman and M. Mahzoun, "Algebraic cryptanalysis of POSEIDON", IACR Cryptology ePrint Archive 2023(537), 19 pages, 2023. BibTex LaTex

111 [Journal article] V. Shoup and N. Smart, "Lightweight Asynchronous Verifiable Secret Sharing with Optimal Resilience", IACR Cryptology ePrint Archive , 56 pages, 2023. BibTex LaTex

112 [Journal article] M. Grujic and I. Verbauwhede, "Optimizing Linear Correctors: A Tight Output Min-Entropy Bound and Selection Technique", IEEE Transactions on Information Forensics and Security 19, pp. 586-600, 2023. BibTex LaTex

113 [Journal article] B. Pinkas, T. Schneider, N. Smart and S. Williams, "Secure Two-Party Computation is Practical", IACR Cryptology ePrint Archive 2009(314), 20 pages, 2023. BibTex LaTex

114 [Journal article] J. Schwidtal, V. Robu, M. Bahloul, I. Scott, T. Mbavarira, J. Manuel Espana, L. Kiesling, P. Piccini, M. Troncia, R. Chitchyan, M. Montakhabi, C. Francis, A. Gorbatcheva, T. Capper, M. Mustafa and M. Andoni, "Emerging business models in local energy markets: A systematic review of peer-to-peer, community self-consumption, and transactive energy models", Renewable and Sustainable Energy Reviews 179(113273), 99 pages, 2023. BibTex LaTex

115 [Journal article] R. Geelen and F. Vercauteren, "Bootstrapping for BGV and BFV Revisited", Journal of Cryptology 36(2), 32 pages, 2023. BibTex LaTex

116 [Journal article] A. Ghosh, J. Bermudo Mera, A. Karmakar, D. Das, S. Ghosh, I. Verbauwhede and S. Sen, "Encapsulation Mechanism Saber With Low-Latency Striding Toom–Cook Multiplication", IEEE Journal of Solid-State Circuits 58(5), 16 pages, 2023. BibTex LaTex

117 [Journal article] A. Ghosh, J. Bermudo Mera, A. Karmakar, D. Das, S. Ghosh and I. Verbauwhede, "A 334 µW 0.158 mm2 ASIC for Post-Quantum Key-Encapsulation Mechanism Saber With Low-Latency Striding Toom–Cook Multiplication", IEEE Journal of Solid-State Circuits 58(8), pp. 2383-2398, 2023. BibTex LaTex

118 [Journal article] S. Su, B. Yang, V. Rozic, M. Yang, M. Zhu, S. Wei and L. Liu, "A Closer Look at the Chaotic Ring Oscillators based TRNG Design", IACR Transactions on Cryptographic Hardware and Embedded Systems 2023(2), pp. 381-417, 2023. BibTex LaTex

119 [Journal article] K. Cong, D. Das, G. Nicolas and J. Park, "Panacea: Non-interactive and Stateless Oblivious RAM", IACR Cryptology ePrint Archive 2023(274), 31 pages, 2023. BibTex LaTex

120 [Journal article] E. Orsini and R. Zanotto, "Simple Two-Round OT in the Explicit Isogeny Model", IACR Cryptology ePrint Archive 2023(269), pp. 1-37, 2023. BibTex LaTex

121 [Journal article] A. Sateesan, J. Biesmans, T. Claesen, J. Vliegen and N. Mentens, "Optimized algorithms and architectures for fast non-cryptographic hash functions in hardware", Microprocessors and Microsystems null(98), 11 pages, 2023. BibTex LaTex

122 [Journal article] K. Jannes, E. Heydari Beni, B. Lagaisse and W. Joosen, "BeauForT: Robust Byzantine Fault Tolerance for Client-Centric Mobile Web Applications", IEEE Transactions on Parallel and Distributed Systems , pp. 1241-1252, 2023. BibTex LaTex

123 [Journal article] M. Montakhabi, S. Van der Graaf and M. Mustafa, "Valuing the value: An affordances perspective on new models in the electricity market", ENERGY RESEARCH & SOCIAL SCIENCE 96(102902), 12 pages, 2023. BibTex LaTex

124 [Journal article] J. D'Anvers, M. Van Beirendonck and I. Verbauwhede, "Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations", IEEE Transactions on Computers 72(2), pp. 321-332, 2023. BibTex LaTex

125 [Journal article] I. Verbauwhede, "Circuits for Security and Secure Circuits: Implementation of cryptographic algorithms", IEEE Solid-State Circuits Magazine 15(1), pp. 20-24, 2023. BibTex LaTex

126 [Journal article] T. Yoshizawa, D. Singelée, J. Tobias Muehlberg, S. DELBRUEL, D. HUGHES, B. Preneel and A. TAHERKORDI, "A Survey of Security and Privacy Issues in V2X Communication Systems", ACM Computing Surveys 55(9), pp. 1-36, 2023. BibTex LaTex

127 [Journal article] A. Guimarães, H. Lima Pereira and B. Van Leeuwen, "Amortized Bootstrapping Revisited: Simpler, Asymptotically-faster, Implemented", IACR Cryptology ePrint Archive 2023(014), pp. 1-41, 2023. BibTex LaTex

128 [Journal article] M. Remmerswaal, L. Wu, S. Tiran and N. Mentens, "AutoPOI: Automated Points Of Interest Selection for Side-channel Analysis", IACR Cryptology ePrint Archive 2023(008), pp. 1-13, 2023. BibTex LaTex

129 [Journal article] A. Abiad, W. Castryck, M. De Boeck, J. Koolen and S. Zeijlemaker, "An infinite class of Neumaier graphs and non-existence results", Journal of Combinatorial Theory, Series A 193(1), 30 pages, 2023. BibTex LaTex

130 [Journal article] C. Bootland, W. Castryck, A. Szepieniec and F. Vercauteren, "SoK: On the security of cryptographic problems from linear algebra", Mathematical Cryptology 3(1), 44 pages, 2023. BibTex LaTex

131 [Journal article] W. Castryck, F. Vermeulen and Y. Zhao, "Scrollar invariants, syzygies and representations of the symmetric group", Journal für die reine und angewandte Mathematik 796, pp. 117-159, 2023. BibTex LaTex

132 [Journal article] J. Gaspoz and S. Dhooghe, "Threshold Implementations in Software: Micro-architectural Leakages in Algorithms", IACR Transactions on Cryptographic Hardware and Embedded Systems 1(2023), pp. 155-179, 2023. BibTex LaTex

133 [Journal article] S. Dhooghe, A. Rezaei Shahmirzadi and A. Moradi, "Low-Latency and Low-Randomness Second-Order Masked Cubic Functions", IACR Transactions on Cryptographic Hardware and Embedded Systems 1(2023), pp. 113-152, 2023. BibTex LaTex

134 [Journal article] H. Hirata, D. Miyahara, V. Arribas Abril, Y. Li, A. Miyaji, S. Petkova-Nikova and K. Sakiyama, "All You Need Is Fault: Zero-Value Attacks on AES and a New λ-Detection M&M", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(1), pp. 133-156, 2023. BibTex LaTex

135 [Journal article] A. Askeland, S. Petkova-Nikova and V. Nikov, "Who Watches the Watchers: Attacking Glitch Detection Circuits", IACR Transactions on Cryptographic Hardware and Embedded Systems 2024(1), pp. 157-179, 2023. BibTex LaTex

136 [Book chapter] V. Tulceanu and B. Preneel, "Modern investigative tools: the use and possible abuse of BCI" In Advances in Intelligent Systems and Computing, Springer-Verlag, in print, 2023. BibTex LaTex

137 [Book chapter] V. Tulceanu and B. Preneel, "Mindprints: world propaganda and EEG" In Advances in Intelligent Systems and Computing, Springer-Verlag, in print, 2023. BibTex LaTex

138 [Thesis] L. Le Jeune, "Machine Learning for Network Intrusion Detection on FPGA", Phd thesis, KU Leuven, N. Mentens and T. Goedemé, 298 pages, 2023. BibTex LaTex

139 [Thesis] T. Yoshizawa, "Digital Certificate Usage and Management in Vehicular Communication Systems", Phd thesis, KU Leuven, B. Preneel, 290 pages, 2023. BibTex LaTex

140 [Thesis] L. Clarysse, A. Bhati and E. Andreeva, "A Web Tool for the Selection of Symmetric Key Modes", Master thesis, KU Leuven, B. Preneel, 84 pages, 2023. BibTex LaTex

141 [Thesis] Y. Xi, J. Zhu, J. Kang and R. Geelen, "An Investigation of Polynomial Activation Functions in Neural Networks", Master thesis, KU Leuven, F. Vercauteren and M. Blaschko, 81 pages, 2023. BibTex LaTex

142 [Thesis] P. Comak De Cnudde, "Analyzing Privacy-Preserving Smart Contracts", Master thesis, KU Leuven, A. Abidin, T. Ashur and B. Preneel, 82 pages, 2023. BibTex LaTex

143 [Thesis] S. Eggers, "Security of Brain Implants", Master thesis, Katholieke Universiteit Leuven, B. Preneel, 97 pages, 2023. BibTex LaTex

144 [Thesis] S. Samanta, "User-centric privacy enhanced wallet", Master thesis, Indian Statistical Institute, B. Preneel and B. Roy, 49 pages, 2023. BibTex LaTex

145 [Thesis] R. Parikh, S. Duttagupta and D. Singelée, "TKBE : Two Key Broadcast Encryption for the IoT", Master thesis, Indian Statistical Institute, B. Preneel and B. Roy, 39 pages, 2023. BibTex LaTex

146 [Thesis] T. Garai, "SCA Resistant Implementation of Post- Quantum Scheme: CRYSTALS - Kyber", Master thesis, Indian Statistical Institute, I. Verbauwhede and B. Roy, 36 pages, 2023. BibTex LaTex

147 [Thesis] X. Fransen, "A Deductively Verifiable Implementation of Shamir Secret Sharing in Rust", Master thesis, KU Leuven, N. Smart and G. Nicolas, 53 pages, 2023. BibTex LaTex

148 [Thesis] K. Cornelis, "Polynomial Optimization For Homomorphic Encryption Schemes", Master thesis, KU Leuven, F. Vercauteren, 62 pages, 2023. BibTex LaTex

149 [Thesis] P. Luyten, "Understanding Kipnis Shamir with two quadrics", Master thesis, KU Leuven, F. Vercauteren, 71 pages, 2023. BibTex LaTex

150 [Thesis] J. Spiessens, "Private Verifiable Computations via Lattice-based SNARKs", Master thesis, KU Leuven, F. Vercauteren, 63 pages, 2023. BibTex LaTex

151 [Thesis] R. Vermeiren, "Cryptanalysis of isogeny-based systems and their implementations", Master thesis, KU Leuven, F. Vercauteren, 59 pages, 2023. BibTex LaTex

152 [Thesis] W. Croux, "Towards a practical key exchange based on oriented isogenies", Master thesis, KU Leuven, F. Vercauteren, 46 pages, 2023. BibTex LaTex

153 [Thesis] A. Van Beersel, "Analysis of Isogeny Graphs with Level Structure", Master thesis, KU Leuven, F. Vercauteren, 56 pages, 2023. BibTex LaTex

154 [Thesis] T. Vlummens, "Analysis of Session Recording Services", Master thesis, KU Leuven, C. Diaz, 51 pages, 2023. BibTex LaTex

155 [Thesis] R. De Koninck, "Enhancing 5G Security: A Comparison of 256-bit Symmetric-key Cryptosystems on FPGA", Master thesis, KU Leuven, B. Preneel, 120 pages, 2023. BibTex LaTex

156 [Thesis] B. De Cock, "Security evaluation of a personal hardware security device", Master thesis, KU Leuven, I. Verbauwhede, 45 pages, 2023. BibTex LaTex

157 [Thesis] R. Geens, " Design of an Application-Specific Integrated Processor for Kyber", Master thesis, KU Leuven, I. Verbauwhede, 96 pages, 2023. BibTex LaTex

158 [Thesis] A. Cloetens, "Secure logic on FPGA's", Master thesis, KU Leuven, I. Verbauwhede, 70 pages, 2023. BibTex LaTex

159 [Thesis] A. Moortgat, "On-Chain Storage of NFT Colletions on the Ethereum Network", Master thesis, KU Leuven, B. Preneel and T. Holvoet, 75 pages, 2023. BibTex LaTex

160 [Thesis] C. Pan, "Implementation of an FPGA-based Low-cost Test Platform for Digital ASIC", Master thesis, KU Leuven, I. Verbauwhede, 68 pages, 2023. BibTex LaTex

161 [Thesis] Q. Vansina, "An extendable hardware architecture for FINAL's bootstrapping", Master thesis, KU Leuven, I. Verbauwhede, 74 pages, 2023. BibTex LaTex

162 [Thesis] T. Vander Beke, "Applying side channel analysis for code coverage feedback in fuzzers", Master thesis, KU Leuven, B. Preneel, 56 pages, 2023. BibTex LaTex

163 [Thesis] T. Thoelen, "Masked Implementation of SHA-256 in Hardware", Master thesis, KU Leuven, V. Rijmen, S. Petkova-Nikova, S. Dhooghe and Z. Zhang, 63 pages, 2023. BibTex LaTex

164 [Thesis] N. Antonijević, D. Singelée, E. Marín Fàbregas, S. Duttagupta and B. Preneel, "Secure Path Verification in Software-defined Networks", Master thesis, KU Leuven, B. Preneel, 77 pages, 2023. PDF BibTex LaTex

165 [Thesis] J. Rots, R. Geelen and H. Lima Pereira, "Conversion between word-wise and Boolean homomorphic encryption schemes", Master thesis, KU Leuven, F. Vercauteren, 82 pages, 2023. BibTex LaTex

166 [Thesis] R. Louwet, A. Bhati and E. Andreeva, "ForkSKINNY on steroids: Combining bit slicing with SIMD", Master thesis, KU Leuven, B. Preneel and M. Vanhoef, 74 pages, 2023. PDF BibTex LaTex

167 [Thesis] P. Sluys, L. Wouters, B. Gierlichs and I. Verbauwhede, "An in-depth security evaluation of the Nintendo DSi gaming console", Master thesis, KU Leuven, I. Verbauwhede, 100 pages, 2023. PDF BibTex LaTex

168 [Thesis] T. Beyne, "A geometric approach to symmetric-key cryptanalysis", Phd thesis, KU Leuven, V. Rijmen, 404 pages, 2023. PDF BibTex LaTex

169 [Thesis] T. Thoelen, "Masked Implementation of SHA-256 in Hardware", Master thesis, KU Leuven, S. Petkova-Nikova and V. Rijmen, 63 pages, 2023. PDF BibTex LaTex

170 [Thesis] A. Purnal, "Cache Side-Channel Attacks on Existing and Emerging Computing Platforms", Phd thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 250 pages, 2023. PDF BibTex LaTex

171 [Thesis] T. Vander Beke, I. Siros and L. Wouters, "Applying side channel analysis for code coverage feedback in fuzzers", Master thesis, KU Leuven, B. Preneel, 56 pages, 2023. PDF 🔗 BibTex LaTex

172 [Thesis] R. Posteuca, "Design and Analysis of Lightweight Symmetric-Key Primitives", Phd thesis, KU Leuven, V. Rijmen and T. Ashur, 236 pages, 2023. PDF 🔗 BibTex LaTex

173 [Thesis] A. Ranea, "White-box Design and Black-box Cryptanalysis of ARX Ciphers", Phd thesis, KU Leuven, B. Preneel and V. Rijmen, 210 pages, 2023. PDF BibTex LaTex

174 [Thesis] T. Tanguy, "Secure MultiParty Computation: Protocols and Applications", Phd thesis, KU Leuven, N. Smart, 296 pages, 2023. PDF BibTex LaTex

175 [Thesis] D. Bozilov, "Low-Latency Threshold Implementations for Side-Channel Protected Cryptographic Hardware", Phd thesis, KU Leuven, B. Preneel and V. Rijmen, 166 pages, 2023. PDF BibTex LaTex

176 [Thesis] M. Diamantino Caribe, "A Novel Post-quantum Authenticated Key Establishment Protocol", Master thesis, Katholieke Universiteit Leuven, B. Preneel and M. Vanhoef, 115 pages, 2023. PDF BibTex LaTex

177 [Thesis] Y. Talibi Alaoui, "Financial Applications for Multiparty Computation", Phd thesis, KU Leuven, N. Smart, 366 pages, 2023. PDF BibTex LaTex

178 [Proceeding] "Selected Areas in Cryptography, 39 Annual International Workshop, SAC 2023", Lecture Notes in Computer Science, C. Carlet, K. Mandal and V. Rijmen (Eds.), Springer-Verlag, 2023. 🔗 BibTex LaTex

179 [Proceeding] "Advances in Cryptology - CRYPTO 2023", Lecture Notes in Computer Science, H. Handschuh and A. Lysyanskaya (Eds.), Springer-Verlag, 2023. BibTex LaTex

180 [Report] C. Ozkan, D. Singelée and B. Preneel, "How Insecure Configurations of Active Directory Could Lead to Full Compromise of SCADA Systems", COSIC Internal Report, 3 pages, 2023. PDF BibTex LaTex

181 [Abstract of talk] B. Askin Ozdemir and T. Beyne, "Poster: Generic Multidimensional Linear Cryptanalysis of Feistel Ciphers", In Proceedings of the 22nd ACM Conference on Computer and Communications Security, 3 pages, 2023. 🔗 BibTex LaTex

182 [Talk] S. Kundu, "A Fault Propagation Attack on Side-Channel Protected LWE-based KEM", Post Quantum Cryptography (PQC) Workshop at International Conference on Security, Privacy and Applied Cryptography Engineering - SPACE 2023, Roorkee, IN, 2023. PDF BibTex LaTex

183 [Talk] B. Preneel, "De rol van cryptografie in de digitale maatschappij", Gastcolleges - Maatschappijkritische reeks Ingenieur & Maatschappij - 2023 (Universiteit Hasselt - Faculteit Industriële ingenieurswetenschappen), Diepenbeek, BE, 2023. BibTex LaTex

184 [Talk] B. Preneel, "The Intersection of Cybersecurity and AI: Opportunities and Challenges", Cyberwal in Galaxia, Transinne, BE, 2023. BibTex LaTex

185 [Talk] W. Castryck, "Isogeny interpolation for elliptic curves", 682, Hyderabad, IN, 2023. BibTex LaTex

186 [Talk] I. Verbauwhede, "Keynote talk", WAHC 2023 – 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Copenhagen, DK, 2023. BibTex LaTex

187 [Talk] B. Preneel, "Post-quantum cryptography: Counting down till 20233", Digital security and everyday life - distinguished lecture series, Passau, DE, 2023. BibTex LaTex

188 [Talk] B. Preneel, "The Intersection of Cybersecurity and AI", Melbourne Connect - The Studio, Melbourne, AU, 2023. BibTex LaTex

189 [Talk] N. Smart, "Can a public blockchain be truly private?", BE-CYBER Experience Sharing Day, Brussels, BE, 2023. BibTex LaTex

190 [Talk] M. Sel, "Evaluation of Trustworthiness using Public and Private Data", 14th IFIP International Conference on Trust Management (IFIPTM 2023), Amsterdam, NL, 2023. BibTex LaTex

191 [Talk] B. Preneel, "Cybersecurity and AI", SECITC 2023, Bucharest, RO, 2023. BibTex LaTex

192 [Talk] B. Preneel, "Blockchain attacks: what are the limits?", TUM Blockchain conference, Munich, DE, 2023. BibTex LaTex

193 [Talk] B. Preneel, "The impact of artificial intelligence on cybersecurity", Cybersecurity and AI: A match made in heaven?, Leuven, BE, 2023. BibTex LaTex

194 [Talk] B. Preneel, "Cybersecurity and AI", Graz security week 2023, Graz , AT, 2023. BibTex LaTex

195 [Talk] B. Askin Ozdemir, "Poster: Privacy-preserving data aggregation with multiple data customers", Privacy Enhancing Technologies Symposium (PETS 23), Lausanne, CH, 2023. BibTex LaTex

196 [Talk] I. Verbauwhede, "DAC60 Celebration Panel: Designing the Future", DAC 60 2023, San Francisco, US, 2023. BibTex LaTex

197 [Talk] C. Diaz, "The Nym Network", Women in Security and Cryptography Workshop (WISC), Bochum, DE, 2023. BibTex LaTex

198 [Talk] B. Preneel, "Hiding in Plain Sight: Location Privacy for the IoT", 5th Interdisciplinary Summerschool on Privacy (ISP 2023), Nijmegen, NL, 2023. BibTex LaTex

199 [Talk] A. Ranea, "Poster: Characteristic automated search of cryptographic algorithms for distinguishing attacks (CASCADA)", JNIC 2023, Vigo, ES, 2023. BibTex LaTex

200 [Talk] S. Kundu, "Masking Lattice-based Post-quantum Cryptography", SAFEST workshop, Tallinn, EE, 2023. BibTex LaTex

201 [Talk] I. Verbauwhede, "Hardware: an essential partner to cryptography", Summer School on real-world crypto and privacy 2023, Vodice, HR, 2023. BibTex LaTex

202 [Talk] W. Castryck, "An efficient break of the supersingular isogeny Diffie-Hellman protocol", Arithmetic, Geometry, Cryptography and Coding Theory, Marseille , FR, 2023. BibTex LaTex

203 [Talk] B. Preneel, "Cybersecurity policies - the never-ending crypto wars", AMUSEC, Marseille, FR, 2023. BibTex LaTex

204 [Talk] M. Gama, "Differentially Private Market Mechanisms with Multiparty Computation", DeFi workshop at FC23, Bol, HR, 2023. BibTex LaTex

205 [Talk] D. Toprakhisar, "Symmetric Block Cipher Design and Physical Security ", TUBITAK Crypto Days 2023, Istanbul, TR, 2023. BibTex LaTex

206 [Talk] A. Bhati, "Expand the Power of the Forc(e)", Rump Session, Eurocrypt 2023, Lyon, FR, 2023. BibTex LaTex

207 [Talk] B. Preneel, "Talk at Cyber Security track", European AI Week, Brussels, BE, 2023. BibTex LaTex

208 [Talk] J. Kang, "On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption", 2nd Annual FHE.org Conference on Fully Homomorphic Encryption, Tokyo, JP, 2023. BibTex LaTex

209 [Talk] J. Bertels, "FHEW Hardware Accelerator", FHE.org, Tokyo, JP, 2023. BibTex LaTex

210 [Talk] J. D'Anvers, W. Legiest, M. Van Beirendonck and I. Verbauwhede, "FPT: a Fixed-Point Accelerator for Torus Fully Homomorphic Encryption", 2nd Annual FHE.org Conference on Fully Homomorphic Encryption, Tokyo, JP, 2023. BibTex LaTex

211 [Talk] J. D'Anvers, M. Van Beirendonck and I. Verbauwhede, "FPT: a Fixed-Point Accelerator for Torus Fully Homomorphic Encryption", 6th HomomorphicEncryption.org Standards Meeting, Seoul, KR, 2023. BibTex LaTex

212 [Talk] R. Geelen and J. Kang, "Poster: On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption", 6th HomomorphicEncryption.org Standards Meeting, Seoul, KR, 2023. BibTex LaTex

213 [Talk] B. Preneel, "Fear and trust in cybersecurity Lesson followed by interdisciplinary debate (Francqui Chair)", Francqui Chair, Louvain-la-Neuve, BE, 2023. BibTex LaTex

214 [Talk] B. Preneel, "Cybersecurity policy and lawful access (Francqui Chair)", Francqui Chair, Louvain-la-Neuve, BE, 2023. BibTex LaTex

215 [Talk] B. Preneel, "Computing on encrypted data (Francqui Chair)", Francqui Chair, Louvain-la-Neuve, BE, 2023. BibTex LaTex

216 [Talk] B. Preneel, "The quantum threat and post-quantum cryptography (Francqui Chair)", Francqui Chair, Louvain-la-Neuve, BE, 2023. BibTex LaTex

217 [Talk] B. Preneel, "New developments in cryptography land (Francqui Chair)", Francqui Chair, Louvain-la-Neuve, BE, 2023. BibTex LaTex

2022

1 [Conf article] A. Sateesan, J. Vliegen and N. Mentens, "An Analysis of the Hardware-Friendliness of AMQ Data Structures for Network Security" In International Conference on Security, Privacy and Applied Cryptography Engineering, Lecture Notes in Computer Science 13783, L. Batina, M. Mondal and S. Picek (Eds.), Springer-Verlag, 287–313 pages, 2022. BibTex LaTex

2 [Conf article] C. Bonte, I. Iliashenko, J. Park, H. Lima Pereira and N. Smart, "FINAL: Faster FHE instantiated with NTRU and LWE" In Advances in Cryptology - ASIACRYPT 2022, Lecture Notes in Computer Science, S. Agrawal and D. Lin (Eds.), Springer-Verlag, 23 pages, 2022. BibTex LaTex

3 [Conf article] Y. Chen, "A Modular Approach to the Security Analysis of Two-Permutation Constructions" In Advances in Cryptology - ASIACRYPT 2022, Lecture Notes in Computer Science, S. Agrawal and D. Lin (Eds.), Springer-Verlag, pp. 379-409, 2022. BibTex LaTex

4 [Conf article] W. Castryck, T. Decru, M. Houben and F. Vercauteren, "Horizontal racewalking using radical isogenies" In Advances in Cryptology - ASIACRYPT 2022, Lecture Notes in Computer Science, S. Agrawal and D. Lin (Eds.), Springer-Verlag, 30 pages, 2022. BibTex LaTex

5 [Conf article] M. Garcia-Constantino, A. Konios, I. Hussein Lopez-Nava, P. Pouliet, I. Ekerete, M. Mustafa, C. D Nugent and G. Morrison, "Analysis of Accelerometer Data for Personalised Abnormal Behaviour Detection in Activities of Daily Living" In International Conference on Ubiquitous Computing & Ambient Intelligence (UCAml) 2022, Lecture Notes in Computer Science, Springer-Verlag, 12 pages, 2022. BibTex LaTex

6 [Conf article] T. Yoshizawa and B. Preneel, "Misbehaviour Reporting in ETSI ITS Standard Considered Broken" In IEEE Conference on Standards for Communications and Networking, 7 pages, 2022. BibTex LaTex

