Geoffroy COUTEAU

French geoffroy.couteau@irif.fr www.geoffroycouteau.fr

Work Experience

Oct 2019 – current	CNRS researcher, IRIF, Université de Paris
Oct 2017 – current	Postdoctoral researcher, Karlsruher Institut für Technologie, Germany
Oct 2014 – Sep 2017	PhD student, École Normale Supérieure de Paris, Crypto Team under the supervision of David Pointcheval and Hoeteck Wee Zero-Knowledge Proofs for Secure Computation
Mar 2014 – Sep 2014	Research intern in cryptography in the Crypto team at École Normale Supérieure de Paris Secure multiparty computation protocols for biometric authentication
Jul 2012 – Sep 2012	Research and Development internship at Criteo, Paris Research & Development (C#, ASP.NET)

Publications

43. Constrained Pseudorandom Functions from Homomorphic Secret Sharing, *EUROCRYPT 2023*, Geoffroy Couteau, Pierre Meyer, Alain Passelègue, and Mahshid Riahinia
42. Sublinear-Communication Secure Multiparty Computation does not require FHE, *EUROCRYPT 2023*, Elette Boyle, Geoffroy Couteau, and Pierre Meyer
41. Short Signatures from Regular Syndrome Decoding in the Head, *EUROCRYPT 2023*, Eliana Carozza, Geoffroy Couteau, and Antoine Joux
40. Fine-Grained Non-Interactive Key-Exchange: Constructions and Lower Bounds, *EUROCRYPT 2023*, Abtin Afshar, Mohammad Mahmoody, and Elahe Sadeghi
39. Oblivious Transfer with Constant Computational Overhead, *EUROCRYPT 2023*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl
38. Improved Private Set Intersection for Sets with Small Entries, *PKC 2023*, Geoffroy Couteau and Dung Bui
37. Pseudorandom Correlation Functions from Variable-Density LPN, Revisited, *PKC 2023*, Geoffroy Couteau and Clément Ducros
36. Sublinear Secure Computation from New Assumptions, *TCC 2022*, Elette Boyle, Geoffroy Couteau, and Pierre Meyer
35. Anonymous Whistleblowing over Authenticated Channels, *TCC 2022*, Thomas Agrikola, Geoffroy Couteau, and Sven Maier
34. Random Sources in Private Computation, *ASIACRYPT 2022*, Geoffroy Couteau and Adi Rosén
33. Non-Interactive Secure Computation of Inner-Product from LPN and LWE, *ASIACRYPT 2022*, Geoffroy Couteau and Maryam Zarezadeh

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. 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

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

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

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

10. Non-Interactive Keyed-Verification Anonymous Credentials *PKC 2019*, Geoffroy Couteau and Michael Reichle
9. On the Concrete Security of Goldreich's Pseudorandom Generator, *ASIACRYPT 2018*, Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Melissa Rossi, and Yann Rotella
8. Compressing Vector-OLE, *CCS 2018*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai
7. New Protocols for Secure Equality Test and Comparison, *ACNS 2018*, Geoffroy Couteau
6. Efficient Designated-Verifier Non-Interactive Zero-Knowledge Proofs of Knowledge *EUROCRYPT 2018*, Pyrros Chaidos, and Geoffroy Couteau
5. Homomorphic Secret Sharing: Optimizations and Applications, *CCS 2017*, Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù
4. Removing the Strong RSA Assumption from Arguments over the Integers, *EUROCRYPT 2017*, Geoffroy Couteau, Thomas Peters, and David Pointcheval
3. Encryption Switching Protocols, *CRYPTO 2016*, Geoffroy Couteau, Thomas Peters, and David Pointcheval
2. Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting, *CRYPTO 2015*, Fabrice Benhamouda, Geoffroy Couteau, David Pointcheval, and Hoeteck Wee
1. Secure Distributed Computation on Private Inputs, *FPS 2015*, Geoffroy Couteau, Thomas Peters, and David Pointcheval

Honors, Awards, and Grants

2023	Invited Spotlight Speaker at ITC 2023 https://itcrypto.github.io/2023/2023cfp.html
Apr. 2022	Paper *On Building Fine-Grained One-Way Functions from Strong Average-Case Hardness*, co-authored with Chris Brzuska, invited to the Journal of Cryptology EUROCRYPT 2022, typically top 3 accepted papers
2022 – 2023	DIM RFSI – project LICENCED (€65k) Principal Investigator
2021 – 2024	ANR JCJC – project SCENE (€170k) Principal Investigator https://anr.fr/fileadmin/aap/2020/selection/aapg-selection-2020-08-02102020.pdf
2018	GDR computer security PhD prize, Honorary Mention https://gdr-securite.irisa.fr/prix-de-these/

