	Lundi	Mardi	Mercredi	Jeudi	Vendredi
9:00	Bienvenue	Thomas Roche Side-Channel Attacks on Secure Elements	Céline Chevalier Cryptography in a Quantum World	Elena Berardini Evaluation codes in the sum-rank metric	Christophe Levrat A divide-and-conquer sumcheck protocol Federico Savasta Efficient Threshold ECDSA on BICYCL Hugo Delavenne Proximity test to codes on graphs by flowering Marc Houben A deterministic algorithm for CSIDH
9:30	Léo Perrin On the Design Criteria for Symmetric Primitives				
10:00		Pause café du matin→10:30	Pause café du matin→10:30	Pause café du matin→10:30	Pause café du matin→10:10
10:30	Pause café du matin→10:45	Marie Bolzer Automated Search for Lightweight (AND, XOR) Implementations of Vectorial Boolean Functions Pierre-Augustin Berthet Code-Based Masking to protect ML-KEM against Side-Channel Analysis and Fault Injection Attacks	Charles Olivier-Anclin k-times Anonymity for Proxy and Sanitizable Signature Nihan Tanisali CRYPTANALYSIS OF A SYSTEM BASED ON GENERALIZED TWISTED REED-SOLOMON CODES	Charles Meyer-Hilfiger Assessing the impact of a variant of the latest dual attack Jean Gasnier Quasi-Abelian AG Codes	Jinwei Zheng Adaptive Hardcore Bit and Quantum Key Leasing over Classical Channel from LWE with Polynomial Modulus Abel Laval KLPT² : Algebraic pathfinding in dimension two and applications Lennart Braun Low-Bandwidth Mixed Arithmetic in VOLE-Based Zero-Knowledge Proofs from Low-Degree PRGs Arthur Herledan Le Merdy Unconditional foundations for supersingular isogeny-based cryptography
11:00	Mathieu Degré Simplifying the Search for Meet-in-the-middle Attacks on AES-Like Compression Functions Clémence Chevignard Reducing the Number of Qubits in Quantum Information Set Decoding	Merlin Fruchon New Perspectives in Differential Cryptanalysis of SPNs Julie Godard Single Trace Side-Channel Attack on the MPC-in-the-Head Framework	Mahshid Riahinia Constrained PRFs Meet Secure Computation Pierre Loisel Exploiting signature leakages: breaking Enhanced pqsigRM	Guilhem Niot Finally! A Compact Lattice-Based Threshold Signature Fabrice Drain Selfdual skew cyclic codes	Clôture
11:30	Aurélien Boeuf The Algebraic Freelunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives Agathe Blanvillain The quantum decoding problem	Dounia M'foukh Improving key-recovery attacks using the State-test technique Thomas Legavre Forge avec 0 information: Attaque par canaux auxiliaires sur HuFu	Houssem Derfoufi The long road to building fully secure chameleon hash function Auguste Warmé-Janville Masking Post-Quantum Signatures in the Threshold-Computation-in-the-Head Framework	→11:30	
12:00	→11:45	→11:45	→11:45	Guilhem Mureau Méthodes algébriques appliquées à la recherche d'isométries de réseaux structurés Virginio Fratianni Constructions of linear codes from vectorial almost bent functions and their subfield codes Anaëlle Le Devehat Classical algorithms for restricted hidden shifts and high-dimensional discrete logarithms with wallabies Jules Baudrin L'auto-équivalence linéaire, un point de vue unifié sur les familles connues de fonctions APN Laz Panard Implementation of ℤalcon: a floatless Falcon scheme Valentina Astore A Geometric Invariant of Linear Rank-Metric Codes	
12:30	Haetham Al Aswad Accelerating the Tower Number Field Sieve with Galois Automorphisms Wouter Rozendaal Abelian Two-Block Group Algebra Quantum Codes Victor Normand IronMaskArithmetic : Comprehensive Verification of Arithmetic Masking Security Samo Novak Quantum error correction with rotors and torsion	Bastien Michel Meet in the Middle (MITM) and Differential MITM attacks on Skinny with MILP Magali Salom Single trace side-channel attack on BIKE Antoine Bak Analyse de primitives symétriques orientées arithmétisation optimisées pour les lookups Daphné Trama Designing a General-Purpose 8-bit (T)FHE Processor Abstraction Guilhem Jazeron Cryptanalyse de Monolith par attaque rebound	Lola-Baie Mallordy Threshold Traceability Protocol for Viral Messages Chloé Baïsse Secret and Shared Keys Recovery on Hamming Quasi-Cyclic with SASCA Estelle Blin Oblivious Identity-Based Encryption in primary order pairing group Dayane Horkos AONT-SS: a new secure multi-cloud storage scheme	12h35 Déjeuner	