7 [Conf article] K. Baghery and N. Bardeh, "Updatable NIZKs from Non-Interactive Zaps" In Cryptology and Network Security, Lecture Notes in Computer Science 13641, E. Bellini, A. Beresford, and A. Patra, (Eds.), Springer-Verlag, pp. 23-43, 2022. BibTex LaTex

8 [Conf article] C. Baum, R. Jadoul, E. Orsini, P. Scholl and N. Smart, "Feta: Efficient Threshold Designated-Verifier Zero-Knowledge Proofs" In ACM Conference on Computer and Communications Security - CCS 2022, ACM, 293–306 pages, 2022. BibTex LaTex

9 [Conf article] T. Ashur, M. Mahzoun and D. Toprakhisar, "Chaghri --- an FHE-friendly Block Cipher" In Proceedings of the 22nd ACM Conference on Computer and Communications Security, Association for Computing Machinery (ACM), ACM, pp. 139-150, 2022. BibTex LaTex

10 [Conf article] K. Cong, D. Das, J. Park and H. Lima Pereira, "SortingHat: Efficient Private Decision Tree Evaluation via Homomorphic Encryption and Transciphering" In ACM Conference on Computer and Communications Security - CCS 2022, ACM, pp. 563-577, 2022. BibTex LaTex

11 [Conf article] S. Dhooghe, A. Rezaei Shahmirzadi and A. Moradi, "Second-Order Low-Randomness D + 1 Hardware Sharing of the AES" In ACM Conference on Computer and Communications Security - CCS 2022, ACM, pp. 815-828, 2022. BibTex LaTex

12 [Conf article] M. Ciampi, E. Orsini and L. Siniscalchi, "Four-Round Black-Box Non-malleable Schemes from One-Way Permutations" In Theory of Cryptography Conference (TCC 2022), Lecture Notes in Computer Science 13748, Springer-Verlag, pp. 300-329, 2022. BibTex LaTex

13 [Conf article] T. Yadav, D. Gosain, A. Herzberg, D. Zappala and K. Seamons, "Automatic Detection of Fake Key Attacks in Secure Messaging" In ACM Conference on Computer and Communications Security - CCS 2022, ACM, pp. 3019-3032, 2022. BibTex LaTex

14 [Conf article] K. Alshmrany, A. Bhayat, F. Brauße, L. Cordeiro, K. Korovin, T. Melham, M. Mustafa, P. Olivier, G. Reger and F. Shmarov, "Position Paper: Towards a Hybrid Approach to Protect Against Memory Safety Vulnerabilities" In Secure Development Conference 2022, IEEE, 7 pages, 2022. BibTex LaTex

15 [Conf article] J. Nightingale, Y. Wang, F. Zobiri and M. Mustafa, "Effect of Clustering in Federated Learning on Non-IID Electricity Consumption Prediction" In IEEE PES Innovative Smart Grid Technologies (ISGT Europe 2022), IEEE, 5 pages, 2022. BibTex LaTex

16 [Conf article] T. Yoshizawa and B. Preneel, "On Handling of Certificate Digest in V2X Communication" In IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2022), IEEE, 6 pages, 2022. BibTex LaTex

17 [Conf article] A. Madhusudan, F. Zobiri and M. Mustafa, "Billing Models for Peer-to-Peer Electricity Trading Markets with Imperfect Bid-Offer Fulfillment" In IEEE International Smart Cities Conference (ISC2 2022), IEEE, 6 pages, 2022. BibTex LaTex

18 [Conf article] A. Aly and S. Cleemput, "A Fast, Practical and Simple Shortest Path Protocol for Multiparty Computation" In European Symposium on Research in Computer Security - ESORICS 2022, Lecture Notes in Computer Science 13556, Springer-Verlag, pp. 749-755, 2022. BibTex LaTex

19 [Conf article] R. Perlner, J. Kelsey and D. Cooper, "Breaking Category Five SPHINCS+ with SHA-256" In Post-Quantum Cryptography, Lecture Notes in Computer Science, J. Hee Cheon and T. Johansson (Eds.), Springer-Verlag, pp. 501-522, 2022. BibTex LaTex

20 [Conf article] A. Brenneis, M. Gottardi, M. Grujic, I. Herrmann, N. Massari, D. Oshinubi, L. Parmesan, M. Perenzoni, T. Strohm, A. Tontini and I. Verbauwhede, "A monolithic SPAD-based random number generator for cryptographic application" In 2022 European Solid-State Circuits Conference (ESSCIRC 2022), IEEE, pp. 73-76, 2022. PDF BibTex LaTex

21 [Conf article] R. Posteuca and V. Rijmen, "RAMus- A New Lightweight Block Cipher for RAM Encryption" In , Lecture Notes in Computer Science 13409, C. Galdi and S. Jarecki (Eds.), Springer-Verlag, 69–92 pages, 2022. BibTex LaTex

22 [Conf article] G. Barbu, W. Beullens, E. Dottax, C. Giraud, A. Houzelot, C. Li, M. Mahzoun, A. Ranea and J. Xie, "ECDSA White-Box Implementations: Attacks and Designs from CHES 2021 Challenge" In Cryptographic Hardware and Embedded Systems - CHES 2022, Lecture Notes in Computer Science 2022, No. 4, Springer-Verlag, 26 pages, 2022. PDF BibTex LaTex

23 [Conf article] A. Peetermans and I. Verbauwhede, "An energy and area efficient, all digital entropy source compatible with modern standards based on jitter pipelining" In Cryptographic Hardware and Embedded Systems - CHES 2022, Lecture Notes in Computer Science 2022, No. 4, Springer-Verlag, pp. 88-109, 2022. PDF BibTex LaTex

24 [Conf article] L. Le Jeune, T. Goedemé and N. Mentens, "Feature dimensionality in CNN acceleration for high-throughput network intrusion detection" In International Conference on Field Programmable Logic and Applications (FPL 2022), IEEE Computer Society 2022, IEEE, 9 pages, 2022. BibTex LaTex

25 [Conf article] A. Ranea, J. Vandersmissen and B. Preneel, "Implicit White-Box Implementations: White-Boxing ARX Ciphers" In Advances in Cryptology - CRYPTO 2022, Lecture Notes in Computer Science, Springer-Verlag, 31 pages, 2022. PDF BibTex LaTex

26 [Conf article] T. Beyne and V. Rijmen, "Differential Cryptanalysis in the Fixed-Key Model" In Advances in Cryptology - CRYPTO 2022, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2022. PDF BibTex LaTex

27 [Conf article] C. Beierle, T. Beyne, P. Felke and G. Leander, "Constructing and Deconstructing Intentional Weaknesses in Symmetric Ciphers" In Advances in Cryptology - CRYPTO 2022, Lecture Notes in Computer Science, Springer-Verlag, 31 pages, 2022. PDF BibTex LaTex

28 [Conf article] T. Beyne and Y. Chen, "Provably Secure Reflection Ciphers" In Advances in Cryptology - CRYPTO 2022, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2022. PDF BibTex LaTex

29 [Conf article] K. Kohls and C. Diaz, "VerLoc: Verifiable Localization in Decentralized Systems" In 31 USENIX Security Symposium 2022, Usenix, 18 pages, 2022. PDF BibTex LaTex

30 [Conf article] A. Purnal, F. Turan and I. Verbauwhede, "Double Trouble: Combined Heterogeneous Attacks on Non-Inclusive Cache Hierarchies" In 31 USENIX Security Symposium 2022, Usenix, 19 pages, 2022. PDF BibTex LaTex

31 [Conf article] A. Senol, G. Acar, F. Borgesius and M. Humbert, "Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission" In 31 USENIX Security Symposium 2022, Usenix, 18 pages, 2022. PDF BibTex LaTex

32 [Conf article] W. Castryck, M. Houben, F. Vercauteren and B. Wesolowski, "On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves" In Algorithmic Number Theory, 15 International Symposium, ANTS 2022, Lecture Notes in Computer Science, Springer-Verlag, 17 pages, 2022. PDF BibTex LaTex

33 [Conf article] M. Houben and M. Streng, "Generalized class polynomials" In Algorithmic Number Theory, 15 International Symposium, ANTS 2022, Lecture Notes in Computer Science, Springer-Verlag, 28 pages, 2022. PDF BibTex LaTex

34 [Conf article] K. Erdayandi, A. Paudel, L. Cordeiro and M. Mustafa, "Privacy-Friendly Peer-to-Peer Energy Trading: A Game Theoretical Approach" In Power & Energy Society General Meeting 2022, IEEE, 5 pages, 2022. PDF BibTex LaTex

35 [Conf article] K. Erdayandi, L. Cordeiro and M. Mustafa, "Towards Privacy Preserving Local Energy Markets" In BibTex

Competitive Advantage in the Digital Economy 2022, IET, 8 pages, 2022. PDF LaTex

36 [Conf article] N. Stricker, J. Liam Albert, M. Rabbani, S. Mayer and A. Gomez, "Secure Communication with Batteryless Sensors" In 2022 11th Mediterranean Conference on Embedded Computing (MECO), IEEE, pp. 1-4, 2022. BibTex LaTex

37 [Conf article] W. Hellemans, M. Rabbani, J. Vliegen and N. Mentens, "FOCUS: Frequency Based Detection of Covert Ultrasonic Signals" In International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2022, Springer International Publishing, pp. 70-86, 2022. BibTex LaTex

38 [Conf article] L. Sun, B. Preneel, W. Wang and M. Wang, "A Greater GIFT: Strengthening GIFT against Statistical Cryptanalysis" In Advances in Cryptology - EUROCRYPT 2022, Lecture Notes in Computer Science, Springer-Verlag, 52 pages, 2022. PDF BibTex LaTex

39 [Conf article] S. Katsumata, W. Beullens, S. Dobson, Y. Lai and F. Pintore, "Group Signature and More from Isogenies and Lattices: Generic, Simple, and Efficient" In Advances in Cryptology - EUROCRYPT 2022, Lecture Notes in Computer Science, Springer-Verlag, 56 pages, 2022. BibTex LaTex

40 [Conf article] J. Vandersmissen, A. Ranea and B. Preneel, "A White-Box Speck Implementation using Self-Equivalence Encodings" In Applied Cryptography and Network Security - ACNS 2022, Lecture Notes in Computer Science, Springer-Verlag, 24 pages, 2022. PDF BibTex LaTex

41 [Conf article] A. Beckers, R. Uytterhoeven, T. Vandenabeele, J. Vliegen, L. Wouters, J. Daemen, W. Dehaene, B. Gierlichs and N. Mentens, "Energy and side-channel security evaluation of near-threshold cryptographic circuits in 28nm FD-SOI technology" In ACM International Conference on Computing Frontiers 2022, A. Bartolini and A. Butko (Eds.), ACM, pp. 258-262, 2022. PDF BibTex LaTex

42 [Conf article] A. Ghosh, J. Bermudo Mera, A. Karmakar, D. Das, S. Ghosh, I. Verbauwhede and S. Sen, "A 334uW 0.158 mm2 Saber Learning with Rounding based Post-Quantum Crypto Accelerator " In IEEE Custom Integrated Circuits Conference (CICC 2022), IEEE, pp. 1-2, 2022. PDF BibTex LaTex

43 [Conf article] A. Beckers, L. Wouters, B. Gierlichs, B. Preneel and I. Verbauwhede, "Provable Secure Software Masking in the Real-World" In Workshop on Constructive Side-Channel Analysis and Secure Design 2022, Lecture Notes in Computer Science 13211, Springer-Verlag, pp. 215-235, 2022. PDF BibTex LaTex

44 [Conf article] L. Wouters, B. Gierlichs and B. Preneel, "On the susceptibility of Texas Instruments SimpleLink platform microcontrollers to non-invasive physical attacks" In Workshop on Constructive Side-Channel Analysis and Secure Design 2022, Lecture Notes in Computer Science 13211, Springer-Verlag, pp. 143-163, 2022. PDF BibTex LaTex

45 [Conf article] M. Gama, F. Zobiri and S. Petkova-Nikova, "Multi-Party Computation Auction Mechanisms for a P2P Electricity Market with Geographical Prioritization" In CIGRE Symposium, pp. 1-13, 2022. PDF BibTex LaTex

46 [Conf article] F. Zobiri, M. Gama, G. Deconinck and S. Petkova-Nikova, "A Privacy-Preserving Peer-to-Peer Market using Demand Response and Multiparty Computation" In CIGRE Symposium, pp. 1-11, 2022. BibTex LaTex

47 [Conf article] E. Manino, L. Cordeiro, D. Carvalho, Y. Dong, J. Rozanova, X. Song, M. Mustafa, A. Freitas, G. Brown, M. Luján and X. Huang, "EnnCore: End-to-End Conceptual Guarding of Neural Architectures" In Workshop on Artificial Intelligence Safety 2022, CEUR-WS, 8 pages, 2022. PDF BibTex LaTex

48 [Conf article] J. Bermudo Mera, A. Karmakar, T. Marc and A. Soleimanian, "Efficient Lattice-Based Inner-Product Functional Encryption" In Public Key Cryptography, 25 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2022, Lecture Notes in Computer Science LCNS 13178, Springer-Verlag, 31 pages, 2022. PDF BibTex LaTex

49 [Conf article] R. Thandi and M. Mustafa, "Privacy-Enhancing Settlements Protocol in Peer-to-Peer Energy Trading Markets" In IEEE PES Innovative Smart Grid Technologies Conference North America(ISGT NA 2022), IEEE, 5 pages, 2022. PDF BibTex LaTex

50

[Conf article] F. Zobiri, M. Gama, S. Petkova-Nikova and G. Deconinck, "A Privacy-Preserving Three-Step Demand Response Market Using Multi-Party Computation" In IEEE PES Innovative Smart Grid Technologies Conference North America(ISGT NA 2022), IEEE, 5 pages, 2022. BibTex LaTex

51 [Conf article] J. Cartlidge, M. Gama, A. Polychroniadou, N. Smart and Y. Talibi Alaoui, "Kicking-the-Bucket: Fast Privacy-Preserving Trading Using Buckets" In Financial Cryptography and Data Security - International Conference, FC 2022, Lecture Notes in Computer Science, Springer-Verlag, 26 pages, 2022. BibTex LaTex

52 [Conf article] S. Atapoor, N. Smart and Y. Talibi Alaoui, "Private Liquidity Matching using MPC" In Topics in Cryptology - CT-RSA 2022, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science LNSC,volume 13161, S. Galbraith (Ed.), Springer-Verlag, pp. 96-119, 2022. BibTex LaTex

53 [Conf article] S. Duttagupta, D. Singelée and B. Preneel, "T-HIBE: A Novel Key Establishment Solution for Decentralized, Multi-Tenant IoT Systems" In 2022 19 IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE Xplore, 9 pages, 2022. BibTex LaTex

54 [Conf article] R. Zhang, D. Zhang, Q. Wang, S. Wu, J. Xie and B. Preneel, "NC-Max: Breaking the Security-Performance Tradeoff in Nakamoto Consensus" In Network and Distributed System Security Symposium (NDSS 2022), Internet Society, 20 pages, 2022. BibTex LaTex

55 [Conf article] E. Pohle, A. Abidin and B. Preneel, "Poster: Fast Evaluation of S-boxes in MPC" In Network and Distributed System Security Symposium (NDSS 2022), Internet Society, 2 pages, 2022. BibTex LaTex

56 [Conf article] L. Le Jeune, A. Sateesan, M. Rabbani, T. Goedemé, J. Vliegen and N. Mentens, "SoK - Network Intrusion Detection on FPGA" In International Conference on Security, Privacy and Applied Cryptography Engineering, Lecture Notes in Computer Science 13162, L. Batina, M. Mondal and S. Picek (Eds.), Springer-Verlag, pp. 242-261, 2022. BibTex LaTex

57 [Conf article] W. Castryck and N. Vander Meeren, "Two remarks on the vectorization problem" In Progress in Cryptology - INDOCRYPT 2022, Lecture Notes in Computer Science, T. Isobe and S. Sarkar (Eds.), Springer-Verlag, pp. 658-678, 2022. BibTex LaTex

58 [Journal article] S. Khan, W. Lee, A. Karmakar, J. Bermudo Mera, A. Majeed and S. Oun Hwang, "Area–Time Efficient Implementation of NIST Lightweight Hash Functions Targeting IoT Applications", IEEE Internet of Things Journal 10(9), pp. 8083-8095, 2022. BibTex LaTex

59 [Journal article] S. Khan, W. Lee, J. Bermudo Mera, A. Karmakar, A. Majeed and S. Oun Hwang, "Area-time Efficient Implementation of NIST Lightweight Hash Functions Targeting IoT Applications", IACR Cryptology ePrint Archive 2022(1716), pp. 1-13, 2022. BibTex LaTex

60 [Journal article] O. Ayalon, E. Redmiles, S. Li and B. Preneel, "Not Only for Contact Tracing: Use of Belgium's Contact Tracing App among Young Adults", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 6,4(2022), pp. 1-26, 2022. BibTex LaTex

61 [Journal article] A. Aghabagherloo, M. Delavar, J. Mohajeri, M. Salmasizadeh and B. Preneel, "An efficient and physically secure privacy-preserving authentication scheme for Vehicular Ad-hoc NETworks (VANETs)", IEEE Access 10(<empty>), 14 pages, 2022. BibTex LaTex

62 [Journal article] F. Aljaafari, L. Cordeiro, M. Mustafa, F. Shmarov, R. Menezes and E. Manino, "Combining BMC and Fuzzing Techniques for Finding Software Vulnerabilities in Concurrent Programs", IEEE Access 10(<empty>), pp. 121365-121384, 2022. BibTex LaTex

63 [Journal article] G. Garofalo, T. Van hamme, D. Preuveneers, W. Joosen, A. Abidin and M. Mustafa, "PIVOT: PrIVate and effective cOntact Tracing", IEEE Internet of Things Journal 9(22), pp. 22466 - 22489, 2022. BibTex LaTex

64 [Journal article] T. Ashur, A. Kindi, W. Meier, A. Szepieniec and B. Threadbare, "Rescue-Prime Optimized", IACR Cryptology ePrint Archive 2022(1577), 10 pages, 2022. BibTex LaTex

65 [Journal article] E. Andreeva, B. Cogliati, V. Lallemand, M. Minier, A. Purnal and A. Roy, "Masked Iterate-Fork- BibTex

Iterate: A new Design Paradigm for Tweakable Expanding Pseudorandom Function", IACR Cryptology ePrint Archive 2022(1534), 47 pages, 2022. LaTex

66 [Journal article] C. Mujdei, A. Beckers, J. Bermudo Mera, A. Karmakar, L. Wouters and I. Verbauwhede, "Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication", ACM Transactions on Embedded Computing Systems 22(1), 26 pages, 2022. BibTex LaTex

67 [Journal article] W. Castryck, M. Houben, F. Vercauteren and B. Wesolowski, "On the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves", Research in Number Theory 8, pp. 1-18, 2022. BibTex LaTex

68 [Journal article] K. Kim, H. Lee, S. Lim, J. Park and I. Yie, "On Pairwise Gaussian Bases And LLl Algorithm For Three Dimensional Lattices", Journal of the Korean Mathematical Society 59(6), pp. 1047-1065, 2022. BibTex LaTex

69 [Journal article] L. Kraleva, M. Mahzoun, R. Posteuca, D. Toprakhisar, T. Ashur and I. Verbauwhede, "Cryptanalysis of Strong Physically Unclonable Functions", IEEE Open Journal of the Solid-State Circuits Society 3(/), pp. 32-40, 2022. BibTex LaTex

70 [Journal article] E. Argones Rúa, T. Van hamme, D. Preuveneers and W. Joosen, "Discriminative training of spiking neural networks organised in columns for stream-based biometric authentication", IET Biometrics 11(5), pp. 485-497, 2022. BibTex LaTex

71 [Journal article] S. Arash Azimi, A. Ranea, J. Mohajeri, M. Reza Aref, V. Rijmen and M. Salmasizadeh, "A Bit-Vector Differential Model for the Modular Addition by a Constant and its Applications to Differential and Impossible-Differential Cryptanalysis", Designs, Codes and Cryptography 90(8), pp. 1797-1855, 2022. BibTex LaTex

72 [Journal article] A. Ranea and V. Rijmen, "Characteristic Automated Search of Cryptographic Algorithms for Distinguishing Attacks (CASCADA)", IET Information Security 16(6), 25 pages, 2022. BibTex LaTex

73 [Journal article] J. He, K. Hu, B. Preneel and M. Wang, "Stretching Cube Attacks: Improved Methods to Recover Massive Superpolies", IACR Cryptology ePrint Archive 2022(1218), 75 pages, 2022. BibTex LaTex

74 [Journal article] D. Chaum, F. Zagórski, B. Zhang, R. Carback, J. Clark, C. Liu, M. Nejadgholi, B. Preneel, A. Sherman, M. Yaksetig and Z. Yin, "VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections", IACR Cryptology ePrint Archive 2022(1212), 4 pages, 2022. BibTex LaTex

75 [Journal article] C. Delpech de Saint Guilhem, E. Orsini, T. Tanguy and M. Verbauwhede, "Efficient Proof of RAM Programs from Any Public-Coin Zero-Knowledge System", Security and Communication Networks (2022), pp. 1-26, 2022. BibTex LaTex

76 [Journal article] I. Chillotti, E. Orsini, P. Scholl, N. Smart and B. Van Leeuwen, "Scooby: Improved Multi-Party Homomorphic Secret Sharing Based on FHE", Security and Communication Networks (2022), pp. 1-35, 2022. BibTex LaTex

77 [Journal article] S. Kundu, J. D'Anvers, M. Van Beirendonck, A. Karmakar and I. Verbauwhede, "Higher-order masked Saber", Security and Communication Networks 13409(2022), pp. 93-116, 2022. BibTex LaTex

78 [Journal article] C. Troncoso, R. Carlos Oliveira, M. Payer, B. Preneel, A. Pyrgelis, M. Salathé, T. Stadler, M. Veale, D. Bogdanov, E. Bugnion, S. Chatel, C. Cremers, S. Gürses, J. Hubaux, D. Jackson, J. Larus and W. Lueks, "Deploying decentralized, privacy-preserving proximity tracing", Communications of the ACM 65(9), 48–57 pages, 2022. BibTex LaTex

79 [Journal article] J. D'Anvers, "One-Hot Conversion: Towards Faster Table-based A2B Conversion", IACR Cryptology ePrint Archive 2022(1099), 23 pages, 2022. BibTex LaTex

80 [Journal article] A. Szepieniec and F. Vercauteren, "Lattice-Based Cryptography in Miden VM", IACR Cryptology ePrint Archive 2022(1041), pp. 1-24, 2022. BibTex LaTex

81 [Journal article] C. Bolchini and I. Verbauwhede, "DATE 2022: Aiming for an Online/ Onsite Format and Finally Moving to Online Only", IEEE Design & Test 39(4), pp. 90-93, 2022. BibTex LaTex

82 [Journal article] G. Rajendran, P. Ravi, J. D'Anvers, S. Bhasin and A. Chattopadhyay, "Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs - Parallel PC Oracle Attacks on Kyber KEM and Beyond", IACR Transactions on Cryptographic Hardware and Embedded Systems 2023(2), pp. 1-24, 2022. BibTex LaTex

83 [Journal article] A. Sateesan, J. Vliegen, J. Daemen and N. Mentens, "Hardware-oriented optimization of Bloom filter algorithms and architectures for ultra-high-speed lookups in network applications", Microprocessors and Microsystems (93), 13 pages, 2022. BibTex LaTex

84 [Journal article] H. Li, N. Mentens and S. Picek, "Maximizing the Potential of Custom RISC-V Vector Extensions for Speeding up SHA-3 Hash Functions", IACR Cryptology ePrint Archive 2022(868), pp. 1-24, 2022. BibTex LaTex

85 [Journal article] M. Gama, Y. Talibi Alaoui, J. Cartlidge and N. Smart, "All for one and one for all: Fully decentralised privacy-preserving dark pool trading using multi-party computation", IACR Cryptology ePrint Archive 2022(923), pp. 1-35, 2022. BibTex LaTex

86 [Journal article] I. Ben Guirat and C. Diaz, "Mixnet optimization methods", Proceedings on Privacy Enhancing Technologies 2022(3), 22 pages, 2022. BibTex LaTex

87 [Journal article] D. Das, E. Vivek Mangipudi and A. Kate, "OrgAn: Organizational Anonymity with Low Latency", Proceedings on Privacy Enhancing Technologies 2022(3), 24 pages, 2022. BibTex LaTex

88 [Journal article] A. Madhusudan, S. Sedaghat, P. Jovanovic and B. Preneel, "Nirvana: Instant and Anonymous Payment-Guarantees", IACR Cryptology ePrint Archive 2022(872), pp. 1-46, 2022. BibTex LaTex

89 [Journal article] I. Chillotti, E. Orsini, P. Scholl, N. Smart and B. Van Leeuwen, "Scooby: Improved Multi-Party Homomorphic Secret Sharing Based on FHE", IACR Cryptology ePrint Archive 2022(862), 35 pages, 2022. BibTex LaTex

90 [Journal article] T. Ashur, L. Kraleva, M. Mahzoun and R. Posteuca, "Differential Cryptanalysis of K-Cipher", IEEE Software, Special Issue on Software Protection 27(1), 11 pages, 2022. BibTex LaTex

91 [Journal article] C. Diaz, H. Halpin and A. Kiayias, "Reward Sharing for Mixnets", Cryptoeconomic Systems 2(1), pp. 1-88, 2022. BibTex LaTex

92 [Journal article] N. Bardeh and V. Rijmen, "New Key Recovery Attack on Reduced-Round AES", IACR Transactions on Symmetric Cryptology 2022(2), pp. 43-62, 2022. BibTex LaTex

93 [Journal article] T. Beyne and Y. Liu, "Truncated Differential Attacks on Contracting Feistel Ciphers", IACR Transactions on Symmetric Cryptology 2022(2), 20 pages, 2022. BibTex LaTex

94 [Journal article] N. Bardeh and V. Rijmen, "New Key-Recovery Attack on Reduced-Round AES", IACR Transactions on Symmetric Cryptology 2022(2), 43–62 pages, 2022. BibTex LaTex

95 [Journal article] W. Lee, H. Seo, S. Oun Hwang, A. Karmakar, J. Bermudo Mera and R. Achar, "DPCrypto: Acceleration of Post-quantum Cryptographic Algorithms using Dot-Product Instruction on GPUs", IEEE Transactions on Circuits and Systems I: Regular Papers 69(9), pp. 3591-3604, 2022. BibTex LaTex

