Geoffroy Couteau

🌐 French ✉ geoffroy.couteau@kit.edu 💻 www.geoffroycouteau.fr

Publications

Conferences

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

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

Encryption Switching Protocols
In CRYPTO 2016
Geoffroy Couteau, Thomas Peters, and David Pointcheval

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

Workshops

Secure Distributed Computation on Private Inputs
In FPS 2015
Geoffroy Couteau, Thomas Peters, and David Pointcheval

Manuscripts

The Usefulness of Sparsifiable Inputs: How to Avoid Subexponential iO
Cryptology ePrint Archive, Report 2018/470
Thomas Agrikola, Geoffroy Couteau, and Dennis Hofheinz

A Note on the Communication Complexity of Multiparty Computation in the Correlated Randomness Model
Cryptology ePrint Archive, Report 2018/465
Geoffroy Couteau

Revisiting Covert Multiparty Computation
Cryptology ePrint Archive, Report 2016/951
Geoffroy Couteau

Work Experience

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 and Awards

2018	Pré-GDR IT security PhD prize, Honorary Mention https://twitter.com/GdrSecInfo/status/1002208472266629120

Invited Speaker

May 2018	Workshop on the Theory and Practice of Secure Multiparty Computation (TPMPC), 2018
Mar 2017	CryptoAction Symposium, 2017
May 2016	Workshop on the 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

Teaching

2017 – current	Bachelor thesis supervisor at KIT, Germany
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*

Services to the Community

Program Committee

2018	INDOCRYPT 2018

External reviewer

Conferences	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	Transactions on Information Forensics Security; Theoretical Computer Science; Design, Codes, and Cryptography.

Organization

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)

Computer Skills

Languages:	C/C++, C#, Java, Python
Softwares:	Mac, Linux (Ubuntu), Windows, Eclipse, Visual Studio, LaTeX, git, svn