Eurocrypt PARIS

April 30th - May 4th, 2017

Conference Program

Eurocrypt 2017 is the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques and it is being organized by the Crypto Team at ENS.

Organizer

Local Conference Organizers

Sunday, April 30th

18:30	**Welcome reception at Campus Jussieu** (4 place Jussieu - 75005 Paris)

Monday, May 1st

	Track A
8:50 - 8:55	Opening remarks
9:00-10:15	**Lattice attacks and constructions 1** *Chair: Leo Ducas*
	Revisiting Lattice Attacks on overstretched NTRU parameters Paul Kirchner, Pierre-Alain Fouque
	Short generators without quantum computers: the case of multiquadratics Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, Christine van Vredendaal
	Computing generator in cyclotomic integer rings Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, Paul Kirchner
10:15-10:20	Track-switch break
10:20-11:20	**Discrete logarithm** *Chair: Robert Granger*
	Computation of a 768-bit prime field discrete logarithm Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, Colin Stahlke
	A kilobit hidden SNFS discrete logarithm computation Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thomé
11:20-11:40	Coffee break
11:40-12:40	**Invited talk: Advances in computer-aided cryptography** Gilles Barthe (IMDEA Software Institute, Spain)
12:40-14:15	Lunch
14:15-15:05	**Lattice attacks and constructions 2** *Chair: Nicolas Gama*
	One-Shot Verifiable Encryption from Lattices Vadim Lyubashevsky, Gregory Neven
	Short Stickelberger Class Relations and application to Ideal-SVP Ronald Cramer, Léo Ducas, Benjamin Wesolowski
15:05-15:10	Track-switch break
15:10-16:00	**Lattice attacks and constructions 3** *Chair: Nicolas Gama*
	Private Puncturable PRFs From Standard Lattice Assumptions Dan Boneh, Sam Kim, Hart Montgomery
	Constraint-hiding constrained PRFs for NC1 from LWE Ran Canetti, Yilei Chen
16:00-16:30	Coffee break
16:30-17:20	**Side-channel attacks and countermeasures** *Chair: Jean-Sebastien Coron*
	Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, Pierre-Yves Strub
	How Fast Can Higher-Order Masking Be in Software? Dahmun Goudarzi, Matthieu Rivain
17:20-17:25	Track-switch break
17:25-18:15	**Elliptic curves** *Chair: San Ling*
	Twisted μ4-normal form for elliptic curves David Kohel
	Efficient compression of SIDH public keys Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, David Urbanik

Monday, May 1st

	Track B
8:50 - 8:55	Opening remarks
9:00-10:15	**Obfuscation and functional encryption** *Chair: Daniel Wichs*
	Robust transforming combiners from indistinguishability obfuscation to functional encryption Prabhanjan Ananth, Aayush Jain, Amit Sahai
	From Minicrypt to Obfustopia via Private-Key Functional Encryption Ilan Komargodski, Gil Segev
	Projective Arithmetic Functional Encryption and Indistinguishability Obfuscation From Degree-5 Multilinear Maps Prabhanjan Ananth, Amit Sahai
10:15-10:20	Track-switch break
10:20-11:20	**Multiparty computation 1** *Chair: Stefan Dziembowski*
	Improved Private Set Intersection against Malicious Adversaries Peter Rindal, Mike Rosulek
	Formal Abstractions for Attested Execution Secure Processors Rafael Pass, Elaine Shi, Florian Tramèr
11:20-11:40	Coffee break
11:40-12:40	**Invited talk: Advances in computer-aided cryptography** *Chair: Jean-Sebastien Coron* Gilles Barthe (IMDEA Software Institute, Spain)
12:40-14:15	Lunch
14:15-15:05	**Universal composability** *Chair: Vlad Kolesnikov*
	Concurrently composable security with shielded super-polynomial simulators Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, Matthias Nagel
	Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, Ivan Visconti
15:05-15:10	Track-switch break
15:10-16:00	**Zero knowledge 1** *Chair: Rafail Ostrovsky*
	Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack Ronald Cramer, Ivan Damgård, Chaoping Xing, Chen Yuan
	Sublinear Zero-Knowledge Arguments for RAM Programs Payman Mohassel, Mike Rosulek, Alessandra Scafuro
16:00-16:30	Coffee break
16:30-17:20	**Functional encryption 1** *Chair: Nuttapong Attrapadung*
	Multi-Input Inner-Product Functional Encryption from Pairings Michel Abdalla, Romain Gay, Mariana Raykova, Hoeteck Wee
	Simplifying Design and Analysis of Complex Predicate Encryption Schemes Shashank Agrawal, Melissa Chase
17:20-17:25	Track-switch break
17:25-18:15	**Functional encryption 2** *Chair: Eyal Kushilevitz*
	On Removing Graded Encodings from Functional Encryption Nir Bitansky, Huijia Lin, Omer Paneth
	Functional Encryption: Deterministic to Randomized Functions from Simple Assumptions Shashank Agrawal, David Wu