96 [Journal article] T. Ashur, C. Li, Y. Liu, J. Lu and B. Sun, "Improved rotational-XOR cryptanalysis of Simon-like block ciphers", IET Information Security 16(4), pp. 282-300, 2022. BibTex LaTex

97 [Journal article] S. Aghili, S. Sedaghat, D. Singelée and M. Gupta, "MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme", Future Generation Computer Systems 131(C), pp. 75-90, 2022. BibTex LaTex

98 [Journal article] V. Rijmen, "De technische aspecten van privacy", Karakter. Tijdschrift van Wetenschap. (78), pp. 19-21, 2022. BibTex LaTex

99 [Journal article] K. Baghery, A. González, Z. Pindado and C. Ràfols, "Signatures of knowledge for Boolean circuits under standard assumptions", Theoretical Computer Science 916(1), pp. 86-110, 2022. BibTex LaTex

100 [Journal article] Y. Chen, A. Dutta and M. Nandi, "Multi-User BBB Security of Public Permutations Based MAC.", BibTex

Cryptography and Communications 14(<empty>), 43 pages, 2022. LaTex

101 [Journal article] I. Iliashenko, M. Izabachene, A. Mertens and H. Lima Pereira, "Homomorphically counting elements with the same property", Proceedings on Privacy Enhancing Technologies 2022(4), pp. 670-683, 2022. BibTex LaTex

102 [Journal article] K. Han, W. Lee, A. Karmakar, J. Bermudo Mera and S. Oun Hwang, "cuFE: High Performance Privacy Preserving Support Vector Machine with Inner-Product Functional Encryption", IACR Cryptology ePrint Archive 2022(482), pp. 1-27, 2022. BibTex LaTex

103 [Journal article] T. Capper, C. Francis, T. Mbavarira, J. Manuel Espana, L. Kiesling, A. Gorbatcheva, M. Mustafa, M. Bahloul, J. Schwidtal, R. Chitchyan, M. Andoni, V. Robu, M. Montakhabi and I. Scott, "Peer-to-Peer, Community Self-Consumption, and Transactive Energy: A Systematic Literature Review of Local Energy Market Models", Renewable and Sustainable Energy Reviews 162(112403), 45 pages, 2022. BibTex LaTex

104 [Journal article] C. Hazay, E. Orsini, P. Scholl and E. Soria-Vazquez, "TinyKeys: A New Approach to Efficient Multi-Party Computation", Journal of Cryptology 35(2), pp. 1-66, 2022. BibTex LaTex

105 [Journal article] A. Lemmens, "Convexity Of Distinct Sum Sets", Studia Scientiarum Mathematicarum Hungarica 59(1), pp. 17-29, 2022. BibTex LaTex

106 [Journal article] J. Kelsey and S. Lucks, "Coalition and Threshold Hash-Based Signatures", IACR Cryptology ePrint Archive 2022(241), pp. 1-40, 2022. BibTex LaTex

107 [Journal article] L. Zhang, F. Qiu, F. Hao and H. Kan, "1-Round Distributed Key Generation With Efficient Reconstruction Using Decentralized CP-ABE", IEEE Transactions on Information Forensics and Security (17), pp. 894-907, 2022. BibTex LaTex

108 [Journal article] J. D'Anvers, D. Heinz, P. Pessl, M. Van Beirendonck and I. Verbauwhede, "Higher-Order Masked Ciphertext Comparison for Lattice-Based Cryptography", IACR Transactions on Cryptographic Hardware and Embedded Systems 2022(2), 24 pages, 2022. BibTex LaTex

109 [Journal article] T. Ashur, M. Khan and K. Nyberg, " Structural and Statistical Analysis of Multidimensional Linear Approximations of Random Functions and Permutations", IEEE Transactions on Information Theory 68(2), pp. 1296-1315 , 2022. BibTex LaTex

110 [Journal article] I. Symeonidis, D. Rotaru, M. Mustafa, B. Mennink, B. Preneel and P. Papadimitratos, "HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System", IEEE Internet of Things Journal 9(1), pp. 129-151, 2022. BibTex LaTex

111 [Journal article] D. Rotaru, N. Smart, T. Tanguy, F. Vercauteren and T. Wood, "Actively Secure Setup for SPDZ", Journal of Cryptology 35(1), pp. 1-32, 2022. BibTex LaTex

112 [Journal article] L. Oldenburg, G. Acar and C. Diaz, "From Onion Not Found to Guard Discovery", Proceedings on Privacy Enhancing Technologies 2022(1), 22 pages, 2022. BibTex LaTex

113 [Journal article] T. Beyne, S. Dhooghe, A. Moradi and A. Rezaei Shahmirzadi, "Cryptanalysis of Efficient Masked Ciphers: Applications to Low Latency", IACR Transactions on Cryptographic Hardware and Embedded Systems 1(2022), 44 pages, 2022. BibTex LaTex

114 [Journal article] W. Castryck and F. Vercauteren, "Breaking the decisional Diffie-Hellman problem for class group actions using genus theory -- extended version", Journal of Cryptology 35(4), 30 pages, 2022. BibTex LaTex

115 [Book chapter] C. Diaz, "Mix networks" In Encyclopedia of Cryptography, Security and Privacy, S. Jajodia, P. Samarati and M. Yung (Eds.), Springer, Berlin, Heidelberg, 5 pages, 2022. BibTex LaTex

116 [Thesis] R. Galvez, "New Privacy Engineering Methods for Artificial Intelligence", Phd thesis, KU Leuven, C. Diaz, 232 pages, 2022. BibTex LaTex

117

[Thesis] J. Bermudo Mera, "Implementation Aspects of Lattice-based Cryptography", Phd thesis, KU Leuven, I. Verbauwhede, 160 pages, 2022. BibTex LaTex

118 [Thesis] L. Kraleva, "Cryptanalysis Techniques for Lightweight Symmetric-Key Primitives", Phd thesis, KU Leuven, V. Rijmen, 200 pages, 2022. BibTex LaTex

119 [Thesis] F. Turan, "FPGA Accelerators for Cryptography and Their Protection in the Cloud", Phd thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 186 pages, 2022. BibTex LaTex

120 [Thesis] M. Kumar, R. Geelen, J. Kang and J. Park, "Secure Data Classification with Homomorphic Encryption", Master thesis, Indian Statistical Institute, F. Vercauteren and B. Roy, 45 pages, 2022. BibTex LaTex

121 [Thesis] K. Orbie, H. Becker, J. Bermudo Mera and A. Karmakar, "Optimizing Dilithium Using the Helium Vector Extension", Master thesis, KU Leuven, I. Verbauwhede, 77 pages, 2022. BibTex LaTex

122 [Thesis] I. Thakur, A. Bhati and E. Andreeva, "A Survey of Password Hashing and Argon2", Master thesis, Indian Statistical Institute (ISI), Calcutta, B. Preneel and B. Roy, 37 pages, 2022. BibTex LaTex

123 [Thesis] D. Cozzo, "Advancing the Mechanisms and Use of Practical Secure Multiparty Computation", Phd thesis, KU Leuven, N. Smart, 296 pages, 2022. BibTex LaTex

124 [Thesis] W. Van Gerwen, S. Duttagupta and D. Singelée, "Blockchain based data management system in an IoT environment", Master thesis, KU Leuven, B. Preneel, 67 pages, 2022. BibTex LaTex

125 [Thesis] W. Legiest, "Quantisation for neural network inference under homomorphic encryption", Master thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 90 pages, 2022. BibTex LaTex

126 [Thesis] T. Decru, "Aspects of Elliptic and Hyperelliptic Curve Isogeny-based Cryptography", Phd thesis, KU Leuven, W. Castryck and F. Vercauteren, pp. 1-230, 2022. BibTex LaTex

127 [Thesis] M. Verbauwhede, "Tools for Integral Cryptanalysis", Master thesis, KU Leuven, B. Preneel and V. Rijmen, 75 pages, 2022. BibTex LaTex

128 [Thesis] S. Muys, "Emotion-based brainwave authentication using a Fuzzy C-means derived symbolic representation of brain language", Master thesis, KU Leuven, B. Preneel, 96 pages, 2022. BibTex LaTex

129 [Thesis] E. Wiels, "Security of Cuckoo Filters in Adversarial Environments", Master thesis, KU Leuven, B. Preneel, 61 pages, 2022. BibTex LaTex

130 [Thesis] J. De Cock, R. Galvez, A. Madhusudan and A. Aghabagherloo, "Bitcoin price prediction using Twitter sentiment and deep learning", Master thesis, KU Leuven, B. Preneel, 50 pages, 2022. BibTex LaTex

131 [Thesis] X. Zhong, "Security Analysis of HyperLogLog", Master thesis, KU Leuven, B. Preneel, 46 pages, 2022. BibTex LaTex

132 [Thesis] W. Van Gerwen, "Blockchain based data management system in an IoT environment", Master thesis, KU Leuven, B. Preneel, 67 pages, 2022. BibTex LaTex

133 [Thesis] L. De Greve, "Brainwave authentication: a fuzzy approach ", Master thesis, KU Leuven, B. Preneel, 74 pages, 2022. BibTex LaTex

134 [Thesis] X. Zou, "Wireless transmitter fingerprinting", Master thesis, KU Leuven, B. Preneel, 62 pages, 2022. BibTex LaTex

135 [Thesis] M. Jacqmotte, "The Rise of the Machines: On the Security of Cellular IoT with Intelligent Fuzzing", Master thesis, KU Leuven, B. Preneel and M. Dieudonné, 134 pages, 2022. BibTex LaTex

136 [Thesis] K. Bringmans, "Microarchitecture-Aware Generation of Memory Access Patterns for Advanced Cache Attacks", Master thesis, KU Leuven, I. Verbauwhede, 117 pages, 2022. BibTex LaTex

137 [Thesis] Z. Lu, "Analysis of the Legendre pseudorandom function, the Playful Cupid attack on PorcRoast", Master thesis, KU Leuven, F. Vercauteren, 51 pages, 2022. PDF BibTex LaTex

138 [Thesis] G. De Ranter, "An Analysis of Modulus and Reduction for the HW Implementations of unrolled-NTT", Master thesis, KU Leuven, I. Verbauwhede, 70 pages, 2022. PDF BibTex LaTex

139 [Thesis] Q. Norga, "Efficient and Secure Conversions between High-Order Arithmetic and Boolean Masking in Hardware for Lattice-Based Crypto", Master thesis, KU Leuven, I. Verbauwhede, 86 pages, 2022. PDF BibTex LaTex

140 [Thesis] L. Nouwen, "Attacking a secure smart card using power analysis", Master thesis, KU Leuven, I. Verbauwhede, 95 pages, 2022. PDF BibTex LaTex

141 [Thesis] J. De Meulemeester, "Let's Get Physical: Exploiting Transient Execution Through Electromagnetic Covert Channels", Master thesis, KU Leuven, I. Verbauwhede, 85 pages, 2022. PDF BibTex LaTex

142 [Thesis] T. Jacqmotte, "Satellite-based location authentication algorithms with Galileo OSNMA", Master thesis, KU Leuven, V. Rijmen and I. Fernandez-Hernandez, 88 pages, 2022. PDF BibTex LaTex

143 [Thesis] R. Nivelle, "Securing Dark Markets with Multi-Party Computation", Master thesis, KU Leuven, N. Smart, 53 pages, 2022. PDF BibTex LaTex

144 [Thesis] T. Narayana, "Fully-homomorphic Encryption in Machine Learning Applications", Master thesis, KU Leuven, F. Vercauteren, 50 pages, 2022. PDF BibTex LaTex

145 [Thesis] H. Yan, "Brain biometry: triggering emotions", Master thesis, KU Leuven, B. Preneel, 49 pages, 2022. PDF BibTex LaTex

146 [Thesis] Y. Chen, "Pseudorandom Permutations and Functions for Lightweight Applications", Phd thesis, KU Leuven, B. Preneel, pp. 1-288, 2022. PDF BibTex LaTex

147 [Proceeding] "International Conference on Security, Privacy and Applied Cryptography Engineering", Lecture Notes in Computer Science 13783, L. Batina, M. Mondal and S. Picek (Eds.), Springer-Verlag, 2022. BibTex LaTex

148 [Proceeding] "Design, Automation and Test in Europe", C. Bolchini, I. Vatajelu and I. Verbauwhede (Eds.), IEEE, 2022. BibTex LaTex

149 [Report] A. Ghosh, J. Bermudo Mera, A. Karmakar, D. Das, S. Ghosh, I. Verbauwhede and S. Sen, "A 334uW 0.158mm2 Saber Learning with Rounding based Post-Quantum Crypto Accelerator", arXiv report, pp. 1-4, 2022. PDF BibTex LaTex

150 [Talk] S. Kundu, "Integration of masking techniques in post-quantum key-encapsulation mechanism Saber to prevent side-channel attacks", 16th International Conference MSAST 2022, Online, On, 2022. ▶ BibTex LaTex

151 [Talk] I. Verbauwhede, "Hardware: an essential partner to cryptography", International Conference on Security, Privacy and Applied Cryptographic Engineering 2022 (SPACE 2022), IN, 2022. BibTex LaTex

152 [Talk] B. Preneel, "Data privacy in a post-quantum computing world", DPO Annual Conference, Online, 2022. BibTex LaTex

153 [Talk] C. Diaz, "Protection of communications metadata", EU Commission workshop on Digital Autonomy and classified information, Brussels, BE, 2022. BibTex LaTex

154 [Talk] B. Preneel, "Keynote Momentum!", Momentum! (CyberSec4Europe), Brussels, BE, 2022. BibTex LaTex

155 [Talk] V. Tulceanu, "Security and the mind: open research directions", 10th International Workshop on Soft Computing Applications 21-23 NOV-2022 Arad, Romania (SOFA 2022), Arad, RO, 2022. BibTex LaTex

156 [Talk] B. Preneel, "Keynote", Zero Trust, de nieuwe norm in cybersecurityland uitgelegd, Kemzeke, BE, BibTex

2022. LaTex

157 [Talk] B. Preneel, "Tussen veiligheid en privacy. Hacking en internetcriminaliteit", Actueel Denken en Leven, Mechelen, BE, 2022. BibTex LaTex

158 [Talk] B. Preneel, "Cyber Security Seminar and Workshops presentation", CriM -- Cyber Security Seminar and Workshops, Oulu, FI, 2022. BibTex LaTex

159 [Talk] I. Verbauwhede, "Hardware acceleration for Fully Homomorphic Encryption", COED Industry Day, Leuven, BE, 2022. BibTex LaTex

160 [Talk] B. Preneel, "Tech meets Real Estate: Non-Fungible Tokens", Postuniversitair Centrum - Tech meets Real Estate, Virtual, 2022. BibTex LaTex

161 [Talk] V. Rijmen, "Is the Fight for Online Privacy a Lost Battle?", Hidden Heroes – A tribute to people who shaped technology, Online, 2022. BibTex LaTex

162 [Talk] S. Kundu, "Side-channel attacks secure post-quantum cryptography", SRC TECHCON 2022, Austin, US, 2022. BibTex LaTex

163 [Talk] B. Preneel, "Current Challenges in the Field of Cybersecurity – State of the Discipline, Challenges", European Conference on Security Research in Cyberspace, Brno, CZ, 2022. BibTex LaTex

164 [Talk] I. Verbauwhede, "Circuits for Security and Secure Circuits", SSCS Webinar, Online, 2022. BibTex LaTex

165 [Talk] V. Rijmen, "Extending the zero-difference attack on AES by using related differences", The Ernst Selmer International Workshop, Geiranger Norway, 2022. BibTex LaTex

166 [Talk] L. Wouters, "Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal", Black Hat USA 2022, Las Vegas, US, 2022. ▶ BibTex LaTex

167 [Talk] B. Preneel, "Three decades of cybersecurity policy: lessons learned ", gdr-secu-jn2022 : Journées Nationales 2022 du GDR Sécurité Informatique, Puteaux, FR, 2022. BibTex LaTex

168 [Talk] B. Preneel, "Proximing and presence tracing in a pandemic: lessons learned", European Interdisciplinary Cybersecurity Conference, Barcelona, ES, 2022. BibTex LaTex

169 [Talk] B. Preneel, "Keynote at International Cybersecurity Challenge", International Cybersecurity Challenge Award Ceremony, Athens, GR, 2022. BibTex LaTex

170 [Talk] B. Preneel, "Cryptocurrencies and blockchains", SecAppDev 2022, Leuven, BE, 2022. BibTex LaTex

171 [Talk] B. Preneel, "Privacy-Friendly Proximity and Presence Tracing", SecAppDev 2022, Leuven, BE, 2022. BibTex LaTex

172 [Talk] B. Preneel, "New developments in cryptography land", SecAppDev 2022, Leuven, BE, 2022. BibTex LaTex

173 [Talk] I. Verbauwhede, "The search for randomness: essential for security", Summer school on real-world crypto and privacy, Sibenik, HR, 2022. BibTex LaTex

174 [Talk] V. Tulceanu, "Brainprints for access control and objective mental monitoring in the military: brainware, AI and security.", Theories of Change in Digital Wellbeing. Evidence based practices across the disciplines, Arad, RO, 2022. BibTex LaTex

175 [Talk] C. Delpech de Saint Guilhem, "Efficient Proof of RAM Programs from Any Public-Coin Zero-Knowledge System", TPMPC 2022, Aarhus, DK, 2022. ▶ BibTex LaTex

176 [Talk] C. Diaz, "Reward Sharing for Mixnets", Invited seminar for the Security Group at Cambridge University, Online, 2022. ▶ BibTex LaTex

177 [Talk] M. Van Beirendonck and R. Geelen, "BASALISC: Flexible Asynchronous Hardware Accelerator for Fully Homomorphic Encryption", 1st Annual FHE.org Conference on Fully Homomorphic Encryption, Trondheim, NO, 2022. BibTex LaTex

178 [Talk] B. Preneel, "Privacy Against Power", CPDP 2022, Brussels, BE, 2022. BibTex LaTex

179 [Talk] B. Preneel, "Cybersecurity and AI: A match made in heaven?", CyberSec Europe, Brussels, BE, 2022. BibTex LaTex

180 [Talk] A. Bhati, "Forkcipher: A Cryptographic Design for Modern Applications", Invited Talk, S&P group, TU Wien, Vienna, AT, 2022. BibTex LaTex

181 [Talk] I. Verbauwhede, "Hardware roots of trust", A29- Hardware and System Security Course, Putten, NL, 2022. BibTex LaTex

182 [Talk] N. Smart, "How to Best Address Blockchain Privacy Concerns? (panel)", Privacy-Enhancing Technology Summit Europe 2022, Zurich, CH, 2022. BibTex LaTex

183 [Talk] M. Grujic and N. Massari, "Monolithic Quantum Random Number Generator", SPIE Photonics Europe, Strasbourg, FR, 2022. BibTex LaTex

184 [Talk] I. Verbauwhede, "Hardware Security: Physical Design versus Side-Channel and Fault Attacks", ISPD '22, Virtual, 2022. BibTex LaTex

185 [Talk] B. Preneel, "Leadership presentation: Privacy and Security Hanging in the Balance", 600 Minutes Cyber Security, Tremelo, BE, 2022. BibTex LaTex

186 [Talk] B. Preneel, "Privacy en veiligheid in de digitale wereld: om vingerafdrukken bij af te vijlen!", House of Flanders Debatlunch, Sint-Katelijne-Waver, BE, 2022. BibTex LaTex

187 [Talk] B. Preneel, "AI Safety & Cybersecurity Discussion panel", Economic Regulation and Impact: is Belgium fit for the AI age?, Online, 2022. BibTex LaTex

188 [Talk] B. Preneel, "Talk on AI & Cybersecurity", AI & Cybersecurity - digital wallonia 4. cyber, Online, 2022. BibTex LaTex

189 [Rump] C. Bex, F. Turan, M. Van Beirendonck and I. Verbauwhede, "Mining CryptoNight-Haven on the Varium C1100 Blockchain Accelerator Card" , International Conference on Field Programmable Logic and Applications (FPL 2022), 2 pages, 2022.

2021

1 [Conf article] H. Chen, I. Iliashenko and K. Laine, "When HEAAN Meets FV: a New Somewhat Homomorphic Encryption with Reduced Memory Overhead" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2021, Lecture Notes in Computer Science, Springer-Verlag, 23 pages, 2021. BibTex LaTex

2 [Conf article] K. Cong, K. Eldefrawy and N. Smart, "Optimizing Registration Based Encryption" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2021, Lecture Notes in Computer Science, Springer-Verlag, 129–157 pages, 2021. BibTex LaTex

3 [Conf article] K. Baghery, D. Cozzo and R. Pedersen, "An Isogeny-Based ID Protocol Using Structured Public Keys" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2021, Lecture Notes in Computer Science, Springer-Verlag, pp. 179-197, 2021. BibTex LaTex

4 [Conf article] R. Pedersen, "DeCSIDH: Delegating isogeny computations in the CSIDH setting" In Progress in Cryptology - INDOCRYPT 2021, Lecture Notes in Computer Science 13143, A. Adhikari, R. Küsters and B. Preneel (Eds.), Springer-Verlag, 29 pages, 2021. BibTex LaTex

5 [Conf article] S. Dhooghe, "Analyzing Masked Ciphers Against Transition and Coupling Effects" In Progress in Cryptology - INDOCRYPT 2021, Lecture Notes in Computer Science 13143, A. Adhikari, R. Küsters and B. Preneel (Eds.), Springer-Verlag, 23 pages, 2021. BibTex LaTex

6 [Conf article] M. Bowman, D. Das, A. Mandal and H. Montgomery, "On Elapsed Time Consensus Protocols" In Progress in Cryptology - INDOCRYPT 2021, Lecture Notes in Computer Science 13143, A. Adhikari, R. Küsters and B. Preneel (Eds.), Springer-Verlag, pp. 559-583, 2021. BibTex LaTex

7 [Conf article] L. De Feo, C. Delpech de Saint Guilhem, T. Fouotsa, P. Kutas, A. Leroux, C. Petit, J. Silva and B. Wesolowski, "SÉTA: Supersingular Encryption from Torsion Attacks" In Advances in Cryptology - ASIACRYPT 2021, Lecture Notes in Computer Science, Springer-Verlag, 33 pages, 2021. BibTex LaTex

8 [Conf article] K. Cong, D. Cozzo, V. Maram and N. Smart, "Gladius: LWR based efficient hybrid public key encryption with distributed decryption" In Advances in Cryptology - ASIACRYPT 2021, Lecture Notes in Computer Science, Springer-Verlag, 125–155 pages, 2021. BibTex LaTex

9 [Conf article] Y. Chen, B. Mennink and B. Preneel, "Categorization of Faulty Nonce Misuse Resistant Message Authentication" In Advances in Cryptology - ASIACRYPT 2021, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2021. BibTex LaTex

10 [Conf article] Y. Chen and S. Tessaro, "Better Security-Effciency Trade-Offs in Permutation-Based Two-Party Computation" In Advances in Cryptology - ASIACRYPT 2021, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2021. BibTex LaTex

11 [Conf article] T. Beyne, "A Geometric Approach to Linear Cryptanalysis" In Advances in Cryptology - ASIACRYPT 2021, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2021. BibTex LaTex

12 [Conf article] R. Pedersen and O. Uzunkol, "Delegating Supersingular Isogenies over $mathbb{F}_{p^2}$ with Cryptographic Applications" In Information Security and Cryptology - ICISC 2021: 24 International Conference, Lecture Notes in Computer Science, J. Park and S. Seo (Eds.), Springer-Verlag, pp. 105-128, 2021. BibTex LaTex

13 [Conf article] M. Zhang, E. Marín Fàbregas, D. Oswald and D. Singelée, "FuzzyKey: Comparing Fuzzy Cryptographic Primitives on Resource-Constrained Devices" In Smart Card Research and Advanced Applications - CARDIS 2021, Lecture Notes in Computer Science, Springer-Verlag, 20 pages, 2021. BibTex LaTex

14 [Conf article] M. Rabbani, A. Braeken, N. Dragoni, E. Dushku, J. Vliegen and N. Mentens, "RESERVE: Remote Attestation of Intermittent IoT Devices" In Proceedings of the n-th ACM Conference on Embedded Networked Sensor Systems 1, Association for Computing Machinery, 578–580 pages, 2021. BibTex LaTex

15 [Conf article] C. Delpech de Saint Guilhem, E. Orsini and T. Tanguy, "Limbo: Efficient Zero-knowledge MPCitH-based Arguments" In ACM Conference on Computer and Communications Security - CCS 2021, ACM, 15 pages, 2021. BibTex LaTex

16 [Conf article] C. Delpech de Saint Guilhem, E. Makri, D. Rotaru and T. Tanguy, "The Return of Eratosthenes: Secure Generation of RSA Moduli using Distributed Sieving" In ACM Conference on Computer and Communications Security - CCS 2021, ACM, 16 pages, 2021. BibTex LaTex

17 [Conf article] I. Ben Guirat, D. Gosain and C. Diaz, "MiXiM: Mixnet design decisions and empirical evaluation" In Proceedings of the 2021 annual ACM workshop on Privacy in the electronic society, Association for Computing Machinery (ACM), ACM, 5 pages, 2021. BibTex LaTex

18 [Conf article] A. Purnal, F. Turan and I. Verbauwhede, "Prime+Scope: Overcoming the Observer Effect for High-Precision Cache Contention Attacks" In ACM Conference on Computer and Communications Security - CCS 2021, ACM, 15 pages, 2021. BibTex LaTex

19 [Conf article] I. Iliashenko, C. Nègre and V. Zucca, "Integer Functions Suitable for Homomorphic Encryption over Finite Fields" In Workshop on Encrypted Computing and Applied Homomorphic Cryptography 2021, Association for Computing Machinery (ACM), M. Brenner, R. Player and K. Rohloff (Eds.), 10 pages, 2021. BibTex LaTex

20 [Conf article] K. Baghery and S. Sedaghat, "Tiramisu: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model" In Cryptology and Network Security, Lecture Notes in Computer Science 13099, M. Conti and M. Stevens (Eds.), Springer-Verlag, 531–551 pages, 2021. PDF ▶ BibTex LaTex

21 [Conf article] S. Sedaghat and B. Preneel, "Cross-Domain Attribute-Based Access Control Encryption" In Cryptology and Network Security, Lecture Notes in Computer Science 13099, M. Conti and M. Stevens (Eds.), Springer-Verlag, pp. 3-23, 2021. PDF ▶ BibTex LaTex

