Eurocrypt 2024 – Affiliated Events Program – Saturday (May 25)

Saturday	**Brainstorm Days** D7.2	**CBCrypto** E1.1	**CrossFyre** D3.2	**CTB** E1.2	**FHE:IDEAs** D1.2	**ProTeCS** D1.1	**TPLC** D5.2
08:30–	Registration						
09:00–10:30	Present ideas, make groups	09:00 Opening speech **Invited Speaker** 09:10 Algebraic methods in code-based cryptography (Simona Samardjiska) **Contributed Talk** 10:10 Properties of Quasi-Cyclic MDPC Codes in Post-Quantum Code-Based Cryptosystems (Gretchen Matthews)	09:00 Opening Remarks 09:10 **Invited Talk 1** (Rei Safavi-Naini) 10:00 Poster Session	– **Invited Talk 1** (Christian Cachin) – Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments (Christian Badertscher, Mahdi Sedaghat, and Hendrik Waldner) – SyRA: Sybil-Resilient Anonymous Signatures with Applications to Decentralized Identity (Elizabeth Crites, Aggelos Kiayias, and Amirreza Sarencheh)	09:00 Functional Bootstrapping and the FHEW-Style Approach to Homomorphic Encryption (Daniele Micciancio) 10:00 Introduction to CKKS Approximate Homomorphic Encryption (Nathan Manohar)	Welcome **Invited talk I** Adventures in Metacryptography: Proof Bugs, Impossible Definitions, and More (Joseph Jaeger)	09:00 Introduction to Laconic Cryptography (Giulio Malvolta) 09:30 Keynote Talk: Attribute-Based Encryption for Circuits of Unbounded Depth from Lattices: Garbled Circuits of Optimal Size, Laconic Function Evaluation, and More (Rachel Lin)
10:30–11:00	Coffee break						
11:00–12:30	Brainstorm on ideas!	**Contributed Talks** 11:00 Dihedral MDPC Quantum Codes (Najda Willenborg) 11:30 Breaking HWQCS: a code-based signature scheme from high weight QC-LDPC codes (Giovanni Tognolini) 12:00 Tighter DFR analysis and new decoders for HQC (Sebastian Bitzer)	11:00 11:00 **Invited Talk 2** (Dörte Resch) 11:50 Paper Session 1 Threshold Structure Preserving Signatures: Strong and Adaptive Security under Standard Assumptions (Jenit Tomy) Enhancing Private Set Intersection for Broader Applications (Peihan Miao) Verifiable Delay Functions and their (Unexpected) Applications (Charlotte Hoffmann)	– Cicada: A framework for private non-interactive on-chain auctions and voting (Noemi Glaeser, István András Seres, Michael Zhu, and Joseph Bonneau) – Rapidash: Atomic Swaps Secure under User-Miner Collusion (Hao Chung, Elisaweta Masserova, Elaine Shi, and Sri Aravinda Krishnan Thyagarajan) – PriDe CT: Towards Public Consensus, Private Transactions, and Forward Secrecy in Decentralized Payments (Yue Guo, Harish Karthikeyan, and Antigoni Polychroniadou) – 10 years of implementation of an usable group signature library: contributing to the design of decentralized identity management systems (David Arroyo, Sergio Chica, Jesús Díaz, and Andrés Marín-López)	11:00 Attacks Against the INDCPA-D Security of Exact FHE Schemes (Damien Stehle) 12:00 FHE for RAM Computation from Ring LWE (Ethan Mook)	**Game-based security** – Non-Committing Encryption as a QROM Playground (Hans Heum) – Please Mind the Gap: From Cryptographic Security Proofs to Attack Trees (Jeremias Mechler) – Enhancing Cryptographic Proofs: A Blended Approach to CryptoBox in EasyCrypt (Charlotte Mylog)	11:00 CCA Security via Hinting PRGs (Venkata Koppula) 11:30 Laconic Function Evaluation for Branching Programs (Mohammad Hajiabadi) 12:00 Batched Threshold Encryption with Applications to Mempool Privacy (Guru Vamsi Policharla)