13:00	12h30 Déjeuner	12h30 Déjeuner	12h30 Déjeuner		
14:00					
14:30	Cyrius Nugier McEliece Parameter Sets Optimized for Processing in Memory Architectures Julia Sauvage Etude de sécurité d'une mise en gage basée sur des systèmes polynomiaux	discussion thématique 1		discussion thématique 2	
15:00	Axel Lemoine Cryptanalyse de McEliece: une approche géométrique River Moreira Ferreira Polynomial-Time Key-Recovery Attack on the NIST Specification of PROV	→15:10		→15:10	
15:30	Mohamed Malhou Code Distinguishers: A Transformer-Based Approach Rosa Fera Hilbert series and degrees of regularity of Oil & Vinegar and Mixed quadratic systems	Damien Vidal Analyzing the Crossbred Algorithm for the MQ Problem Marina Checri On the practical CPAD security of "exact" and threshold FHE schemes and libraries Pierre Pébereau Geometric approach to the cryptanalysis of UOV-based signatures Marc Renard Relations Among New CCA Security Notions for Approximate FHE Alban Gilard Improving the understanding of the Support-Minors modeling of a MinRank problem by computing its Hilbert series Anas Boudi Multiplications efficaces pour le chiffrement homomorphe		Samuel Bouaziz-Ermann The Wonderful World of Quantum Pseudorandomness François Palma Arithmétique modulaire très efficace grâce aux nombre premiers PMNS-friendly Virgile Guemard Moderate length quantum Tanner codes with good performances Kayodé Epiphane Nouetowa Analyse d'une généralisation du cryptosystème de Loidreau. Nicolas Saussay Réseaux quotientés et codes stabilisateurs locaux Rakhi Pratihar New classes of efficiently decodable rank-metric codes	
16:00	Pause après-midi→16:15				
16:30	Lucas Ottow Threshold Niederreiter: Chosen-Ciphertext Security and Improved Distributed Decoding Loris Bergerat Accelerating TFHE with Sorted Bootstrapping Techniques	Pause après-midi→16:55		Pause après-midi→16:55	
17:00	Mickael Hamdad Algorithms for Bichromatic Closest Pairs Problem and application to Code-based Cryptography Nicolas Bon Transistor: a FHE-friendly stream cipher	Antoine Dequay Algorithmes pour correspondances modulaires entre variétés abéliennes à structure de niveau Henry Bambury Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms		Pierrick Dartois SQIsign2D-West: faster, safer and compact signatures with 2-dimensional isogenies Martin Scotti Intersecting codes in the rank metric	
17:30	→17:15	Julien Soumier Computing isomorphisms between products of supersingular elliptic curves, and cryptographic applications. Julien Cam Post-Quantum Identity-Based Encryption from ML-KEM		Nicolas Sarkis Halving differential additions on Kummer lines Charles Brion Algebraic Cryptanalysis of Subcode Equivalence Problem in Rank Metric	
18:00	Valerian Hatey Analysis of the decoding problem in the sublinear regime Antonina Bondarchuk Downlink (T)FHE ciphertexts compression	Alexandre Benoist The distribution of Elkies primes Antoine Douteau Système de preuves à divulgation nulle de connaissance reposant sur Hint-MLWE			
	Antoine Mesnard Security of BIKE against failure attacks Baptiste Germon Extending and optimizing the quasidifferential framework				
	19h Dîner	19h Dîner	18h15 Rump Session 19h Dîner 20h30 AG C2	19h Dîner	

Version ical: `https://members.loria.fr/EThome/c2.ics` ; date du document: 01/04/2025 18:59