Monday, April 24th, Morning

	Auditorium Lumière	Forum 1	Forum 2
9:00-9:15	**Opening Remarks (plenary - Auditorium Lumière)**		
9:15-10:15	**Invited Talk: Guy Rothblum Indistinguishable Predictions and Multi-Group Fair Learning (plenary - Auditorium Lumière)**		
	Coffee break		
10:45-11:45	**Fully Homomorphic Encryption**	**Lower Bounds**	**Blockcipher Cryptanalysis**
	Efficient FHEW Bootstrapping with Small Evaluation Keys, and Applications to Threshold Homomorphic Encryption	*Worst-Case Subexponential Attacks on PRGs of Constant Degree or Constant Locality* - **Early Career Best Paper Award**	*Truncated Boomerang Attacks and Application to AES-based Ciphers*
	On Polynomial Functions Modulo p^e and Faster Bootstrapping for Homomorphic Encryption	*Fine-Grained Non-Interactive Key-Exchange: Constructions and Lower Bounds*	*Better Steady than Speedy: Full Break of SPEEDY-7-192*
	Functional Commitments for All Functions, with Transparent Setup and from SIS	*Speak Much, Remember Little: Cryptography in the Bounded Storage Model, Revisited*	*Exploiting Non-Full Key Additions: Full-Fledged Automatic Demirci-Sel{\c{c}}uk Meet-in-the-Middle Cryptanalysis of SKINNY*
11:55-12:35	**Fully Homomorphic Encryption (cont.)**	**Lower Bounds (cont.)**	**Blockcipher Cryptanalysis (cont.)**
	Batch Bootstrapping I: A New Framework for SIMD Bootstrapping in Polynomial Modulus	*Non-uniformity and Quantum Advice in the Quantum Random Oracle Model*	*Efficient Detection of High Probability Statistical Properties of Cryptosystems via Surrogate Differentiation*
	Batch Bootstrapping II: Bootstrapping in Polynomial Modulus Only Requires $\tilde O(1)$ FHE Multiplications in Amortization	*Black-Box Separations for Non-Interactive Commitments in a Quantum World*	*Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks*

Monday, April 24th, Afternoon

	Auditorium Lumière	Forum 1	Forum 2
14:35-15:15	**Authenticated Key Exchange**	**Differential Privacy**	**Oblivious Transfer**
	Password-Authenticated TLS via OPAQUE and Post-Handshake Authentication	*A Theory of Composition for Differential Obliviousness*	*Reverse Firewalls for Oblivious Transfer Extension and Applications to Zero-Knowledge*
	Randomized Half-Ideal Cipher on Groups with applications to UC (a)PAKE	*On Differential Privacy and Adaptive Data Analysis with Bounded Space*	*Oblivious Transfer with Constant Computational Overhead*
15:25-16:05	**Real World Crypto**	**Lattice Cryptanalysis**	**Oblivious Transfer (cont.)**
	End-to-End Encrypted Zoom Meetings: Proving Security and Strengthening Liveness	*Finding many Collisions via Reusable Quantum Walks - Application to Lattice Sieving*	*Endemic Oblivious Transfer via Random Oracles, Revisited*
	Caveat Implementor! Key Recovery Attacks on MEGA	*Just how hard are rotations of Z^n? Algorithms and cryptography with the simplest lattice*	*A New Framework for Quantum Oblivious Transfer*
	Coffee break		
16:35-17:35	**Garbling Schemes and Oblivious Transfer**	**Quantum Cryptography**	**Side-Channel Attacks and Masking**
	New Ways to Garble Arithmetic Circuits	*Public Key Encryption with Secure Key Leasing*	*Improved Power Analysis Attacks on Falcon*
	Actively Secure Half-Gates with Minimum Overhead under Duplex Networks	*Another Round of Breaking and Making Quantum Money: How to Not Build It from Lattices, and More*	*Effective and Efficient Masking with Low Noise using Small-Mersenne-Prime Ciphers*
	Half-Tree: Halving the Cost of Tree Expansion in COT and DPF	*From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments*	*One-Hot Conversion: Towards Faster Table-based A2B Conversion*

Tuesday, April 25th

	Auditorium Lumière	Forum 1	Forum 2
9:00-10:00	**Non-Interactive MPC**	**Messaging and Message Franking**	**Hash Function Cryptanalysis**
	Black-Box Reusable NISC with Random Oracles	*Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging*	*Meet-in-the-Middle Preimage Attacks on Sponge-based Hashing*
	Maliciously-Secure MrNISC in the Plain Model	*End to End Secure Messaging with Traceability Only for Illegal Content*	*Analysis of RIPEMD-160: New Collision Attacks and Finding Characteristics with MILP*
	Minimizing Setup in Broadcast-Optimal Two Round MPC	*Asymmetric Group Message Franking: Definitions & Constructions*	*Collision Attacks on Round-Reduced SHA-3 Using Conditional Internal Differentials*
	Coffee break		
10:30-11:30	**Symmetric Design 1**	**Theory of Public-Key Cryptography**	**Oblivious Data Access 1**
	From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications	*Deniable Authentication when Signing Keys Leak*	*Optimal Single-Server Private Information Retrieval*
	Coefficient Grouping: Breaking Chaghri and More	*Let Attackers Program Ideal Models: Modularity and Composability for Adaptive Compromise*	*Weighted ORAM, with Applications to Searchable Symmetric Encryption*
	Pitfalls and Shortcomings for Decompositions and Alignment	*Almost Tight Multi-User Security under Adaptive Corruptions & Leakages in the Standard Model*	*NanoGRAM: Garbled RAM with $\widetilde{O}(\log N)$ Overhead*
11:40-12:40	**Isogeny 1 (plenary - Auditorium Lumière)**		
	An Efficient Key Recovery Attack on SIDH - **Best Paper Award**		
	A Direct Key Recovery Attack on SIDH - **Honourable Mention**		
	Breaking SIDH in Polynomial Time - **Honourable Mention**		
	Free afternoon		
19:00-19:30	**IACR Award Ceremony (plenary - Auditorium Lumière)**		
19:30-22:45	**Rump Session (plenary - Auditorium Lumière)**		

