Sunday, April 30th

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

Monday, May 1st

	Track A	Track B	
8:50 - 8:55	Opening remarks		8:50 - 8:55
9:00-10:15	**Lattice attacks and constructions 1** *Chair: Leo Ducas*	**Obfuscation and functional encryption** *Chair: Daniel Wichs*	9:00-10:15
	Revisiting Lattice Attacks on overstretched NTRU parameters Paul Kirchner, Pierre-Alain Fouque	**Robust transforming combiners from indistinguishability obfuscation to functional encryption** Prabhanjan Ananth, Aayush Jain, Amit Sahai	
	Short generators without quantum computers: the case of multiquadratics Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, Christine van Vredendaal	**From Minicrypt to Obfustopia via Private-Key Functional Encryption** Ilan Komargodski, Gil Segev	
	Computing generator in cyclotomic integer rings Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, Paul Kirchner	**Projective Arithmetic Functional Encryption and Indistinguishability Obfuscation From Degree-5 Multilinear Maps** Prabhanjan Ananth, Amit Sahai	
10:15-10:20	Track-switch break		10:15-10:20
10:20-11:20	**Discrete logarithm** *Chair: Robert Granger*	**Multiparty computation 1** *Chair: Stefan Dziembowski*	10:20-11:20
	Computation of a 768-bit prime field discrete logarithm Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, Colin Stahlke	**Improved Private Set Intersection against Malicious Adversaries** Peter Rindal, Mike Rosulek	
	A kilobit hidden SNFS discrete logarithm computation Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thomé	**Formal Abstractions for Attested Execution Secure Processors** Rafael Pass, Elaine Shi, Florian Tramèr	
11:20-11:40	Coffee break		11:20-11:40
11:40-12:40	**Invited talk: Advances in computer-aided cryptography** Gilles Barthe (IMDEA Software Institute, Spain)		11:40-12:40
12:40-14:15	Lunch		12:40-14:15
14:15-15:05	**Lattice attacks and constructions 2** *Chair: Nicolas Gama*	**Universal composability** *Chair: Vlad Kolesnikov*	14:15-15:05
	One-Shot Verifiable Encryption from Lattices Vadim Lyubashevsky, Gregory Neven	**Concurrently composable security with shielded super-polynomial simulators** Brandon Broadnax, Nico Döttling, Gunnar Hartung, Jörn Müller-Quade, Matthias Nagel	
	Short Stickelberger Class Relations and application to Ideal-SVP Ronald Cramer, Léo Ducas, Benjamin Wesolowski	**Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs** Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, Ivan Visconti	
15:05-15:10	Track-switch break		15:05-15:10
15:10-16:00	**Lattice attacks and constructions 3** *Chair: Nicolas Gama*	**Zero knowledge 1** *Chair: Rafail Ostrovsky*	15:10-16:00
	Private Puncturable PRFs From Standard Lattice Assumptions Dan Boneh, Sam Kim, Hart Montgomery	**Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack** Ronald Cramer, Ivan Damgård, Chaoping Xing, Chen Yuan	
	Constraint-hiding constrained PRFs for NC1 from LWE Ran Canetti, Yilei Chen	**Sublinear Zero-Knowledge Arguments for RAM Programs** Payman Mohassel, Mike Rosulek, Alessandra Scafuro	
16:00-16:30	Coffee break		16:00-16:30
16:30-17:20	**Side-channel attacks and countermeasures** *Chair: Jean-Sebastien Coron*	**Functional encryption 1** *Chair: Nuttapong Attrapadung*	16:30-17:20
	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	**Multi-Input Inner-Product Functional Encryption from Pairings** Michel Abdalla, Romain Gay, Mariana Raykova, Hoeteck Wee	
	How Fast Can Higher-Order Masking Be in Software? Dahmun Goudarzi, Matthieu Rivain	**Simplifying Design and Analysis of Complex Predicate Encryption Schemes** Shashank Agrawal, Melissa Chase	
17:20-17:25	Track-switch break		17:20-17:25
17:25-18:15	**Elliptic curves** *Chair: San Ling*	**Functional encryption 2** *Chair: Eyal Kushilevitz*	17:25-18:15
	Twisted μ4-normal form for elliptic curves David Kohel	**On Removing Graded Encodings from Functional Encryption** Nir Bitansky, Huijia Lin, Omer Paneth	
	Efficient compression of SIDH public keys Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, David Urbanik	**Functional Encryption: Deterministic to Randomized Functions from Simple Assumptions** Shashank Agrawal, David Wu	

Tuesday, May 2nd

	Track A	Track B	
9:00-10:15	**Lattice attacks and constructions 4** *Chair: Leo Ducas*	**Multiparty computation 2** *Chair: Abhi Shelat*	9:00-10:15
	Random Sampling Revisited: Lattice Enumeration with Discrete Pruning Yoshinori Aono, Phong Q. Nguyen	**Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation** Elette Boyle, Niv Gilboa, Yuval Ishai	
	On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL Martin R. Albrecht	**On the Exact Round Complexity of Self-Composable Two-Party Computation** Sanjam Garg, Susumu Kiyoshima, Omkant Pandey	
	Small CRT-Exponent RSA Revisited Atsushi Takayasu, Yao Lu, Liquiang Peng	**High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority** Jun Furukawa, Yehuda Lindell, Ariel Nof, Or Weinstein	

Tuesday, May 2nd

10:15-10:20	Track-switch break	10:15-10:20
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	**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	10:20-11:10
11:10-11:40	Coffee break		1:10-11:40
11:40-12:40	**Invited talk: Living Between the Ideal and Real Worlds** Nigel Smart (University of Bristol)		11:40-12:40
18:30	Rump session		18:30

Wednesday, May 3rd

	Track A	Track B	
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	**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	9:00-9:50
9:50-9:55	Track-switch break		9:50-9:55
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	**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	9:55-10:45
10:45-11:15	Coffee break		10:45-11:15
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	**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	11:15-12:05
12:05-14:00	Lunch		12:05-14:00
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	**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	14:00-14:50
14:50-15:20	Coffee break		14:50-15:20
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	**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	15:20-16:10
16:15-17:15	IACR Membership Meeting		16:15-17:15
19:00	Banquet at Pavillon Dauphine (Place du Maréchal de Lattre de Tassigny - 75116 Paris)		19:00

Thursday, May 4th

	Track A	Track B	
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	**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	9:00-10:15
10:15-10:45	Coffee break		10:15-10:45
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	**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	10:45-12:00