Eurocrypt 2025 – Affiliated Events Schedule (Saturday, May 3)

Time	s106	s116	s109	s108	b15	b03	b04
	ProTeCS	**Isogeny**	**AICRYPT**	**CTB25**	**CBCrypto**	**Alg. Hash**	**LLE**
08:30	Registration (closes at 17:00)						
09:30	**Welcome** 9:40 **Invited Talk** *Counting Unpredictable Bits: A simple PRNG form One-Way Functions* N. Mazor	**Present ideas, make groups**	9:25 **Opening Remarks** 9:30 **Cryptographic Backdoors in ML** *Spot-Check: Integrity Verification for Outsourced ML via Hidden Backdoors* A. Grigor, I. Martinovic 10:00 *Oblivious Defense in ML Models: Backdoor Removal without Detection* S. Goldwasser, J. Shafer, N. Vafa, V. Vaikuntanathan.	9:45 **Welcome and Intro** 10:00 **Invited Talk** D. Slamanig	**Brief Welcome** 9:32 **Invited Talk** *Practical Post-Quantum Signatures from the Code Equivalence Problem* E. Persichetti	**Welcome and Intros** 9:45 *Poseidon Initiative Update* A. Sanso 10:00 *Groebner Basis Analysis of Poseidon* K. Koshatko	9:25 Opening 09:30 **Tutorial:** *Basics on Hardware and Low-Latency* T. Moos 10:00 **Tutorial:** *State of the Art on Designing Low-Latency Primitives* S. Rasoolzadeh
10:30	Coffee break						
11:00	**Proof techniques for game-based security** *Lazy "Twenty Questions" as a Proof Principle– How a pen-and-paper one-liner becomes an EasyCrypt library* F. Dupressoir *The Power of Halting in Security Games* I. Stepanovs 12:00 **Key exchange security** *Towards formally verifying the security reductions of the TLS 1.3 key schedule in SSBee* A. Rajabi *The Humble Power of the T-transformation* H. Heum	**Brainstorm on ideas!**	**Cryptography for Privacy-Preserving ML** *Willow: Secure Aggregation with One-Shot Clients* J. Bell-Clark, A. Gascon, B. Li, M. Raykova, P. Schoppmann 11:30 *Private Deep Neural Newtork Inference Engines with Homomorphic Encryption* A.J. Peña, L. Martens, P. Mehta, Z. Pindado, T. Spendlhofer. 12:00 *Private Deep Learning on Vertically Partitioned Datasets* P. Newton 12:30 *Fartech'd: Side-Channel Privacy Attacks in Confidential VMs* R. Zhang, A. Cheu, A. Gascon, D. Moghimi, P. Schoppmann, M. Schwarz, O. Suciu	*Refinement-based Verification of Protocols with Quantitative Values* A. Li, I. Rakotonirina *Homomorphic Signature-based Witness Encryption and Applications* A. Kavousi, I.A. Seres *Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee* A. Cimatti, F. De Sclavis, G. Galano, S. Giammusso, M. Iezzi, A. Muci, M. Nardelli, M. Pedicini *Jigsaw: Doubly Private Smart Contracts* S. Garg, A. Goel, D. Kolonelos, R. Sinha	*Construction-D Lattices from AG codes* E. Kirshanova *On the Construction of LDOI Group Codes with a Binary Adjacency Matrix* C. Martínez, F. Molina *Tiny keys for the Convolutional Niederreiter Cryptosystem with GRS Codes* P. Almeida, M. Beltrá Vidal, D. Napp *Algebraic Syndrome Decoding* L. Ran, S. Samardjiska, M. Trimoska *Can we speed up Information Set Decoding by Using Extension Field Structure?* F. Elbro, V. Weger	*Practical Cryptanalysis: Poseidon Bounties Claimed* G. Vitto 11:30 *Practical Cryptanalysis: Poseidon Bounties Claimed. Part 2* G. Vitto 12:00 *Target Collision Resistance: Security Requierements in the Context of Hash-based signatures* M. Kudinov 12:30 *Poseidon over Finite FFT-fields* A. Sanso	**Invited Talk:** *Review of Low Latency Primitives - Focus on the Non-Linear Layer* G. Leander 12:00 **Invited Talk:** *External Memory Security on Microcontroller: An Impossible Quest?* G. Van Assche, R. Susella