Saturday	**Brainstorm Days** D7.2	**CBCrypto** E1.1	**CrossFyre** D3.2	**CTB** E1.2	**FHE:IDEAs** D1.2	**ProTeCS** D1.1	**TPLC** D5.2
12:30–13:30	Lunch break						
13:30–15:00	Afternoon session I	**Contributed Talks** 13:30 Breaking Four Code-Based Cryptosystems (Stefan Ritterhoff) 14:00 SDitH in Hardware (Sanjay Deshpande) 14:30 Public-Key Encryption based on Supercode Decoding (Anmoal Porwal)	**Panel Discussion** on Gender-related Issues with Huijia (Rachel) Lin, Dakshita Khurana, Anne Canteaut, Agnès Leroy	– **Invited Talk 2** (Jens Groth) – Naysayer proofs (Istvan Andras Seres, Noemi Glaeser, and Joseph Bonneau) – vetKeys: How a Blockchain Can Keep Many Secrets (Andrea Cerulli, Aisling Connolly, Gregory Neven, Franz-Stefan Preiss, and Victor Shoup)	13:30 BGV and BFV Bootstrapping: History, State-of-the-Art, and Future Perspectives (Robin Geelen) 14:15 Security Guidelines for Implementing Homomorphic Encryption (Rachel Player)	**Invited talk II** Mechanizing Cryptographic Reductions by Bi-Deduction (Adrien Koutsos)	13:30 **Keynote Talk:** Removing Trust Assumptions from Advanced Encryption Schemes (David Wu) 14:30 Replacing Full Homomorphism with Laconic Structure (or, Trapdoor Hash Functions and Their Many Applications) (Tamer Mour)
15:00–15:30	Coffee break						
15:30–17:00	– Afternoon session II – Present ideas/obstacles	**Contributed Talks** 13:30 On the Rank of Random Binary Sub-Matrices and its Impact for Information Set Decoding Algorithms (Bénédikt Tran) 14:00 Extending Interactive Oracle Proofs to General Linear Codes (Adrien Pasquereau) 14:30 Asymptotic Cost Comparison of Generic Rank Decoders (Hugo Sauerbier Couvée)	15:30 Paper Session 2 Security Bounds for Proof-Carrying Data from Straightline Extractors (Ziyi Guan) Solving the Tensor Isomorphism Problem on Special Orbits with Low Rank Points (Laurane Marco) Mathematical Tools for Post-Quantum Cryptography (Soda Diop) 16:10 Lightning Talks 16:50 Closing Remarks	– Improved YOSO Randomness Generation with Worst-Case Corruptions (Chen-Da Liu-Zhang, Elisaweta Masserova, João Ribeiro, Pratik Soni, and Sri Aravindakrishnan Thyagarajan) – Fait Accompli Committee Selection: Improving the Size-Security Tradeoff of Stake-Based Committees (Peter Gaži, Aggelos Kiayias, and Alexander Russell) – Practical Provably Secure Flooding for Blockchains (Chen-Da Liu-Zhang, Christian Matt, Ueli Maurer, Guilherme Rito, and Søren Eller Thomsen) – Updatable Privacy-Preserving Blueprints (Bernardo David, Felix Engelmann, Tore Frederiksen, Markulf Kohlweiss, Elena Pagnin, and Mikhail Volkhov)	15:30 Multiparty Homomorphic Encryption: from Theory to Practice (Christian Mouchet) 16:15 Threshold Fully Homomorphic Encryption From LWE – Challenges and Perspectives (Katharina Boudgoust)	**Simulation-based security** – Universal Composability with Effect Handlers (Jesse Sigal) – Universal Composability with Global Generic Groups (Jan Bobolz)	15:30 The Communication Complexity of Oblivious Transfer (Pedro Branco) 16:00 Rate-1 Non-Interactive Zero-knowledge without Lattices (Akshayaram Srinivasan) 16:30 Beyond Garbling: Efficient Advanced Encryption Schemes without Trusted Authority (Dimitris Kolonelos)
17:00	End of day						

Eurocrypt 2024 – Affiliated Events Program – Sunday (May 26)

Sunday	**Brainstorm Days** D7.2	**CBCrypto** E1.1	**AB+** D1.1	**AICrypt** D7.1	**CAW** E1.2	**HyPETs** D1.2	**WCCA+CTF** D5.2
08:30–	Registration						
09:00–10:30	– Catch up with everybody – Morning session I	**Invited Speaker** 09:30 “Hints for Codes and Lattices” (Alexander May)	9:00 Opening Remarks 9:15 Attributes and Blindness (Anna Lysyanskaya)	**Side-Channel Analysis** 09:00 **Keynote Talk** (Bart Preneel) 10:00 The more, the merrier? A step-by-step inter-device analysis for transfer learning side-channel attacks (L. Grootjen, Z. Liu and I. Buhan) 10:20 Exploring DNN Weights Extraction via Deep Learning Physical Side-Channel Analysis (D. Lauret and Z. Liu)	9:00 CAW: Bridging the gap between theory and practice (Matilda Backendal, Miro Haller) 9:10 Practical Private Information Retrieval for Real Databases (Sofía Celi, Alex Davidson) 9:35 How to Encrypt a File at Scale (Moreno Ambrosin, Fernando Lobato Meeser) 10:00 Analyzing Cryptography in Context: The Case Study of Apple's CSAM Scanning Proposal (Gabriel Kaptchuk)	9:00 Tutorial 1: Cat or Dog? What PETS Are and How to Choose Them (Nigel Smart) 9:45 Tutorial 2: Introduction to FHE and CKKS performance improvements (Damien Stehle)	09:00 Introduction to crypto code audits: the why’s and how’s (Tommaso Gagliardoni) 09:30 Side-channel attacks and common pitfalls (Adina Nedelcu) 10:00 Vulnerabilities in building blocks (Luca Dolfi)
10:30–11:00	Coffee break						
11:00–12:30	Morning session II	**Contributed Talks** 11:00 “FuLeakage: Breaking FuLeeca by Learning Attacks” (Felicitas Hörmann) 11:30 “On Linear Equivalence, Canonical Forms, and Digital Signatures” (Tung Chou) 12:00 “Lattice approach to Lee metric decoding” (Karan Khathuria)	11:00 Decentralized Single-use Credentials (Foteini Baldimtsi) 11:30 Privacy-Preserving Single Sign-On (Anja Lehmann) 12:00 PIR: Recent Developments and Advancements (Sofia Celi)	**Homomorphic Encryption and Verification of ML** 11:00 Encrypted Image Classification with Low Memory Footprint using Fully Homomorphic Encryption (L. Rovida and A. Leporati) 11:20 Homomorphic WiSARDs: Efficient Weightless Neural Network training over encrypted data (L. Neumann, A. Guimarães, D. F. Aranha and E. Borin) 11:40 PrivaTree: Private Decision Tree Evaluation by means of Homomorphic Encryption (M. Checri, A. Boudguiga, J.-P. Bultel, O. Chakraborty, Pierre-Emmanuel Clet and Renaud Sirdey)	11:00 Why we can't have nice (cryptographic) things (Henry Corrigan-Gibbs (invited speaker)) 11:45 Joint session on secure group messaging – WhatsUpp with Sender Keys? Analysis, Improvements and Security Proofs (Daniel Collins, Phillip Gajland) – Unidirectional Group Messaging: Simple, Secure, and Efficient Solutions (Paul Rösler)	11:00 Tutorial 3: Introduction to SMPC and hybrid privacy preserving applications (Mariya Georgieva, Sergiu Carpov) 11:45 Tutorial 4: Real world PETs use cases (Jan Weinreich, Manuel Capel)	11:00 Lost in translation: from paper to code (Adina Nedelcu) 11:30 MPC and Threshold Signatures 1 (Luca Dolfi) 12:00 MPC and Threshold Signatures 2 (Tommaso Gagliardoni)

