	CBC (room A02)	CrossFyre (room A03)
08:30 – 09:00	Registration	
09:00 – 10:30	**Invited talk** **McTiny: McEliece for tiny network servers (Dan Bernstein)**	**Session B** **On the Privacy-Preserving V2G Payment Scheme P6V2G and Scenario Specific Privacy** Rebecca Schwerdt **Yet another Holy Grail in crypto: (efficient) zero-knowledge proofs for lattice problems** Cecilia Boschini **Privado: Privacy-Preserving Group-Based Advertising in Online Social Networks using Multiple Independent Providers** Sanaz Taheri Boshrooyeh
10:30 – 11:00	Coffee Break	
11:00 – 12:30	**Paper presentations** **Quantum Resistant Public Key Encryption Scheme HermitianRLCE** G. Matthews, Y. Wang **Design of LEDAkem and LEDApkc instances with tight parameters and bounded decryption failure rate** M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, P. Santini **Introducing arithmetic failures to accelerate QC-MDPC code-based cryptography** A. Guimarães, E. Borin, D. F. Aranha **DAGS Reloaded: Revisiting Dyadic Key Encapsulation** G. Banegas, P. S. L. M. Barreto, B. Odilon Boidje, P. -L. Cayrel, G. Ndollane Dione, K. Gaj, C. Thiecoumba Gueye, R. Haeussler, J. Belo Klamti, O. Ndiaye, D. Tri Nguyen, E. Persichetti, J. Ricardini	**Session C** **Stronger Lower Bounds for Online ORAM** Veronika Slívová **Keynote** **Women in Computer Science from a Social Science and Gender Studies** Bianca Prietl
12:30 – 14:00	Lunch	
14:00 – 15:30	**Contributed talks** **How to combine Reed-Muller and Goppa codes in McEliece type cryptosystem** I. Dumer, G. Kabatiansky, E. Krouk **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes** T. Debris-Alazard, N. Sendrier, J.-P. Tillich **New McEliece cryptosystem using Reed-Solomon codes over an extension field** K. Khathuria, J. Rosenthal, V. Weger **Loong: new IND-CCA-secure code-based public-key schemes** L.-P. Wang	**Session D** **Algebraic construction of lattices in the Ring-LWE problem** Jheyne Ortiz **More efficient updatable zk-SNARKs** Arantxa Zapico **Applied post-quantum cryptography for embedded systems** Soundes Marzougui **Anomaly Detection of IOT Nodes using Power Signature** Maria Ashraf **Towards Cognitive Obfuscation – Analyzing Human Factors to Impede Hardware Reverse Engineering** Carina Wiesen
15:30 – 16:00	Coffee Break	
16:00 – 17:30	**Working and discussion session**	**Session E** **Efficient and Proactive Long-Term Secure Secret Sharing-based Storage Systems** Giulia Traverso **Interview: Oded Goldreich**

	PENCIL (room A01)	WhibOx (room A5)	WSM (room A4)
08:30 – 08:50	Registration		
08:50 – 10:30	**Keynote 1 – A Consensus Taxonomy in the Blockchain Era (Juan Garay)** **Afgjort – A Semi-Synchronous Finality Layer for Blockchains** B. Magri, J. Buus Nielsen, D. Tschudi **Pixel: Multi-Signatures for Consensus** M. Drijvers, S. Gorbunov, G. Neven, H. Wee **A Framework for Anonymous Lottery-Based Protocols in the Proof-of-Stake Setting** F. Baldimtsi, V. Rajeev Madathil, A. Scafuro, L. Zhou	**White-box designs** **White-box cryptography: between academia and industry (Part 1)** Andrey Bogdanov **White-box cryptography: between academia and industry (Part 2)** Andrey Bogdanov	*<< starts 09:00 >>* **Secure messaging, MLS and Wire** Raphael Robert **Definitional Foundations of Ratcheting and their Impact on Practice** Paul Roesler
10:30 – 11:00	Coffee Break		
11:00 – 12:30	**Keynote 2 (Charles Hoskinson)** **Asymmetric Distributed Trust** (PRIViLEDGE Session) C. Cachin, B. Tackmann **Publicly Verifiable Proofs from Blockchains and the Attacks of the Clones in Proof-of-Stake Blockchains** A. Scafuro, L. Siniscalchi. I. Visconti **Timed Signatures and Zero-Knowledge Proofs - Timestamping in the Blockchain Era** A. Abadi, M. Ciampi, A. Kiayias, V. Zikas	**White-box designs** **White-box and asymmetrically hard crypto design** Alex Biryukov **New encodings for white-box implementations** Adrian Ranea	**Encryption is not enough - using mix-networks for anonymous messaging** Ania Piotrowska **Messaging Layer Security: Past, Present, and Future** Richard Barnes
12:30 – 14:00	Lunch		
14:00 – 15:30	**Keynote 3 – Why should I believe that? (Jens Groth)** **Fully Homomorphic NIZK and NIWI Proofs** P. Ananth, A. Deshpande, Y. Kalai, A. Lysyanskaya **Zether: Towards Privacy in a Smart Contract World** B. Bünz, S. Agrawal, M. Zamani, D. Boneh **ZEXE: Enabling Decentralized Private Computation** S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra, H. Wu	**Attacks on white-box cryptography** **Grey-box attacks, four years later** Philippe Teuwen **A DFA attack on white-box implementations of AES with external encodings** Alessandro Amadori	**On the Security and Insecurity of TreeKEM** Yevgeniy Dodis **Message Franking: Invisible Salamanders, Encryptment, and AMFs** Paul Grubbs
15:30 – 16:00	Coffee Break		
16:00 – 17:30	**On QA-NIZK in the BPK Model** (PRIViLEDGE Session) B. Abdolmaleki, H. Lipmaa, J. Siim, M. Zajac **Verifiable MPC and DLT** B. Schoenmakers, T. Segers **Quisquis: A New Design for Anonymous Cryptocurrencies** P. Fauzi, C. Orlandi, S. Meiklejohn, R. Mercer **Initial Public Offering (IPO) on Permissioned Blockchain using Secure Multiparty Computation** F. Benhamouda, A. De Caro, S. Halevi, T. Halevi, C. Jutla, Y. Manevich, Q. Zhang **Universally Composable and Privacy-Preserving Audit Logs Using Bulletin Board** J. Camenisch, M. Drijvers, M. Dubovitskaya, A. Kaplan **Bootstrapping Online Trust: Timeline Activity Proofs over Public Ledgers** C. Catalin Dragan, M. Manulis	**Attacks on white-box cryptography** **DCA attacks against internally encoded white-box implementations** Junwei Wang **Security assessment of WhibOx 2017 candidates** Alexander Treff	**A Proper Security Level for Postcompromise Secure Messaging** Serge Vaudenay **Discussion and wrap up**

