Curriculum Vitæ

1 General information

Geoffroy Couteau

Born on 08/30/1991. Married, two children (born 2022 and 2025).
Nationality: French
URL for website: `http://geoffroycouteau.fr`
ORCID: 0000-0002-6645-0106
Personal address: 13 rue Dumur, 92110, Clichy

Education

- Doctor of Computer Science, École Normale Supérieure de Paris (PSL University), Nov. 30, 2017
- Master of Research in Computer Science (MPRI), Université de Paris, September 2014
- Engineering Degree, Télécom Paristech, September 2014

Current position

Chargé de Recherche (CRCN) at CNRS.
IRIF, UMR 8243, CNRS & Université Paris Cité (since October 2019)
HDR defended on March 20, 2024.

Postdoctoral position: Karlsruhe Institute of Technology (Karlsruhe, Germany), from October 2017 to September 2019. Financial support: ERC PREP-CRYPTO (PI: Dennis Hofheinz).

Research

Area: cryptography, and neighboring areas such as security and complexity theory.

Publications: 66 publications in peer-reviewed international conferences and journals, including 37 in top conferences and journals (CRYPTO, EUROCRYPT, CCS, FOCS, Journal of Cryptology) and 20 in strong ('rank A') conferences and journals (ASIACRYPT, TCC, ITCS, RANDOM, ToSC).

Invited Talks: Fourth Information-Theoretic Cryptography conference (ITC 2023).

Recent Contracts: Principal investigator of OBELiSC (ERC Starting Grant, 2024 – 2029, €1.5M), SCENE (ANR JCJ, 2021 – 2024, €170k), and LICENCED (DIM RFSI, 2022 – 2023, €60k). Local coordinator & work package manager of SecureCompute (PEPR Cybersécurité, 2022 – 2028, €5M / €1M IRIF). Member of BARRACUDA (ANR PRC, 2021 – 2025) and A2C (ANR JCJC, 2024 – 2027).

Animation and responsibilities

- Member of the scientific council of the UFR (since 2020) and of the laboratory (since 2023). President of the IRIF & Environment commission (since 2022).
- **Program committees:** Communication in Cryptology 2024, CSF (2023, 2022), CRYPTO 2023, PKC 2022, SCN 2022, EUROCRYPT (2021, 2020), IWSEC (2021, 2020), TCC (2019, 2024), WAHC (2022, 2021, 2020, 2019)
- **Membership in thesis juries:**
  ▶ Sacha Servan-Schreiber, MIT (Boston, USA), New Tools for On-the-Fly Secure Computation, *Examiner*, December 2024.
  ▶ Lennart Braun, Aarhus University (Aarhus, Denmark), Cryptography after Prime Time, *Reviewer* & *Examiner*, September 2024.
  ▶ Axel Durbet, Université Clermont Auvergne, Une approche cryptographique des systèmes d'authentification biométrique respectant la vie privée, *Reviewer* & *Examiner*, November 2024.
  ▶ Jules Maire, Sorbonne Université, Zero-Knowledge Arguments from Secure Multiparty Computation, *Examiner*, October 2024.
  ▶ Sihang Pu, CISPA Helmholtz Center for information security (Saarbrucken, Germany), *Reviewer*

& *Examiner*, October 2023.
▶ Javier Silva, UPF (Barcelona, Spain), *Examiner*, March 2021.
▶ Clara Pernot, INRIA Paris, *Examiner*, February 2024.
▶ Thibauld Feneuil, Sorbonne University, *Examiner*, October 2023.

- **Reviewer for international funding agencies:** German National Research Center for Applied Cybersecurity (ATHENE), 2023 and 2025. Independent Research Fund Denmark (DFF), 2022. Israel Science Foundation (ISF), 2022 and 2023.
- Member of the **organizing committee of ICALP'22**, responsible for the conference budget (conceiving and maintaining the budget, validating every spending, finding sponsors, organizing the conference in a hybrid mode to mitigate its environmental impact).

Diffusion, supervision and teaching

- Supervision of 6 PhDs (three defended), 10 postdocs (incl. 5 starting in early 2025), 5 Master students, 7 summer interns, and 4 extended visits ($>$ 5 months) of PhD students.
- Teaching on average 80 hours / year at Université Paris Cité, Télécom Paris, ENS Lyon, EIDD, ANSSI, and Sorbonne Université from 2019 to 2024.
- Intervention in the written press: with Pierre-Evariste Dagand, I contributed a blog post[1] to Binaire, a blog of the newspaper Le Monde.
- I am strongly involved in disseminating knowledge about cryptography to students and cryptography enthusiasts. In particular, I am an active contributors to the cryptography StackExchange network[2].
- I coauthored a book chapter for an upcoming book on advanced methods in cryptography. The chapter is available on my website[3].
- I recently completed a book, *An Introduction to Silent Secure Computation*[4].