Sunday	**Brainstorm Days** D7.2	**CBCrypto** E1.1	**AB+** D1.1	**AICrypt** D7.1	**CAW** E1.2	**HyPETs** D1.2	**WCCA+CTF** D5.2
				12:00 Efficient Verification Framework for Large-Scale Machine Learning Models (A. Grigor, A. Kravchenko and G. Wiese) 12:20 Ensuring Privacy and Robustness in Computation of Machine Learning Algorithms (C. Oikonomou and K. Sotiraki)			
12:30–13:30	Lunch break						
13:30–15:00	Afternoon session I 13:30 POKE: A Framework for Efficient PKEs, Split KEMs, and OPRFs from Higher-dimensional Isogenies (Andrea Basso)	**Work in Groups and Poster Session**	13:30 On Two-Witness Blind Signature Schemes from Groups (Julia Kastner) 14:00 Challenges of Schnorr-like Post-Quantum Blind Signatures (Shuichi Katsumata) 14:30 Round-Optimal Lattice-Based Blind Signatures: Constructions and Limitations (Ngoc Khanh Nguyen)	**Federated Learning** 13:30 **Keynote Talk:** Facial Misrecognition Systems (Adi Shamir) 14:30 Non-Interactive Secure Aggregation and its Applications to Federated Learning (H. Karthikeyan and A. Polychroniadou)	13:30 Securing semi-open group messaging (Fernando Virdia) 14:00 A Computational Security Analysis of Signal's PQXDH handshake (Rune Fiedler) 14:30 Bytes to schlep? Use a FEP: Hiding Protocol Metadata with Fully Encrypted Protocols (Aaron Johnson)	13:30 Practical session 1: Machine learning workflows using Inpher's XOR Platform (Marc Desgroseilliers, Tim Sonnenberg)	13:30 CTF registration and tutorial. Be on time here! 14:00 CTF portal opens, competition starts.
15:00–15:30	Coffee break						
15:30–17:00	– Afternoon session II – Present your achievements!	**Contributed Talks** 15:30 "Group Factorisation for Smaller Signatures from Cryptographic Group Actions" (Giuseppe D'Alconzo) 16:00 "Complexity of Solving Syndrome Decoding Problems as a System of Multivariate Equations" (Alex Pellegrini) 16:30 Closing speech	15:30 Pairing-Free Blind Signatures from CDH Assumptions (Stefano Tessaro) 16:00 Security of signatures with randomizable keys and related applications (Octavio Pérez Kempner) 16:30 Equivalence Class Signatures - Theory and Applications (Daniel Slamanig)	**15:20 (!) Neural distinguishers & PUFs** 15:20 **Keynote Talk:** Touching Points of Cryptography and AI (Moti Yung) 16:20 5 Years of Neural Distinguishers (D. Gerault and A. Hambitzer) 16:40 Provable Learnability Assessment of PUFs in Pre-silicon Phase (D. Chatterjee)	15:30 Computing on your data with MPC (Christopher Patton) 16:00 Panel on standardization	15:30 Practical session 2: New FFT and arithmetic API for Fully Homomorphic Encryption Libraries (Nicolas Gama, Maurice Shih) 16:15 Practical session 3: Confidential smart contracts using threshold FHE and the Zama fhEVM (Morten Dahl)	(CTF competition, cont'd)
17:00	End of day						