Pierrick Méaux

Cryptography Researcher – Symmetric Cryptography, Boolean Functions, Fully Homomorphic Encryption, and Side-Channel Security

pierrick.meaux.lu@gmail.com | +33 6 03 43 44 69 | Esch-sur-Alzette, Luxembourg

Research Profile

Researcher in cryptography working on the design and analysis of structured symmetric primitives under modern cryptographic constraints. My work combines symmetric cryptography, Boolean functions, and advanced settings such as fully homomorphic encryption and side-channel security. I develop new constructions, cryptographic criteria, and adapted analysis techniques for advanced cryptographic settings.

45 publications in peer-reviewed venues, including EUROCRYPT, CRYPTO, ASIACRYPT, TCHES, ToSC, IEEE Transactions on Information Theory, and journals in cryptography and discrete mathematics.

Positions

2021–2026 Associate Researcher, University of Luxembourg, SnT, Applied Crypto Group

Continuation and development of research directions on structured symmetric cryptography and Boolean functions, with applications to fully homomorphic encryption and side-channel security. Contributions include new constructions, analysis techniques, and cryptographic criteria under structural constraints. Funded by ERC CLOUDMAP.

2018–2021 Postdoctoral Researcher, Université Catholique de Louvain, Crypto Group

Research period marking the expansion of expertise from homomorphic encryption and symmetric cryptography toward side-channel security and leakage-related cryptography, while continuing research on Boolean functions and structured constructions. Contributions include transciphering, masking, physical learning problems, and algebraic methods for applied security questions. Recipient and PI of the FRS-FNRS "Moove In" postdoctoral grant.

2014–2017 PhD in Mathematics, ENS / INRIA / Paris Sciences et Lettres

Thesis: *Hybrid Fully Homomorphic Framework*. Supervised by David Pointcheval and Vadim Lyubashevsky.

Research Contributions

- **Structured symmetric primitives and transciphering.** Design and analysis of simple symmetric constructions, including stream cipher and block cipher paradigms, with a sustained line of work on homomorphic-friendly primitives.
- **Boolean functions with provable cryptographic properties.** Study of Boolean function classes under structural constraints, including weightwise and slice-based settings, with results on algebraic immunity, nonlinearity, and related cryptographic criteria.
- **Cryptanalysis and security evaluation.** Analysis of structured symmetric constructions against algebraic, fast algebraic, statistical, and implementation-oriented attacks.
- **Cryptography under advanced constraints.** Design and analysis of primitives under constraints arising from homomorphic evaluation and implementation security, including leakage and fault attacks.

Selected Publications

Nostalgia cipher: can filtered LFSRs be secure again? An application to Hybrid Homomorphic Encryption with sub-50 ms latency. ToSC 2025. .

Secure and Efficient Transciphering for FHE-based MPC. TCHES 2025. .

Towards practical transciphering for FHE with setup independent of the plaintext space. CiC 2024. .

Generalized Feistel Ciphers for Efficient Prime Field Masking. EUROCRYPT 2024. .

Effective and Efficient Masking with Low Noise Using Small-Mersenne-Prime Ciphers. EUROCRYPT 2023. .

Learning With Physical Rounding for Linear and Quadratic Leakage Functions. CRYPTO 2023. .

Towards Globally Optimized Hybrid Homomorphic Encryption Featuring the Elisabeth Stream Cipher. ASIACRYPT 2022. .

A Complete Study of Two Classes of Boolean Functions: Direct Sums of Monomials and Threshold Functions. IEEE Transactions on Information Theory 2022. .

Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. EUROCRYPT 2016. .

From at Least $n/3$ to at Most $3\sqrt{n}$: Correcting the Algebraic Immunity of the Hidden Weight Bit Function. LATINCRYPT 2025. .

Funding and Projects

- **FRS-FNRS "Moove In" postdoctoral grant**, PI, 2019–2021.
- Research staff on ERC CLOUDMAP, ERC SWORD, CHIST-ERA SECODE, H2020 SAFECrypto, FUI CryptoComp, ANR CLE.
- Mobility grant from FRS-FNRS, Belgium, 2020.

Supervision and Teaching

- Supervision of Master students and research interns in cryptography; 6 out of 7 supervised Master internships have resulted in peer-reviewed publications, with the most recent work currently under review.
- Co-supervision and mentoring of PhD research: Clément Hoffmann, UCL; 9 publications during the PhD, including 6 joint papers, with continued collaboration after completion.
- Lecturer, *Security 1*, University of Luxembourg, 2023–2024 and 2025–2026.
- Teaching assistant in cryptology, blockchain, theory of computation, optimization, algebra and analysis.

Professional Service

- Program Committee member: TCHES 2022–2024 and 2026–2027, ASIACRYPT 2023 and 2026, FHE 2026, BFA 2025–2026, SETA 2026, SCN 2024, INSCRYPT 2023, ISC 2025, ICSP 2021, A2C 2019.
- Active reviewer for conferences and journals in cryptography and discrete mathematics, with approximately 50 reviews and subreviews per year.
- Reviewer for funding agencies, including ANR and occasional external reviewing for U.S. funding programs.
- Guest editor, *Cryptography*, special issue on side-channel and fault injection attacks.

International Collaborations

Frequent research visits, typically several per year, closely integrated with ongoing research projects and resulting in sustained collaborations and joint publications. Recent collaborations and visits include ANSSI, IMDEA Software Institute, NTT Tokyo, University of Bergen / Selmer Center, Shanghai University, NISER Bhubaneswar, IIIT Vadodara, ISTA Vienna, and LIRMM, several of which developed into long-term collaborations.