Lorenzo Grassi

Curriculum Vitae

✱ *Born: Italy, October 1989*
l.grassi@tue.nl
lorenzo@ponos.technology
https://lorenzo3grassi.github.io/

Updated: January 2026

Current Position

From 01/02/2025 **Assistant Professor in (Symmetric) Cryptography**
Eindhoven University of Technology (TU/e), Eindhoven, the Netherlands
(Department of Mathematics and Computer Science)
- Analysis and design of symmetric cryptographic primitives over prime fields and integer rings for modern applications
- *Group Leader:* Prof. Tanja Lange (Coding Theory and Cryptology Group)

Impact

ORCID: https://orcid.org/0000-0003-1140-0520
(https://scholar.google.com/citations?user=bbbOVyMAAAAJ)

No. publications: **50**

No. citations: **3371** (Google Scholar – 01/02/2026)

H-index: **25** (Google Scholar – 01/02/2026)

Education

From 01/09/2015 to 26/04/2019 **PhD in Symmetric Cryptography**
IAIK, Graz University of Technology, Graz (Austria)
- *Thesis Title:* "Cryptanalysis of AES-like Ciphers and Reviving Old Design Ideas for New Constructions"
- *Supervisor:* Prof. Christian Rechberger

From 10/2011 to 27/02/2014 **Master Degree's in Mathematics**
University of the Study of Milano (Italy)
- *Final grades:* 110/110 cum laude (i.e., highest possible grade in Italian system)

From 09/2008 to 10/2011 **Bachelor's degree in Mathematics for Applications**
University of the Study of Milano (Italy)

Research and Professional Experience

From 01/04/2023 to 31/12/2025 **Consultant at Ponos Technology – Cryptographer** (*20% of the time*)
- Analysis and design of Zero-Knowledge friendly symmetric cryptographic primitives targeting efficient Hardware implementation

From 15/03/2023 to 28/02/2025 **PostDoc in Symmetric Cryptography** (*80% of the time*)
Ruhr University Bochum, Bochum, Germany
- *Supervisor:* Prof. Gregor Leander

From 01/03/2020 to 28/02/2023 **PostDoc in Symmetric Cryptography**
Radboud University, Nijmegen (Netherlands)
- *Supervisor:* Prof. Joan Daemen

From 01/02/2022 to 28/02/2023 **Consultant at Ponos Technology – Cryptographer** (*Contract Hours*)

From 27/04/2019 to 29/02/2020 **PostDoc in Symmetric Cryptography**
IAIK, Graz University of Technology, Graz (Austria)
- *Supervisor:* Prof. Christian Rechberger

From 23/06/2014 to 22/12/2014 **Internship at STMicroelectronics – Cryptographer**
Agrate Brianza (Italy)
- *Tutor:* Eng. Guido Marco Bertoni (AST Security Lab)

Research Grants

ERC 2024 "*SYMPZON – Getting SYMmetric CryPtography Out of its Comfort ZONe*", European Research Council (ERC) Starting Grant, for 5 years starting in January 2025 – approx 1.500.000 euro

"*Design and Cryptanalysis of Symmetric Cryptographic Primitives for Zero-Knowledge Applications*", Ethereum Foundation – Academic Grant Program 2024,[1] for 1 year starting in June 2024 – approx 50.000 euro

"*Design and Cryptanalysis of Symmetric Cryptographic Primitives for Secure Computations*", CASA Jump.Start Program for Postdocs[2] (Germany), for 2 years starting in March 2023 – approx 200.000 euro

PhD Students

From 01/10/2025 Berenika Richterová
Supported by the ERC starting grant 2024 "SYMPZON"

From 01/02/2026 Matthijs Bosch
Supported by the ERC starting grant 2024 "SYMPZON"

From 01/03/2026 Aimad Chabounia
Supported by the ERC starting grant 2024 "SYMPZON"

Service – Program Committees and Editorial Boards

FSE/ToSC 2025: ***General Co-Chair*** (together with Prof. Marco Pedicini)