22 [Conf article] Y. Lai, S. Galbraith and C. Delpech de Saint Guilhem, "Compact, Efficient and UC-Secure Isogeny-Based Oblivious Transfer" In Advances in Cryptology - EUROCRYPT 2021, Lecture Notes in Computer Science 12698, A. Canteaut and F. Standaert (Eds.), Springer-Verlag, 25 pages, 2021. PDF BibTex LaTex

23 [Conf article] W. Beullens, "Improved cryptanalysis of UOV and Rainbow" In Advances in Cryptology - EUROCRYPT 2021, Lecture Notes in Computer Science 12698, A. Canteaut and F. Standaert (Eds.), Springer-Verlag, pp. 348-373, 2021. PDF ▶ BibTex LaTex

24 [Conf article] A. Ben-Efraim, K. Cong, E. Omri, E. Orsini, N. Smart and E. Soria-Vazquez, "Large Scale, Actively Secure Computation from LPN and Free-XOR Garbled Circuits" In Advances in Cryptology - EUROCRYPT 2021, Lecture Notes in Computer Science 12698, A. Canteaut and F. Standaert (Eds.), Springer-Verlag, pp. 33-63, 2021. PDF BibTex LaTex

25 [Conf article] E. Makri and T. Wood, "Full-Threshold Actively-Secure Multiparty Arithmetic Circuit Garbling" In Progress in Cryptology - LATINCRYPT 2021, Lecture Notes in Computer Science LNCS 12912, P. Longa and C. Ràfols (Eds.), Springer-Verlag, 31 pages, 2021. PDF BibTex LaTex

26 [Conf article] D. Archer, S. Atapoor and N. Smart, "The Cost of IEEE Arithmetic in Secure Computation" In Progress in Cryptology - LATINCRYPT 2021, Lecture Notes in Computer Science LNCS 12912, P. Longa and C. Ràfols (Eds.), Springer-Verlag, pp. 431-452, 2021. PDF ▶ BibTex LaTex

27 [Conf article] M. Montakhabi, S. Van der Graaf, P. Ballon and M. Mustafa, "Prosumers' Business Models in Future Electricity Markets; Peer-to-Peer, Community Self-Consumption, and Transactive Energy Models" In Business Model Conference 2021, Open Journal Systems, 7 pages, 2021. BibTex LaTex

28 [Conf article] T. Yoshizawa, D. Singelée and B. Preneel, "A New Privacy Enhancing Beacon Scheme in V2X Communication" In Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, Lecture Notes in Computer Science, Springer-Verlag, 12 pages, 2021. ▶ BibTex LaTex

29 [Conf article] T. Beyne, Y. Chen, C. Dobraunig and B. Mennink, "Multi-User Security of the Elephant v2 Authenticated Encryption Mode" In Selected Areas in Cryptography, 28 Annual International Workshop, SAC 2021, Lecture Notes in Computer Science, R. AlTawy and A. Hülsing (Eds.), Springer-Verlag, 24 pages, 2021. PDF BibTex LaTex

30 [Conf article] T. Beyne, S. Dhooghe, A. Ranea and D. Sijacic, "A Low-Randomness Second-Order Masked AES" In Selected Areas in Cryptography, 28 Annual International Workshop, SAC 2021, Lecture Notes in Computer Science, R. AlTawy and A. Hülsing (Eds.), Springer-Verlag, 27 pages, 2021. PDF BibTex LaTex

31 [Conf article] R. Jadoul, N. Smart and B. Van Leeuwen, "MPC for Q_2 Access Structures over Rings and Fields" In Selected Areas in Cryptography, 28 Annual International Workshop, SAC 2021, Lecture Notes in Computer Science, R. AlTawy and A. Hülsing (Eds.), Springer-Verlag, 21 pages, 2021. PDF ▶ BibTex LaTex

32 [Conf article] S. Osuka, D. Fujimoto, A. Beckers, B. Gierlichs, Y. Hayashi and I. Verbauwhede, "A Study on Output Bit Tampering of True Random Number Generators Using Time-Varying EM Waves" In APEMC 2025, IEEE, 4 pages, 2021. PDF BibTex LaTex

33 [Conf article] A. Senol, G. Acar and M. Humbert, "Think Before You Type: A Study of Email Exfiltration Before Form Submission" In SecWeb Workshop, 13 pages, 2021. PDF BibTex LaTex

34 [Conf article] S. Scherrer, C. Wu, Y. Chiang, B. Rothenberger, D. Asoni, A. Sateesan, J. Vliegen, N. Mentens, H. Hsiao and A. Perrig, "Low-Rate Overuse Flow Tracer (LOFT): An Efficient and Scalable Algorithm for Detecting Overuse Flows" In International Symposium on Reliable Distributed Systems, IEEE, 12 pages, 2021. PDF BibTex LaTex

35 [Conf article] T. Claesen, A. Sateesan, J. Vliegen and N. Mentens, "Novel Non-cryptographic Hash Functions for Networking and Security Applications on FPGA" In Euromicro conference on Digital System Design (DSD), IEEE, 8 pages, 2021. BibTex LaTex

36 [Conf article] T. Beyne, "Linear Cryptanalysis of FF3-1 and FEA" In Advances in Cryptology - CRYPTO 2021, Lecture Notes in Computer Science, Springer-Verlag, pp. 41-69, 2021. BibTex LaTex

37 [Conf article] L. Oldenburg and F. Tschorsch, "Strong Anonymity is Not Enough: Introducing Fault Tolerance to Planet-Scale Anonymous Communication Systems" In 2021 International Conference on Availability, Reliability and Security (ARES 2021), ACM, 6 pages, 2021. BibTex LaTex

38 [Conf article] O. Mirzamohammadi, A. Aghabagherloo, J. Mohajeri, M. Salmasizadeh and M. Reza Aref, "Analysis and Improvement of the SPACF Scheme in Vehicular Ad-hoc Networks" In 18th International ISC(Iranian Society of Cryptology) Conference on Information Security and Cryptology , IEEE, 7 pages, 2021. BibTex LaTex

39 [Conf article] W. Beullens, L. Disson, R. Pedersen and F. Vercauteren, "CSI-RAShi: Distributed key generation for CSIDH" In Post-Quantum Cryptography, Lecture Notes in Computer Science 12841, J. Hee Cheon and J. Tillich (Eds.), Springer-Verlag, pp. 257-276, 2021. BibTex LaTex

40 [Conf article] W. Castryck, A. Dooms, C. Emerencia and A. Lemmens, "A fusion algorithm for solving the hidden shift problem in finite abelian groups" In Post-Quantum Cryptography, Lecture Notes in Computer Science 12841, J. Hee Cheon and J. Tillich (Eds.), Springer-Verlag, pp. 133-153, 2021. BibTex LaTex

41 [Conf article] M. Montakhabi, S. Van der Graaf, A. Madhusudan, R. Sarenche and M. Mustafa, "Fostering Energy Transition in Smart Cities: DLTs for Peer-to-Peer Electricity Trading" In International Workshop on Smart Circular Economy, IEEE, 7 pages, 2021. BibTex LaTex

42 [Conf article] K. Miteloudi, L. Batina, J. Daemen and N. Mentens, "ROCKY: Rotation Countermeasure for the Protection of Keys and Other Sensitive Data" In International Conference on Systems, Architectures, MOdeling and Simulation (IC-SAMOS 2021), IEEE, 12 pages, 2021. BibTex LaTex

43 [Conf article] M. Mansouri, W. Ben Jaballah, M. Onen, M. Rabbani and M. Conti, "FADIA: FAirness-Driven collaboratIve remote Attestation" In Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2021), ACM, 12 pages, 2021. BibTex LaTex

44 [Conf article] L. Le Jeune, T. Goedemé and N. Mentens, "Towards Real-Time Deep Learning-based Network Intrusion Detection on FPGA" In Applied Cryptography and Network Security - ACNS 2021, Lecture Notes in Computer Science, Springer-Verlag, 18 pages, 2021. BibTex LaTex

45 [Conf article] W. Castryck and T. Decru, "Multiradical isogenies" In Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics 779, S. Anni, V. Karemaker and E. Lorenzo Garcia (Eds.), American Mathematical Society, pp. 57-89, 2021. BibTex LaTex

46 [Conf article] T. Ashur and D. Toprakhisar, "A Comperative Study of Vision and AES in FHE Setting" In Proceedings of the Symposium on Information Theory in the Benelux 2021, R. Van Sloun and B. Škoric (Eds.), Werkgemeenschap voor Informatie- en Communicatietheorie, pp. 106-111, 2021. BibTex LaTex

47 [Conf article] L. Kraleva and C. Li, "On the SNOW Stream Ciphers" In Proceedings of the Symposium on Information Theory in the Benelux 2021, R. Van Sloun and B. Škoric (Eds.), Werkgemeenschap voor Informatie- en Communicatietheorie, pp. 116-123, 2021. BibTex LaTex

48 [Conf article] K. Baghery, C. Delpech de Saint Guilhem, E. Orsini, N. Smart and T. Tanguy, "Compilation of Function Representations for Secure Computing Paradigms" In Topics in Cryptology - CT-RSA 2021, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 12704, K. Paterson (Ed.), Springer-Verlag, 32 pages, 2021. BibTex LaTex

49 [Conf article] D. Cozzo, N. Smart and Y. Talibi Alaoui, "Secure Fast Evaluation of Iterative Methods: With an BibTex

Application to Secure PageRank" In Topics in Cryptology - CT-RSA 2021, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 12704, K. Paterson (Ed.), Springer-Verlag, pp. 1-25, 2021. LaTex

50 [Conf article] C. Baum, C. Delpech de Saint Guilhem, D. Kales, E. Orsini, P. Scholl and G. Zaverucha, "Banquet: Short and Fast Signatures from AES" In Public Key Cryptography, 24 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2021, Lecture Notes in Computer Science, Springer-Verlag, 39 pages, 2021. BibTex LaTex

51 [Conf article] S. Zeitouni, J. Vliegen, T. Frassetto, D. Koch, A. Sadeghi and N. Mentens, "Trusted Configuration in Cloud FPGAs" In 2021 Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2021), IEEE, pp. 233-241, 2021. BibTex LaTex

52 [Conf article] R. Amos, G. Acar, E. Lucherini, M. Kshirsagar, A. Narayanan and J. Mayer, "Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset" In Proceedings of the The Web (WWW) Conference, ACM, 22 pages, 2021. BibTex LaTex

53 [Conf article] E. Argones Rúa, T. Van hamme, W. Joosen and D. Preuveneers, "Gait Authentication based on Spiking Neural Networks" In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Lecture Notes in Informatics (LNI) LNI P315, A. Brömme, C. Busch, N. Damer, A. Dantcheva, M. Gomez-Barrero, K. Raja and C. Rathgeb (Eds.), Bonner Köllen Verlag, pp. 51-60, 2021. BibTex LaTex

54 [Conf article] K. Baghery, M. Kohlweiss, J. Siim and M. Volkhov, "Another Look at Extraction and Randomization of Groth's zk-SNARK" In Financial Cryptography and Data Security - International Conference, FC 2021, Lecture Notes in Computer Science, Springer-Verlag, pp. 457-475, 2021. BibTex LaTex

55 [Conf article] E. Makri, D. Rotaru, F. Vercauteren and S. Wagh, "Rabbit: Efficient Comparison for Secure Multi-Party Computation" In Financial Cryptography and Data Security - International Conference, FC 2021, Lecture Notes in Computer Science, Springer-Verlag, 21 pages, 2021. BibTex LaTex

56 [Conf article] C. Brunner, A. Madhusudan, D. Engel and B. Preneel, "Off-chain state channels in the energy domain" In IEEE PES Innovative Smart Grid Technologies Conference North America(ISGT NA 2021), IEEE, pp. 1-5, 2021. BibTex LaTex

57 [Conf article] S. Bhattacharya and I. Verbauwhede, "Exploring Micro-architectural Side-channel Leakages through Statistical Testing" In Design, Automation and Test in Europe, IEEE, 4 pages, 2021. BibTex LaTex

58 [Journal article] D. Bozilov, M. Knežević and V. Nikov, "Optimized threshold implementations: securing cryptographic accelerators for low-energy and low-latency applications", Journal of Cryptographic Engineering 12(1), pp. 15-51, 2021. BibTex LaTex

59 [Journal article] J. Winderickx, A. Braeken, D. Singelée and N. Mentens, "In-depth energy analysis of security algorithms and protocols for the Internet of Things", Journal of Cryptographic Engineering (2021), 13 pages, 2021. BibTex LaTex

60 [Journal article] T. Fritzmann, M. Van Beirendonck, D. Basu Roy, P. Karl, T. Schamberger, I. Verbauwhede and G. Sigl, "Masked Accelerators and Instruction Set Extensions for Post-Quantum Cryptography", IACR Transactions on Cryptographic Hardware and Embedded Systems 2022(1), 47 pages, 2021. BibTex LaTex

61 [Journal article] J. Trautmann, A. Beckers, L. Wouters, B. Gierlichs, J. Teich, I. Verbauwhede and S. Wildermann, "Semi-Automatic Locating of Cryptographic Operations in Side-Channel Traces", IACR Transactions on Cryptographic Hardware and Embedded Systems 2022(1), pp. 345-366, 2021. BibTex LaTex

62 [Journal article] H. Beckers, J. Bermudo Mera, A. Karmakar, J. Yiu and I. Verbauwhede, "Polynomial multiplication on embedded vector architectures", IACR Transactions on Cryptographic Hardware and Embedded Systems 2022(1), pp. 482-505, 2021. BibTex LaTex

63 [Journal article] M. Kim, S. Hong, J. Hubaux, D. Kim, K. Lauter, Y. Ma, L. Ohno-Machado, H. Sofia, Y. Son, Y. Song, J. Troncoso-Pastoriza, A. Ozgun Harmanci, X. Jiang, J. Bossuat, S. Carpov, J. Hee Cheon, I. Chillotti, W. Cho, D. Froelicher, N. Gama and M. Georgieva, "Ultrafast homomorphic encryption models enable secure BibTex LaTex

outsourcing of genotype imputation", Cell Systems 12(11), pp. 1108-1120, 2021.

64 [Journal article] T. Van hamme, E. Argones Rúa, W. Joosen and D. Preuveneers, "On the Security of Biometrics and Fuzzy Commitment Cryptosystems: a Study on Gait Authentication", IEEE Transactions on Information Forensics and Security <empty>(<empty>), pp. 5211-5224, 2021. BibTex LaTex

65 [Journal article] J. Cartlidge, N. Smart and Y. Talibi Alaoui, "Multi-Party Computation Mechanism for Anonymous Equity Block Trading: A Secure Implementation of Turquoise Plato Uncross", Intelligent Systems in Accounting, Finance and Management 28(4), pp. 239-267, 2021. BibTex LaTex

66 [Journal article] V. Dudjak, B. Lormeteau, M. Mustafa, Y. Wang, C. Francis, F. Zobiri, D. Parra, A. Papaemmanouil, D. Neves, T. Alskaif, S. Khadem, A. Pena-Bello, P. Saggese, B. Bowler, M. Andoni, M. Bertolini and Y. Zhou, "Impact of Local Energy Markets Integration in Power Systems Layer: A Comprehensive Review", Journal of Applied Energy 301(117434), 13 pages, 2021. BibTex LaTex

67 [Journal article] Y. Chen, A. Luykx, B. Mennink and B. Preneel, "Systematic Security Analysis of Stream Encryption With Key Erasure", IEEE Transactions on Information Theory 63(11), pp. 7518-7534, 2021. BibTex LaTex

68 [Journal article] V. Arribas Abril, S. Petkova-Nikova and Z. Zhang, "LLTI: Low-Latency Threshold Implementations", IEEE Transactions on Information Forensics and Security (16), pp. 5108-5123, 2021. BibTex LaTex

69 [Journal article] M. Grujic and I. Verbauwhede, "TROT: A Three-Edge Ring Oscillator based True Random Number Generator with Time-to-Digital Conversion", IEEE Transactions on Circuits and Systems I: Regular Papers 1(1), 14 pages, 2021. BibTex LaTex

70 [Journal article] H. Beckers, J. Bermudo Mera, A. Karmakar, J. Yiu and I. Verbauwhede, "Polynomial multiplication on embedded vector architectures", IACR Cryptology ePrint Archive 2021(998), 29 pages, 2021. BibTex LaTex

71 [Journal article] W. Beullens, S. Dobson, S. Katsumata, Y. Lai and F. Pintore, "Group Signatures and More from Isogenies and Lattices: Generic, Simple, and Efficient", IACR Cryptology ePrint Archive 2021(1366), 56 pages, 2021. BibTex LaTex

72 [Journal article] A. Adavoudi Jolfaei, S. Aghili and D. Singelée, "A Survey on Blockchain-based IoMT Systems: Towards Scalability", IEEE Access 9(<empty>), 28 pages, 2021. BibTex LaTex

73 [Journal article] R. Galvez, V. Moonsamy and C. Diaz, "Less is More: A privacy-respecting Android malware classifier using Federated Learning", Proceedings on Privacy Enhancing Technologies 2021(4), 20 pages, 2021. BibTex LaTex

74 [Journal article] J. Park, "Homomorphic Encryption for Multiple Users With Less Communications", IEEE Access 9(<empty>), pp. 135915-135926, 2021. BibTex LaTex

75 [Journal article] I. Ekerete, M. Garcia-Constantino, A. Konios, M. Mustafa, Y. Diaz-Skeete, C. Nugent and J. McLaughlin, "Fusion of Unobtrusive Sensing Solutions for Home-Based Activity Recognition and Classification Using Data Mining Models and Methods", Applied Sciences 11(19), pp. 1-16, 2021. BibTex LaTex

76 [Journal article] W. Beullens, "MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps", IACR Cryptology ePrint Archive 2021(1144), 24 pages, 2021. BibTex LaTex

77 [Journal article] M. Mustafa, A. Konios and M. Garcia-Constantino, "IoT-based Activities of Daily Living for Abnormal Behaviour Detection: Privacy Issues and Potential Countermeasures", IEEE Internet of Things magazine 4(3), pp. 90-95, 2021. BibTex LaTex

78 [Journal article] J. Liu, V. Rijmen, Y. Hu, J. Chen and B. Wang, "WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix", SCIENCE CHINA INFORMATION SCIENCES (65), 15 pages, 2021. BibTex LaTex

79 [Journal article] W. Lueks, J. Benzler, D. Bogdanov, G. Kirchner, R. Lucas, R. Oliveira, B. Preneel, M. Salathé, C. Troncoso and V. Von Wyl, "Toward a Common Performance and Effectiveness Terminology for Digital Proximity BibTex LaTex

Tracing Applications", Frontiers in Digital Health 3( ), pp. 1-12, 2021.

80 [Journal article] W. Li, J. Li, D. Gu, C. Li and T. Cai, "Statistical Fault Analysis of the Simeck Lightweight Cipher in the Ubiquitous Sensor Networks", IEEE Trans. Information Forensics and Security 16(<empty>), pp. 4224-4233, 2021. BibTex LaTex

81 [Journal article] M. Montakhabi, F. Zobiri, S. Van der Graaf, G. Deconinck, D. Orlando, P. Ballon and M. Mustafa, "An Ecosystem View of Peer-to-Peer Electricity Trading: Scenario Building by Business Model Matrix to Identify New Roles", energies 14 (12), 23 pages, 2021. BibTex LaTex

82 [Journal article] V. Rijmen, "Editorial", Journal of Cryptography 34(3), 1 pages, 2021. BibTex LaTex

83 [Journal article] Y. Dimova, G. Acar, L. Olejnik, W. Joosen and T. Van Goethem, "The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion", Proceedings on Privacy Enhancing Technologies 2021(3), 19 pages, 2021. BibTex LaTex

84 [Journal article] I. Iliashenko and V. Zucca, "Faster Homomorphic Comparison Operations for BGV and BFV", Proceedings on Privacy Enhancing Technologies 2021(3), pp. 246-264, 2021. BibTex LaTex

85 [Journal article] S. Sadeghi, V. Rijmen and N. Bagheri, "Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK", Designs, Codes and Cryptography 89(7), 43 pages, 2021. BibTex LaTex

86 [Journal article] T. Ashur, C. Li, Y. Liu and J. Lu, " On the Effect of the Key-expansion Algorithm in Simon-like Ciphers", The Computer Journal (00), 26 pages, 2021. BibTex LaTex

87 [Journal article] S. Dhooghe and S. Petkova-Nikova, "Resilient uniformity: applying resiliency in masking", Cryptogr. Commun., Special Issue on Mathematical Methods for Cryptography 14(1), 18 pages, 2021. BibTex LaTex

88 [Journal article] S. Sheshank Burra, N. Smart, E. Larraia, J. Nielsen, P. Sebastian Nordholt, C. Orlandi, E. Orsini and P. Scholl, "High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer", Journal of Cryptology 34(3), 72 pages, 2021. BibTex LaTex

89 [Journal article] R. Jadoul, N. Smart and B. Van Leeuwen, "MPC for Q2 Access Structures over Rings and Fields", IACR Cryptology ePrint Archive 2021(841), 59 pages, 2021. BibTex LaTex

90 [Journal article] T. Ashur, E. Cohen, C. Hazay and A. Yanai, " A New Framework for Garbled Circuits", IACR Cryptology ePrint Archive 2021(739), 25 pages, 2021. BibTex LaTex

91 [Journal article] A. Peetermans, V. Rozic and I. Verbauwhede, "Design and Analysis of Configurable Ring Oscillators for True Random Number Generation based on Coherent Sampling", ACM Transactions on Reconfigurable Technology and Systems 14(2), 21 pages, 2021. BibTex LaTex

92 [Journal article] A. Bhati, E. Andreeva, D. Vizár and B. Preneel, "1, 2, 3, Fork: Counter Mode Variants based on a Generalized Forkcipher", IACR Transactions on Symmetric Cryptology 2021(3), 34 pages, 2021. BibTex LaTex

93 [Journal article] S. Aghili, H. Mala, C. Schindelhauer, M. Shojafar and R. Tafazolli, "Closed-loop and open-loop authentication protocols for blockchain-based IoT systems", Information Processing and Management 58(4), 16 pages, 2021. BibTex LaTex

94 [Journal article] X. Huang, T. Yoshizawa and S. Backia Mary Baskaran, "Authentication Mechanisms in the 5G System", Journal of ICT Standardization 9(2), pp. 61-78, 2021. BibTex LaTex

95 [Journal article] A. Purnal, L. Giner, D. Gruss and I. Verbauwhede, "Systematic Analysis of Randomization-based Protected Cache Architectures", IEEE Security & Privacy (2021), 16 pages, 2021. BibTex LaTex

96 [Journal article] J. D'Anvers, E. Orsini and F. Vercauteren, "Error Term Checking: Towards Chosen Ciphertext Security without Re-encryption", ACM ASIA Public-Key Cryptography Workshop (2021), 27 pages, 2021. BibTex LaTex

97

[Journal article] J. Winderickx, A. Braeken and N. Mentens, "Enhanced end-to-end security through symmetric-key cryptography in wearable medical sensor networks", Health and Technology (95), pp. 511-523, 2021. BibTex LaTex

98 [Journal article] J. Winderickx, P. Bellier, P. Duflot and N. Mentens, "Communication and Security Trade-Offs for Battery-Powered Devices: A Case Study on Wearable Medical Sensor Systems", IEEE Access (9), pp. 67466-67476, 2021. BibTex LaTex

99 [Journal article] R. Sarenche, M. Salmasizadeh, M. Hassan Ameri and M. Reza Aref, "A secure and privacy-preserving protocol for holding double auctions in smart grid", Elsevier Science Information Sciences 557(1), pp. 108-129, 2021. PDF BibTex LaTex

100 [Journal article] M. Van Beirendonck, J. D'Anvers, A. Karmakar, J. Balasch and I. Verbauwhede, "A Side-Channel Resistant Implementation of SABER", ACM Journal on Emerging Technologies in Computing Systems 17(2), 25 pages, 2021. PDF BibTex LaTex

101 [Journal article] M. Alam, S. Bhattacharya and D. Mukhopadhyay, "Victims can be Saviors: A Machine Learning based detection for Micro-Architectural Side-Channel Attacks", ACM Journal on Emerging Technologies in Computing Systems 17(2), 20 pages, 2021. BibTex LaTex

102 [Journal article] A. Sateesan, S. Sinha, S. K.G. and A. Vinod, "A Survey of Algorithmic and Hardware Optimization Techniques for Vision Convolutional Neural Networks on FPGAs", Neural Processing Letters <empty>(<empty>), 46 pages, 2021. PDF BibTex LaTex

103 [Journal article] T. Ashur and R. Posteuca, "How to Backdoor a Cipher", IACR Cryptology ePrint Archive 2021(442), 17 pages, 2021. PDF BibTex LaTex

104 [Journal article] S. De Figueiredo, A. Madhusudan, V. Reniers, S. Petkova-Nikova and B. Preneel, "Exploring the Storj Network: a Security Analysis", ACM/SIGAPP Symposium on Applied Computing (36), pp. 257-264, 2021. PDF BibTex LaTex

105 [Journal article] S. Canard and C. Li, "Towards Practical Intrusion Detection System over Encrypted Traffic", IET Information Security 15(3), pp. 231-246, 2021. PDF BibTex LaTex

106 [Journal article] S. Batsleer and J. D'Anvers, "Multitarget decryption failure attacks and their application to Saber and Kyber", IACR Cryptology ePrint Archive 2021(193), 34 pages, 2021. PDF BibTex LaTex

107 [Journal article] A. Kim, Y. Polyakov and V. Zucca, "Revisiting Homomorphic Encryption Schemes for Finite Fields", IACR Cryptology ePrint Archive 2021(204), 46 pages, 2021. PDF BibTex LaTex

108 [Journal article] C. Bonte, N. Smart and T. Tanguy, "Thresholdizing HashEdDSA: MPC to the Rescue", International Journal of Information Security 20(1), pp. 879-894, 2021. BibTex LaTex

109 [Journal article] A. Bhati, E. Andreeva and D. Vizár, "OAE-RUP: A Strong Online AEAD Security Notion and its Application to SAEF", IACR Cryptology ePrint Archive 2021(103), 34 pages, 2021. PDF BibTex LaTex

110 [Journal article] I. Fernandez-Hernandez, T. Ashur and V. Rijmen, "Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols", IEEE Transactions on Aerospace and Electronic Systems 57(3), pp. 1827-1839, 2021. PDF BibTex LaTex

111 [Journal article] L. Wouters, B. Gierlichs and B. Preneel, "My other car is your car: compromising the Tesla Model X keyless entry system", IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(4), pp. 149-172, 2021. PDF BibTex LaTex

112 [Journal article] J. Bermudo Mera, A. Karmakar, S. Kundu and I. Verbauwhede, "Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms", IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(4), pp. 474-509, 2021. PDF ▶ 🔗 BibTex LaTex

113 [Journal article] A. Abidin, M. El Soussi, J. Romme, P. Boer, D. Singelée and C. Bachmann, "Secure, Accurate, and Practical Narrow-Band Ranging System", IACR Transactions on Cryptographic Hardware and Embedded BibTex LaTex

Systems 2021(2), 30 pages, 2021.