2 Scientific output

Summary of my research activity

My research work addresses a broad range of questions and challenges within the field of cryptography, and some neighboring fields such as security and complexity theory. More specifically, most of my contributions to cryptography fit within one or several of the following topics:

- **Secure Computation**, a branch of cryptography that develops methods to distributively perform calculations on sensitive inputs without compromising their privacy. My research work has contributed to secure computation at large, both on practical aspects (developing protocols with better concrete efficiency) and theoretical aspects (studying the theoretical feasibility of secure computation under constraints on resources and for various adversarial models).
- **Zero-knowledge proofs**, a class of cryptographic primitives whose purpose is to allow a prover to demonstrate the truth of a statement, while concealing all other information beyond this. My contributions range from theoretical questions regarding the existence of zero-knowledge proofs with minimal interactivity to the design of concretely efficient zero-knowledge proofs and their application to real-world security problems.
- **The theoretical foundations of cryptography.** My research in this area studies both the minimal hardness assumptions on which cryptography can be based and the existence of cryptographic primitives in low-complexity classes. My work also investigates connections between cryptography and various fields of complexity theory such as fine-grained complexity, learning theory, circuit lower bounds, oracle separations, and average-case hardness.

[1] https://www.lemonde.fr/blog/binaire/2023/05/26/controler-lacces-aux-sites-web-pour-adultes-est-ce-possible/
[2] https://crypto.stackexchange.com/users/31767/geoffroy-couteau
[3] https://geoffroycouteau.github.io/assets/pdf/HSS_FSS.pdf4
[4] https://link.springer.com/book/9783032070883?srsltid=AfmBOoo_E9c8niSHQPQ2SAXMETRn6JRSieOexcO3bE5LzMB_YCspMOm6

Among these topics, the study of **secure computation** is my core activity. A significant portion of my work is motivated by the goal of making secure computation widely usable in the real-world. This is true both of my more practice-oriented work (finding faster and lighter secure computation methods) and of my more theoretical work (where I seek to pinpoint why some paradigms seem to be inherently stuck at some theoretical barriers) – practical results and theoretical results are tightly intertwined in my articles, and often feed into each other.

Full list of publications

In cryptography, conference publications are typically preferred over journals and are the primary means for disseminating new results. The most prestigious cryptography conferences are CRYPTO and EUROCRYPT, followed by ASIACRYPT and TCC, and the other conferences of the International Association for Cryptologic Research (PKC, FSE/ToSC, CHESS). The most prestigious security conferences are CCS, S&P, NDSS, and Usenix, and the most prestigious theoretical computer science conferences are FOCS and STOC. The top cryptography journal, the Journal of Cryptography (whose level is on par with CRYPTO and EUROCRYPT), publishes extended version of papers previously published at top IACR conferences or original papers.

There is no notion of first author: authors are ranked alphabetically on the papers. Since 2015, my work has resulted in 66 publications, all at peer-reviewed international conferences and journals (including 37 in top conferences and journals, and 20 in other 'rank A' conferences and journals).

66. Pseudorandom Correlation Functions for Garbled Circuits, *TCC 2025*, Geoffroy Couteau, Srinivas Devadas, Alexander Koch, and Sacha Servan-Schreiber

65. Multiparty Homomorphic Secret Sharing and More from LPN and MQ, *TCC 2025*, Geoffroy Couteau, Naman Kumar, and Xiaxi Ye

64. Fast Pseudorandom Correlation Functions from Sparse LPN, *ASIACRYPT 2025*, Lennart Braun, Geoffroy Couteau, Kelsey Melissaris, Mahshid Riahinia, and Elahe Sadeghi

63. SoK: On Shallow Weak PRFs, *ToSC 2025*, Christina Boura, Geoffroy Couteau, Léo Perrin, and Yann Rotella

62. Instantiating the Hash-Then-Evaluate Paradigm: Strengthening PRFs, PCFs, and OPRFs, *Cryptography and Communications 2025*, Chris Brzuska, Geoffroy Couteau, Christoph Egger, and Pierre Meyer

61. Structured-Seed Local Pseudorandom Generators and their Applications, *RANDOM 2025*, Benny Applebaum, Dung Bui, Geoffroy Couteau, and Nikolas Melissaris

60. Downlink (T)FHE ciphertexts compression, *SAC 2025*, Antonina Bondarchuk, Olive Chakraborty, Geoffroy Couteau, and Renaud Sirdey

59. $\omega(1/\lambda)$-Rate Boolean Garbling Scheme from Generic Groups, *CRYPTO 2025*, Geoffroy Couteau, Carmit Hazay, Aditya Hegde, and Naman Kumar