Program Committee Member: **EUROCRYPT 2026** – **EUROCRYPT 2024**
CRYPTO 2026 – **CRYPTO 2025** – **CRYPTO 2024**
ASIACRYPT 2023
SCN 2026
LightSEC 2025
Africacrypt 2023 – Africacrypt 2022

Member of the Editorial Board: **FSE/ToSC 2023/2024**
FSE/ToSC 2022/2023
FSE/ToSC 2021/2022

SPRING 2026:[3] Co-organizer (together with Prof. Marco Pedicini)

ALPSY 2024:[4] Co-organizer (together with Prof. Arnab Roy, Prof. Christian Rechberger, and Reinhard Lueftenegger)

External Reviewer: Top-level conferences and journals, including: CRYPTO, EUROCRYPT, ASIACRYPT, FSE/ToSC, Journal of Cryptology, and DCC (Designs, Codes and Cryptography)

[1] https://esp.ethereum.foundation/academic-grants
[2] https://casa.rub.de/en/jobs/casa-jump-start-program-for-postdocs
[3] https://lorenzo3grassi.github.io/SPRING26/spring26.html
[4] https://alpsy-workshop.github.io/alpsy24/

Publications

Please, note (1st) that IACR's CRYPTO, EUROCRYPT and ASIACRYPT are generally considered the most important publication venues in the world for cryptographic academic research (A*-rank conference are highlighted), and (2nd) that, in cryptography, authors are always listed in alphabetical order.

FSE/ToSC 2025(4) M. Urani, L. Grassi: *"Corrigendum to "Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$ – Application to Poseidon""*. DOI: ???

CiC 2(4) L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, M. Schofnegger, V. Schröppel, Z. Wu: *"Poseidon(2)b - Binary Field Versions of Poseidon/Poseidon2"*. DOI: 10.62056/a66ce0zn4

TCHES 2025(4) B. Balon, L. Grassi, P. Méaux, T. Moos, F.-X. Standaert, M. J. Steiner: *"mid-pSquare: Leveraging the Strong Side-Channel Security of Prime-Field Masking in Software"*. DOI: 10.46586/TCHES.V2025.I4.486-519

Designs, Codes and Cryptography, 2025 L. Grassi: *"On Generalizations of the Lai-Massey Scheme"*. DOI: 10.1007/S10623-025-01672-2

FSE/ToSC 2025(2) L. Grassi, K. Koschatko, C. Rechberger: *"Poseidon and Neptune: Gröbner Basis Cryptanalysis Exploiting Subspace Trails"*. DOI: 10.46586/TOSC.V2025.i2.34-86

TCHES 2025(2) C. Bouvier, L. Grassi, D. Khovratovich, K. Koschatko, C. Rechberger, F. Schmid, M. Schofnegger: *"Skyscraper: Fast Hashing on Big Primes"*. DOI: 10.46586/TCHES.V2025.I2.743-780

FSE/ToSC 2024(4) F. Liu, K. Koschatko, L. Grassi, H. Yan, S. Chen, S. Banik, W. Meier : *"Opening the Blackbox: Collision Attacks on Round-Reduced Tip5, Tip4, Tip4′ and Monolith"*. DOI: 10.46586/TOSC.V2024.I4.97-137

ASIACRYPT 2024 A. F. Gutierrez, L. Grassi, G. Leander, F. Sibleyras, Y. Todo: *"Generic Practical Cryptanalysis for the Sum of Round-Reduced Block Ciphers and ZIP-AES"*. DOI: 10.1007/978-981-96-0947-5_10

FSE/ToSC 2024(3) L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger, R. Walch: *"Monolith: Circuit-Friendly Hash Functions with New Nonlinear Layers for Fast and Constant-Time Implementations"*. DOI: 10.46586/tosc.v2024.i3.44-83

SAC 2024 L. Grassi, F. Liu, C. Rechberger, F. Schmid, R. Walch, Q. Wang: *"Minimize the Randomness in Rasta-Like Designs: How Far Can We Go? (Application to Pasta)"*. DOI: 10.1007/978-3-031-82841-6_9