Invited Speaker

Jun 2023	Conference: Invited Spotlight Speaker at ITC 2023
Jun 2022	Seminar: ENS Crypto Seminar, Paris, France
Apr 2022	Seminar: UC Berkeley Crypto Reading Group, Berkeley, USA
Oct 2021	Seminar: CWI Crypto Student Seminar, Amsterdam, Netherlands
Aug 2021	Summer School: Coding Techniques & Advanced Post-Quantum Cryptography (Digital CISPA summer school 2021)
Jun 2021	Workshop: FILOFOCS, Tel-Aviv, Israel
May 2021	Seminar: ENS Lyon Student Seminar, Lyon, France
May 2021	Seminar: MIT Cryptography and Information Security Seminar, Cambridge, USA
Apr 2021	Seminar: UVSQ Crypto Seminar, Versailles, France
Mar 2021	Seminar: Boston University Security Seminar, Boston, USA
Oct 2020	Seminar: UCLA Crypto Seminar, Los Angeles, USA

Sep 2020	Seminar: Cryptography, Network Security and Cybersecurity, West Bengal, India
Nov 2019	Workshop: FILOFOCS, Tel-Aviv, Israel
Nov 2019	Seminar: C2 seminar, Paris, France
Oct 2019	Seminar: ENS Lyon Crypto Seminar, Lyon, France
Feb 2019	Seminar: ENS Lyon Crypto Seminar, Lyon, France
Jan 2019	Seminar: University of Rennes 1 Crypto Seminar, Rennes, France
Jul 2018	Seminar: UCL Crypto Group Seminar, Louvain-la-neuve, Belgium
Jun 2018	Seminar: University of Luxembourg Crypto Seminar, Esch-sur-Alzette, Luxembourg
May 2018	Workshop: Theory and Practice of Secure Multiparty Computation (TPMPC), 2018
Sep 2017	Seminar: Paris Crypto Day, Paris, France
Mar 2017	Workshop: CryptoAction Symposium, 2017
Nov 2016	Seminar: University of Rennes 1 Crypto Seminar, Rennes, France
May 2016	Workshop: Theory and Practice of Secure Multiparty Computation (TPMPC), 2016

Education

2014 – 2017	PhD Thesis, École Normale Supérieure de Paris, Crypto Team *Zero-Knowledge Proofs for Secure Computation*
2013 – 2014	Parisian Master of Research in Computer Science (MPRI), University of Paris-Diderot, Paris *Specialization in algorithmic and cryptography* *highest honours*
2011 – 2014	Engineering school, Télécom ParisTech, Paris *Algebra, Cryptography, Algorithmic and Theoretical Computer Science*
2008 – 2011	Preparatory class for entrance to Grandes Ecoles (MPSI, MP*), Lycée Buffon, Paris
Jul 2008	Bachelor's degree *highest honours*

Supervising

Postdocs	Oct. 2022 –: Blathazar Bauer Nov. 2022 –: Alexander Koch Nov. 2022 –: Christoph Egger Dec. 2022 –: Sven Meier
PhD Students	Oct. 2021 –: Bui Dung, Secure Computation for Privacy-Preserving Analysis of Medical Data Oct. 2021 –: Clément Ducros, Linear Codes for Quantum-Resistant Secure Computation (co-advised with Alain Couvreur) Oct. 2021 –: Eliana Carozza, Quantumly hard algebraic problems and their advanced cryptographic applications (co-advised with Antoine Joux) Oct. 2021 –: Ulysse Léchine, Average-case hardness, entropy, and one-way functions (co-advised with Thomas Seiller) Sep. 2020 –: Pierre Meyer, Secure computation with restricted communication (co-advised with Elette Boyle, IDC, Israel)
Master Students	Mar. 2021 – Sep. 2021: Clément Ducros, Linear time encodable codes meet secure computation Mar. 2021 – Sep. 2021: Thi Thuy Dung Bui, Batch equality tests and secure comparison from pseudorandom correlation generators Feb. 2020 – Aug. 2020: Michael Reichle, Zero-Knowledge Proofs Apr. 2019 – Oct. 2019: Dominik Hartmann, Compilers for Non-Interactive Zero-Knowledge Proofs