Wednesday, April 26th, Morning

	Auditorium Lumière	Forum 1	Forum 2
9:00-10:00	**Invited Talk: Vadim Lyubashevsky Lattice Cryptography: What Happened and What's Next (plenary - Auditorium Lumière)**		
	Coffee break		
10:30-11:30	**Signature Schemes 1**	**Attribute Based Encryption and Friends**	**(Zero-Knowledge) Proofs 1**
	A Lower Bound on the Length of Signatures Based on Group Actions and Generic Isogenies	*Fully Adaptive Decentralized Multi-Authority ABE*	*Witness-Succinct Universally-Composable SNARKs*
	Short Signatures from Regular Syndrome Decoding in the Head	*On the Optimal Succinctness and Efficiency of Functional Encryption and Attribute-Based Encryption*	*SNARGs and PPAD Hardness from the Decisional Diffie-Hellman Assumption*
	The Return of the SDitH	*Registered Attribute-Based Encryption*	*Proof-Carrying Data From Arithmetized Random Oracles*
11:40-12:20	**Signature Schemes 1 (cont.)**	**Attribute Based Encryption and Friends (cont.)**	**(Zero-Knowledge) Proofs 1 (cont.)**
	Chopsticks: Fork-Free Two-Round Multi-Signatures from Non-Interactive Assumptions	*Unbounded Quadratic Functional Encryption and More from Pairings*	*Supersingular Curves You can Trust*
	Threshold and Multi-Signature Schemes from Linear Hash Functions	*Multi-key and Multi-input Predicate Encryption from Learning with Errors*	*On Valiant's Conjecture: Impossibility of Incrementally Verifiable Computation from Random Oracles*

Wednesday, April 26th, Afternoon

	Auditorium Lumière	Forum 1	Forum 2
14:20-15:00	**Efficient MPC Constructions**	**Traitor Tracing Schemes**	**Symmetric Design 2**
	Sublinear-Communication Secure Multiparty Computation does not require FHE	*Broadcast, Trace and Revoke with Optimal Parameters from Polynomial Hardness*	*Generic Attack on Duplex-Based AEAD Modes using Random Function Statistics*
	Actively Secure Arithmetic Computation and VOLE with Constant Computational Overhead	*Traitor Tracing with N^(1/3)-size Ciphertext and O(1)-size Keys from k-Lin*	*Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More*
15:10-15:50	**Efficient MPC Constructions (cont.)**	**Pseudorandom Functions**	**Symmetric Design 2 (cont.)**
	SuperPack: Dishonest Majority MPC with Constant Online Communication	*Privately Puncturing PRFs from Lattices: Adaptive Security and Collusion Resistant Pseudorandomness*	*Impossibility of Indifferentiable Iterated Blockciphers from 3 or Less Primitive Calls*
	Detect, Pack and Batch: Perfectly-Secure MPC with Linear Communication and Constant Expected Time	*Constrained Pseudorandom Functions from Homomorphic Secret Sharing*	*Optimal Security for Keyed Hash Functions: Avoiding Time-Space Tradeoffs for Finding Collisions*
		Coffee break	
16:20-17:20	**Isogenies 2**	**Oblivious Data Access 2**	**Symmetric Design 3**
	M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information	*Lower Bound Framework for Differentially Private and Oblivious Data Structures*	*Proof of Mirror Theory for a Wide Range of $ \xi_{\max}$*
	New Algorithms for the Deuring Correspondence: Towards Practical and Secure SQISign Signatures	*Lower Bounds for (Batch) PIR with Private Preprocessing*	*Non-Adaptive Universal One-Way Hash Functions from Arbitrary One-Way Functions*
	Disorientation Faults in CSIDH	*How to Compress Encrypted Data*	*XOCB: Beyond-Birthday-Bound Secure Authenticated Encryption Mode with Rate-One Computation*
17:30-18:30	**IACR Membership Meeting (plenary - Auditorium Lumière)**		
19:00-21:30	**Banquet (Forum 3)**		

Thursday, April 27th

	Auditorium Lumière	Forum 1
9:00-10:00	**(Zero-Knowledge) Proofs 2**	**Signature Schemes 2**
	Speed-Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions	*Revisiting BBS Signatures*
	HyperPlonk: Plonk with Linear-Time Prover and High-Degree Custom Gates	*Revisiting BBS Signatures*
	Spartan and Bulletproofs are Simulation-Extractable (for free!)	*Rai-Choo! Evolving Blind Signatures to the Next Level*
Coffee break		
10:30-11:30	**Public-Key Cryptanalysis**	**MPC and Proofs**
	On the Hardness of the Finite Field Isomorphism Problem	*Complete Characterization of Broadcast and Pseudo-Signatures from Correlations*
	New Time-Memory Trade-Offs for Subset Sum -- Improving ISD in Theory and Practice	*Privacy-Preserving Blueprints*
	A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions	*An Incremental PoSW for General Weight Distributions*
11:40-12:20	**Lattice Constructions**	**Non-malleable Commitments and Obfuscation**
	Succinct Vector, Polynomial, and Functional Commitments from Lattices	*On Non-uniform Security for Black-box Non-Interactive CCA Commitments*
	Efficient Laconic Cryptography from Learning With Errors	*Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum iO*