114 [Journal article] A. Chakraborty, S. Bhattacharya, M. Alam, D. Mukhopadhyay and S. Patranabis, "RASSLE: Return Address Stack based Side-channel LEakage", IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2), 29 pages, 2021. BibTex LaTex

115 [Journal article] S. Bhasin, J. D'Anvers, D. Heinz, T. Poppelmann and M. Van Beirendonck, "Attacking and Defending Masked Polynomial Comparison for Lattice-Based Cryptography", IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2), 25 pages, 2021. BibTex LaTex

116 [Journal article] M. Van Beirendonck, J. D'Anvers and I. Verbauwhede, "Analysis and Comparison of Table-based Arithmetic to Boolean Masking", IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2), 22 pages, 2021. BibTex LaTex

117 [Journal article] A. Rezaei Shahmirzadi, D. Bozilov and A. Moradi, "New First-Order Secure AES Performance Records", IACR Cryptology ePrint Archive 2021(037), 25 pages, 2021. BibTex LaTex

118 [Journal article] L. Le Jeune, T. Goedemé and N. Mentens, "Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework", IEEE Access 9(<empty>), pp. 63995-64015, 2021. BibTex LaTex

119 [Thesis] A. Beckers, "Practical Fault Attacks on Cryptographic Devices", Phd thesis, Katholieke Universiteit Leuven, B. Gierlichs and I. Verbauwhede, pp. 1-162, 2021. BibTex LaTex

120 [Thesis] S. Dhooghe, "New Security Models for Passive and Active Physical Attacks", Phd thesis, KU Leuven, V. Rijmen and S. Petkova-Nikova, 198 pages, 2021. BibTex LaTex

121 [Thesis] J. Bertels, F. Turan, M. Van Beirendonck, J. Bermudo Mera and A. Karmakar, "Fastest Homomorphic Encryption in the West Made Faster", Master thesis, KU Leuven, I. Verbauwhede, 72 pages, 2021. BibTex LaTex

122 [Thesis] A. Dutta, A. Bhati and E. Andreeva, "A Catalogue for Provably Secure Symmetric Modes and Primitives", Master thesis, Indian Statistical Institute (ISI), Calcutta, B. Preneel and B. Roy, 90 pages, 2021. BibTex LaTex

123 [Thesis] B. Van der Vliet, "Improving resistance against poisoning attacks in a federated malware classifier", Master thesis, KU Leuven, C. Diaz, pp. 1-53, 2021. BibTex LaTex

124 [Thesis] T. Claesen, "Analysis and implementation of novel non-cryptographic hash functions", Master thesis, KU Leuven, N. Mentens, A. Sateesan and J. Vliegen, 50 pages, 2021. BibTex LaTex

125 [Thesis] E. Makri, "Secure and Efficient Computing on Private Data", Phd thesis, KU Leuven, B. Preneel and F. Vercauteren, 246 pages, 2021. BibTex LaTex

126 [Thesis] J. Hoes, "Rise of the Machines - On the Security of Cellular IoT Devices", Master thesis, Katholieke Universiteit Leuven, M. Dieudonné and B. Preneel, 76 pages, 2021. BibTex LaTex

127 [Thesis] H. Heerwegh, "Groups of Unknown Order", Master thesis, KU Leuven, F. Vercauteren, W. Castryck and I. Iliashenko, 75 pages, 2021. BibTex LaTex

128 [Thesis] S. Ampe, "Towards a speed-up of CRS using binary fields", Master thesis, KU Leuven, W. Castryck and F. Vercauteren, 109 pages, 2021. BibTex LaTex

129 [Thesis] Y. Vermeire, "Mobile Collaborative Authentication", Master thesis, Katholieke Universiteit Leuven, A. Abidin and B. Preneel, 103 pages, 2021. BibTex LaTex

130 [Thesis] C. Bonte, W. Castryck, I. Iliashenko and W. Manhaeve, "Training least squares support vector machines with homomorphic encryption", Master thesis, KU Leuven, F. Vercauteren, 55 pages, 2021. BibTex LaTex

131 [Thesis] J. Kang, "Efficient Homomorphic Encryption for Fixed Point Arithmetic", Master thesis, KU Leuven, F. Vercauteren, I. Iliashenko and C. Bonte, 47 pages, 2021. BibTex LaTex

132 [Thesis] P. Thijs, "Conversion algorithms between homomorphic encryption schemes", Master thesis, KU Leuven, F. Vercauteren and I. Iliashenko, 56 pages, 2021. BibTex LaTex

133 [Thesis] B. Veys, "Security Analysis of IoT Devices: the 'Trifo Ironpie m6' Smart Robot Vacuum Cleaner", Master thesis, KU Leuven, B. Preneel and F. Piessens, 55 pages, 2021. BibTex LaTex

134 [Thesis] T. Feys, "Evaluating neural network based time series classification architectures for side-channel attacks", Master thesis, KU Leuven, B. Preneel, 88 pages, 2021. BibTex LaTex

135 [Thesis] C. Mujdei, "Side-Channel Attacks on Post-Quantum Cryptography", Master thesis, KU Leuven, I. Verbauwhede, 87 pages, 2021. BibTex LaTex

136 [Thesis] K. Keersmaekers, J. Bermudo Mera, A. Karmakar and F. Turan, "A Compact and Flexible Hardware Accelerator for NTRU Polynomial Multiplication using NTT ", Master thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 58 pages, 2021. BibTex LaTex

137 [Thesis] K. Stefanidis - Vozikis, "A Distributed Performance Measurement Tool for Tor Browser", Master thesis, KU Leuven, C. Diaz and F. Piessens, 63 pages, 2021. BibTex LaTex

138 [Thesis] C. Bonte, "Optimising Privacy-Preserving Computations", Phd thesis, KU Leuven, B. Preneel and F. Vercauteren, 266 pages, 2021. BibTex LaTex

139 [Thesis] R. Geelen, "Bootstrapping Algorithms for BGV and FV", Master thesis, KU Leuven, F. Vercauteren, 71 pages, 2021. BibTex LaTex

140 [Thesis] K. Everaert, "Evaluating machine learning assisted side-channel attacks", Master thesis, KU Leuven, B. Preneel, pp. 1-40, 2021. BibTex LaTex

141 [Thesis] L. Berghman, "Side-channel evaluation and countermeasures for ForkSkinny software implementations", Master thesis, KU Leuven, B. Preneel, pp. 1-139, 2021. BibTex LaTex

142 [Thesis] J. Biesmans and M. Dekeyser, "Embedded FPGA for cryptography", Master thesis, UHasselt, KU Leuven, N. Mentens, pp. 1-54, 2021. BibTex LaTex

143 [Thesis] S. Smith, "On Verifiable Document Redacting Using Groth's zk-SNARKs", Master thesis, KU Leuven, N. Smart and K. Baghery, pp. 1-62, 2021. BibTex LaTex

144 [Thesis] O. Zajonc, "Exploring Information Leaked by Using the PageRank Algorithm in a MPC Setting", Master thesis, KU Leuven, N. Smart, D. Cozzo and Y. Talibi Alaoui, pp. 1-44, 2021. BibTex LaTex

145 [Thesis] Y. Zheng, "A large-scale longitudinal Analysis of Web Tracking", Master thesis, KU Leuven, C. Diaz, pp. 1-56, 2021. BibTex LaTex

146 [Thesis] L. Wouters, "Fault Attack on IND-CCA secure Saber.KEM", Master thesis, KU Leuven, I. Verbauwhede, pp. 1-66, 2021. BibTex LaTex

147 [Thesis] J. D'Anvers, "Design and Security Analysis of Lattice-based Post-Quantum Encryption", Phd thesis, KU Leuven, I. Verbauwhede and F. Vercauteren, 204 pages, 2021. BibTex LaTex

148 [Thesis] J. Vandersmissen, "A White-Box Speck Implementation using Self-Equivalence Encodings", Master thesis, KU Leuven, F. Piessens, B. Preneel and A. Ranea, 68 pages, 2021. BibTex LaTex

149 [Thesis] W. Beullens, "The Design and Cryptanalysis of Post-Quantum Digital Signature Algorithms", Phd thesis, KU Leuven, B. Preneel and F. Vercauteren, 338 pages, 2021. BibTex LaTex

150 [Thesis] C. Bootland, "Efficiency and security aspects of lattice-based cryptography", Phd thesis, KU Leuven, B. Preneel and F. Vercauteren, 300 pages, 2021. BibTex LaTex

151 [Proceeding] "Progress in Cryptology - INDOCRYPT 2021", Lecture Notes in Computer Science 13143, A. BibTex

Adhikari, R. Küsters and B. Preneel (Eds.), Springer-Verlag, 2021. LaTex

152 [Proceeding] "Transactions in Cryptographic Hardware and Embedded Systems (TCHES)", Lecture Notes in Computer Science 2021(2), E. De Mulder and P. Schwabe (Eds.), Springer-Verlag, 2021. BibTex LaTex

153 [Proceeding] "International Conference on Security, Privacy and Applied Cryptography Engineering", Lecture Notes in Computer Science 13162, L. Batina, M. Mondal and S. Picek (Eds.), Springer-Verlag, 2021. BibTex LaTex

154 [Book] S. Sinha Roy and I. Verbauwhede, "Lattice-Based Public-Key Cryptography in Hardware", Springer, 101 pages, 2021. BibTex LaTex

155 [Report] S. Aghili and D. Singelée, "ProTego-ACC: Access control and key management for healthcare systems", ProTego white paper, pp. 1-11, 2021. PDF BibTex LaTex

156 [Report] J. Pilet, B. Preneel, S. Erzeel, O. Pereira, F. Sbaraglia, A. Tibbaut, X. Carpent and R. Dandoy, "Studie over de mogelijkheid om online stemmen in België in te voeren (luik 2)", Report for PROJECT NETVOTING_BE, pp. 1-45, 2021. PDF BibTex LaTex

157 [Report] J. Pilet, B. Preneel, S. Erzeel, O. Pereira, F. Sbaraglia, A. Tibbaut, X. Carpent and R. Dandoy, "Etude sur la possibilité d'introduire le vote Internet en Belgique (2)", Report for PROJECT NETVOTING_BE, pp. 1-43, 2021. PDF BibTex LaTex

158 [Report] C. Diaz, H. Halpin and A. Kiayias, "The Nym Network", Whitepaper, 38 pages, 2021. BibTex LaTex

159 [Abstract of talk] M. Montakhabi, S. Van der Graaf, A. Madhusudan and M. Mustafa, "Distributed Ledger Technologies to Foster Energy Transition in Smart Cities: Peer-to-Peer Electricity Trading Case", In Workshop The City as a License: Design, Rights and Civics in a Blockchain Society - CivicBlockchain 2021, 3 pages, 2021. PDF BibTex LaTex

160 [Talk] J. Neyts and B. Preneel, "Privacy-Preserving Contact Tracing: Experiences from Belgium and the EU", Global Crisis in Context: Belgian and Korean Approaches to the COVID-19 Pandemic, Hybrid, 2021. BibTex LaTex

161 [Talk] I. Verbauwhede, "Hardware Security: looking for the roots of trust", High-Tech Women in Science and Technology, Darmstadt, DE, 2021. BibTex LaTex

162 [Talk] B. Preneel, "The cryptographic year in perspective & a vision for the future", ISSE Webinar Series Building a new and Secure Future, Online, 2021. BibTex LaTex

163 [Talk] N. Mentens, "Security challenges and opportunities in emerging device technologies: a case study on flexible electronics", CARDIS 2021, Lübeck, DE, 2021. BibTex LaTex

164 [Talk] B. Preneel, "Coronalert: Lessons Learned from Digital Proximity Tracing", Werkgroepsymposium: Pandemic Preparedness: Looking Back and Looking Forward, Leuven, BE, 2021. BibTex LaTex

165 [Talk] B. Preneel, "Cryptomunten en blockchain: hype of trend?", Actueel Denken en Leven Turnhout, Turnhout, BE, 2021. BibTex LaTex

166 [Talk] B. Preneel, "VoteXX: Coercion Resistance for the Real World", UMBC Center for Cybersecurity, Online, 2021. BibTex LaTex

167 [Talk] N. Smart, "MPC solutions", MPC Data Privacy & Security Conference, Online, 2021. BibTex LaTex

168 [Talk] B. Preneel, "On General Trends in Security and Privacy", 25th Anniversary of Graduate School of Informatics, Online, 2021. ▶ BibTex LaTex

169 [Talk] D. Singelée, "Location proofs: How to realise location-based authentication by relying on commercial-off-the-shelf devices?", AriadNext workshop on remote ID verification, Rennes, FR, 2021. PDF BibTex LaTex

170 [Talk] B. Preneel, "Technology and Control", XI Encuentro de Cloud Security Alliance España, Madrid, ES, 2021. BibTex LaTex

171 [Talk] C. Diaz, "Metadata and ML-based traffic analysis", DEXA Panel: Big Minds Sharing their Vision on the Future of AI, Online, On, 2021. BibTex LaTex

172 [Talk] V. Rijmen, "Threshold implementations", RCD 2021, Bucharest, RO, 2021. BibTex LaTex

173 [Talk] V. Rijmen, "Differential cryptanalysis using quasi differential trails", BFA 2021, Rosendal, NO, 2021. BibTex LaTex

174 [Talk] B. Preneel, "An introduction to blockchain and cryptocurrencies", RAIS Summer School, Entrepreneurial Event and Workshop, Heraklion, GR, 2021. BibTex LaTex

175 [Talk] V. Rijmen, "Galileo authentication", ISCISC 2021, Tehran, IR, 2021. BibTex LaTex

176 [Talk] S. Kundu, "Quantum secure public-key cryptography: history and current developments", Weekly Seminar at IAI TCG CREST , Kolkata, IN, 2021. PDF BibTex LaTex

177 [Talk] B. Preneel, "Cryptography and network security", e International School on Foundations of Security Analysis and Design (FOSAD), University Residential Center of Bertinoro, 2021. BibTex LaTex

178 [Talk] B. Preneel, "The Future of Security and Privacy (keynote)", 16th International Meeting on Fully Three-Dimensional Image Reconstruction in Radiology and Nuclear Medicine (Fully3D), Online, 2021. BibTex LaTex

179 [Talk] B. Preneel, "Post Covid-19 - Ensuring the future of free movement", EEMA's Annual Conference Webinar 2021, Online, 2021. BibTex LaTex

180 [Talk] I. Verbauwhede, "Recent Result with EM attacks: Passive observation and active perturbation", The “Future of Cryptographic Engineering” Webinar, Online, 2021. BibTex LaTex

181 [Talk] J. D'Anvers and M. Van Beirendonck, "Techniques for Masking Saber and Kyber ", Third PQC Standardization Conference, Virtual, 2021. PDF ▶ BibTex LaTex

182 [Talk] I. Verbauwhede, "Secure Hardware Design: Starting from the Roots of Trust", ICHSA 2021, Online, 2021. ▶ BibTex LaTex

183 [Talk] I. Verbauwhede, "Secure Hardware Design: Starting from the Roots of Trust (keynote)", European Test Symposium 2021, BE, 2021. BibTex LaTex

184 [Talk] B. Preneel, "Unlocking of encrypted Sky ECC chat services", Belgian Cyber Security Coalition Crypto Focus Group Meeting, Online, 2021. BibTex LaTex

185 [Talk] B. Preneel, "Keynote on Contact and presence tracing", EIT Digital webinar, Online, 2021. BibTex LaTex

186 [Talk] B. Preneel, "The encryption dilemma - Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK)?", Webinar - The encryption dilemma - Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK)?, Online, 2021. BibTex LaTex

187 [Talk] B. Preneel, "Introduction to Resilience (keynote)", Infosecurity.be, Data & Cloud Expo, Online, 2021. BibTex LaTex

188 [Talk] B. Preneel, "Big data against corona: mass surveillance or privacy by design?", Dentity & Access Management - The Online Event About Digital Identities & Trust, Online, 2021. BibTex LaTex

189 [Talk] B. Preneel, "Keynote at Lailec 2021", Leuven AI Law & Ethics Conference 2021, Online, 2021. BibTex LaTex

190 [Talk] B. Preneel, "The future of Security and Privacy", ICT inspiratiedag (Securitas), Online, 2021. ▶ BibTex LaTex

191 [Talk] B. Preneel, "Proximity tracing with Coronalert: lessons learned (2)", ViSP Distinguished Lecture Series, Online, 2021. BibTex LaTex

192 [Talk] B. Preneel, "How can big data help you? (Live Webinar About Big Data Against Corona)", Online event Identity & Access Management Belgium, Online, 2021. BibTex LaTex

193 [Talk] B. Preneel, "Cryptocurrencies and enterprise blockchains: two sides of one tapestry", Blockchain Summit 2021, Brussels, BE, 2021. BibTex LaTex

194 [Talk] C. Delpech de Saint Guilhem, "Banquet: Short and Fast Signatures from AES", NTNU Applied Cryptology Lab Seminar, Trondheim, 2021. BibTex LaTex

195 [Talk] B. Preneel, "Proximity tracing with Coronalert: lessons learned (1)", CIF Seminar, Online, 2021. ▶ BibTex LaTex

196 [Talk] B. Preneel, "European-Wide Privacy-Preserving Proximity Tracing", SAPHIRe online webinar, Online, 2021. ▶ BibTex LaTex

197 [Talk] L. Wouters, "My other car is your car: Compromising the Tesla Model X keyless entry system", Real World Crypto, 2021. PDF ▶ BibTex LaTex

198 [Patent] A. Abidin and E. Argones Rúa, "Authentication method and system", Patent number US11171785B2, KU Leuven, 2021. BibTex LaTex

2020

1 [Conf article] E. Orsini, "Efficient, Actively Secure MPC with a Dishonest Majority: A Survey" In International Workshop on the Arithmetic of Finite Fields (WAIFI 2024), Lecture Notes in Computer Science LNCS, J. Bajard and A. Topuzoglu (Eds.), Springer-Verlag, pp. 42-71, 2020. BibTex LaTex

2 [Conf article] L. Kraleva, R. Posteuca and V. Rijmen, "Cryptanalysis of the Permutation Based Algorithm SpoC" In Progress in Cryptology - INDOCRYPT 2020, Lecture Notes in Computer Science 12578, K. Bhargavan, E. Oswald and M. Prabhakaran (Eds.), Springer-Verlag, pp. 273-293, 2020. BibTex LaTex

3 [Conf article] K. Baghery, Z. Pindado and C. Ràfols, "Simulation Extractable Versions of Groth's zk-SNARK Revisited" In International Conference on Cryptology and Network Security, CANS 2020, Lecture Notes in Computer Science 12579, S. Krenn, H. Shulman and S. Vaudenay (Eds.), Springer-Verlag, pp. 453-461, 2020. PDF ▶ BibTex LaTex

4 [Conf article] A. Sateesan, S. Sinha and S. K.G., "DASH: Design Automation for Synthesis and Hardware Generation for CNN" In International Conference on Field-Programmable Technology, 4 pages, 2020. PDF BibTex LaTex

5 [Conf article] C. Delpech de Saint Guilhem, E. Orsini, C. Petit and N. Smart, "Semi-commutative Masking: A Framework for Isogeny-Based Protocols, with an Application to Fully Secure Two-Round Isogeny-Based OT" In International Conference on Cryptology and Network Security, CANS 2020, Lecture Notes in Computer Science 12579, S. Krenn, H. Shulman and S. Vaudenay (Eds.), Springer-Verlag, pp. 235-258, 2020. PDF ▶ BibTex LaTex

6 [Conf article] S. Arash Azimi, A. Ranea, J. Mohajeri, M. Reza Aref, V. Rijmen and M. Salmasizadeh, "A Bit-Vector Differential Model for the Modular Addition by a Constant" In Advances in Cryptology - ASIACRYPT 2020, Lecture Notes in Computer Science 12492, K. Kim (Ed.), Springer-Verlag, 30 pages, 2020. PDF ▶ BibTex LaTex

7 [Conf article] W. Castryck, T. Decru and F. Vercauteren, "Radical isogenies" In Advances in Cryptology - ASIACRYPT 2020, Lecture Notes in Computer Science 12492, K. Kim (Ed.), Springer-Verlag, pp. 493-519, 2020. PDF ▶ BibTex LaTex

8 [Conf article] T. Beyne, S. Dhooghe and Z. Zhang, "Cryptanalysis of Masked Ciphers: A not so Random Idea" In Advances in Cryptology - ASIACRYPT 2020, Lecture Notes in Computer Science 12492, K. Kim (Ed.), Springer-Verlag, 35 pages, 2020. PDF ▶ BibTex LaTex

9 [Conf article] H. Chen, M. Kim, I. Razenshteyn, D. Rotaru, Y. Song and S. Wagh, "Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning" In Advances in Cryptology - ASIACRYPT 2020, Lecture Notes in Computer Science 12492, K. Kim (Ed.), Springer-Verlag, 40 pages, 2020. PDF ▶ BibTex LaTex

10 [Conf article] W. Beullens, S. Katsumata and F. Pintore, "Calamari and Falafl: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices" In Advances in Cryptology - ASIACRYPT 2020, Lecture Notes in BibTex LaTex

Computer Science 12492, K. Kim (Ed.), Springer-Verlag, pp. 464-492, 2020.

11 [Conf article] V. Arribas Abril, F. Wegener, A. Moradi and S. Petkova-Nikova, "Cryptographic Fault Diagnosis using VerFI" In IEEE International Symposium on Hardware-Oriented Security and Trust - HOST 2020, ISBN, IEEE, 12 pages, 2020. BibTex LaTex

12 [Conf article] H. Halpin, "A Critique of Immunity Passports and W3C Decentralized Identifiers" In Security Standardisation Research, Lecture Notes in Computer Science LNCS, M. Mehrnezhad, C. Mitchell and T. Van der Merwe (Eds.), Springer-Verlag, 23 pages, 2020. BibTex LaTex

13 [Conf article] W. Zellinger, V. Wieser, D. Brunner, L. Fischer, R. Galvez, M. Kumar, J. Langer, B. Moser and N. Shepeleva, "Beyond Federated Learning: On Confidentiality-Critical Machine Learning Applications in Industry" In Procedia Computer Science, Elsevier, 17 pages, 2020. BibTex LaTex

14 [Conf article] A. Deprez, E. Andreeva, J. Bermudo Mera, A. Karmakar and A. Purnal, "Optimized Software Implementations for the Lightweight Encryption Scheme ForkAE" In Smart Card Research and Advanced Applications - CARDIS 2020, Lecture Notes in Computer Science, Springer-Verlag, 16 pages, 2020. BibTex LaTex

15 [Conf article] S. Dhooghe and S. Petkova-Nikova, "Let's Tessellate: Tiling for Security Against Advanced Probe and Fault Adversaries" In Smart Card Research and Advanced Applications - CARDIS 2020, Lecture Notes in Computer Science, Springer-Verlag, 24 pages, 2020. BibTex LaTex

16 [Conf article] T. Yoshizawa and B. Preneel, "Verification Schemes of Multi-SIM Devices in Mobile Communication Systems" In ACM International Symposium on Mobility Management and Wireless Access 2020, 7 pages, 2020. BibTex LaTex

17 [Conf article] M. Willocx, D. Singelée, J. Lapon and V. Naessens, "Supporting Contact Tracing by Privacy-Friendly Registration at Catering Facilities" In European Symposium on Software Engineering, S. Gorlatch and F. José Garcia-Penalvo (Eds.), ACM, pp. 162-167, 2020. BibTex LaTex

18 [Conf article] M. Labafniya, S. Etemadi Borujeni and N. Mentens, "Evolvable Hardware Architectures on FPGA for Side-channel Security" In ACNS workshop on Artificial Intelligence in Hardware Security (AIHWS), Lecture Notes in Computer Science, Springer-Verlag, 18 pages, 2020. BibTex LaTex

19 [Conf article] A. Ranea and B. Preneel, "On Self-Equivalence Encodings in White-Box Implementations" In Selected Areas in Cryptography, 29 Annual International Workshop, SAC 2020, Lecture Notes in Computer Science, Springer-Verlag, 30 pages, 2020. BibTex LaTex

20 [Conf article] E. Andreeva, A. Bhati and D. Vizár, "Nonce-Misuse Security of the SAEF Authenticated Encryption Mode" In Selected Areas in Cryptography, 29 Annual International Workshop, SAC 2020, Lecture Notes in Computer Science, Springer-Verlag, 23 pages, 2020. BibTex LaTex

21 [Conf article] D. Bozilov, M. Eichlseder, M. Knežević, B. Lambin, G. Leander, T. Moos, V. Nikov, S. Rasoolzadeh, Y. Todo and F. Wiemer, "PRINCEv2 More Security for (Almost) No Overhead" In Selected Areas in Cryptography, 29 Annual International Workshop, SAC 2020, Lecture Notes in Computer Science, Springer-Verlag, pp. 483-511, 2020. BibTex LaTex

22 [Conf article] Q. Wang, J. Beysens, S. Pollin and D. Singelée, "Securing IoT Through Coverage-Bounding Wireless Communication With Visible Light" In International Conference on Network Protocols - ICNP 2020, IEEE, 2 pages, 2020. BibTex LaTex

23 [Conf article] M. Rabbani, J. Vliegen, M. Conti and N. Mentens, "SHeFU: Secure Hardware-Enabled Protocol for Firmware Updates" In IEEE International Symposium on Circuits and Systems (ISCAS 2020), IEEE, 5 pages, 2020. BibTex LaTex

24 [Conf article] A. Basso, J. Bermudo Mera, J. D'Anvers, A. Karmakar, S. Sinha Roy, M. Van Beirendonck and F. Vercauteren, "SABER: Mod-LWR based KEM round 3" In First PQC Standardization Conference, 44 pages, 2020. BibTex LaTex