EUROCRYPT 2024 L. Grassi, L. Masure, P. Méaux, T. Moos, F.-X. Standaert: *"Generalized Feistel Ciphers for Efficient Prime Field Masking"*. DOI: 10.1007/978-3-031-58734-4_7

CRYPTO 2023 L. Grassi, Y. Hao, C. Rechberger, M. Schofnegger, R. Walch, Q. Wang: *"Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications"*. DOI: 10.1007/978-3-031-38548-3_19

CRYPTO 2023 L. Grassi, I. Manterola Ayala, M. Norberg Hovd, H. Raddum, Q. Wang, M. Øygarden: *"Cryptanalysis of Symmetric Primitives over Rings and a Key Recovery Attack on Rubato"*. DOI: 10.1007/978-3-031-38548-3_11

CRYPTO 2023 F. Liu, L. Grassi, C. Bouvier, W. Meier, T. Isobe: *"Coefficient Grouping for Complex Affine Layers"*. DOI: 10.1007/978-3-031-38548-3_18

FSE/ToSC 2023(2) L. Grassi: *"Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives"*. DOI: 10.46586/tosc.v2023.i2.94-131

AFRICACRYPT 2023 L. Grassi, D. Khovratovich, M. Schofnegger: *"Poseidon2: A Faster Version of the Poseidon Hash Function"*. DOI: 10.1007/978-3-031-37679-5_8

AFRICACRYPT 2023 G. Giordani, L. Grassi, S. Onofri, M. Pedicini: *"Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via Multiple Local Maps"*. DOI: 10.1007/978-3-031-37679-5_7

TCHES 2023(3) C. Dobraunig, L. Grassi, L. Helminger, C. Rechberger, M. Schofnegger, R. Walch: *"Pasta: A Case for Hybrid Homomorphic Encryption"*. DOI: 10.46586/tches.v2023.i3.30-73

EUROCRYPT 2023 L. Grassi, M. Øygarden, M. Schofnegger, R. Walch: *"From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications"*. DOI: 10.1007/978-3-031-30634-1_9

ASIACRYPT 2022 L. Grassi, B. Mennink: *"Security of Truncated Permutation Without Initial Value"*. DOI: 10.1007/978-3-031-22966-4_21

ACM CCS 2022 L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger, R. Walch: *"Reinforced Concrete: Fast Hash Function for Zero Knowledge Proofs and Verifiable Computation"*. DOI: 10.1145/3548606.3560686

FSE/ToSC 2022(3) L. Grassi, S. Onofri, M. Pedicini, L. Sozzi: *"Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$"*. DOI: 10.46586/tosc.v2022.i3.20-72

FSE/ToSC 2022(2) A. Mehrdad, J. Daemen, L. Grassi, S. Mella: *"Differential Trail Search in Cryptographic Primitives with Big-Circle Chi"*. DOI: 10.46586/tosc.v2022.i2.253-288

ACISP 2022 L. Grassi, C. Rechberger: *"Truncated Differential Properties of the Diagonal Set of Inputs for 5-round AES"*. DOI: 10.1007/978-3-031-22301-3_2

FSE/ToSC 2022(1) L. Grassi, D. Khovratovich, S. Rønjom, M. Schofnegger: *"The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $(\mathbb{F}_p)^n$"*. DOI: 10.46586/tosc.v2022.i1.5-37

FSE/ToSC 2022(1) C. Cid, L. Grassi, A. Gunsing, R. Lüftenegger, C. Rechberger, M. Schofnegger: *"Influence of the Linear Layer on the Algebraic Degree in SP-Networks"*. DOI: 10.46586/tosc.v2022.i1.110-137

FSE/ToSC 2021(2) L. Grassi, C. Rechberger, M. Schofnegger: *"Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer"*. DOI: 10.46586/tosc.v2021.i2.314-352

