Time	Room 1			Room 2		
Wednesday April 4, 2018						
09:15	Welcoming Remarks					
09:30	**Invited Talk Chair: Claudio Orlandi**					
	Elette	Boyle	Can we access at Database Both Locally and Privately?			
10:30	***Break***					
11:00	**MPC I Chair: Claudio Orlandi**			**Key Exchange Chair: Chris Brzuska**		
	Eylon	Yogev	Distributed Computing Made Secure: A New Cycle Cover Theorem	Julia	Hesse	Fuzzy Password-Authenticated Key Exchange
	Mark	Simkin	Yet Another Compiler for Active Security or: Efficient MPC Over Arbitrary Rings	Jacqueline	Brendel	Breakdown Resilience of Key Exchange Protocols and the Cases of NewHope and TLS
	Stefan	Dziembowski	Position-Based Cryptography and Multi-Party Communication Complexity	Daniel	Slamanig	Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange
12:30	***Lunch***					
14:00	**Amortized Complexity Chair: Milena Djukanovic**			**Side-Channel Attacks Chair: Viktoria Villanyi**		
	Carla	Rafòls	New Techniques for Structual Batch Verification in Bilinear Groups	Thomas	Prest	Grafting Trees: a Fault Attack against the SPHINCS framework
	Clara	Paglialonga	Amortizing Randomness Complexity in Private Circuits	Estuardo	Alpirez Bock	Differential Computational Analysis of White-Box Crypto Revisited
15:00	***Break***					
15:30	**Non-Malleable Codes Chair: Claudio Orlandi**			**Standards Chair: Viktoria Villanyi**		
	Daniele	Venturi	Continuously Non-Malleable Codes: A Tutorial	Benjamin R.	Curtis	LWE-based Submissions to NIST
				Joanne	Woodage	An Analysis of the NIST SP 800-90A DRBGs
16:30	**Lightning talk session, Chair: Daniele Venturi**					
17:00	**MC Meeting (1 hour)**					
18:00	***End of MC Meeting***					
18:30	***Departure from the Hotel by taxi for a short visit to King's Nichola's palace and dinner in the Restaurant King's Garden***					

Time	**Room 1**			**Room 2**		
Thursday April 5, 2018						
09:30	**Invited Talk Chair: Chris Brzuska**					
	Krzysztof	Pietrzak	Proof Systems for Blockchains: Proofs of (Catalytic) Space and Sequential Work			
10:30	***Break***					
11:00	**Anonymity Chair: Milena Djukanovic**			**Lattices Chair: Dario Fiore**		
	Ruxandra F.	Olimid	The Problem of Private Identification	Cecilia	Boschini	Floppy-Sized Group Signatures from Lattices
	Sanaz Taheri-Boshrooyeh		Inonymous: Anonymous Invitation-Based System	Carsten	Baum	Zero-Knowledge Proofs for Lattice-Based Cryptography
	Antonio	Faonio	Optimistic Mixing, Revisited	Mélissa	Rossi	Masking Lattice-based Fiat-Shamir-with-aborts signatures at any order
12:30	***Lunch***					
14:00	**Secure Messaging Chair: Chris Brzuska**			**MPC II Chair: Stefan Dziembowski**		
	Paul	Rösler	Complexity of Group Communication in Instant Messaging	Rafael	Dowsley	A Framework for Efficient Adaptively Secure Composable Oblivious Transfer in the ROM
	Luke	Garratt	On Ends-to-Ends Encryption: Better Group Messaging	Mark	Simkin	Oblivious RAM with Small Storage Overhead
15:00	***Break***					
15:30	**Subversion Chair: Daniele Venturi**			**Primitives Chair: Dario Fiore**		
	Christian	Janson	Backdoored Hash Functions: Immunizing HMAC and HKDF	Thomas	Peters	Receipt-Freeness: New Definitions & Contructions
	Luca	Nizzardo	Zero Knowledge, subversion-resistance and concrete attacks	Elena	Pagnin	Multi-Key Homomorphic Authenticators
	Sogol	Mazaheri	Self-Guarding Cryptographic Protocols against Algorithm Substitution Attacks	Rafael	Kurek	Simple and Efficient PRFs with Tight Security via All-Prefix Universal Hash Functions
17:00	***End of technical program***					
18:30	***Departure from the hotel for a 30 min. walk along the sea to the Restaurant St. Olive***					