

Curriculum Vitæ

1 General information

Geoffroy Couteau

Born on 08/30/1991.

Nationality: French

URL for website: <http://geoffroycouteau.fr>

ORCID: 0000-0002-6645-0106

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.

Assignment: IRIF, UMR 8243, CNRS & Université Paris Cité (since October 2019)

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

Research

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

Publications: 45 publications in peer-reviewed international conferences, including 29 in top conferences (CRYPTO, EUROCRYPT, CCS, FOCS) and 10 in strong ('rank A') conferences (ASIACRYPT, TCC, ITCS).

Contracts

As principal investigator:

- **ERC Starting Grant – project OBELISC** (€1.5M). The project will start in 2024.
- **ANR JCJC Grant – project SCENE** (€170k). The project spans from January 2021 to December 2024 and involves Adi Rosén (DR CNRS, IRIF) and Yann Rotella (MCF, UVSQ).
- **DIM RFSI Grant – project LICENCED** (€65k). The project dealt with the study of linear codes for use in secure computation. It lasted from 2022 to 2023.

In addition, I am a local coordinator and work package manager of the **PEPR Cybersécurité – project SecureCompute** (€5M, incl. €1M for IRIF). The project SecureCompute revolves around a consortium of three institutes: ENS/PSL, CNRS, and CEA. David Pointcheval is the principal investigator and the coordinator for ENS/PSL. I am the main coordinator for CNRS and the manager of the Secure Computation work package (WP4).

Animation and responsibilities

- Member of the scientific council of the UFR (since 2020) and of the scientific council of the laboratory (since 2023).
- President of the IRIF & Environment commission (since 2022).
- **Program committees and editorial boards:** Communication in Cryptology (2024), CSF (2023, 2022), CRYPTO 2023, PKC 2022, SCN 2022, EUROCRYPT (2021, 2020), IWSEC (2021, 2020), TCC (2024, 2019), WAHC (2022, 2021, 2020, 2019)

- **Membership in thesis juries:** Sihang Pu, CISA Helmholtz Center for information security (Saarbrücken, Germany) – Reviewer & Examiner, October 2023; Javier Silva, UPF (Barcelona, Spain), – Examiner, March 2021; Clara Pernot, INRIA Paris – Examiner, February 2024; Thibault Feneuil, Sorbonne University – Examiner, October 2023.
- **Reviewer for international funding agencies:** German National Research Center for Applied Cybersecurity (ATHENE), 2023; Independent Research Fund Denmark (DFF), 2022; Israel Science Foundation (ISF), 2022 and 2023
- Member of the **organizing committee of ICALP’22**, responsible for the entire 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 5 PhDs (one defended), 4 postdocs, 4 Master students, 4 interns.
- Teaching on average 80 hours / year at Université Paris Cité, Télécom Paris, ENS Lyon, EIDD, ANSSI, and Sorbonne Université.
- Intervention in the written press: with Pierre-Evariste Dagand, I contributed a blog post¹ 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 network²
- I coauthored a book chapter for an upcoming book on advanced methods in cryptography. The chapter is available on my website³.

Scientific distinctions

- My paper *On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness*, co-authored with Chris Brzuska and presented at EUROCRYPT 2022, was invited to the Journal of Cryptology
- I received a honorary mention for my PhD from the GDR computer security PhD prize⁴.
- I was an invited Spotlight Speaker at the fourth Information-Theoretic Cryptography Conference ITC 2023

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.

¹<https://www.lemonde.fr/blog/binaire/2023/05/26/controler-laces-aux-sites-web-pour-adultes-est-ce-possible/>

²<https://crypto.stackexchange.com/users/31767/geoffroy-couteau>

³https://geoffroycouteau.github.io/assets/pdf/HSS_FSS.pdf

⁴gdr-securite.iris.fr/prix-de-these/

- **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.

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

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 Mahmoodi, 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 Kloof, 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 Kloof, 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