EUROCRYPT 2021 C. Dobraunig, L. Grassi, A. Guinet, D. Kuijsters *"Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields"*. DOI: 10.1007/978-3-030-77886-6_1

USENIX-Security 2021 L. Grassi, D. Khovratovich, C. Rechberger, A. Roy, M. Schofnegger: *"Poseidon: A New Hash Function for Zero-Knowledge Proof Systems"*. Link: `https://www.usenix.org/conference/usenixsecurity21/presentation/grassi`

INDOCRYPT 2020 L. Grassi, M. Schofnegger: *"Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box"*. DOI: 10.1007/978-3-030-65277-7_14

ASIACRYPT 2020 M. Eichlseder, L. Grassi, R. Lüftenegger, M. Øygarden, C. Rechberger, M. Schofnegger, Q. Wang: *"An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC"*. DOI: 10.1007/978-3-030-64837-4_16

SAC 2020 T. Cui, L. Grassi: *"Algebraic Key-Recovery Attacks on Reduced-Round Xoofff"*. DOI: 10.1007/978-3-030-81652-0_7

SAC 2020 L. Grassi, G. Leander, C. Rechberger, C. Tezcan, F. Wiemer: *"Weak-Key Distinguishers for AES"*. DOI: 10.1007/978-3-030-81652-0_6

EUROCRYPT 2020 L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, M. Schofnegger: *"On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy"*. DOI: 10.1007/978-3-030-45724-2_23

Designs, Codes and Cryptography, 2020 L. Grassi, C. Rechberger: *"Revisiting Gilbert's known-key distinguisher"*. DOI: 10.1007/s10623-020-00756-5

ASIACRYPT 2019 M. Albrecht, C. Cid, L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schofnegger: *"Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC"*. DOI: 10.1007/978-3-030-34618-8_13

SAC 2019 L. Grassi: *"Probabilistic Mixture Differential Cryptanalysis on round-reduced AES"*. DOI: 10.1007/978-3-030-38471-5_3

ESORICS 2019 M. Albrecht, L. Grassi, L. Perrin, S. Ramacher, C. Rechberger, D. Rotaru, A. Roy, M. Schofnegger: *"Feistel Structures for MPC, and More"*. DOI: 10.1007/978-3-030-29962-0_8

FSE/ToSC 2018(2) L. Grassi: *"Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES"*. DOI: 10.13154/tosc.v2018.i2.133-160

ASIACRYPT 2018 L. Grassi, M. Naya-Plasencia, A. Schrottenloher: *"Quantum Algorithms for the k-xor Problem"*. DOI: 10.1007/978-3-030-03326-2_18

CRYPTO 2018 C. Dobraunig, M. Eichlseder, L. Grassi, V. Lallemand, G. Leander, E. List, F. Mendel, C. Rechberger: *"Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit"*. DOI: 10.1007/978-3-319-96884-1_22

CT-RSA 2018 L. Grassi: *"MixColumns Properties and Attacks on (Round-Reduced) AES with a Single Secret S-Box"*. DOI: 10.1007/978-3-319-76953-0_13

CT-RSA 2018 Q. Wang, L. Grassi, C. Rechberger: *"Zero-Sum Partitions of PHOTON Permutations"*. DOI: 10.1007/978-3-319-76953-0_15

EUROCRYPT 2017 L. Grassi, C. Rechberger, S. Rønjom: *"A New Structural-Differential Property of 5-Round AES"*. DOI: 10.1007/978-3-319-56614-6_106

FSE/ToSC 2016(2) L. Grassi, C. Rechberger, S. Rønjom: *"Subspace Trail Cryptanalysis and its Applications to AES"*. DOI: 10.13154/tosc.v2016.i2.192-225

ASIACRYPT 2016 M.R. Albrecht, L. Grassi, C. Rechberger, A. Roy, T. Tiessen: *"MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity"*. DOI: 10.1007/978-3-662-53887-6_7