58. Multi-key Homomorphic Secret Sharing, *EUROCRYPT 2025*, Geoffroy Couteau, Lalita Devadas, Aditya Hegde, Abhishek Jain, and Sacha Servan-Schreiber

57. Breaking the $1/\lambda$-Rate Barrier for Arithmetic Garbling, *EUROCRYPT 2025*, Geoffroy Couteau, Carmit Hazay, Aditya Hegde, and Naman Kumar

56. Enhanced Trapdoor Hashing from DDH and DCR, *EUROCRYPT 2025*, Geoffroy Couteau, Aditya Hegde, and Sihang Pu

55. An Efficient ZK Compiler from SIMD Circuits to General Circuits, *Journal of Cryptology 2025*, Dung Bui, Haotian Chu, Geoffroy Couteau, Xiao Wang, Chenkai Weng, Kang Yang, and Yu Yu

54. On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness, *Journal of Cryptology 2025*, Chris Brzuska and Geoffroy Couteau

53. On Bounded Storage Key Agreement and One-Way Functions, *TCC 2024*, Chris Brzuska, Christoph Egger, Geoffroy Couteau, and Willy Quach

52. Depth-Reduction Algorithms for Directed Acyclic Graphs and Applications to Secure Multiparty Computation, *TCC 2024*, Pierre Charbit, Geoffroy Couteau, Pierre Meyer, and Reza Naserasr

51. FOLEAGE: F4-OLE-Based Multi-Party Computation for Boolean Circuits, *ASIACRYPT 2024*, Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, and Sacha Servan-Schreiber

50. Lightweight Oblivious Transfer with a Public-Key Setup, *ASIACRYPT 2024*, Geoffroy Couteau, Lalita Devadas, Srinivasan Devadas, Alexander Koch, and Sacha Servan-Schreiber

49. Faster Signatures from MPC-in-the-Head, *ASIACRYPT 2024*, Dung Bui, Eliana Carozza, Geoffroy Couteau, Dahmun Goudarzi, and Antoine Joux

48. Instantiating the Hash-Then-Evaluate Paradigm: Strengthening PRFs, PCFs, and OPRFs, *SCN 2024*, Chris Brzuska, Geoffroy Couteau, Christoph Egger, and Pierre Meyer

47. Fine-Grained Non-Interactive Key Exchange, Revisited, *CRYPTO 2024*, Balthazar Bauer, Geoffroy Couteau, and Elahe Sadeghi

46. 10-Party Sublinear Secure Computation from Standard Assumptions, *CRYPTO 2024*, Geoffroy Couteau and Naman Kumar

45. Fast Public-Key Silent OT and More from Constrained Naor-Reingold, *EUROCRYPT 2024*, Dung Bui, Geoffroy Couteau, Pierre Meyer, Alain Passelègue, Mahshid Riahinia

44. A Note on Non-Interactive Zero-Knowledge from CDH, *CRYPTO 2023*, Geoffroy Couteau, Abhishek Jain, Zhengzhong Jin, and Willy Quach

43. Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding, *CRYPTO 2023*, Maxime Bombar, Geoffroy Couteau, Alain Couvreur, and Clément Ducros

42. Constrained Pseudorandom Functions from Homomorphic Secret Sharing, *EUROCRYPT 2023*, Geoffroy Couteau, Pierre Meyer, Alain Passelègue, and Mahshid Riahinia

41. Sublinear-Communication Secure Multiparty Computation does not require FHE, *EUROCRYPT 2023*, Elette Boyle, Geoffroy Couteau, and Pierre Meyer

40. Short Signatures from Regular Syndrome Decoding in the Head, *EUROCRYPT 2023*, Eliana Carozza, Geoffroy Couteau, and Antoine Joux

39. Fine-Grained Non-Interactive Key-Exchange: Constructions and Lower Bounds, *EUROCRYPT 2023*, Abtin Afshar, Geoffroy Couteau, Mohammad Mahmoody, and Elahe Sadeghi

38. Oblivious Transfer with Constant Computational Overhead, *EUROCRYPT 2023*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl

37. Improved Private Set Intersection for Sets with Small Entries, *PKC 2023*, Geoffroy Couteau and Dung Bui

36. Pseudorandom Correlation Functions from Variable-Density LPN, Revisited, *PKC 2023*, Geoffroy Couteau and Clément Ducros

35. Sublinear Secure Computation from New Assumptions, *TCC 2022*, Elette Boyle, Geoffroy Couteau, and Pierre Meyer

34. Anonymous Whistleblowing over Authenticated Channels, *TCC 2022*, Thomas Agrikola, Geoffroy Couteau, and Sven Maier

33. Random Sources in Private Computation, *ASIACRYPT 2022*, Geoffroy Couteau and Adi Rosén

32. Non-Interactive Secure Computation of Inner-Product from LPN and LWE, *ASIACRYPT 2022*, Geoffroy Couteau and Maryam Zarezadeh