13:00	Lunch break						
14:15	**Frameworks, models and assumptions** *Is it better or worse (UC-wise)* S. Bayreuther *What can the Algebraic Group Model tell us about proof techniques in the Generic Group Model* J. Januzelli	**Afternoon session**	**Keynote Talk: TBA** N. Carlini	14:00 **Invited Talk: TBD** L. Nizzardo *Putting Symbils on a Diet: Securing Distributed Hash Tables using Proofs of Space* C. Günter, K. Pietrzak *Nakamoto Consensus from Multiple Resources* M.A. Baig, C.U. Günter, K. Pietrzak	*Leveraging Spherical Codes for Commitment over Gaussian UNCs* A.K. Yadav, M. Mamindlapally, A. J. Budkuley *SPARK: Subcode Permutation Argument of Knowledge* S. Ritterhoff, H. Sauerbier Couvée	**Group Work**	**Invited Talk: TBA** F. Mendel
15:15	Coffee break						
15:45	**Proofs for proof systems** *Special Soundness of Non-Interactive Polynomial Commitment Schemes* J. Siim *Commit-and-Prove System for Vectors and Applications to Threshold Signing* C. Özbay *Expected (polynomial) time in cryptography* M. Klooβ 17:15 **Anonymity models** *Privacy Proofs for Anonymous Communication Networks* C. Coijanovic	**Afternoon session** 16:45 **Present ideas/obstacles** 17:15 Onwards: **Explore Madrid with us!**	**Neural Distinguishers, Adversarial Resistance and LLM for Cryptography** 15:45 *Adversarial-Resistant AI Using Cryptograhic Primitives: A Commitment-Based Approach to Secure Explainability and Confidentiality* S. Biswal 16:15 *Generic Partial Decryption as Feature Engineering for Neural Distinguishers* R. Brunelli, D. Gerault, E. Bellini, A. Hambitzer, M. Pedicini 16:45 *An LLM Framework For Cryptography Over Chat Channels* D. Gligoroski, M. Raikwar, S.K. Jha 17:15 **Closing Remarks**	16:00 *Traceable Verifiable Random Functions* D. Boneh, A. Partap, L. Rotem *A Tale of Time Release powered by Blockchain and IBE* S. Wohnig, G. Avitabile, N. Dötling, B. Magri, C. Sakkas, L. Hanzlik	*Sneaking up the Ranks: Partial Key Exposure Attacks on Rank-Based Sehcmes* G. D'Alconzo, A. Esser, A. Gangemi, C. Sanna *An algebraic approach for the cryptanalysis of QC-MDPC code-based schemes* A. Meneghetti, F. Zanetti *AI for Code-based Cryptography: A Machine Learning Approach to Code Distinguishability* M. Malhou, L. Perret, K. Lauter *Improved Key Attack on the MinRank Encryption Scheme on Matrix Codes* A. Porwarl, A. Wachter-Zeh, P. Loidreau	**Group work**	**Invited Talk: TBA** M. Naya-Plasencia 16:30 **Invited Talk: TBA** C. Dobraunig
17:45	End of day						

Eurocrypt 2025 – Affiliated Events Schedule (Sunday, May 4t)

Time	s106	s116	s109	s108	b15	b03	b04	b05
	QuRCrypt	Isogeny	CAW	CAPS	CBCrypto	Alg. Hash	TPLC	PBC
08:30	Registration (closes at 14:00)							