Tuesday, May 2nd

	Track A
9:00-10:15	**Lattice attacks and constructions 4** *Chair: Leo Ducas*
	Random Sampling Revisited: Lattice Enumeration with Discrete Pruning Yoshinori Aono, Phong Q. Nguyen
	On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL Martin R. Albrecht
	Small CRT-Exponent RSA Revisited Atsushi Takayasu, Yao Lu, Liquiang Peng
10:15-10:20	Track-switch break
10:20-11:10	**Symmetric cryptanalysis 1** *Chair: Maria Naya-Plasencia*
	Conditional Cube Attack on Reduced-Round Keccak Sponge Function Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, Jingyuan Zhao
	New Collision Attacks on Round-Reduced Keccak Kexin Qiao, Ling Song, Meicheng Liu, Jian Guo
11:0-11:40	Coffee break
11:40-12:40	**Invited talk: Living Between the Ideal and Real Worlds** *Chair : Jesper Buus Nielsen* Nigel Smart (University of Bristol)
18:30	Rump session

	Track B
9:00-10:15	**Multiparty computation 2** *Chair: Abhi Shelat*
	Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation Elette Boyle, Niv Gilboa, Yuval Ishai
	On the Exact Round Complexity of Self-Composable Two-Party Computation Sanjam Garg, Susumu Kiyoshima, Omkant Pandey
	High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority Jun Furukawa, Yehuda Lindell, Ariel Nof, Or Weinstein
10:15-10:20	Track-switch break
10:20-11:10	**Zero knowledge 2** *Chair: Miyako Ohkubo*
	Removing the Strong RSA Assumption from Arguments over the Integers Geoffroy Couteau, Thomas Peters, David Pointcheval
	Magic Adversaries Versus Individual Reduction: Science Wins Either Way Yi Deng
11:0-11:40	Coffee break
11:40-12:40	**Invited talk: Living Between the Ideal and Real Worlds** *Chair : Jesper Buus Nielsen* Nigel Smart (University of Bristol)
18:30	Rump session

Wednesday, May 3rd

	Track A
9:00-9:50	**Provable Security for Symmetric Cryptography 1** *Chair : Eike Kiltz*
	The Multi-User Security of Double Encryption Viet Tung Hoang, Stefano Tessaro
	Public-Seed Pseudorandom Permutations Pratik Soni, Stefano Tessaro
9:50-9:55	Track-switch break
9:55-10:45	**Blockchain** *Chair: Brent Waters*
	Decentralized Anonymous Micropayments Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, Pratyush Mishra
	Analysis of the Blockchain Protocol in Asynchronous Networks Rafael Pass, Lior Seeman, Abhi Shelat
10:45-11:15	Coffee break
11:15-12:05	**Provable Security for Symmetric Cryptography 2** *Chair: Aggelos Kiayias*
	Modifying an Enciphering Scheme after Deployment Paul Grubbs, Thomas Ristenpart, Yuval Yarom
	Separating Semantic and Circular Security for Symmetric-Key Bit Encryption from the Learning with Errors Assumption Rishab Goyal, Venkata Koppula, Brent Waters
12:05-14:00	Lunch
14:00-14:50	**Symmetric-key constructions** *Chair: Daniel Wichs*
	Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts Gorjan Alagic, Alexander Russell
	Boolean Searchable Symmetric Encryption with Worst-Case Sub-Linear Complexity Seny Kamara, Tarik Moataz
14:50-15:20	Coffee break
15:20-16:10	**Symmetric cryptanalysis 2** *Chair: Maria Naya-Plasencia*
	New Impossible Differential Search Tool from Design and Cryptanalysis Aspects Yu Sasaki, Yosuke Todo
	A New Structural-Differential Property of 5-Round AES Lorenzo Grassi, Christian Rechberger, Sondre Rønjom
16:15-17:15	**IACR Membership Meeting**
19:00	Banquet at Pavillon Dauphine (Place du Maréchal de Lattre de Tassigny - 75116 Paris)