25 [Conf article] L. Kraleva, T. Ashur and V. Rijmen, "Rotational Cryptanalysis on MAC Algorithm Chaskey" In Applied Cryptography and Network Security - ACNS 2020, Lecture Notes in Computer Science, E. Casalicchio, M. Conti, A. Spognardi and J. Zhou (Eds.), Springer-Verlag, pp. 153-168, 2020. BibTex LaTex

26 [Conf article] E. Orsini, N. Smart and F. Vercauteren, "Overdrive2k: Efficient Secure MPC over Z_2^k from Somewhat Homomorphic Encryption." In Topics in Cryptology - CT-RSA 2020, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science, Springer-Verlag, pp. 254-283, 2020. BibTex LaTex

27 [Conf article] K. Baghery, "Subversion-Resistant Commitment Schemes: Definitions and Constructions" In 13th International Workshop on Security and Trust Management - STM 2020, Lecture Notes in Computer Science 12386, K. Markantonakis and M. Petrocchi (Eds.), Springer-Verlag, pp. 106-122, 2020. BibTex LaTex

28 [Conf article] E. Andreeva, A. Bhati, A. Deprez, J. Pittevils, A. Roy and D. Vizár, "New Results and Insights on ForkAE" In NIST Lightweight Cryptography Workshop 2020, 17 pages, 2020. BibTex LaTex

29 [Conf article] Y. Koyen, A. Peetermans, V. Rozic and I. Verbauwhede, "Attacking Hardware Random Number Generators in a Multi-Tenant Scenario" In International Workshop on Fault Diagnosis and Tolerance in Cryptography 2020, IEEE, 8 pages, 2020. BibTex LaTex

30 [Conf article] M. Montakhabi, S. Van der Graaf, P. Ballon and M. Mustafa, "Sharing beyond Peer-to-peer Trading: Collaborative (open) Business Models as a Pathway to Smart Circular Economy in Electricity Markets" In Int. Conf. on Distributed Computing in Sensor Systems 2020, IEEE, pp. 482-489, 2020. BibTex LaTex

31 [Conf article] A. Sateesan, J. Vliegen, J. Daemen and N. Mentens, "Novel Bloom filter algorithms and architectures for ultra-high-speed network security applications" In Euromicro conference on Digital System Design (DSD), IEEE, pp. 262-269, 2020. BibTex LaTex

32 [Conf article] I. Ekerete, M. Garcia-Constantino, Y. Diaz, O. Giggins, M. Mustafa, A. Konios, P. Pouliet, C. D Nugent and J. McLaughlin, "Data Mining and Fusion of Unobtrusive Sensing Solutions for Indoor Activity Recognition" In Int. Conf. of the Engineering in Medicine & Biology Society (EMBC 2020), IEEE, pp. 5357-5361, 2020. BibTex LaTex

33 [Conf article] I. Kabin, Z. Dyka, D. Klann, N. Mentens, L. Batina and P. Langendoerfer, "Breaking a fully Balanced ASIC Coprocessor Implementing Complete Addition Formulas on Weierstrass Elliptic Curves" In DIGITAL SYSTEM DESIGN Architectures, Methods and Tools, IEEE Computer Society Press, pp. 270-276, 2020. BibTex LaTex

34 [Conf article] M. Brandalero, T. Goedemé, N. Mentens, D. Göhringer, M. Hübner, M. Ali, L. Le Jeune, H. Gerardo Munoz Hernandez, M. Veleski, B. Da Silva, J. Lemeire, K. Van Beeck and A. Touhafi, "AITIA: Embedded AI Techniques for Embedded Industrial Applications" In IEEE International Conference on Omni-layer Intelligent systems (COINS), IEEE, 7 pages, 2020. BibTex LaTex

35 [Conf article] T. Beyne, A. Canteaut, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo and F. Wiemer, "Out of Oddity -- New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems" In Advances in Cryptology - CRYPTO 2020, Lecture Notes in Computer Science 12171, D. Micciancio and T. Ristenpart (Eds.), Springer-Verlag, 30 pages, 2020. BibTex LaTex

36 [Conf article] C. Baum, E. Orsini, P. Scholl and E. Soria-Vazquez, "Efficient Constant-Round MPC with Identifiable Abort and Public Verifiability" In Advances in Cryptology - CRYPTO 2020, Lecture Notes in Computer Science 12171, D. Micciancio and T. Ristenpart (Eds.), Springer-Verlag, pp. 562-592, 2020. BibTex LaTex

37 [Conf article] W. Castryck, J. Sotakova and F. Vercauteren, "Breaking the decisional Diffie-Hellman problem for class group actions using genus theory" In Advances in Cryptology - CRYPTO 2020, Lecture Notes in Computer Science 12171, D. Micciancio and T. Ristenpart (Eds.), Springer-Verlag, pp. 92-120, 2020. BibTex LaTex

38 [Conf article] K. de Boer, L. Ducas, A. Pellet--Mary and B. Wesolowski, "Random Self-reducibility of Ideal-SVP via Arakelov Random Walks" In Advances in Cryptology - CRYPTO 2020, Lecture Notes in Computer Science 12171, D. Micciancio and T. Ristenpart (Eds.), Springer-Verlag, 36 pages, 2020. BibTex LaTex

39 [Conf article] T. Ashur and S. Dhooghe, "Prelude to Marvellous (With the Designers' Commentary, Two Bonus Tracks, and a Foretold Prophecy)" In The Conference for Failed Approaches and Insightful Losses in Cryptology 2020, N. Mouha (Ed.), 26 pages, 2020. PDF ▶ BibTex LaTex

40 [Conf article] C. Delpech de Saint Guilhem, M. Fischlin and B. Warinschi, "Authentication in Key-Exchange: Definitions, Relations and Composition" In 33 IEEE Computer Security Foundations Workshop (CSFW-33), IEEE, pp. 288-303, 2020. PDF BibTex LaTex

41 [Conf article] A. Beckers, M. Kinugawa, J. Balasch, Y. Hayashi and I. Verbauwhede, "Design and Evaluation of a Spark Gap Based EM-fault Injection Setup" In IEEE International Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity - IEEE EMC + SIPI 2020, ieee, 4 pages, 2020. PDF BibTex LaTex

42 [Conf article] G. Dessouky, P. Jauernig, N. Mentens, A. Sadeghi and E. Stapf, "INVITED: AI Utopia or Dystopia - On Securing AI Platforms" In 58 Design Automation Conference (DAC 2020), IEEE, 6 pages, 2020. BibTex LaTex

43 [Conf article] J. Bermudo Mera, F. Turan, A. Karmakar, S. Sinha Roy and I. Verbauwhede, "Compact domain-specific co-processor for accelerating module lattice-based KEM" In 58 Design Automation Conference (DAC 2020), IEEE, 6 pages, 2020. PDF BibTex LaTex

44 [Conf article] T. Ashur, C. Li, Y. Liu, J. Lu and B. Sun, "Rotational-XOR Cryptanalysis of Simon-like Block Ciphers" In Information Security and Privacy - 2020 Australasian Conference, ACISP 2020, Lecture Notes in Computer Science, H. Cui and J. Liu (Eds.), Springer-Verlag, pp. 105-124, 2020. PDF BibTex LaTex

45 [Conf article] I. Ben Guirat and D. Gosain, "Mixim: A General Purpose Simulator for mixnet" In 2020 Hot Topics in Privacy Enhancing Technologies (HotPETs 2020) , 3 pages, 2020. PDF BibTex LaTex

46 [Conf article] K. Baghery, A. González, Z. Pindado and C. Ràfols, "Signatures of Knowledge for Boolean Circuits under Standard Assumptions" In Progress in Cryptology - AFRICACRYPT 2020, Lecture Notes in Computer Science 12174), A. Nitaj and A. Youssef (Eds.), Springer-Verlag, pp. 24-44, 2020. PDF BibTex LaTex

47 [Conf article] W. Castryck and F. Vermeulen, "Lifting low-gonal curves for use in Tuitman's algorithm" In Algorithmic Number Theory, 14 International Symposium, ANTS 2020, Lecture Notes in Computer Science MSP Open Book Series 4, Springer-Verlag, pp. 109-125, 2020. PDF ▶ BibTex LaTex

48 [Conf article] D. Cozzo and N. Smart, "Sashimi: Cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol" In Post-Quantum Cryptography, Lecture Notes in Computer Science 12100, A. Joux and N. Sendrier (Eds.), Springer-Verlag, 18 pages, 2020. PDF BibTex LaTex

49 [Conf article] W. Castryck and T. Decru, "CSIDH on the surface" In Post-Quantum Cryptography, Lecture Notes in Computer Science 12100, A. Joux and N. Sendrier (Eds.), Springer-Verlag, pp. 111-129, 2020. PDF ▶ BibTex LaTex

50 [Conf article] W. Beullens and C. Delpech de Saint Guilhem, "LegRoast: Efficient post-quantum signatures from the Legendre PRF" In Post-Quantum Cryptography, Lecture Notes in Computer Science 12100, A. Joux and N. Sendrier (Eds.), Springer-Verlag, 21 pages, 2020. PDF ▶ BibTex LaTex

51 [Conf article] H. Chen, I. Chillotti, Y. Dong, O. Poburinnaya, I. Razenshteyn and M. Sadegh Riazi, "SANNS: Scaling Up Secure Approximate k-Nearest Neighbors Search" In 2020 USENIX Security Symposium 2020, Usenix, 18 pages, 2020. PDF BibTex LaTex

52 [Conf article] M. Montakhabi, F. Zobiri, S. Van der Graaf, G. Deconinck, D. Orlando, S. Vanhove, R. Callaerts and M. Mustafa, "New Roles in Peer-to-Peer Electricity Markets: Value Network Analysis" In International Energy Conference - ENERGYCon 2020, IEEE, 6 pages, 2020. PDF BibTex LaTex

53 [Conf article] Y. Gao, V. Reniers, R. Zhang, P. Viviani, A. Madhusudan, B. Lagaisse, S. Petkova-Nikova, D. Van Landuyt, W. Joosen, R. Lombardi and B. Preneel, "Authenticated and Auditable Data Sharing via Smart Contract" In Proceedings of the 2020 ACM Symposium on Applied Computing, ACM, 8 pages, 2020. PDF BibTex LaTex

54 [Conf article] M. Garcia-Constantino, A. Konios, M. Mustafa, G. Morrison and C. Nugent, "Ambient and Wearable BibTex

Sensor Fusion for Abnormal Behaviour Detection in Activities of Daily Living" In PerCom Workshop on Pervasive Health Technologies, IEEE, 7 pages, 2020. LaTex

55 [Conf article] A. Abidin, S. Vanhove, F. Zobiri, R. Callaerts, G. Deconinck, S. Van der Graaf, A. Madhusudan, M. Montakhabi, M. Mustafa, S. Petkova-Nikova, D. Orlando and J. Schroers, "Poster: SNIPPET - Secure and Privacy-Friendly Peer-to-Peer Electricity Trading" In Network and Distributed System Security Symposium (NDSS 2020), Internet Society, 2 pages, 2020. BibTex LaTex

56 [Conf article] S. Siby, M. Juarez Miro, C. Diaz, C. Troncoso and N. Vallina-Rodriguez, "Encrypted DNS --> Privacy? A Traffic Analysis Perspective" In Network and Distributed System Security Symposium (NDSS 2020), Internet Society, 18 pages, 2020. BibTex LaTex

57 [Conf article] A. Beckers, M. Kinugawa, D. Fujimoto, Y. Hayashi, J. Balasch, B. Gierlichs and I. Verbauwhede, "Design Considerations for EM Pulse Fault Injection" In Smart Card Research and Advanced Applications - CARDIS 2019, Lecture Notes in Computer Science 11833, S. Belaïd and T. Guneysu (Eds.), Springer-Verlag, pp. 176-192, 2020. BibTex LaTex

58 [Conf article] D. Sijacic, J. Balasch and I. Verbauwhede, "Sweeping for Leakage in Masked Circuit Layouts" In Design, Automation and Test in Europe, IEEE, 6 pages, 2020. BibTex LaTex

59 [Conf article] M. Alam, A. Singh, S. Bhattacharya, D. Mukhopadhyay and K. Pratihar, "In-situ Extraction of Randomness from Computer Architecture Through Hardware Performance Counters." In Smart Card Research and Advanced Applications - CARDIS 2019, Lecture Notes in Computer Science 11833, S. Belaïd and T. Guneysu (Eds.), Springer-Verlag, 17 pages, 2020. BibTex LaTex

60 [Conf article] A. Chakraborty, S. Bhattacharya, S. Saha and D. Mukhopadhyay, "EXPLFRAME: EXPLOITING PAGE FRAME CACHE FOR FAULT ANALYSIS OF BLOCK CIPHERS" In Design, Automation and Test in Europe, IEEE, 4 pages, 2020. BibTex LaTex

61 [Conf article] D. Bozilov, M. Knežević and V. Nikov, "Optimized Threshold Implementations: Minimizing the Latency of Secure Cryptographic Accelerators" In Smart Card Research and Advanced Applications - CARDIS 2019, Lecture Notes in Computer Science 11833, S. Belaïd and T. Guneysu (Eds.), Springer-Verlag, pp. 20-39, 2020. BibTex LaTex

62 [Conf article] M. Montakhabi, A. Madhusudan, S. Van der Graaf, A. Abidin and M. Mustafa, "Sharing Economy in Future Electricity Markets: Security and Privacy Analysis" In Workshop on Decentralized IoT Systems and Security (DISS) 2020, co-located with NDSS 2020 , Internet Society, 6 pages, 2020. BibTex LaTex

63 [Conf article] S. Agrawal and A. Pellet--Mary, "Indistinguishability Obfuscation Without Maps: Attacks and Fixes for Noisy Linear FE" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, 30 pages, 2020. BibTex LaTex

64 [Conf article] L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru and M. Schofnegger, "On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, 57 pages, 2020. BibTex LaTex

65 [Conf article] J. D'Anvers, M. Rossi and F. Virdia, "(One) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, 33 pages, 2020. BibTex LaTex

66 [Conf article] W. Beullens, "Sigma protocols for MQ, PKP and SIS, and fishy signature schemes" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, 30 pages, 2020. BibTex LaTex

67 [Conf article] W. Castryck, L. Panny and F. Vercauteren, "Rational isogenies from irrational endomorphisms" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, pp. 523-548, 2020. BibTex LaTex

68 [Conf article] W. Zhang, "test" In Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science 12106, A. Canteaut and Y. Ishai (Eds.), Springer-Verlag, 8 pages, 2020. BibTex LaTex

69 [Journal article] A. Lemmens, "On syzygies of Segre embeddings of P^1 X P^1.", Communications in Algebra 48(12), pp. 1-20, 2020. BibTex LaTex

70 [Journal article] T. Ashur, S. Dhooghe and A. Szepieniec, "Rescue-Prime: a Standard Specification (SoK)", IACR Cryptology ePrint Archive 2020(1143), 16 pages, 2020. BibTex LaTex

71 [Journal article] T. Ashur, S. D'haeseleer, R. Posteuca and D. Sijacic, "Generalized Matsui Algorithm 1 with Application for the Full DES", Security and Communication Networks (2020), pp. 448-467, 2020. BibTex LaTex

72 [Journal article] W. Castryck, R. Cluckers, P. Dittmann and K. Nguyen, "The dimension growth conjecture, polynomial in the degree and without logarithmic factors", Algebra & Number Theory 14(8), pp. 2261-2294, 2020. BibTex LaTex

73 [Journal article] A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe and A. Szepieniec, "Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols", IACR Transactions on Symmetric Cryptology 2020(3), pp. 1-45, 2020. BibTex LaTex

74 [Journal article] T. Beyne and C. Li, "Cryptanalysis of the MALICIOUS Framework", IACR Cryptology ePrint Archive 2020(1032), 6 pages, 2020. BibTex LaTex

75 [Journal article] F. Turan and I. Verbauwhede, "Trust in FPGA-accelerated Cloud Computing", ACM Computing Surveys 53(6), 28 pages, 2020. BibTex LaTex

76 [Journal article] P. Socha, J. Brejnik, J. Balasch, M. Novotny and N. Mentens, "Side-channel countermeasures utilizing dynamic logic reconfiguration: Protecting AES/Rijndael and Serpent encryption in hardware", Microprocessors and Microsystems (78), pp. 103208:1-10, 2020. BibTex LaTex

77 [Journal article] Y. Liu, W. Zhang, B. Sun, V. Rijmen, G. Liu, C. Li, S. Fu and M. Cao, "The phantom of differential characteristics", Designs, Codes and Cryptography 88(11), pp. 2289 - 2311, 2020. BibTex LaTex

78 [Journal article] T. Beyne, A. Canteaut, G. Leander, M. Naya-Plasencia, L. Perrin and F. Wiemer, "Report on the security of the Rescue hash function", IACR Cryptology ePrint Archive 2020(820), 32 pages, 2020. BibTex LaTex

79 [Journal article] T. Beyne, "Block Cipher Invariants as Eigenvectors of Correlation Matrices", Journal of Cryptology 33(3), 28 pages, 2020. BibTex LaTex

80 [Journal article] F. Turan and I. Verbauwhede, "Proxy Re-Encryption for Accelerator Confidentiality in FPGA-Accelerated Cloud", IACR Cryptology ePrint Archive 2020(805), 5 pages, 2020. BibTex LaTex

81 [Journal article] T. Beyne, Y. Chen, C. Dobraunig and B. Mennink, "Dumbo, Jumbo, and Delirium: Parallel Authenticated Encryption for the Lightweight Circus", IACR Transactions on Symmetric Cryptology 2020(Special Issue 1), pp. 5-30, 2020. BibTex LaTex

82 [Journal article] D. Sijacic, J. Balasch, B. Yang, S. Ghosh and I. Verbauwhede, "Towards efficient and automated side-channel evaluations at design time", Journal of Cryptographic Engineering 10(3), pp. 305-319, 2020. BibTex LaTex

83 [Journal article] C. Bootland, W. Castryck, I. Iliashenko and F. Vercauteren, "Efficiently Processing Complex-Valued Data in Homomorphic Encryption", Journal of Mathematical Cryptology 14(1), pp. 55-65, 2020. BibTex LaTex

84 [Journal article] M. Tiepelt and J. D'Anvers, " Exploiting Decryption Failures in Mersenne Number Cryptosystems", ACM ASIA Public-Key Cryptography Workshop (7), 11 pages, 2020. BibTex LaTex

85 [Journal article] A. Abidin, "On detecting relay attacks on RFID systems using qubits", Cryptography 4(2), 12 pages, 2020. BibTex LaTex

86

[Journal article] W. Beullens, T. Beyne, A. Udovenko and G. Vitto, "Cryptanalysis of the Legendre PRF and Generalizations", IACR Transactions on Symmetric Cryptology 2020(1), 18 pages, 2020. BibTex LaTex

87 [Journal article] B. Bilgin, L. De Meyer, S. Duval, I. Levi and F. Standaert, "Low AND Depth and Efficient Inverses: a Guide on S-boxes for Low-latency Masking", IACR Transactions on Symmetric Cryptology 2020(1), pp. 143-184, 2020. BibTex LaTex

88 [Journal article] S. Bhattacharya, C. Maurice, S. Bhasin and D. Mukhopadhyay, "Branch Prediction Attack on Blinded Scalar Multiplication", IEEE Transactions on Computers 69(5), 16 pages, 2020. BibTex LaTex

89 [Journal article] F. Turan, S. Sinha Roy and I. Verbauwhede, "HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA", IEEE Transactions on Computers 69(8), 12 pages, 2020. BibTex LaTex

90 [Journal article] L. Wouters, V. Arribas Abril, B. Gierlichs and B. Preneel, "Revisiting a Methodology for Efficient CNN Architectures in Profiling Attacks", IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(3), pp. 147-168, 2020. BibTex LaTex

91 [Journal article] M. Tiepelt and J. D'Anvers, "Exploiting Decryption Failures in Mersenne Number Cryptosystems", IACR Cryptology ePrint Archive 2020(367), 11 pages, 2020. BibTex LaTex

92 [Journal article] J. Tetu, L. Trudeau, M. Van Beirendonck, A. Balatsoukas-Stimming and P. Giard, "A Standalone FPGA-Based Miner for Lyra2REv2 Cryptocurrencies", IEEE Transactions on Circuits and Systems I: Regular Papers 67(4), pp. 1194 - 1206, 2020. BibTex LaTex

93 [Journal article] M. Labafniya, S. Picek, S. Etemadi Borujeni and N. Mentens, "On the feasibility of using evolvable hardware for hardware trojan detection and prevention", Applied Soft Computing (92), 11 pages, 2020. BibTex LaTex

94 [Journal article] I. Chillotti, N. Gama, M. Georgieva and M. Izabachene, "TFHE: Fast Fully Homomorphic Encryption Over the Torus", Journal of Cryptology 33(1), pp. 34-91, 2020. BibTex LaTex

95 [Journal article] J. Bermudo Mera, F. Turan, A. Karmakar, S. Sinha Roy and I. Verbauwhede, " Compact domain-specific co-processor for accelerating module lattice-based key encapsulation mechanism", IACR Cryptology ePrint Archive 2020(321), 15 pages, 2020. BibTex LaTex

96 [Journal article] L. Wouters, J. Van den Herrewegen, F. Garcia, D. Oswald, B. Gierlichs and B. Preneel, "Dismantling DST80-based Immobiliser Systems", IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(2), pp. 99-127, 2020. BibTex LaTex

97 [Journal article] J. Bermudo Mera, A. Karmakar and I. Verbauwhede, " Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography", IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(2), 23 pages, 2020. BibTex LaTex

98 [Journal article] D. Yuxing Huang, N. Apthorpe, F. Li, G. Acar and N. Feamster, "IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 4(2), 14 pages, 2020. BibTex LaTex

99 [Journal article] Y. Hao, L. Jiao, C. Li, W. Meier, Y. Todo and Q. Wang, "Links between Division Property and Other Cube Attack Variants", IACR Transactions on Symmetric Cryptology 2020(1), 363–395 pages, 2020. BibTex LaTex

100 [Journal article] R. Posteuca, "Related-key Differential Slide Attack Against Fountain V1", PROCEEDINGS OF THE ROMANIAN ACADEMY SERIES A-MATHEMATICS PHYSICS TECHNICAL SCIENCES INFORMATION SCIENCE 21(1), pp. 61 - 68, 2020. BibTex LaTex

101 [Journal article] A. Szepieniec and T. Ashur, "EAGLESONG: An ARX Hash With Fast Diffusion ", PROCEEDINGS OF THE ROMANIAN ACADEMY SERIES A-MATHEMATICS PHYSICS TECHNICAL SCIENCES INFORMATION SCIENCE 21(1), pp. 69-76, 2020. BibTex LaTex

102 [Journal article] G. Acar, S. Englehardt and A. Narayanan, "No boundaries: data exfiltration by third parties BibTex

embedded on web pages", Proceedings on Privacy Enhancing Technologies 2020(4), 19 pages, 2020. LaTex

103 [Journal article] J. Bermudo Mera, A. Karmakar and I. Verbauwhede, " Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography", IACR Cryptology ePrint Archive 2020(268), 23 pages, 2020. BibTex LaTex

104 [Journal article] T. Ashur, T. Beyne and V. Rijmen, "Revisiting the Wrong-Key-Randomization Hypothesis", Journal of Cryptology 33(2), pp. 567-594, 2020. BibTex LaTex

105 [Journal article] F. Wegener, L. De Meyer and A. Moradi, "Spin Me Right Round Rotational Symmetry for FPGA-Specific AES: Extended Version", Journal of Cryptography 33(3), pp. 1114-1155, 2020. BibTex LaTex

106 [Journal article] W. Castryck, F. Cools, J. Demeyer and A. Lemmens, "Canonical syzygies of smooth curves on toric surfaces", Journal of Pure and Applied Algebra 224(2), pp. 507-527, 2020. BibTex LaTex

107 [Journal article] W. Castryck, T. Decru and B. Smith, "Hash functions from superspecial genus-2 curves using Richelot isogenies", Journal of Mathematical Cryptology 14(1), pp. 268-292, 2020. BibTex LaTex

108 [Journal article] M. Sakalli, S. Akleylek, K. Akkanat and V. Rijmen, "On the automorphisms and isomorphisms of MDS matrices and their efficient implementations", Turkish Journal of Electrical Engineering & Computer Sciences 28(1), pp. 275-287, 2020. BibTex LaTex

109 [Journal article] J. Byszewski, G. Cornelissen and M. Houben, "Dynamically affine maps in positive characteristic", Contemporary Mathematics 744(<empty>), 31 pages, 2020. BibTex LaTex

110 [Thesis] D. Sijacic, "Design Time Evaluation of Side-Channel Attack Resistant Cryptographic Implementations", Phd thesis, KU Leuven, J. Balasch and I. Verbauwhede, pp. 1-180, 2020. BibTex LaTex

111 [Thesis] L. De Meyer, "Cryptography in the Presence of Physical Attacks: Design, Implementation and Analysis", Phd thesis, KU Leuven, B. Bilgin and V. Rijmen, 298 pages, 2020. BibTex LaTex

112 [Thesis] F. Theuns, "Lowering the decryption failure rate of R-LWE based cryptography", Master thesis, KU Leuven, I. Verbauwhede and F. Vercauteren, 72 pages, 2020. BibTex LaTex

113 [Thesis] K. Baghery, "Reducing trust and improving security in zk-SNARKs and commitments", Phd thesis, University of Tartu, H. Lipmaa, pp. 1-245, 2020. BibTex LaTex

114 [Thesis] S. Batsleer, "Breaking Post-Quantum Encryption using Decryption Failures", Master thesis, KU Leuven, I. Verbauwhede and F. Vercauteren, 83 pages, 2020. BibTex LaTex

115 [Thesis] D. De Troch, "dPACE, a decentralized Privacy-preserving, yet Accountable Car sharing Environment", Master thesis, KU Leuven, B. Preneel, 117 pages, 2020. BibTex LaTex

116 [Thesis] M. Wera, J. Bermudo Mera, A. Karmakar and F. Turan, "A compact HW-SW codesign of NTRU KEM", Master thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 58 pages, 2020. BibTex LaTex