	CBC (room A02)	QuAC (room A03)	SPY (room A01)
08:30 – 09:00	Registration		
09:00 – 10:30	**Invited talk (Ray Perlner)**	*<< starts 09:30 >>* **Quantum Search Beyond Grover** Stacey Jeffery	*<< starts 09:45 >>* **"If Technology Allows For It" – the current debate on the usage of surveillance software by the German police** Marie Bröckling
10:30 – 11:00	Coffee Break		
11:00 – 12:30	**Paper presentations** **Practical Algebraic Attack on DAGS** M. Bardet, M. Bertin, A. Couvreur, A. Otmani **Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes** P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi **On IND-CCA1 Security of Randomized McEliece Encryption in the Standard Model** F. A. Farro, K. Morozov **Weak Keys in the Faure-Loidreau Cryptosystem** T. Jerkovits, H. Bartz	**Quantum Algorithms for Optimization over Finite Fields and Applications in Cryptanalysis** Yu-Ao Chen	**Corporate surveillance of everyday life – How companies use personal data against people** Wolfie Christl **The European Intelligence Oversight Network: a quest for better control instruments** Thorsten Wetzling
12:30 – 14:00	Lunch		
14:00 – 15:30	**Contributed talks** **Generalization of the ball-collision algorithm** V. Weger, C. Interlando, K. Khathuria, N. Rohrer, J. Rosenthal **Backflip: An Improved QC-MDPC Bit-Flipping Decoder** N. Sendrier, V. Vasseur **Implementation of Code-based KEMs submitted to NIST on Optical Communication Systems** J. Y. Cho **Ternary Syndrome Decoding for Large Weights** R. Bricout, A. Chailloux, T. Debris-Alazard, M. Lequesne	*<< starts 13:45 >>* **New Algorithms for Quantum Symmetric Cryptanalysis** André Schrottenloher **Non-Asymptotic Quantum Resource Estimation** Vlad Gheorghiu	**Silicon Valley and China** Ryan Gallagher **Secret Sharing for Journalists and Whistleblowers** Phil Rogaway
15:30 – 16:00	Coffee Break		
16:00 – 17:30	**Working and discussion session**	*<< starts 16:15 >>* **Quantum Hidden Shift Algorithms 2.0** Greg Kuperberg	**Hunting Political Bots on Twitter – Joining Captain Ahab** Orr Dunkelman **Mix-networks against mass surveillance** Ania Piotrowska

	OPACity (room A4)	WhibOx (room A5)	Tamarin Tutorial (TPT) (room A2)
08:30 – 09:00	Registration		
09:00 – 10:30	**Theory (joint session in room A5)** *<< starts 08:50 >>* **Foundations of program obfuscation** Rachel Lin **Obfuscation from LWE? proofs, attacks, candidates** Hoeteck Wee		**Initial lecture** Cas Cremers
10:30 – 11:00	Coffee Break		
11:00 – 12:30	**Theory (joint session in room A5)** **White-box crypto and obfuscation: relations and attacks** Brice Minaud		**Hands-on**
12:30 – 14:00	Lunch		
14:00 – 15:30	**Bootstrapping Obfuscation from Noisy Linear FE** Shweta Agrawal **Attacks on GGH13-based Obfuscation** Alice Pellet–Mary **Simple Obfuscation for Simple Functionalities** Ward Beullens	**Tools and Demos** **Optimize your binary tracing: an example with an ECDSA implementation** Guillaume Vinet **Exploring different faulting techniques for stressing white-box cryptography binaries** Guillaume Vinet	**Advanced lecture** Jannik Dreier
15:30 – 16:00	Coffee Break		
16:00 – 17:30	**Panel: New Directions for Obfuscation** with Tancrède Lepoint, Rachel Lin, Amit Sahai, Brent Waters	**Tools and Demos** **Synthesis tools for white-box implementations** Aleksei Udovenko **Call for contribution for a new white-box analytic tools** Junwei Wang **Panel: The white-box contest** *<< starts 17:15 >>*	**Hands-on**