31. Sharp: Short Relaxed Range Proofs, *CCS 2022*, Geoffroy Couteau, Dahmun Goudarzi, Michael Klooß, and Michael Reichle

30. Correlated Pseudorandomness from Expand-Accumulate Codes, *CRYPTO 2022*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl

29. On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness, *EUROCRYPT 2022*, Chris Brzuska and Geoffroy Couteau

28. Statistical ZAPs from Group-Based Assumptions, *TCC 2021*, Geoffroy Couteau, Shuichi Katsumata, Elahe Sadeghi, and Bogdan Ursu

27. On Derandomizing Yao's Weak-to-Strong OWF Construction, *TCC 2021*, Chris Brzuska, Geoffroy Couteau, Pihla Karanko, and Felix Rohrbach

26. Efficient NIZKs for Algebraic Sets, *ASIACRYPT 2021*, Geoffroy Couteau, Helger Lipmaa, Roberto Parisella, and Arne Tobias Ødegaard

25. Low-Complexity Weak Pseudorandom Functions in AC0[MOD2], *CRYPTO 2021*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl

24. Silver: Silent VOLE and Oblivious Transfer from Hardness of Decoding Structured LDPC Codes, *CRYPTO 2021*, Geoffroy Couteau, Srinivasan Raghuraman, and Peter Rindal

23. Partially-Fair Computation from Timed-Release Encryption and Oblivious Transfer, *ACISP 2021*, Geoffroy Couteau, Bill Roscoe, and Peter Ryan

22. Breaking the Circuit Size Barrier for Secure Computation under Quasi-Polynomial LPN, *EUROCRYPT 2021*, Geoffroy Couteau and Pierre Meyer

21. Efficient Range Proofs with Transparent Setup from Bounded Integer Commitments, *EUROCRYPT 2021*, Geoffroy Couteau, Michael Klooß, Huang Lin, and Michael Reichle

20. Black-Box Uselessness: Composing Separations in Cryptography , *ITCS 2021*, Geoffroy Couteau, Pooya Farshim, and Mohammad Mahmoody

19. On Pseudorandom Encodings, *TCC 2020*, Thomas Agrikola, Geoffroy Couteau, Yuval Ishai, Stanislaw Jarecki, Amit Sahai

18. Pseudorandom Correlation Functions from Variable-Density LPN, *FOCS 2020*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Scholl

17. Shorter Non-Interactive Zero-Knowledge Arguments and ZAPs for Algebraic Languages *CRYPTO 2020*, Geoffroy Couteau, Dominik Hartmann

16. Efficient Pseudorandom Correlation Generators from Ring-LPN, *CRYPTO 2020*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Scholl

15. Non-Interactive Zero-Knowledge in Pairing-Free Groups from Weaker Assumptions, *EUROCRYPT 2020*, Geoffroy Couteau, Shuichi Katsumata, and Bogdan Ursu

14. The Usefulness of Sparsifiable Inputs: How to Avoid Subexponential iO *PKC 2020*, Thomas Agrikola, Geoffroy Couteau, and Dennis Hofheinz

13. 2019 Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation, *CCS 2019*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal,Peter Scholl

12. Efficient Pseudorandom Correlation Generators: Silent OT Extension and More, *CRYPTO 2019*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Scholl

11. A Note on the Communication Complexity of Multiparty Computation in the Correlated Randomness Model, *EUROCRYPT 2019*, Geoffroy Couteau

10. Designated-Verifier Pseudorandom Generators, and their Applications *EUROCRYPT 2019*, Geoffroy Couteau and Dennis Hofheinz

9. Non-Interactive Keyed-Verification Anonymous Credentials *PKC 2019*, Geoffroy Couteau and Michael Reichle

8. On the Concrete Security of Goldreich's Pseudorandom Generator, *ASIACRYPT 2018*, Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Melissa Rossi, and Yann Rotella

7. Compressing Vector-OLE, *CCS 2018*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai

6. New Protocols for Secure Equality Test and Comparison, *ACNS 2018*, Geoffroy Couteau

5. Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge *EUROCRYPT 2018*, Pyrros Chaidos, and Geoffroy Couteau

4. Homomorphic Secret Sharing: Optimizations and Applications, *CCS 2017*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù

3. Removing the Strong RSA Assumption from Arguments over the Integers, *EUROCRYPT 2017*, Geoffroy Couteau, Thomas Peters, and David Pointcheval

2. Encryption Switching Protocols, *CRYPTO 2016*, Geoffroy Couteau, Thomas Peters, and David Pointcheval

1. Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting, *CRYPTO 2015*, Fabrice Benhamouda, Geoffroy Couteau, David Pointcheval, and Hoeteck Wee