117 [Thesis] S. Kundu, A. Karmakar and J. Bermudo Mera, "Examining Various Implementation and Design Choices of LWR based KEM", Master thesis, Indian Statistical Institute, B. Preneel and B. Roy, 68 pages, 2020. BibTex LaTex

118 [Thesis] E. Karagiannakou, "Best of Both Worlds: Prime Field PGV Constructions", Master thesis, KU Leuven, B. Preneel, pp. 1-54, 2020. BibTex LaTex

119 [Thesis] A. Bel Ventosa, J. Bermudo Mera, A. Karmakar and F. Turan, "Secure IoT for the future", Bachelor thesis, Katholieke Universiteit Leuven, E. Pallares and I. Verbauwhede, 46 pages, 2020. BibTex LaTex

120 [Thesis] A. Karmakar, "Design and implementation aspects of post-quantum cryptography", Phd thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 152 pages, 2020. BibTex LaTex

121 [Thesis] Z. Zheng, A. Karmakar and J. Bermudo Mera, "Encrypted Cloud using GPUs", Master thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 48 pages, 2020. BibTex LaTex

122 [Thesis] A. Deprez, E. Andreeva, J. Bermudo Mera, A. Karmakar and A. Purnal, "Optimized software implementations for lightweight authentication schemes", Master thesis, Katholieke Universiteit Leuven, B. Preneel and I. Verbauwhede, 100 pages, 2020. PDF BibTex LaTex

123 [Thesis] S. De Figueiredo, "Comparing peer-to-peer storage solutions", Master thesis, KU Leuven, B. Preneel, pp. 1-61, 2020. PDF BibTex LaTex

124 [Thesis] A. De Volder, "Comparing blockchain-based peer-to-peer storage solutions", Master thesis, KU Leuven, B. Preneel, pp. 1-120, 2020. PDF BibTex LaTex

125 [Thesis] V. Arribas Abril, "Design and Verification of Side-Channel and Fault Attacks Countermeasures", Phd thesis, Katholieke Universiteit Leuven, S. Petkova-Nikova and V. Rijmen, 248 pages, 2020. PDF BibTex LaTex

126 [Thesis] J. Winderickx, "Energy-efficient and secure implementations for the IoT", Phd thesis, KU Leuven, N. Mentens and D. Singelée, pp. 1-190, 2020. PDF BibTex LaTex

127 [Thesis] K. Chuang, "Highly Reliable Physically Unclonable Functions: Design, characterization and security analysis", Phd thesis, Katholieke Universiteit Leuven, I. Verbauwhede, 148 pages, 2020. PDF BibTex LaTex

128 [Thesis] C. Li, "New Methods for Symmetric Cryptography", Phd thesis, Katholieke Universiteit Leuven, B. Preneel, 292 pages, 2020. PDF BibTex LaTex

129 [Proceeding] "Progress in Cryptology - INDOCRYPT 2020", Lecture Notes in Computer Science 12578, K. Bhargavan, E. Oswald and M. Prabhakaran (Eds.), Springer-Verlag, 2020. BibTex LaTex

130 [Proceeding] "The Conference for Failed Approaches and Insightful Losses in Cryptology 2020", N. Mouha (Ed.), 2020. BibTex LaTex

131 [Book] J. Daemen and V. Rijmen, "The Design of Rijndael: The Advanced Encryption Standard (AES)", Springer-Verlag, 298 pages, 2020. BibTex LaTex

132 [Report] J. Pilet, B. Preneel, S. Erzeel, O. Pereira, F. Sbaraglia, A. Tibbaut, X. Carpent and R. Dandoy, "Studie over de mogelijkheid om online stemmen in België in te voeren (luik 1)", Report for PROJECT NETVOTING_BE, pp. 1-177, 2020. PDF BibTex LaTex

133 [Report] J. Pilet, B. Preneel, S. Erzeel, O. Pereira, F. Sbaraglia, A. Tibbaut, X. Carpent and R. Dandoy, "Étude sur la possibilité d'introduire le vote Internet en Belgique (1)", Report for PROJECT NETVOTING_BE, pp. 1-170, 2020. PDF BibTex LaTex

134 [Report] T. Ashur, G. Marshalko and G. Pradel, "Information technology — Non-repudiation — Part 1: General", ISO/IEC 13888-1:2020, 28 pages, 2020. BibTex LaTex

135 [Report] T. Ashur, G. Marshalko and G. Pradel, "Information technology — Non-repudiation — Part 3: Mechanisms using asymmetric techniques", ISO/IEC 13888-3:2020, 13 pages, 2020. BibTex LaTex

136 [Report] C. Troncoso, L. Barman, S. Chatel, K. Paterson, D. Basin, J. Beutel, D. Jackson, M. Roeschlin, P. Leu, B. Preneel, M. Payer, N. Smart, A. Abidin, S. Gürses, M. Veale, C. Cremers, M. Backes, N. Ole Tippenhauer, R. Binns, C. Cattuto, A. Barrat, J. Hubaux, D. Fiore, M. Barbosa, R. Oliveira, J. Pereira, M. Salathé, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis and D. Antonioli, "Decentralized Privacy-Preserving Proximity Tracing", Report, pp. 1-46, 2020. BibTex LaTex

137 [Report] C. Dupont, V. Cilli, E. Omersa, C. Borrett, M. Moulac, P. Vogiatzoglou and S. Petkova-Nikova, "Study on the retention of electronic communications non-content data for law enforcement purposes", Report, 268 pages, 2020. PDF BibTex LaTex

138 [Talk] B. Preneel, "Design and Deployment of Coronalert", Maatschappelijke waarden bij digitale innovatie: wie, wat en hoe? (KVAB), Online, 2020. ▶ BibTex LaTex

139 [Talk] C. Diaz, "Network-level privacy", Latin American Bitcoin & Blockchain Conference (LABITCONF BibTex

2020), Online, 2020. LaTex

140 [Talk] G. Deconinck, M. Mustafa, S. Petkova-Nikova, Y. Wang and F. Zobiri, "Peer-to-peer Energy Trading Without Revealing Sensitive Information", Annual INFORMS meeting, 2020. BibTex LaTex

141 [Talk] C. Diaz, "Anonymous communications: onion routing, mixnets, p2p networks", CYD Cyber-Defence Campus Conference, CH, 2020. BibTex LaTex

142 [Talk] B. Preneel, "Big data against corona: mass surveillance or privacy by design?", 17th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2020), Online, 2020. BibTex LaTex

143 [Talk] B. Preneel, "Middaggesprek 29 oktober 2020 - Onderzoek voor defensie II, met Bart Preneel en Luc De Vos", KU Leuven Metaforum, Leuven, BE, 2020. ▶ BibTex LaTex

144 [Talk] C. Diaz, "Why We Need Network-Level Privacy: P2P, Tor, and Mixnets", zkp & privacy summit, Online, 2020. BibTex LaTex

145 [Talk] C. Diaz, "Why We Need Network Level Privacy", The Magical Crypto Conference (MCC) 2021, Online, 2020. ▶ BibTex LaTex

146 [Talk] B. Preneel, "Cybersecurity: hoe veilig zijn onze industriële controlesystemen?", Cybersecurity, key in de industrie! (ONLINE event) - IE-net, Online, 2020. BibTex LaTex

147 [Talk] B. Preneel, "COVID-19 contact tracing: the usefulness of mobile apps", SAPHIRe online interactive workshop, Online, 2020. BibTex LaTex

148 [Talk] N. Smart, "Privacy-enhancing Technologies", IMA Mathematics 2020 Online Series, Online, 2020. BibTex LaTex

149 [Talk] B. Preneel, "Cyber Talk: Contact tracing apps: balancing public health and personal privacy", Cyber Security Coalition, Online, 2020. BibTex LaTex

150 [Talk] B. Preneel, "Cryptography for data protection and privacy", IPEN 2020 Online Workshop, Online, 2020. BibTex LaTex

151 [Talk] N. Mentens, "Invited talk at the High-Tech Women forum", High-Tech Women forum, DE, 2020. BibTex LaTex

152 [Patent] F. Turan, P. Koeberl, S. Schulz, A. Trivedi and S. Weber, "Scalable Runtime Validation for on-device Design Rule Checks", Patent number US2021110099, Intel Corporation , 2020. BibTex LaTex

153 [Patent] A. Peetermans, V. Rozic and I. Verbauwhede, " Random Number Generator ", Patent number US10761809B1, KU Leuven, 2020. PDF BibTex LaTex

2019

1 [Conf article] D. Cozzo and N. Smart, "Sharing the LUOV: Threshold Post-Quantum Signatures" In Cryptography and Coding, 17 IMA International Conference, Lecture Notes in Computer Science LNCS, Springer-Verlag, pp. 128-153, 2019. PDF BibTex LaTex

2 [Conf article] N. Smart and Y. Talibi Alaoui, "Distributing Any Elliptic Curve Based Protocol" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2019, Lecture Notes in Computer Science 11929 , M. Albrecht (Ed.), Springer-Verlag, pp. 342-366, 2019. PDF BibTex LaTex

3 [Conf article] K. Baghery, "Subversion-Resistant Simulation (Knowledge) Sound NIZKs" In Institute of Mathematics and its Applications International Conference on Cryptography and Coding 2019, Lecture Notes in Computer Science 11929 , M. Albrecht (Ed.), Springer-Verlag, 42–63 pages, 2019. BibTex LaTex

4 [Conf article] D. Rotaru and T. Wood, " MArBled Circuits: Mixing Arithmetic and Boolean Circuits with Active Security" In Progress in Cryptology - INDOCRYPT 2020, Lecture Notes in Computer Science 12578, K. BibTex LaTex

Bhargavan, E. Oswald and M. Prabhakaran (Eds.), Springer-Verlag, pp. 227-249, 2019.

5 [Conf article] W. Beullens, J. Faugere, E. Koussa, G. Macario-Rat, J. Patarin and L. Perret, "PKP-Based Signature Scheme" In Progress in Cryptology - INDOCRYPT 2020, Lecture Notes in Computer Science 12578, K. Bhargavan, E. Oswald and M. Prabhakaran (Eds.), Springer-Verlag, pp. 3-22, 2019. BibTex LaTex

6 [Conf article] E. Kavun, N. Mentens, J. Vliegen and T. Yalcin, "Efficient Utilization of DSPs and BRAMs Revisited: New AES-GCM Recipes on FPGAs" In 2019 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2019, IEEE Computer Society, 2 pages, 2019. BibTex LaTex

7 [Conf article] E. Andreeva, V. Lallemand, A. Purnal, R. Reyhanitabar, A. Roy and D. Vizár, "Forkcipher: a New Primitive for Authenticated Encryption of Very Short Messages" In Advances in Cryptology - ASIACRYPT 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 153-182, 2019. BibTex LaTex

8 [Conf article] W. Beullens, T. Kleinjung and F. Vercauteren, "CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations" In Advances in Cryptology - ASIACRYPT 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 227-247, 2019. BibTex LaTex

9 [Conf article] C. Lee, A. Pellet--Mary, D. Stehlé and A. Wallet, "An LLL Algorithm for Module Lattices" In Advances in Cryptology - ASIACRYPT 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 59-90, 2019. BibTex LaTex

10 [Conf article] H. Chen, I. Chillotti and Y. Song, "Multi-Key Homomophic Encryption from TFHE" In Advances in Cryptology - ASIACRYPT 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 446-472, 2019. BibTex LaTex

11 [Conf article] I. Verbauwhede and K. Chuang, "Security and Reliability - Friend or Foe?" In IEEE International Electron Devices Meeting, IEEE, pp. 13.4.1-13.4.4, 2019. BibTex LaTex

12 [Conf article] D. Bozilov, V. Nikov and V. Rijmen, "Design Trade-offs in Threshold Implementations" In International Conference on Electronics, Circuits, and Systems 2019, IEEE, pp. 751-754, 2019. BibTex LaTex

13 [Conf article] F. Goovaerts, G. Acar, R. Galvez, F. Piessens and M. Vanhoef, "Improving Privacy through Fast Passive Wi-Fi Scanning" In Proceedings of the 2019 Nordic Workshop on Secure Computer Systems (NORDSEC 2019) LNCS, 11875, A. Askarov and W. Rafnsson (Eds.), pp. 37-52, 2019. BibTex LaTex

14 [Conf article] E. Marín Fàbregas, N. Bucciol and M. Conti, "An In-depth Look Into SDN Topology Discovery Mechanisms: Novel Attacks and Practical Countermeasures" In ACM Conference on Computer and Communications Security - CCS 2019, J. Katz and X. Wang (Eds.), ACM, pp. 1101-1114, 2019. BibTex LaTex

15 [Conf article] H. Chen, I. Chillotti and L. Ren, "Onion Ring ORAM: Efficient Constant Bandwidth Oblivious RAM from (Leveled) TFHE" In ACM Conference on Computer and Communications Security - CCS 2019, J. Katz and X. Wang (Eds.), ACM, pp. 345-360, 2019. BibTex LaTex

16 [Conf article] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, N. Feamster, E. Felten, P. Mittal, A. Narayanan and D. Yuxing Huang, "Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices" In ACM Conference on Computer and Communications Security - CCS 2019, J. Katz and X. Wang (Eds.), ACM, pp. 131-147, 2019. BibTex LaTex

17 [Conf article] A. Aly, E. Orsini, D. Rotaru, N. Smart and T. Wood, "Zaphod: Efficiently Combining LSSS and Garbled Circuits in SCALE" In Workshop on Encrypted Computing and Applied Homomorphic Cryptography 2019, Association for Computing Machinery (ACM), pp. 33-44, 2019. BibTex LaTex

18 [Conf article] A. Mathur, G. Acar, M. Chetty, M. Friedman, E. Lucherini, J. Mayer and A. Narayanan, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" In Proceedings of the ACM on Human-Computer Interaction 3, ACM, pp. 81:1-81:32, 2019. BibTex LaTex

19 [Conf article] A. Purnal, E. Andreeva, A. Roy and D. Vizár, "What the Fork: Implementation Aspects of a Forkcipher" In NIST Lightweight Cryptography Workshop 2019, 12 pages, 2019. BibTex LaTex

20 [Conf article] T. Yoshizawa, S. Backia Mary Baskaran and A. Kunz, "Overview of 5G URLLC System and Security Aspects in 3GPP" In IEEE Conference on Standards for Communications and Networking, J. Lopez-Soler and T. Taleb (Eds.), 5 pages, 2019. PDF BibTex LaTex

21 [Conf article] T. Yoshizawa and B. Preneel, "Survey of Security Aspects of V2X Standards and Related Issues" In IEEE Conference on Standards for Communications and Networking, J. Lopez-Soler and T. Taleb (Eds.), 5 pages, 2019. PDF BibTex LaTex

22 [Conf article] F. Turan and I. Verbauwhede, "Propagating Trusted Execution through Mutual Attestation" In Workshop on System Software for Trusted Execution, ACM, 6 pages, 2019. PDF BibTex LaTex

23 [Conf article] J. Winderickx, P. Bellier, P. Duflot, D. Coppieters and N. Mentens, "Communication and security trade-offs for wearable medical sensor systems in hospitals" In Proceedings of the International Conference on Embedded Software - EMSOFT 2019, IEEE Press, 2 pages, 2019. PDF BibTex LaTex

24 [Conf article] S. Atapoor and K. Baghery, "Simulation Extractability in Groth's zk-SNARK" In European Symposium on Research in Computer Security - ESORICS 2019, Lecture Notes in Computer Science 11737, A. Biryukov, C. Pérez Solà, J. Garcia-Alfaro and G. Navarro-Arribas (Eds.), Springer-Verlag, 336–354 pages, 2019. PDF BibTex LaTex

25 [Conf article] A. Abidin, A. Aly and M. Mustafa, "Collaborative Authentication using Threshold Cryptography" In Emerging Technologies for Authorization and Authentication, 18 pages pages, 2019. PDF BibTex LaTex

26 [Conf article] O. Alhawi, M. Mustafa and L. Cordeiro, "Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification" In International Workshop on Secure Internet of Things (SIoT) 2019, IEEE, 17 pages, 2019. PDF BibTex LaTex

27 [Conf article] A. Peetermans, V. Rozic and I. Verbauwhede, "A Highly-Portable True Random Number Generator based on Coherent Sampling" In International Conference on Field Programmable Logic and Applications (FPL 2019), IEEE Computer Society, IEEE, 7 pages, 2019. PDF BibTex LaTex

28 [Conf article] V. Arribas Abril, "Beyond the Limits: SHA-3 in Just 49 Slices" In International Conference on Field Programmable Logic and Applications (FPL 2019), IEEE Computer Society, IEEE, 6 pages, 2019. PDF BibTex LaTex

29 [Conf article] P. Socha, J. Brejnik, S. Jerabek, M. Novotny and N. Mentens, "Dynamic Logic Reconfiguration Based Side-Channel Protection of AES and Serpent" In DSD, IEEE Computer Society, IEEE, pp. 277-282, 2019. PDF BibTex LaTex

30 [Conf article] N. Mentens, J. Genoe, T. Vandenabeele, L. Verschueren, D. Smets, W. Dehaene and K. Myny, "Security on Plastics: Fake or Real?" In Cryptographic Hardware and Embedded Systems - CHES 2019, Lecture Notes in Computer Science 2019 (4), Springer-Verlag, pp. 1-16, 2019. PDF BibTex LaTex

31 [Conf article] A. Konios, M. Garcia-Constantino, S. Christopoulos, M. Mustafa, I. Ekerete, C. Shewell, C. Nugent and G. Morrison, "Probabilistic Analysis of Temporal and Sequential Aspects of Activities of Daily Living for Abnormal Behaviour Detection" In International Conference on Ubiquitous Intelligence and Computing, IEEE, 8 pages, 2019. PDF BibTex LaTex

32 [Conf article] D. Shi, S. Sun, Y. Sasaki, C. Li and L. Hu, " Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS" In Advances in Cryptology - CRYPTO 2019, Lecture Notes in Computer Science, Springer-Verlag, 31+73 pages, 2019. PDF BibTex LaTex

33 [Conf article] Y. Chen, E. Lambooij and B. Mennink, "How to Build Pseudorandom Functions From Public Random Permutations" In Advances in Cryptology - CRYPTO 2019, Lecture Notes in Computer Science, Springer-Verlag, 27 pages, 2019. PDF BibTex LaTex

34 [Conf article] A. Szepieniec and B. Preneel, "Block-Anti-Circulant Unbalanced Oil and Vinegar" In Selected Areas in Cryptography, 26 Annual International Workshop, SAC 2019, Lecture Notes in Computer Science, K. Paterson and D. Stebila (Eds.), Springer-Verlag, pp. 0-0, 2019. PDF BibTex LaTex

35 [Conf article] C. Li and B. Preneel, "Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree" In Selected Areas in Cryptography, 26 Annual International Workshop, SAC 2019, Lecture Notes in Computer Science, K. Paterson and D. Stebila (Eds.), Springer-Verlag, 22 pages, 2019.

BibTex LaTex

36 [Conf article] L. De Meyer, C. Delpech de Saint Guilhem, E. Orsini and N. Smart, "BBQ: Using AES in Picnic Signatures" In Selected Areas in Cryptography, 26 Annual International Workshop, SAC 2019, Lecture Notes in Computer Science, K. Paterson and D. Stebila (Eds.), Springer-Verlag, 24 pages, 2019.

BibTex LaTex

37 [Conf article] C. Baum, D. Cozzo and N. Smart, "Using TopGear in Overdrive: a more efficient ZKPoK for SPDZ" In Selected Areas in Cryptography, 26 Annual International Workshop, SAC 2019, Lecture Notes in Computer Science, K. Paterson and D. Stebila (Eds.), Springer-Verlag, 28 pages, 2019.

BibTex LaTex

38 [Conf article] Y. Lu, A. Purnal, S. Vandenhende, C. Lee, I. Verbauwhede and H. Chang, "A Lightweight 1.16 pJ/bit Processor for the Authenticated Encryption Scheme KetjeSR" In 2019 International Symposium on VLSI Design, Automation and Test , IEEE, 4 pages, 2019.

BibTex LaTex

39 [Conf article] J. Cartlidge, N. Smart and Y. Talibi Alaoui, "MPC Joins The Dark Side" In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (ASIACCS 2019), Association for Computing Machinery (ACM), ACM, pp. 148-159 , 2019.

BibTex LaTex

40 [Conf article] M. Kraitsberg, Y. Lindell, V. Osheter, N. Smart and Y. Talibi Alaoui, "Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme" In Information Security and Privacy - 2019 Australasian Conference, ACISP 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 192-210, 2019.

BibTex LaTex

41 [Conf article] K. Baghery, "On the Efficiency of Privacy-Preserving Smart Contract Systems" In Progress in Cryptology - AFRICACRYPT 2019, Lecture Notes in Computer Science 11627, J. Buchmann, A. Nitaj and T. Rachidi (Eds.), Springer-Verlag, 118–136 pages, 2019.

BibTex LaTex

42 [Conf article] B. Abdolmaleki, K. Baghery, H. Lipmaa, J. Siim and M. Zajac, "UC-Secure CRS Generation for SNARKs" In Progress in Cryptology - AFRICACRYPT 2019, Lecture Notes in Computer Science 11627, J. Buchmann, A. Nitaj and T. Rachidi (Eds.), Springer-Verlag, 99–117 pages, 2019.

BibTex LaTex

43 [Conf article] C. Bootland, W. Castryck, A. Szepieniec and F. Vercauteren, "A Framework for Cryptographic Problems from Linear Algebra" In Number Theoretic Methods in Cryptology 2019, Journal of Mathematical Cryptology special issue JMC , De Gruyter, 23 pages, 2019.

BibTex LaTex

44 [Conf article] A. Aly and N. Smart, "Benchmarking Privacy Preserving Scientific Operations" In Applied Cryptography and Network Security - ACNS 2019, Lecture Notes in Computer Science 11464, R. Deng and M. Yung (Eds.), Springer-Verlag, 20 pages, 2019.

BibTex LaTex

45 [Conf article] B. Abdolmaleki, K. Baghery, H. Lipmaa, J. Siim and M. Zajac, "DL-Extractable UC-Commitment Schemes" In Applied Cryptography and Network Security - ACNS 2019, Lecture Notes in Computer Science 11464, R. Deng and M. Yung (Eds.), Springer-Verlag, 385–405 pages, 2019.

BibTex LaTex

46 [Conf article] E. Marín Fàbregas, E. Argones Rúa, D. Singelée and B. Preneel, "On the Difficulty of Using Patients Physiological Signals in Cryptographic Protocols" In 2019 ACM Symposium on Access Control Models and Technologies , Association for Computing Machinery (ACM), ACM, 11 pages, 2019.

BibTex LaTex

47 [Conf article] A. Beckers, J. Balasch, B. Gierlichs, I. Verbauwhede, S. Osuka, M. Kinugawa, D. Fujimoto and Y. Hayashi, "Characterization of EM faults on ATmega328p" In Joint IEEE International Symposium on Electromagnetic Compatibility (EMC) / IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC), 4 pages, 2019.

BibTex LaTex

48 [Conf article] A. Karmakar, S. Sinha Roy, O. Reparaz, F. Vercauteren and I. Verbauwhede, "Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on Falcon." In 2019 Design Automation Conference (DAC 2019), IEEE, 16 pages, 2019.