ACM CCS 2016 L. Grassi, C. Rechberger, D. Rotaru, P. Scholl, N. P. Smart: *"MPC-Friendly Symmetric Key Primitives"*. DOI: 10.1145/2976749.2978332

INDOCRYPT 2016 L. Grassi, C. Rechberger: *"Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE"*. DOI: 10.1007/978-3-319-49890-4_18

SPACE 2015 G. M. Bertoni, L. Grassi, F. Melzani: *"Simulations of Optical Emissions for Attacking AES and Masked AES."*. DOI: 10.1007/978-3-319-24126-5_11

M. Sansottera, L. Grassi and A. Giorgilli: *"On the relativistic Lagrange-Laplace secular dynamics for extrasolar systems."* Proceedings of the International Astronomical Union, **9**, 2014. DOI: 10.1017/S174392131400787X

Teaching Activities and Student Supervision

(WiSe ≡ Winter Semester – SuSe ≡ Summer Semester)

WiSe 2025/2026 "*Introduction to Cryptology*", Bachelor's course (TU/e), Lecturer

WiSe 2023/2024 "*Symmetric Cryptanalysis*", Master's course (RUB), Teaching Assistant

WiSe 2022/2023 "*Cryptology*", Master's course (Radboud University), Guest Lecturer (1 lecture)

WiSe 2022/2023 "*Computer Security*", Bachelor's course (Radboud University), Teaching Assistant

WiSe 2019/2020 – 2018/2019 – 2017/2018 "*Applied Cryptography 1*", Master's course (TU Graz), Co-Lecturer

SuSe 2018/2019 – 2017/2018 – 2016/2017 "*Applied Cryptography 2*", Master's course (TU Graz), Co-Lecturer

Supervision of Bachelor/Master Thesis/Project

(Co-supervised with Prof. Bart Mennink* and Prof. Christian Rechberger†)

Quinn Ketelaars	Master Thesis 2025/2026: "*Round-Level Gröbner Basis Attacks of Poseidon and Neptune*"
Sjors Clabbers*	Bachelor Thesis 2021/2022: "*Linear Cryptanalysis of round-reduced GIFT*"
Giulio Arrigoni†	Bachelor Thesis 2019/2020: "*Analysis of 5- and 6-round AES*"
Bernhard Ablinger†	Master Project 2018/2019: "*Higher-Order Differential over GF(p)*"
Matthias Niel†	Master Project 2017/2018: "*Mean and Variance Distinguishers for AES*"

Talks

02/2026	**Workshop on Zero-Knowledge, Succinct Proofs, and Symmetric Cryptography (ZKSC 2026)**: "Greek and Roman Gods in Symmetric Crypto" Vienna (Austria), joint work
11/2025	**Crypto Working Group**: "Symmetric Primitives for MPC-/ZK-/HE-Applications" Utrecht (Netherlands), joint work
12/2024	**University of Novi Sad**: "Symmetric Primitives for Future Applications: Poseidon" virtual
06/2024	**Xuejia Lai's 70th Birthday**: "Lai-Massey Scheme: Possible Generalizations" virtual
03/2024	**FSE/ToSC**: "Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives" Leuven (Belgium)
12/2023	**Asian Workshop on Symmetric Key Cryptography (ASK)**: "Horst and Amaryllises: Possible Generalizations of the Feistel and of the Lai-Massey Schemes" Guangzhou (China)
09/2023	**Convegno UMI Crittografia e Codici**: "Symmetric Primitives for MPC-/ZK-/FHE-Applications" Perugia (Italy), joint work
09/2023	**Università degli Studi Roma Tre**: "Symmetric Primitives for MPC-/ZK-/FHE-Applications" Roma (Italy), joint work
03/2023	**FSE/ToSC**: "Security of Truncated Permutation Without Initial Value" Kobe (Japan), joint work with: S. Onofri, M. Pedicini, L. Sozzi
12/2022	**ASIACRYPT**: " Security of Truncated Permutation Without Initial Value" Taipei (Taiwan), joint work with: B. Mennink
11/2022	**ACISP**: " Truncated Differential Properties of the Diagonal Set of Inputs for 5-round AES" virtual, joint work with: C. Rechberger
09/2022	**FrisiaCrypt**: " Re-thinking Feistel and Lai-Massey schemes: the birth of Horst and Amaryllises" Terschelling (the Netherlands)
09/2022	**ERC Workshop: New Directions in Cryptanalysis of AES**: "Cryptanalysis of round-reduced AES" Tel Aviv (Israel), joint work
07/2022	**Université Catholique de Louvain**: "Design and Security Analysis of Symmetric Primitives for Multi-Party Computation" Louvain (Belgium), joint work
05/2022	**University of Twente**: "Symmetric Primitives for Multi-Party Computation (MPC) Application" Twente (the Netherlands), joint work
03/2022	**FSE/ToSC**: "The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over $(\mathbb{F}_p)^n$" Athens (Greece), joint work with: D. Khovratovich, S. Rønjom, M. Schofnegger
03/2022	**Universität Innsbruck**: "Symmetric Primitives for Multi-Party Computation (MPC) Application" Innsbruck (Austria), joint work
12/2020	**INDOCRYPT**: "Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box", virtual, joint work with: M. Schofnegger

