Accepted Papers:

#	Authors	Title	Decision
1	Agnese Gini and Pierrick Meaux	On the algebraic immunity of weightwise perfectly balanced functions	ACCEPT
2	Suthee Ruangwises	Physical Zero-Knowledge Proof for Five Cells	ACCEPT
3	Daniel Escudero and Serge Fehr	On Fully-Secure Honest Majority MPC without n^2 Round Overhead	ACCEPT
4	Krijn Reijnders	Effective Pairings in Isogeny-based Cryptography	ACCEPT
5	Hernán Darío Vanegas Madrigal, Daniel Cabarcas Jaramillo and Diego F. Aranha	Privacy-preserving edit distance computation using secret-sharing protocols	ACCEPT
6	Kohei Nakagawa, Atsushi Fujioka, Akira Nagai, Junichi Tomida, Keita Xagawa and Kan Yasuda	Making the Identity-Based Diffie-Hellman Key Exchange Efficiently Revocable	ACCEPT
7	Charlotte Hoffmann and Mark Simkin	Stronger Lower Bounds for Leakage-Resilient Secret Sharing	SHEPHERDING
8	Carla Ràfols and Alexandros Zacharakis	Folding Schemes with Selective Verification⋆	ACCEPT
9	Gustavo Banegas, Valerie Gilchrist, Anaëlle Le Dévéhat and Benjamin Smith	Fast and Frobenius: Rational Isogeny Evaluation over Finite Fields	ACCEPT
10	Sebastian Faller, Johannes Ernst and Astrid Ottenhues	Composable Oblivious Pseudo-Random Functions via Garbled Circuits	SHEPHERDING
11	Joan Boyar, Simon Erfurth, Kim S. Larsen and Ruben Niederhagen	Quotable Signatures for Authenticating Shared Quotes	ACCEPT
12	Thomas Decru, Luciano Maino and Antonio Sanso	Towards a Quantum-resistant weak Verifiable Delay Function	ACCEPT
13	Alexandre Augusto Giron, João Pedro Adami do Nascimento, Ricardo Custódio, Lucas Perin and Victor Mateu	Post-Quantum Hybrid KEMTLS Performance in Simulated and Real Network Environments	ACCEPT
14	Matteo Campanelli, Nicolas Gailly, Rosario Gennaro, Philipp Jovanovic, Mara Mihali and Justin Thaler	Testudo: Efficient SNARKs with Smaller Setups	ACCEPT
15	Helger Lipmaa and Roberto Parisella	Set (Non-)Membership NIZKs from Determinantal Accumulators	ACCEPT
16	Emanuele Bellini, Nitin Satpute, Juan Grados, Mohamed Rachidi, Joan Daemen and Solane El Hirch	Accelerating an Extreme Amount of Symmetric Cipher Evaluations for High-order Avalanche Tests	ACCEPT
17	Ivan Damgård, Divya Ravi, Luisa Siniscalchi and Sophia Yakoubov	Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Channels	ACCEPT
18	Semyon Novoselov	On the discrete logarithm problem in the ideal class group of multiquadratic fields	ACCEPT
19	Karim Baghery, Axel Mertens and Mahdi Sedaghat	Benchmarking the Setup of Updatable zk-SNARKs	ACCEPT