Wednesday, May 3rd

	Track B
9:00-9:50	**Security models 1** *Chair : Krzysztof Pietrzak*
	Cryptography with Updates Prabhanjan Ananth, Aloni Cohen, Abhishek Jain
	Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited Yevgeniy Dodis, Siyao Guo, Jonathan Katz
9:50-9:55	Track-switch break
9:55-10:45	**Security models 2** *Chair : Krzysztof Pietrzak*
	Toward Fine-Grained Blackbox Separations Between Semantic and Circular-Security Notions Mohammad Hajiabadi, Bruce M. Kapron
	A Note on Perfect Correctness by Derandomization Nir Bitansky, Vinod Vaikuntanathan
10:45-11:15	Coffee break
11:15-12:05	**Memory hard functions** *Chair : Ilya Mironov*
	Depth-Robust Graphs and Their Cumulative Memory Complexity Joël Alwen, Jeremiah Blocki, Krzysztof Pietrzak
	Scrypt is Maximally Memory-Hard Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, Stefano Tessaro
12:05-14:00	Lunch
14:00-14:50	**Obfuscation 1** *Chair : Nir Bitansky*
	Patchable Indistinguishability Obfuscation: iO for Evolving Software Prabhanjan Ananth, Abhishek Jain, Amit Sahai
	Breaking the Sub-Exponential Barrier in Obfustopia Sanjam Garg, Omkant Pandey, Akshayaram Srinivasan, Mark Zhandry
14:50-15:20	Coffee break
15:20-16:10	**Obfuscation 2** *Chair : Nir Bitansky*
	Lattice-Based SNARGs and Their Application to More Efficient Obfuscation Dan Boneh, Yuval Ishai, Amit Sahai, David J. Wu
	Cryptanalyses of Candidate Branching Program Obfuscators Yilei Chen, Craig Gentry, Shai Halevi
16:15-17:15	**IACR Membership Meeting**
19:00	Banquet at Pavillon Dauphine (Place du Maréchal de Lattre de Tassigny - 75116 Paris)

Thursday, May 4th

	Track A	
9:00-10:15	**Quantum cryptography**	*Chair: Fabrice Benhamouda*
	Quantum Authentication and Encryption with Key Recycling Serge Fehr, Louis Salvail	
	Quantum authentication with key recycling Christopher Portmann	
	Relativistic (or 2-prover 1-round) zero-knowledge protocol for NP secure against quantum adversaries André Chailloux, Anthony Leverrier	
10:15-10:45	Coffee break	
10:45-12:00	**Public-key encryption and key-exchange**	*Chair: Fabrice Benhamouda*
	Adaptive partitioning Dennis Hofheinz	
	0-RTT Key Exchange with Full Forward Secrecy Felix Günther, Britta Hale, Tibor Jager, Sebastian Lauer	

	Track B	
9:00-10:15	**Multiparty computation 3**	*Chair: Jesper Buus Nielsen*
	Faster Secure Two-Party Computation in the Single-Execution Setting Xiao Wang, Alex J. Malozemoff, Jonathan Katz	
	Non-Interactive Secure 2PC in the Offline/Online and Batch Settings Payman Mohassel, Mike Rosulek	
	Hashing Garbled Circuits for Free Xiong Fan, Chaya Ganesh, Vladimir Kolesnikov	
10:15-10:45	Coffee break	
10:45-12:00	**Multiparty computation 4**	*Chair: Jesper Buus Nielsen*
	Computational integrity with a public random string from quasi-linear PCPs Eli Ben-Sasson, Iddo Ben-Tov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, Madars Virza	
	Ad Hoc PSM Protocols: Secure Computation without Coordination Amos Beimel, Yuval Ishai, Eyal Kushilevitz	
	Topology-Hiding Computation Beyond Logarithmic Diameter Adi Akavia, Tal Moran	

Special thanks to our

Platinum Sponsors

almerys
innovation for life

ENS
FONDATION

THALES

Gold Sponsors

ANSSI

AIRBUS

HUAWEI

Microsoft
Research

NXP

Rambus

Sponsors

cnrs
dépasser les frontières

CRYPTO EXPERTS

Google

IBM

IET Information Security

Inria
INVENTORS FOR THE DIGITAL WORLD

list
cea tech

orange

SAFRAN

WALLIX
TRACE, AUDIT & TRUST