Bachelor Students	Oct. 2018 – Feb. 2019: Sebastian Faller, Lattice-Based Implicit Zero-Knowledge Arguments May 2018 – Sept. 2018: Michael Reichle, Keyed-Verification Non-Interactive Anonymous Credentials Nov. 2017 – Mar. 2018: Samuel Kopmann, Improved Designated-Verifier Non-Interactive Zero-Knowledge Arguments
Interns & visitors	Jun. 2022 – Jul. 2022: Jonathan Etou (Intern) Jun. 2022 – Jul. 2022: Elahe Sadeghi (visiting PhD student) May 2021 – Jun. 2021: Milan Gonzalez-Thauvin (Intern) Nov. 2020 – Apr. 2021: Maryam Zarezadeh (visiting PhD student) Jul. 2020 – Oct. 2020: Elahe Sadeghi (Summer intern) Nov. 2019 – Jan. 2020: Pierre Meyer (Intern)

Teaching

Current	Interactive and Non-Interactive Proofs in Complexity and Cryptography, M1, ENS Lyon (since 2022) Secure Computation, M1, Télécom Paris (2014 – 2017, since 2019) Introduction à la sécurité, M1, IEDD (since 2020) Secure Computation, ANSSI (2021, 2023)
Past	Analyse de données, L3, Sorbonne université (2019 – 2021) Mathématiques discrètes, L3, Université de Paris (2020 – 2022) Concepts Informatique, L1, Université de Paris (2020) Analyse de données, L3, Sorbonne université Seminar Organization, KIT, Germany: Advanced Topics in Lattice-Based Cryptography, Foundations of Lattice-Based Cryptography, Non-Interactive Zero-Knowledge Proofs, Public-Coin Zero-Knowledge Proofs, Cryptography for Smart Meters (2017 – 2019) Teaching assistant at Polytech Paris UMPC: applied algebra, compiling (master level), Java, C (bachelor level) (2014 – 2017)

Thesis Committee

March 2021	Javier Silva, Zero-knowledge proofs and isogeny-based cryptosystems (Examiner)

Services to the Community

Program Committee

2023	CSF 2023, CRYPTO 2023
2022	PKC 2022, CSF 2022, SCN 2022, TCC 2022, WAHC 2022
2021	EUROCRYPT 2021, IWSEC 2021, WAHC 2021
2020	EUROCRYPT 2020, IWSEC 2020, WAHC 2020
2019	TCC 2019, WAHC 2019
2018	INDOCRYPT 2018

Reviewer

Conferences	TCHESS 2022; CRYPTO 2022; EUROCRYPT 2022; TCC 2021; ASIACRYPT 2021; CRYPTO 2021; PKC 2021; STOC 2021; ASIACRYPT 2020; TCC 2020; FOCS 2020; CRYPTO 2020; ITCS 2020; SAC 2019; CRYPTO 2019; PKC 2019; TCC 2018; CCS 2018; CRYPTO 2018; EUROCRYPT 2018; PKC 2018; ASIACRYPT 2017; TCC 2017; ICALP 2017; ACNS 2017; PKC 2017; CT-RSA 2017; CRYPTO 2016; PKC 2016; CT-RSA 2015; EUROCRYPT 2015.
Journals	Computer Journal (2023); Design, Codes, and Cryptography (2022); IEICE (2021); Discrete Mathematics (2021); Journal of Cryptology (2020); ACM Transaction on Computation Theory (2020); Transaction on Dependable and Secure Computing (2020); SN Applied science (2020); Transactions on Information Forensics & Security (2019, 2020); Theoretical Computer Science (2019); Design, Codes, and Cryptography (2018).
Grants	Independent Research Fund Denmark (DFF), 2022; Israel Science Foundation (ISF), 2022

Organization

2020 – 2022	Member of the organization team of ICALP 2022, Paris; handling financial aspects and sponsoring (general chair: Thomas Colcombet)
Apr. 2020 – Sep. 2020	Organizer of a regular seminar on privacy in contact tracing (presentations and debates with experts on security and inventors of the StopCovid protocol, co-organized with Alain Passelègue)
2017	Organizer of the Crypto Working Group, ENS Participation to the organization of EUROCRYPT 2017