09:00	**Keynote Presentation** *Conquer the SVP 200 Challenge* J. Ding 10:00 *Protecting against a semi-trusted third party with Hybrid Crypto* J. Munilla, A. Braeken 10:15 *The Hybrid State-of-Play: How to Securely Combine Quantum and Classical Key Establishment Technologies* C. Strieks, L. Perret	**Catch up with everybody** 9:30 **Morning session**	**CAW: Introduction** M. Backendal, M. Haller, L. Hetz, M. Scarlata 9:05 *RSA Blind Signatures with Public Metadata* G. Amjad 9:25 *Blockcipher-Based Key Commitment for Nonce-Derived Schemes* N. Ebeid 9:45 **Invited Talk** *Revisiting Keyed-Verification Credentials* M. Orrù	**Workshop Introduction and Security Overview** D. Connolly, P. Haselwarter, S. Oechsner 9:30 *Primitives: KEM-DEM Security Pen & Paper Proof* D. Stebila 9:45 *KEM-DEM & more in ProofFrog* D. Stebila	**Invited Talk:** *CROSS: Signature Scheme with Restricted Errors* Violetta Wegger *A BKW-Style Solver for the Restricted Decoding Problem* V. Nguyen, T. Johansson, Q. Guo	*Poseidon over Binary Fields* D. Khovratovich 9:15 *Correlation Intractability Challenges* D. Khovratovich 9:45 *Algebraic Analysis of Poseidon* A. Roy 10:15 *Group Results and discussion*	**Keynote Talk:** *Anonymous Permutation Routing* R. Ostrovsky 10:00 *A Framework for Witness Encryption from Linearly Verifiable SNARKs* A. Kothapalli	9:10 **Opening** 9:15 **First session** *Lumora: A family of permutation based wide-block ciphers for PQC zkSNARK applications* G. Guang *Permutation-Based Hash Chains with Application to Password Hashing* C. Lefevre
10:30	Coffee break							
11:00	*PQC in X.509 and OpenPGP and BSI recommendations* S. Kousidis, F. Strenzke 11:15 *Leveraging kleptography to strenghten post-quantum cryptography* E. Pérez-Ramos, O. Suárez-Doro, C. Hernández-Goya, P. Caballero-Gil 11:30 *Solving LWE search from a dual attack equivalent* R. Frot and D. Zentai 11:45 *The inpact of MLWE on Web User Experience and mTLS Applications* M. Anastasova, P. Kampanakis. 12:00 *Extension of root-based attacks against PLWE instances* R. Martín, I. Blanco-Chacón, R. Durán. 12:15 *CCA-attacks on lattice-based encryption-decryption schemes* A. Hernández-Costoya, A. Larraya-Sancho, M.A. Marco Buzurnáriz 12:30 *Exploring Non-Linear Activation Function Approximations in Fully Homomorphic Encryption* M. Rodríguez-Vega, P. Caballero-Gil.	**Morning session**	*To Trust, or Not to Trust: Results from Analyzing and Refining Bluetooth Secure Connections* O. Sanina 11:25 *Advanced KEM Concepts: (Hybrid) Obfuscation and Verifiable Decapsulation* F. Günter 11:50 *Linear-Time Accumulation Schemes* Giacomo Fenzi 12:15 **Invited Talk** *On the limits of PETs when designing to prevent harm* C. Troncoso	*KEM-DEM & more in EasyCrypt* F. Dupressoir 12:00 *Protocols: Key Exchange Security Pen & Paper Proof* D. Riepel 12:15 *Key Exchange & more in ProVerif* V. Cheval	*Post-Quantum Blind Signatures from Matrix Dode Equivalence* V. Kuchta, J. LeGrow, E. Persichetti *SPECK: Signature from Permutation Equivalence of Codes and Kernel* R. Schiavoni, M. Baldi, M. Battagliola, D. De Zuane, R. El Mechri, P. Santini *VOLEiTH signatures from Restricted Decoding Problems* S. Bitzer, V. Weger *VOLEiTH signatures based on the linear equivalence problem* M. Battagliola, L. Mattiuz, A. Meneghetti *Towards Hardware Acceleration of LESS with Canonical Forms* L. Beckwith, K. Gaj	11:00 **Joint session with Permutation Based Crypto** *Quantum Security of Sponges* D. Unruh *Fiat Shamir with Sponges* M. Orru	**Keynote Talk:** *Geometry of Secure Computation* H. Maji 12:00 *Laconic MPC, PIR and Public-Key Operations* M. Hajiabadi 12:30 *Laconic PSI and the Encryption Debate* J. Bartusek	11:00 **Joint session with Algebraic Hash (go to b03!!)