12/2020 **De Componendis Cifris**: "Symmetric-Key Encryption Schemes for MPC Applications", virtual, joint work

11/2020 **Università degli Studi di Milano**: "Cryptanalysis of round-reduced AES: New Results", virtual, joint work

10/2020 **SAC**: "Weak-Key Distinguishers for AES", virtual, joint work with: G. Leander, C. Rechberger, C. Tezcan, F. Wiemer

01/2020 **Dagstuhl Seminar**: "Higher-Order Differential Attacks on Ciphers with Low-Degree Polynomial S-Boxes in $GF(2^n)$: Open Problems", Dagstuhl (Germany), joint work

11/2019 **Università degli Studi Roma Tre**: "Cryptanalysis of round-reduced AES: New Results", Roma (Italy), joint work

08/2019 **SAC**: "Probabilistic Mixture Differential Cryptanalysis on round-reduced AES", Waterloo (Canada)

09/2018 **Centre INRIA de Paris**: "Cryptanalysis of round-reduced AES: New Results", Paris (France), joint work

04/2018 **CT-RSA**: "MixColumns Properties and Attacks on (Round-Reduced) AES with a Single Secret S-Box", San Francisco (USA)

04/2018 **CT-RSA**: "Zero-Sum Partitions of PHOTON Permutations", San Francisco (USA), joint work with: Q. Wang, C. Rechberger

03/2018 **FSE/ToSC**: "Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES", Paris (France)

11/2017 **Technical University of Denmark**: "Cryptanalysis of AES: New Results", Copenaghen (Denmark), joint work

05/2017 **EUROCRYPT**: "A New Structural-Differential Property of 5-Round AES", Paris (France), joint work with: C. Rechberger, S. Rønjom

03/2017 **FSE/ToSC**: "Subspace Trail Cryptanalysis and its Applications to AES", Tokyo (Japan), joint work with: C. Rechberger, S. Rønjom

12/2016 **INDOCRYPT**: "Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE", Kolkata (India), joint work with: C. Rechberger

12/2015 **SPACE**: "Simulations of Optical Emissions for Attacking AES and Masked AES", Jaipur (India), joint work with: G. M. Bertoni, F. Melzani

References

Prof. **Tanja Lange**
tanja@hyperelliptic.org
Eindhoven University of Technology, Eindhoven (the Netherlands)

Prof. **Christian Rechberger**
christian.rechberger@iaik.tugraz.at – christian.rechberger@tugraz.at
IAIK, Graz University of Technology, Graz (Austria)

Prof. **Gregor Leander**
gregor.leander@rub.de
Ruhr-University Bochum, Bochum (Germany)

Prof. **Joan Daemen**
joan@cs.ru.nl – j.daemen@cs.ru.nl
Digital Security, Radboud University, Nijmegen (the Netherlands)