Gaëtan Cassiers, Ph.D.

gaetan@cassiersg.be
https://perso.cassiersg.be

Experience

Jan. 2024 –	**Postdoctoral researcher.** Belgian Fund for Scientific Research (F.R.S.-FNRS).
Oct. 2022 – Dec. 2023	**Postdoctoral researcher.** IAIK, TU Graz (Austria).
Feb. 2022 –	**Administrator, contributor.** SIMPLE-Crypto (https://www.simple-crypto.dev/).
Oct. 2018 – Sept. 2022	**Research fellow.** Belgian Fund for Scientific Research (F.R.S.-FNRS).
Jul. – Aug. 2017	**Intern.** Center for Bits and Atoms, Massachusetts Institute of Technology.

Education

2018 – 2022	**Ph.D. Engineering, UCLouvain** Thesis: *Composable and efficient masking schemes for side-channel secure implementations.* Supervisor: François-Xavier Standaert
2016 – 2018	**M.Sc. Electrical Engineering, UCLouvain** Thesis: *Masking Against Side-Channel Attacks: Security and Performance Improvements*. Thesis supervisor: François-Xavier Standaert
2013 – 2016	**B.Sc. Engineering, UCLouvain**

Publications

Journal Articles

[1] Aikata, Andrea Basso, Gaëtan Cassiers, Ahmet Can Mert, and Sujoy Sinha Roy. "Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 366–390. DOI: 10.46586/tches.v2023.i3.366-390.

[2] Melissa Azouaoui, Olivier Bronchain, Gaëtan Cassiers, Clément Hoffmann, Yulia Kuzovkova, Joost Renes, Tobias Schneider, Markus Schönauer, François-Xavier Standaert, and Christine van Vredendaal. "Protecting Dilithium against Leakage Revisited Sensitivity Analysis and Improved Implementations". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.4 (2023), pp. 58–79. DOI: 10.46586/tches.v2023.i4.58-79.

[3] Gaëtan Cassiers and Olivier Bronchain. "SCALib: A Side-Channel Analysis Library". In: *J. Open Source Softw.* 8.86 (2023), p. 5196. DOI: 10.21105/joss.05196.

[4] Gaëtan Cassiers, Henri Devillez, François-Xavier Standaert, and Balazs Udvarhelyi. "Efficient Regression-Based Linear Discriminant Analysis for Side-Channel Security Evaluations Towards Analytical Attacks against 32-bit Implementations". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 270–293. DOI: 10.46586/tches.v2023.i3.270-293.

[5] Gaëtan Cassiers, Loïc Masure, Charles Momin, Thorben Moos, and François-Xavier Standaert. "Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.2 (2023), pp. 482–518. DOI: 10.46586/tches.v2023.i2.482-518.

[6] Loïc Masure, Gaëtan Cassiers, Julien M. Hendrickx, and François-Xavier Standaert. "Information Bounds and Convergence Rates for Side-Channel Security Evaluators". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 522–569. DOI: 10.46586/tches.v2023.i3.522-569.

[7] Olivier Bronchain and Gaëtan Cassiers. "Bitslicing Arithmetic/Boolean Masking Conversions for Fun and Profit with Application to Lattice-Based KEMs". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 553–588. DOI: 10.46586/tches.v2022.i4.553-588.

[8] Yaobin Shen, Thomas Peters, François-Xavier Standaert, Gaëtan Cassiers, and Corentin Verhamme. "Triplex: an Efficient and One-Pass Leakage-Resistant Mode of Operation". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 135–162. DOI: 10.46586/tches.v2022.i4.135-162.

[9] Gaëtan Cassiers, Benjamin Grégoire, Itamar Levi, and François-Xavier Standaert. "Hardware Private Circuits: From Trivial Composition to Full Verification". In: *IEEE Trans. Computers* 70.10 (2021), pp. 1677–1690. DOI: 10.1109/TC.2020.3022979.

[10] Gaëtan Cassiers and François-Xavier Standaert. "Provably Secure Hardware Masking in the Transition- and Glitch-Robust Probing Model: Better Safe than Sorry". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.2 (2021), pp. 136–158. DOI: 10.46586/tches.v2021.i2.136-158.