** *Quantum Security of Sponges* D. Unruh *Fiat Shamir with Sponges* M. Orru
13:00	Lunch break							
14:15	**Panel: Convergence of Quantum and Post-Quantum Cryptography** S. Celi, P. Martín-Fernández, E. Sáenz de Cabezón, P. Caballero Gil.	**Afternoon session**	*Generic Anonimity Wrapper for Messaging Protocols* L. Thiempt 14:45 *Designing Secret Recovery in Signal Messenger* E. Dauterman	14:15 *Key Exchange & more in: Tamarin* C. Cremers	*Secure and Efficient Ligero Based Verifiable Delay Function* D. Değirmenci, O. Yayla *RHQC: post-quantum racheted key exchange from coding assumptions* J. Juaneda, M. Dehez-Clementi, J. Lacan, J-C. Deneuville	**Group Work**	**Keynote Talk:***Succint Obfuscation via Mathematical Proofs* A. Jain	**Third session** *On Some Variants of Cube-Attack-Like Cryptanalysis on SHA-3 Designs* M. Vaziri *On solving challenges in the Keccak Crunchy Crypto Contest* X. Lin
15:15	Coffee break							
15:45	*A Zero-Knowledge Proof based on shellability of simplicial complexes* D. Escánez-Exposito, P. Caballero-Gil, E. Sáenz de Cabezón, P. Munarriz-Senosiain. 16:00 *BB84-Inspired Quantum Zero-Knowledge Proof for User Authentication over Quantum Channel* J. Garcia-Diaz, D. Escánez-Exposito, P. Caballero-Gil, J. Molina. 16:15 *The Butterfly Protocol: QKD as a Service Without the "Weakest Link" Vulnerability* S. Kozlovics, E. Kalnina, J. Viksna, K. Petrucena, E. Rencis 16:30 *Entanglement-Based QKD Proposal Without Sharing Measurement Bases* D. Escánez-Exposito, P. Caballero-Gil. 16:45 *Confidential QUBO solver* M. Caruso, D. Escánez-Exposito, P. Caballero-Gil, C. Kuchkovsky 17:00*On a Quantum Search for Short Vectors in Lattices using QRISP* J. Bernabé-Rodriguez, I. Seco-Aguirre, C. Regueiro, O. Lage.	16:15 **Present your Achievements!!**	*Shadowfax: Combiners for Deniability* P. Gajland 16:05 *Designing a Post-Quantum Ratchet for Signal Messenger* R. Schmidt 16:35 **Discussion with C. Troncoso and M. Orrù**	**Round Table with Tool Developers: The State of Computer-Aided Proofs of Security**	*A Lattice Approach to the BIKE Cryptosystem* M. Schaller *Skew Reed-Solomon codes to the ReSkew: a new code-based cryptosystem* F. Hörman, A-L. Horlemann *A knapsack McEliece-based public key cryptosystem* J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro.	**Group results and wrap-up**	*Succint Trapdoor Hash Functions and Applications* P. Branco 16:15 *Multiparty Distributed Point Functions* A. Goel 16:45 *TBD* D. Abram	**Fourth session** *Insights into the Algebraic Structure of &Chi* B. Kriepke *Some Observations About the Ascon and Keccak S-box and Potential Applications in Cryptanalysis* N.T. Courtois
17:15	End of day							