BibTex LaTex

49 [Conf article] M. Grujic, V. Rozic, D. Johnston, J. Kelsey and I. Verbauwhede, "Design Principles for True Random Number Generators for Security Applications (invited)" In 2019 Design Automation Conference (DAC 2019), IEEE, 3 pages, 2019. BibTex LaTex

50 [Conf article] L. Batina, P. Jauernig, N. Mentens, A. Sadeghi and E. Stapf, "INVITED: In Hardware We Trust: Gains and Pains of Hardware-assisted Security." In 2019 Design Automation Conference (DAC 2019), IEEE, pp. 441-444, 2019. BibTex LaTex

51 [Conf article] I. Symeonidis, J. Schroers, M. Mustafa and G. Biczok, "Towards Systematic Specification of Non-Functional Requirements for Sharing Economy Services" In International Workshop on Smart Circular Economy, IEEE, 7 pages, 2019. BibTex LaTex

52 [Conf article] M. Van Beirendonck, L. Trudeau, P. Giard and A. Balatsoukas-Stimming, "A Lyra2 FPGA Core for Lyra2REv2-Based Cryptocurrencies" In IEEE International Symposium on Circuits and Systems (ISCAS 2019), IEEE, 5 pages, 2019. BibTex LaTex

53 [Conf article] R. Zhang and B. Preneel, "Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security" In IEEE Symposium on Security and Privacy (SP 2019), IEEE, 13 pages, 2019. BibTex LaTex

54 [Conf article] T. Ashur, O. Dunkelman and N. Masalha, "Linear Cryptanalysis Reduced Round of Piccolo-80" In The 8th International Symposium on Cyber Security, Cryptology and Machine Learning, Lecture Notes in Computer Science, Springer-Verlag, pp. 16-32, 2019. BibTex LaTex

55 [Conf article] H. Chen, I. Chillotti and Y. Song, "Improved Bootstrapping for Approximate Homomorphic Encryption" In Advances in Cryptology - EUROCRYPT 2019, Lecture Notes in Computer Science 11477, Y. Ishai and V. Rijmen (Eds.), Springer-Verlag, pp. 34-54, 2019. BibTex LaTex

56 [Conf article] G. Hanrot, A. Pellet--Mary and D. Stehlé, "Approx-SVP in ideal lattices with pre-processing" In Advances in Cryptology - EUROCRYPT 2019, Lecture Notes in Computer Science 11477, Y. Ishai and V. Rijmen (Eds.), Springer-Verlag, 30 pages, 2019. BibTex LaTex

57 [Conf article] A. Abidin, "Quantum Distance Bounding" In Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM, 6 pages, 2019. BibTex LaTex

58 [Conf article] T. Decru, L. Panny and F. Vercauteren, "Faster SeaSign signatures through improved rejection sampling" In Post-Quantum Cryptography, Lecture Notes in Computer Science, Springer-Verlag, pp. 271-285, 2019. BibTex LaTex

59 [Conf article] J. D'Anvers, I. Verbauwhede and F. Vercauteren, "The impact of error dependencies on Ring/Mod-LWE/LWR based schemes" In Post-Quantum Cryptography, Lecture Notes in Computer Science, Springer-Verlag, 12 pages, 2019. BibTex LaTex

60 [Conf article] S. Dhooghe and S. Petkova-Nikova, "My Gadget Just Cares For Me - How NINA Can Prove Security Against Combined Attacks" In Topics in Cryptology - CT-RSA 2019, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 11405, M. Matsui (Ed.), Springer-Verlag, 38 pages, 2019. BibTex LaTex

61 [Conf article] J. D'Anvers, Q. Guo, T. Johansson, A. Nilsson, I. Verbauwhede and F. Vercauteren, "Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes" In Public Key Cryptography, 22 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2019, Lecture Notes in Computer Science, Springer-Verlag, 35 pages, 2019. BibTex LaTex

62 [Conf article] W. Beullens and H. Wee, "Obfuscating Simple Functionalities from Knowledge assumptions" In Public Key Cryptography, 22 IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2019, Lecture Notes in Computer Science, Springer-Verlag, pp. 254 - 283, 2019. BibTex LaTex

63 [Conf article] T. Ashur, S. Cancela, J. David Calle, I. Fernandez-Hernandez, V. Rijmen and C. Sarto, "Toward an Operational Navigation Message Authentication Service: Proposal and Justification of Additional OSNMA Protocol Features" In European Navigation Conference 2019, 6 pages, 2019. BibTex LaTex

64 [Conf article] A. Purnal, V. Arribas Abril and L. De Meyer, "Trade-offs in Protecting Keccak against Combined Side-channel and Fault Attacks" In Workshop on Constructive Side-Channel Analysis and Secure Design 2019, Lecture Notes in Computer Science, Springer-Verlag, 18 pages, 2019. PDF BibTex LaTex

65 [Conf article] J. Vliegen, M. Rabbani, M. Conti and N. Mentens, "SACHa: Self-Attestation of Configurable Hardware" In Design, Automation and Test in Europe, IEEE, pp. 746-751, 2019. PDF BibTex LaTex

66 [Conf article] D. Shanmugasundaram Veeraraghavan, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede, "An In-depth and Black-Box Characterization of the Effects of Laser Pulses on ATmega328P" In Smart Card Research and Advanced Applications - CARDIS 2018, Lecture Notes in Computer Science 11389, B. Bilgin and J. Fischer (Eds.), Springer-Verlag, pp. 156-170, 2019. PDF 🔗 BibTex LaTex

67 [Conf article] N. Smart and T. Wood, "Error Detection in Monotone Span Programs with Application to Communication-Efficient Multi-party Computation" In Topics in Cryptology - CT-RSA 2019, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 11405, M. Matsui (Ed.), Springer-Verlag, pp. 210-229, 2019. PDF BibTex LaTex

68 [Conf article] E. Makri, D. Rotaru, N. Smart and F. Vercauteren, "EPIC: Efficient Private Image Classification (or: Learning from the Masters)" In Topics in Cryptology - CT-RSA 2019, The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science 11405, M. Matsui (Ed.), Springer-Verlag, pp. 473-492, 2019. PDF BibTex LaTex

69 [Conf article] A. Madhusudan, I. Symeonidis, M. Mustafa, R. Zhang and B. Preneel, "SC2Share: Smart Contract for Secure Car Sharing" In International Conference on Information Systems Security and Privacy, Proceedings of the International Conference on Information Systems Security and Privacy , 9 pages, 2019. PDF BibTex LaTex

70 [Conf article] S. Sinha Roy, F. Turan, K. Järvinen, F. Vercauteren and I. Verbauwhede, "FPGA-based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data" In IEEE International Symposium on High-Performance Computer Architecture, IEEE, 12 pages, 2019. PDF BibTex LaTex

71 [Conf article] J. D'Anvers, A. Karmakar, S. Sinha Roy and F. Vercauteren, "SABER: Mod-LWR based KEM round 2" In First PQC Standardization Conference, 29 pages, 2019. PDF BibTex LaTex

72 [Journal article] S. Li, S. Sun, D. Shi, C. Li and L. Hu, "Lightweight Iterative MDS Matrices: How Small Can We Go?", IACR Transactions on Symmetric Cryptology 2019(4), pp. 147-170, 2019. PDF BibTex LaTex

73 [Journal article] E. Argones Rúa, A. Abidin, R. Peeters and J. Romme, "Efficient and Privacy-Preserving Cryptographic Key Derivation from Continuous Sources", IEEE Transactions on Information Forensics and Security 14(11), pp. 2834-2847, 2019. PDF BibTex LaTex

74 [Journal article] L. De Meyer, "Recovering the CTR_DRBG State in 256 Traces", IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(1), 29 pages, 2019. PDF BibTex LaTex

75 [Journal article] M. Albrecht, A. Davidson, A. Deo and N. Smart, "Round-optimal Verifiable Oblivious Pseudorandom Functions From Ideal Lattices", IACR Cryptology ePrint Archive 2019(1271), 45 pages, 2019. PDF BibTex LaTex

76 [Journal article] S. SubramanyaRao and E. Argones Rúa, "Comments on a recently proposed Privacy Preserving Lightweight Biometric Authentication System for IoT Security", arXiv 1910(01446), 11 pages, 2019. PDF BibTex LaTex

77 [Journal article] L. Kraleva, N. Manev and V. Rijmen, "Correlation distribution analysis of a two round key-alternating block cipher", Tatra Mt. Math. Publ. 73(1), 18 pages, 2019. PDF BibTex LaTex

78 [Journal article] M. Vanhoef and E. Ronen, "Dragonblood: A Security Analysis of WPA3's SAE Handshake ", IEEE Security & Privacy <empty>(<empty>), 17 pages, 2019. PDF BibTex LaTex

79 [Journal article] S. Cohney, A. Kwong, S. Paz, D. Genkin, N. Heninger, E. Ronen and Y. Yarom, "Pseudorandom Black Swans: Cache Attacks on CTR_DRBG.", IEEE Security & Privacy <empty>(<empty>), 20 pages, 2019. PDF BibTex LaTex

80 [Journal article] J. D'Anvers, M. Tiepelt, I. Verbauwhede and F. Vercauteren, "Timing Attacks on Error Correcting Codes in Post-Quantum Schemes", Theory of Implementation Security 1(2019), 17 pages, 2019.
BibTex
LaTex

81 [Journal article] H. Gross, L. De Meyer, K. Stoffelen, M. Krenn and S. Mangard, "Masking the AES with Only Two Random Bits", Theory of Implementation Security 1(2019), 14 pages, 2019.
BibTex
LaTex

82 [Journal article] S. Dhooghe, S. Petkova-Nikova and V. Rijmen, "Threshold Implementations in the Robust Probing Model", Theory of Implementation Security 1(2019), 8 pages, 2019.
BibTex
LaTex

83 [Journal article] M. Rabbani, J. Vliegen, J. Winderickx, M. Conti and N. Mentens, "SHeLA: Scalable Heterogeneous Layered Attestation", IEEE Internet of Things Journal 19(9), 12 pages, 2019.
BibTex
LaTex

84 [Journal article] W. Castryck, F. Cools, J. Demeyer and A. Lemmens, "Computing graded Betti tables of toric surfaces", Transactions of the American Mathematical Society (1), 35 pages, 2019.
BibTex
LaTex

85 [Journal article] V. Arribas Abril, S. Petkova-Nikova and V. Rijmen, "Guards in action: First-order SCA secure implementations of KETJE without additional randomness", Microprocessors and Microsystems (71), 10 pages, 2019.
BibTex
LaTex

86 [Journal article] N. Pirotte, J. Vliegen, L. Batina and N. Mentens, "Balancing elliptic curve coprocessors from bottom to top", Microprocessors and Microsystems 71(1), 11 pages, 2019.
BibTex
LaTex

87 [Journal article] S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs and I. Verbauwhede, " EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage", IEEE Transactions on Electromagnetic Compatibility 61(4), pp. 1122-1128, 2019.
BibTex
LaTex

88 [Journal article] L. Segers, R. Smeets, M. Carlier, A. Braeken, A. Touhafi, K. Steenhaut, N. Mentens and K. Aerts, "Pogo-Pin-JTAG-Programmer-Box: A Low-Cost JTAG Programmer Interface for the Wireless Embedded Zolertia-Z1 Platform", Sensors 19 (13)(2945), g012:1-g012:6, 2019.
BibTex
LaTex

89 [Journal article] M. Carlier, A. Braeken, B. Lemmens, R. Smeets, L. Segers, K. Steenhaut, A. Touhafi, N. Mentens and K. Aerts, "6LoWPAN – Towards Zero-Configuration for Wireless Building Automation: System Architecture", Sensors 19 (13)(2945), d002:1-d002:6, 2019.
BibTex
LaTex

90 [Journal article] T. Van hamme, G. Garofalo, E. Argones Rúa, W. Joosen and D. Preuveneers, "A Systematic Comparison of Age and Gender Prediction on IMU Sensor-Based Gait Traces", Sensors 19 (13)(2945), 16 pages, 2019.
BibTex
LaTex

91 [Journal article] K. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten and I. Verbauwhede, "A Physically Unclonable Function Using Soft Oxide Breakdown Featuring 0% Native BER and 51.8fJ/bit in 40nm CMOS", IEEE Journal of Solid-State Circuits 54(10), 12 pages, 2019.
BibTex
LaTex

92 [Journal article] Y. Lindell, B. Pinkas, N. Smart and A. Yanai, "Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ", Journal of Cryptology 32(3), 1026?1069 pages, 2019.
BibTex
LaTex

93 [Journal article] B. Cogliati and T. Tanguy, "Multi-user security bound for filter permutators in the random oracle model", Designs, Codes and Cryptography 87(7), pp. 1621-1638, 2019.
BibTex
LaTex

94 [Journal article] L. De Meyer and B. Bilgin, "Classification of Balanced Quadratic Functions", IACR Transactions on Symmetric Cryptology 2019(2), pp. 169-192, 2019.
BibTex
LaTex

95 [Journal article] J. Tobias Muehlberg, J. Van Bulck, P. Maene, J. Noorman, B. Preneel, I. Verbauwhede and F. Piessens, "Architectural Security for Embedded Control Systems", IEEE Software Blog /(/), online, 2019.
BibTex
LaTex

96 [Journal article] L. Wouters, E. Marín Fàbregas, T. Ashur, B. Gierlichs and B. Preneel, "Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars", IACR Transactions on Cryptographic Hardware and Embedded Systems 2019(3), pp. 66-85, 2019.
BibTex
LaTex

97 [Journal article] L. De Meyer, B. Bilgin and O. Repáraz, "Consolidating Security Notions in Hardware Masking", IACR Transactions on Cryptographic Hardware and Embedded Systems 2019(3), pp. 119-147, 2019. BibTex LaTex

98 [Journal article] J. Vliegen, M. Rabbani, M. Conti and N. Mentens, "A Novel FPGA Architecture and Protocol for the Self-attestation of Configurable Hardware", IACR Cryptology ePrint Archive 2019(405), 11 pages, 2019. BibTex LaTex

99 [Journal article] Y. Hao, T. Isobe, L. Jiao, C. Li, W. Meier, Y. Todo and Q. Wang, "Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly", IEEE Transactions on Computers 99(<empty>), 16 pages, 2019. BibTex LaTex

100 [Journal article] F. Turan and I. Verbauwhede, "Compact and Flexible FPGA Implementation of Ed25519 and X25519", ACM Transactions on Embedded Computing Systems 18(3), 21 pages, 2019. BibTex LaTex

101 [Journal article] R. Meester, B. Preneel and S. Wenmackers, "Reply to Lucas & Henneberg: Are human faces unique?", Forensic Science International 297(1), pp. 217-220, 2019. BibTex LaTex

102 [Journal article] M. Tolga Sakall{i}, S. Akleylek, V. Rijmen and Y. c{C}engellenmic{s}, "a new matrix form to generate all 3x3 involutory MDS matrices over $mathbb{F}_{2^m}$", Information Processing Letters (147), pp. 61-68, 2019. BibTex LaTex

103 [Journal article] M. Mustafa, S. Cleemput, A. Abidin and A. Aly, "A Secure and Privacy-preserving Protocol for Smart Metering Operational Data Collection", IEEE Transactions on Smart Grid 10(6), pp. 6481-6490, 2019. BibTex LaTex

104 [Journal article] J. Sepulveda, S. Liu and J. Bermudo Mera, "Post-Quantum Enabled Cyber Physical Systems", IEEE Embedded Systems Letters 11(4), 5 pages, 2019. BibTex LaTex

105 [Journal article] J. Delvaux, "Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF-FSMs", IEEE Transactions on Information Forensics and Security <empty>(<empty>), 16 pages, 2019. BibTex LaTex

106 [Journal article] S. Bratus, M. Locasto, L. Sassaman and M. Patterson, "Security Applications of Formal Language Theory ", IEEE Software, Special Issue on Software Protection 68(7), pp. 489-500, 2019. BibTex LaTex

107 [Journal article] J. Bos and S. Friedberger, "Arithmetic considerations for isogeny based cryptography", IEEE Software, Special Issue on Software Protection 68(7), pp. 979-990, 2019. BibTex LaTex

108 [Journal article] Y. Komano, K. Sakiyama, M. Iwamoto and I. Verbauwhede, "Single-Round Pattern Matching Key Generation Using Physically Unclonable Function", Security and Communication Networks 2019(1), pp. 1719585:1-1719585:13, 2019. BibTex LaTex

109 [Journal article] S. Li, S. Sun, C. Li, Z. Wei and L. Hu, " Constructing Low-latency Involutory MDS Matrices with Lightweight Circuit", IACR Transactions on Symmetric Cryptology 2019(1), 19+15 pages, 2019. BibTex LaTex

110 [Journal article] W. Zhang and V. Rijmen, "Division cryptanalysis of block ciphers with a binary diffusion layer", IET Information Security 13(2), pp. 87 - 95, 2019. BibTex LaTex

111 [Journal article] W. Castryck and K. Nguyen, "New bounds for exponential sums with a non-degenerate phase polynomial", Journal de Math&eacute;matiques Pures et Appliqu&eacute;es 130(1), pp. 93-111, 2019. BibTex LaTex

112 [Journal article] A. Gorodilova, N. Tokareva, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, S. Petkova-Nikova, S. Picek, A. Oblaukhov, B. Preneel and V. Rijmen, "Problems and solutions from the fourth International Students' Olympiad in Cryptography (NSUCRYPTO).", Cryptologia 43(2), pp. 138-174, 2019. BibTex LaTex

113 [Thesis] E. Porto Balsa, "Chaff-based profile obfuscation", Phd thesis, KU Leuven, C. Diaz and B. Preneel, 314+30 pages, 2019. BibTex LaTex

114 [Thesis] R. Zhang, "Analyzing and Improving Proof-of-Work Consensus Protocols", Phd thesis, KU Leuven, B. Preneel, 219 pages, 2019. BibTex LaTex

115 [Thesis] P. Maene, "Lightweight Roots of Trust for Modern Systems-on-Chip", Phd thesis, KU Leuven, I. Verbauwhede, 168 pages, 2019. BibTex LaTex

116 [Thesis] R. Dedoncker, "Security Aspects of Deterministic Secure Quantum Communication Protocols", Master thesis, Katholieke Universiteit Leuven, A. Abidin, W. De Roeck and B. Preneel, 64 pages, 2019. BibTex LaTex

117 [Thesis] K. Verhulst, "Power Analysis and Masking of Saber", Master thesis, KU Leuven, I. Verbauwhede, 70 pages, 2019. BibTex LaTex

118 [Thesis] S. Friedberger, "Security of Cryptographic Implementations", Phd thesis, KU Leuven, J. Hermans and B. Preneel, pp. 1-216, 2019. BibTex LaTex

119 [Thesis] M. Juarez Miro, "Design and Evaluation of Website Fingerprinting Techniques", Phd thesis, KU Leuven, C. Diaz, 333 pages, 2019. BibTex LaTex

120 [Thesis] T. Georgios, "Application of Deep Learning on Side Channel Analysis", Master thesis, KU Leuven, I. Verbauwhede, pp. 1-47, 2019. BibTex LaTex

121 [Thesis] M. Laurent, "Fault attack on a PIN-check", Master thesis, KU Leuven, I. Verbauwhede, 95 pages, 2019. BibTex LaTex

122 [Thesis] M. Van Beirendonck, "Hardware Countermeasures Against Passive and Active Implementation Attacks", Master thesis, KU Leuven, S. Petkova-Nikova, V. Rijmen and I. Verbauwhede, 92 pages, 2019. BibTex LaTex

123 [Thesis] S. Bos, "Secure Machine Learning for Privacy Preserving Genetic Disease Identification", Master thesis, KU Leuven, F. Vercauteren, pp. 1-47, 2019. BibTex LaTex

124 [Thesis] T. Marchant, "GELD: Blockchain with Balances", Master thesis, KU Leuven, N. Smart, 95 pages, 2019. BibTex LaTex

125 [Thesis] S. D'haeseleer, "Hardware design for cryptanalysis", Master thesis, KU Leuven, T. Ashur, D. Sijacic and I. Verbauwhede, 79 pages, 2019. BibTex LaTex

126 [Thesis] T. Beyne, "Linear Cryptanalysis in the Weak Key Model", Master thesis, KU Leuven, V. Rijmen, 104 pages, 2019. BibTex LaTex

127 [Thesis] J. Aerts, "The dynamic Buchberger algorithm; an analysis of the Hilbert heuristic", Master thesis, KU Leuven, F. Vercauteren, 90 pages, 2019. BibTex LaTex

128 [Thesis] A. Boucquey, "Verbeterd Kuperbergalgoritme", Master thesis, KU Leuven, F. Vercauteren, 47 pages, 2019. BibTex LaTex

129 [Thesis] S. Kalantari, "Email Tracking: a Study on its Prevalence", Master thesis, KU Leuven, C. Diaz and F. Piessens, pp. 1-69, 2019. BibTex LaTex

130 [Thesis] K. Vanderlocht, "Veiligheidsanalyse van het draadloos huisautomatisatieprotocol Z-wave", Master thesis, KU Leuven, F. Piessens and B. Preneel, pp. 1-61, 2019. BibTex LaTex

131 [Thesis] E. Van Looy, "Fuzzing Universal Plug and Play", Master thesis, KU Leuven, F. Piessens and B. Preneel, pp. 1-70, 2019. BibTex LaTex

132 [Thesis] S. Mestdagh, "Fuzzing Universal Plug and Play", Master thesis, KU Leuven, F. Piessens and B. Preneel, pp. 1-105, 2019. BibTex LaTex

133 [Thesis] I. Iliashenko, "Optimisations of fully homomorphic encryption", Phd thesis, KU Leuven, B. Preneel and F. Vercauteren, 226 pages, 2019. BibTex LaTex

134 [Thesis] H. De Plaen, "Privacy-friendly machine learning algorithms for intrusion detection systems", Master thesis, Katholieke Universiteit Leuven, A. Abidin, A. Aly and B. Preneel, 117 pages, 2019. BibTex LaTex

135 [Proceeding] "TIS '2019: Proceedings of the 2019 ACM Workshop on Theory of Implementation Security" ACM, B. Bilgin, S. Petkova-Nikova and V. Rijmen (Eds.), ACM, 2019. BibTex LaTex

136 [Proceeding] "European Symposium on Research in Computer Security - ESORICS 2019", Lecture Notes in Computer Science 11737, A. Biryukov, C. Pérez Solà, J. Garcia-Alfaro and G. Navarro-Arribas (Eds.), Springer-Verlag, 2019. BibTex LaTex

137 [Proceeding] "Advances in Cryptology - EUROCRYPT 2019", Lecture Notes in Computer Science 11477, Y. Ishai and V. Rijmen (Eds.), Springer-Verlag, 2019. BibTex LaTex

138 [Report] A. Purnal and I. Verbauwhede, "Advanced profiling for probabilistic Prime+Probe attacks and covert channels in ScatterCache", arXiv report, 8 pages, 2019. BibTex LaTex

139 [Report] J. Hermans and R. Peeters, "Vingerafdrukken op de Belgische eID - Technische analyse", COSIC internal report, 22 pages, 2019. BibTex LaTex

140 [Abstract of talk] A. Peetermans, M. Grujic, V. Rozic and I. Verbauwhede, "A Self-Calibrating True Random Number Generator", In International Conference on Field Programmable Logic and Applications (FPL 2019), 1 pages, 2019. BibTex LaTex

141 [Abstract of talk] S. Osuka, D. Fujimoto, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, I. Verbauwhede and Y. Hayashi, "Fundamental Study on Randomness Evaluation Method of RO-Based TRNG Using APD", In Joint IEEE International Symposium on Electromagnetic Compatibility (EMC) / IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC), 1 pages, 2019. BibTex LaTex

142 [Abstract of talk] T. Ashur and A. Luykx, "An Account on the ISO/IEC Standardization of Simon and Speck", In Real World Crypto 2019, 2 pages, 2019. BibTex LaTex

143 [Talk] A. Abidin, "Mitigating relay attacks with distance bounding", CSfR2019 - CyberSecurity for Robotics conference 2019, Bilbao, ES, 2019. BibTex LaTex

144 [Talk] C. Diaz, "Inteligencia Artificial: Seguridad y Privacidad", II Jornadas Internacionales en Ciberinteligencia de la Guardia Civil, Aranjuez , ES, 2019. BibTex LaTex

145 [Talk] B. Preneel, "Software Security: Squaring the Circle? (keynote)", International Workshop on Software Protection, 2019. BibTex LaTex

146 [Talk] I. Verbauwhede, "The Need for Hardware Roots of Trust (keynote)", ACM CCS, London, GB, 2019. BibTex LaTex

147 [Talk] I. Verbauwhede, "Biggest Failures in Security", Dagstuhl-Seminar 19451, Wadern, DE, 2019. BibTex LaTex

148 [Talk] C. Diaz, "Lightning Network: Privacy Threats Towards Network Adversaries", The Lightning Conference, Berlin, DE, 2019. BibTex LaTex

149 [Talk] B. Preneel, "Cryptocurrencies and Distributed Consensus: Hype and Science (keynote)", ESORICS 2019, LU, 2019. BibTex LaTex

150 [Talk] V. Rijmen, "Algorithmic Countermeasures Against Combined Fault and Side-Channel Attacks", RCD 2019, Bucharest, RO, 2019. BibTex LaTex

151 [Talk] N. Mentens, "Security on Plastics: Fake or Real?", TU Darmstadt CROSSING conference, Darmstadt, DE, 2019. BibTex LaTex

152 [Talk] N. Mentens, "Security on Plastics: Fake or Real? (Cyber Security Days for Industry)", Cyber Security Days for Industry, AU, 2019. BibTex LaTex

153 [Talk] B. Preneel, "Challenges for Security and Privacy", Cyber Security Days for Industry , Graz, AT, 2019. BibTex LaTex

154 [Talk] I. Verbauwhede, "Hardware Security and Cryptography Essentials", Test Spring School at the European BibTex

Test Symposium, Bremen, DE, 2019. LaTex

155 [Talk] C. Diaz, "Network-layer anonymity for privacy-enhanced dapps", Dappcon, Berlin, DE, 2019. ▶ BibTex LaTex

156 [Talk] N. Mentens, "Hands-on tutorial", SAC Summer School, Waterloo, CA, 2019. BibTex LaTex

157 [Talk] I. Verbauwhede, "Secure composition for Hardware Systems", Dagstuhl-Seminar 19301, Wadern, DE, 2019. BibTex LaTex

158 [Talk] C. Diaz, "Strong network anonymity with Mixnets", CASA Distinguished Lecture at Rurh University Bochum, Bochum, DE, 2019. BibTex LaTex

159 [Talk] C. Diaz, "Introduction to Privacy Technologies", COSIC Course 2019, Leuven, BE, 2019. ▶ BibTex LaTex

160 [Talk] V. Rijmen, "A policy-maker's guide to cryptography", CONNECT University Summer School, Brussels, BE, 2019. BibTex LaTex

161 [Talk] C. Diaz, "What is Anonymity in Digital Systems? ", Academic Perspectives on Cybersecurity Challenges - Cyber Week., Tel Aviv, IL, 2019. BibTex LaTex

162 [Talk] M. Grujic, "A Multimode Ring Oscillator based TRNG for FPGAs", 17th CryptArchi Workshop, Prague, CZ, 2019. BibTex LaTex

163 [Talk] N. Mentens, "Hands-on hardware tutorial", Summer School on Real-world Crypto and Privacy, Šibenik, HR, 2019. BibTex LaTex

164 [Talk] I. Verbauwhede, "Random Numbers on FPGAs: Contradiction to the Deterministic Behavior", Design Automation Conference 2019, Las Vegas, US, 2019. BibTex LaTex

165 [Talk] I. Verbauwhede, "Invited presentation", Combined SHIVA final workshop and EU TRUDEVICE workshop, Baden-Baden , DE, 2019. BibTex LaTex

166 [Talk] I. Verbauwhede, "Design Methods for Hardware Roots of Trust", RISE spring school 2019, Belfast, NI, 2019. BibTex LaTex

167 [Talk] I. Verbauwhede, "Design methods for hardware roots of trust (RISE)", UK RISE Research institute for Secure Hardware & Embedded systems, GB, 2019. BibTex LaTex

168 [Talk] C. Diaz, "Anonymity loves company, and funding", Computers, Privacy and Data Protection (CPDP 2019), Brussels, BE, 2019. ▶ BibTex LaTex

169 [Talk] T. Ashur, B. Gierlichs, E. Marín Fàbregas, B. Preneel and L. Wouters, "Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars (Invited talk)", Real World Crypto, San Jose, US, 2019. BibTex LaTex

170 [Talk] N. Mentens, "Invited talk at ETH Zürich", ETH Zürich, CH, 2019. BibTex LaTex

171 [Talk] N. Mentens, "Invited talk at Leiden University", Leiden University, Leiden, NL, 2019. BibTex LaTex

172 [Talk] N. Mentens, "Invited talk at SeHAS Workshop at HiPEAC", SeHAS Workshop at HiPEAC, ES, 2019. BibTex LaTex

173 [Talk] N. Mentens, "Invited talk at KPMG-KU Leuven Innovation event", KPMG-KU Leuven Innovation event, BE, 2019. BibTex LaTex

174 [Patent] M. Conti, N. Mentens and J. Vliegen, "Configurable hardware device", Patent number WO/2019/211125, KU Leuven, Università degli Studi di Padova, 2019. BibTex LaTex

175 [Patent] N. Mentens, F. Regazzoni and E. Charbon, "Reconfigurable logic circuit", Patent number WO/2019/101660, KU Leuven, EPFL, Università della Svizzera italiana, 2019. BibTex LaTex