[11] Charles-Henry Bertrand Van Ouytsel, Olivier Bronchain, Gaëtan Cassiers, and François-Xavier Standaert. "How to fool a black box machine learning based side-channel security evaluation". In: *Cryptogr. Commun.* 13.4 (2021), pp. 573–585. DOI: 10.1007/s12095-021-00479-x.

[12] Davide Bellizia, Francesco Berti, Olivier Bronchain, Gaëtan Cassiers, Sébastien Duval, Chun Guo, Gregor Leander, Gaëtan Leurent, Itamar Levi, Charles Momin, Olivier Pereira, Thomas Peters, François-Xavier Standaert, Balazs Udvarhelyi, and Friedrich Wiemer. "Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher". In: *IACR Trans. Symmetric Cryptol.* 2020.S1 (2020), pp. 295–349. DOI: 10.13154/tosc.v2020.iS1.295-349.

[13] Gaëtan Cassiers and François-Xavier Standaert. "Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference". In: *IEEE Trans. Inf. Forensics Secur.* 15 (2020), pp. 2542–2555. DOI: 10.1109/TIFS.2020.2971153.

[14] Weijia Wang, Pierrick Méaux, Gaëtan Cassiers, and François-Xavier Standaert. "Efficient and Private Computations with Code-Based Masking". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2020.2 (2020), pp. 128–171. DOI: 10.13154/tches.v2020.i2.128-171.

[15] Gaëtan Cassiers and François-Xavier Standaert. "Towards Globally Optimized Masking: From Low Randomness to Low Noise Rate or Probe Isolating Multiplications with Reduced Randomness and Security against Horizontal Attacks". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2019.2 (2019), pp. 162–198. DOI: 10.13154/tches.v2019.i2.162-198.

Conference Papers

[16] Sonia Belaïd, Gaëtan Cassiers, Matthieu Rivain, and Abdul Rahman Taleb. "Unifying Freedom and Separation for Tight Probing-Secure Composition". In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 440–472. DOI: 10.1007/978-3-031-38548-3_15.

[17] Charles Momin, Gaëtan Cassiers, and François-Xavier Standaert. "Handcrafting: Improving Automated Masking in Hardware with Manual Optimizations". In: *Constructive Side-Channel Analysis and Secure Design - 13th International Workshop, COSADE 2022, Leuven, Belgium, April 11-12, 2022, Proceedings*. Ed. by Josep Balasch and Colin O'Flynn. Vol. 13211. Lecture Notes in Computer Science. Springer, 2022, pp. 257–275. DOI: 10.1007/978-3-030-99766-3_12.

[18] Corentin Verhamme, Gaëtan Cassiers, and François-Xavier Standaert. "Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Competition's Finalists". In: *Smart Card Research and Advanced Applications - 21st International Conference, CARDIS 2022, Birmingham, UK, November 7-9, 2022, Revised Selected Papers*. Ed. by Ileana Buhan and Tobias Schneider. Vol. 13820. Lecture Notes in Computer Science. Springer, 2022, pp. 290–308. DOI: 10.1007/978-3-031-25319-5_15.

[19] Gaëtan Cassiers, Sebastian Faust, Maximilian Orlt, and François-Xavier Standaert. "Towards Tight Random Probing Security". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*. Ed. by Tal Malkin and Chris Peikert. Vol. 12827. Lecture Notes in Computer Science. Springer, 2021, pp. 185–214. DOI: 10.1007/978-3-030-84252-9_7.

[20] Charles Momin, Gaëtan Cassiers, and François-Xavier Standaert. "Unprotected and Masked Hardware Implementations of Spook v2". In: *Security and Implementation of Lightweight Cryptography Workshop, Proceedings*. 2021.

[21] Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. "Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography - A Practical Guide Through the Leakage-Resistance Jungle". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part I*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12170. Lecture Notes in Computer Science. Springer, 2020, pp. 369–400. DOI: 10.1007/978-3-030-56784-2_13.

[22] Weijia Wang, Chun Guo, François-Xavier Standaert, Yu Yu, and Gaëtan Cassiers. "Packed Multiplication: How to Amortize the Cost of Side-Channel Masking?" In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December*

7-11, 2020, Proceedings, Part I. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. Lecture Notes in Computer Science. Springer, 2020, pp. 851–880. DOI: 10.1007/978-3-030-64837-4_28.

