Geoffroy Couteau

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

Publications

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

| Breaking the Circuit Size Barrier for Secure Computation under Quasi-Polynomial LPN
In EUROCRYPT 2021
Geoffroy Couteau and Pierre Meyer

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

| Black-Box Uselessness: Composing Separations in Cryptography
In ITCS 2021
Geoffroy Couteau, Pooya Farshim, and Mohammad Mahmoody

2020 | On Pseudorandom Encodings
In TCC 2020
Thomas Agrikola, Geoffroy Couteau, Yuval Ishai, Stanislaw Jarecki, Amit Sahai

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

| Shorter Non-Interactive Zero-Knowledge Arguments and ZAPs for Algebraic Languages
In CRYPTO 2020
Geoffroy Couteau, Dominik Hartmann

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

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

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

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

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

| A Note on the Communication Complexity of Multiparty Computation in the Correlated Randomness Model
In EUROCRYPT 2019
Geoffroy Couteau

| Designated-Verifier Pseudorandom Generators, and their Applications
In EUROCRYPT 2019

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

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)

Honors, Awards, and Grants

Jan. 2021 – Jan. 2025 | 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

Mar 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 Crypo 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

PhD Students	Sep. 2020 –: Pierre Meyer, Secure computation with restricted communication (co-supervised 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	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

2020 – 2021	Secure Computation, M1, Télécom ParisTech Secure Computation, ANSSI Analyse de données, L3, Sorbonne université Introduction à la sécurité, M1, IEDD Mathématiques discrètes, L3, Université de Paris
2019 – 2020	Secure Computation, M1, Télécom ParisTech Concepts Informatique, L1, Université de Paris Analyse de données, L3, Sorbonne université
2017 – 2019	Seminar Organization, KIT, Germany May. 2019 – Jul. 2019: Advanced Topics in Lattice-Based Cryptography May. 2019 – Jul. 2019: Foundations of Lattice-Based Cryptography Oct. 2018 – Feb. 2019: Non-Interactive Zero-Knowledge Proofs Oct. 2018 – Feb. 2019: Public-Coin Zero-Knowledge Proofs May. 2018 – Jul. 2018: Cryptography for Smart Meters
2014 – 2017	Teaching assistant at Polytech Paris UMPC 2016 – 2017 Applied Algebra, Compiling (master level) 2014 – 2016 Java, C (bachelor level), Compiling (master level)
	Lectures at Télécom ParisTech *Secure Multiparty Computation*

Thesis Committee

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

Services to the Community

Program Committee

2022	PKC 2022
2021	EUROCRYPT 2021, IWSEC 2021
2020	EUROCRYPT 2020, IWSEC 2020, WAHC 2020
2019	TCC 2019, WAHC 2019
2018	INDOCRYPT 2018

External reviewer

Conferences	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	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).

Organization

2020 – 2022	I am one of the organizers of the upcoming ICALP 2022, to be held in Paris (with Thomas Colcombet, local chair, and Eva Ryckelynck)
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

Languages

French:	Native
English:	Fluent (C1 CEFR)
German:	Intermediate (B1 CEFR)