[23] Gilles Barthe, Sonia Belaïd, Gaëtan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire, and François-Xavier Standaert. "maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults". In: *Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part I*. Ed. by Kazue Sako, Steve A. Schneider, and Peter Y. A. Ryan. Vol. 11735. Lecture Notes in Computer Science. Springer, 2019, pp. 300–318. DOI: 10.1007/978-3-030-29959-0_15.

[24] Gaëtan Cassiers, Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. "SpookChain: Chaining a Sponge-Based AEAD with Beyond-Birthday Security". In: *Security, Privacy, and Applied Cryptography Engineering - 9th International Conference, SPACE 2019, Gandhinagar, India, December 3-7, 2019, Proceedings*. Ed. by Shivam Bhasin, Avi Mendelson, and Mridul Nandi. Vol. 11947. Lecture Notes in Computer Science. Springer, 2019, pp. 67–85. DOI: 10.1007/978-3-030-35869-3_7.

Book Chapters

[25] Gaëtan Cassiers. "Probing Model". In: *Encyclopedia of Cryptography, Security and Privacy*. Ed. by Sushil Jajodia, Pierangela Samarati, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2022, pp. 1–3. ISBN: 978-3-642-27739-9. DOI: 10.1007/978-3-642-27739-9_1699-1.

Other works (incl. unpublished)

[26] Sonia Belaïd, Gaëtan Cassiers, Camille Mutschler, Matthieu Rivain, Thomas Roche, François-Xavier Standaert, and Abdul Rahman Taleb. "Towards Achieving Provable Side-Channel Security in Practice". In: *IACR Cryptol. ePrint Arch.* (2023), p. 1198.

[27] Gaëtan Cassiers, Löic Masure, Charles Momin, Thorben Moos, Amir Moradi, and François-Xavier Standaert. "Randomness Generation for Secure Hardware Masking - Unrolled Trivium to the Rescue". In: *IACR Cryptol. ePrint Arch.* (2023), p. 1134.

[28] Gaëtan Cassiers. "Composable and efficient masking schemes for side-channel secure implementations". PhD thesis. Catholic University of Louvain, Louvain-la-Neuve, Belgium, 2022.

[29] Olivier Bronchain, Gaëtan Cassiers, and François-Xavier Standaert. "Give Me 5 Minutes: Attacking ASCAD with a Single Side-Channel Trace". In: *IACR Cryptol. ePrint Arch.* (2021), p. 817.

[30] Davide Bellizia, Francesco Berti, Olivier Bronchain, Gaëtan Cassiers, Sébastien Duval, Chun Guo, Gregor Leander, Gaëtan Leurent, Itamar Levi, Charles Momin, Olivier Pereira, Thomas Peters, François-Xavier Standaert, Balazs Udvarhelyi, and Friedrich Wiemer. "Spook: Updates on the Round-2 Submission". In: *NIST Lightweight Cryptography Round 2 Candidates* (2020).

[31] Olivier Brochain, Gaëtan Cassiers, and François-Xavier Standaert. *Secure and Efficient Masking of Lightweight Ciphers in Software and Hardware (with Application to the Spook AEAD)*. 2020.

Grants and Awards

2023	ICTEAM thesis award.
2023 - 2026	Postdoctoral fellowship from the Belgian Fund for Scientific Research (F.R.S.-FNRS).
2018 - 2022	Ph.D. fellowship from the Belgian Fund for Scientific Research (F.R.S.-FNRS).

Academic activities

Teaching Assistant at UCLouvain

2021	Project in Electrical Engr.: Integration of wireless embedded sensing systems [LELEC2102]
	Project in Electrical Engr.: Optimization of wireless embedded sensing systems [LELEC2103]
2019, 2020, 2021	Cryptography [LMAT2450]
2018, 2019, 2020	Privacy Enhancing technology [LELEC2770]
2018	Basic analog and digital electronic circuits [LELEC1530]

Academic activities (continued)

Teaching at TU Graz

2023	Side-channel secutiry (masking lectures).

Service

	Co-organizer of the SMAesH Challenge at CHES 2023.
	PC member of CRYPTO 2023 and CCS 2023.
2022	Co-organizer of the Spook SCA Challenge at CHES 2022.
2021-2022	PC member for the CHES 2022 artifacts.
	Reviewer or external reviewer: TCHES, Journal of Cryptographic Engineering, Cryptography and Communications, HOST 2020, Eurocrypt 2020, Asiacrypt 2021, CRPTO 2022, Eurocrypt 2023.