Programme JC2 2023

Lundi	Mardi	Mercredi	Jeudi	Vendredi
8h45-9h **Accueil**				
9h – 10h Gilles Zémor - **Recent constructions of asymptotically good quantum LDPC codes.**	9h – 10h Alice Pellet-Mary - **Lattices in cryptography: cryptanalysis, constructions and reductions**	9h – 10h30 Guilhem Niot – **Koganei, a hash-and-sign digital signature based on unstructured lattices** Julien Devevey – **G+G: A Fiat-Shamir Lattice Signature Based on Convolved Gaussians** Corentin Jeudy – **Signature avec Protocoles Efficaces sur les Réseaux Euclidiens, Application aux Accréditations Anonymes** Calvin Abou Haidar - **Efficient Updatable Public Key Encryption from Lattices** Thi Thu Quyen Nguyen - **Antrag: Annular NTRU Trapdoor Generation Making Mitaka As Secure As Falcon**	9h – 10h Christina Boura - **Differential cryptanalysis : An old but still powerful technique**	9h - 10h Damien Vergnaud - **Calcul distribué « dans la tête » : techniques et applications**
10h - 10h30 Virgile Guemard - **Lift of quantum CSS codes and applications** Paul Hermouet - **Semi-Quantum Copy-Protection and More**	10h – 10h40 Présentation du GT Parité et du projet de charte		10h – 10h30 Valerian Hatey – **Représentations ternaires** Sabira El Khalfaoui – **A code-based digital signature scheme for post-quantum security**	10h – 10h20 Matteo Abbondat – **Probabilistic Analysis of LLL-based Decoder of Interleaved Chinese Remainder Codes** Wouter Rozendaal – **A Worst-Case Analysis of a Renormalisation Decoder for Kitaev's Toric Code**
Pause café	Pause café thématique (10h40 – 11h10)	Pause café thématique	Pause café thématique	Pause café (10h20-10h50)
11h – 12h30 Mickaël Hamdad – **Shooting for the Stars! The May-Ozerov Algorithm for Syndrome Decoding is "Galactic"** Etienne Burle - **Fonctions à trappe fondées sur la métrique rang avec erreurs homogènes** Thibauld Feneuil – **Post-Quantum Signatures from Secure Multiparty Computation** Maxime Bombar – **Pseudorandom Correlation Generators from the Hardness of Decoding Quasi-Abelian Codes** Victor Dyseryn – **PERK: Compact Signature Scheme Based on a New Variant of the Permuted Kernel Problem**	11h10 – 12h30 Guillaume Goy – **A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext** Ninon Calleja Albillo – **How not to use deep learning for side channel attacks** Guilhèm Assael – **Attaque simple par canaux auxiliaires de la transformée en nombres entiers pour Cortex-M4** Benjamin Malthiery – **Proposition d'une nouvelle approche de Strong PUF multidimensionnelle basée sur une couche mince multifonctionnelle**	11h – 12h30 Julia Sauvage - **Vers des outils de référence et de nouveaux algorithmes pour la résolution des systèmes polynomiaux quadratiques booléens** Haetham Al Aswad - **Discrete Logarithm Factory** Ambroise Fleury – **We Are on the Same Side. Alternative Sieving Strategies for the Number Field Sieve** Florette Martinez – **Attaques sur le Knapsack Generator elliptique et ses généralisations** Agathe Houzelot – **Implémentations Boîte-Blanche de l'ECDSA**	11h – 12h30 Nicolas Sarkis - **Better scalar multiplication on elliptic curves using theta models** Andersson Calle Viera – **Implémentation de signature à base de réseau sécurisée contre les attaques par canaux auxiliaires.** Camille Mutschler - **Estimateur de complexité de gadgets masqués** Clementine Gritti – **Benchmarking quantum-resistant authentification in IoT** Abdel Taleb – **Security of Concrete Implementations in the Random Probing Model: A Complete Methodology**	10h50 – 11h30 Charles Olivier-Anclin – **Practical Construction for Secure Trick-Taking Games Even With Cards Set Aside** Hugo Beguinet – **A different approach of Fiat-Shamir with aborts signatures using polytopes** **FIN – 11h30**
Pause repas	Pause repas	Pause Repas	Pause repas	
14h30-15h30 Ahmed Alharbi - **Revisiting the Long Message Attack & Auditing its Cost** Dounia M'Foukh – **Cryptanalysis using Truncated Differential** Aurélien Boeuf - **Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES** Viet-Sang Nguyen – **Linear Cryptanalysis and Countermeasures in Persistent Fault Model** Samuel Bouaziz-Ermann – **On the impossibility of Quantum Public Key Encryption**	14h30-15h30 Marina Checri - **Lightweight FHE-based Protocols Achieving Results Consistency for Data Encrypted Under Different Keys** Nicolas Bon – **Evaluation optimisée de circuits booléens en TFHE** Daphné Trama – **Building Blocks for LSTM Homomorphic Evaluation with TFHE** Loris Bergerat - **Faster Secret Keys for (T)FHE** Mahshid Riahinia – **Constrained Pseudorandom Functions from Homomorphic Secret Sharing**		14h30-15h30 Léo Ackermann – **Post-quantum encryption from lattice isomorphisms** Guilhem Mureau – **One the module-Lattice Isomorphism Problem** Joël Felderhoff – **Improved worst-case to average-case reduction for ideal-SVP** Pouria Fallahpour – **Obliviously Sampling Hard Instances of Lattice problems**	
Mini-pause	Mini-pause		Mini-pause	
15h40-16h40 Augustin Bariant – **Truncated Boomerang Attacks and Application to AES-based Ciphers** Margot Funk – **Algorithms and Models for the Differential Analysis of the AES** Rachelle Heim-Boissier **- Cryptanalysis of Elisabeth-4**	15h40-16h40 Anaïs Barthoulot – **Dualy Computable Cryptographic Accumulators** Paola de Perthuis – **Mises en gage coucou : chiffrement par enregistrement et mises en gage de tables de clés et valeurs pour de grandes entrées** Ferran Alborch Escobar – **Computational Differential Privacy for Encrypted Databases Supporting Linear Queries**		15h40-16h40 Clémence Bouvier - **Anemoi: Exploiting the Link between Arithmetization-Orientation and CCZ-Equivalence** Margarita Cordero – **On Impossible Boomerang Attacks** Jules Baudrin – **Commutative Cryptanalysis Made Practical**	
Pause café	Pause café		Pause café	
17h – 18h30 Jean Gasnier – **An Algebraic Point of View on the Generation of Pairing-Friendly Curves** Arthur Herlédan Le Merdy – **Le problème EndRing connaissant un endomorphisme** Pierrick Dartois – **Signing with higher dimensional isogenies** Abel Laval – **Malleable commitments from group actions and zero-knowledge proofs for circuits based on isogenies** Sabrina Kunzweiler – **Efficient Computation of (3^n,3^n)-isogenies** Dimitri Koshelev – **Subgroup membership testing on elliptic curves via the Tate pairing**	17h – 18h30 Kayodé Epiphane Nouetowa – **Décodage itératif des codes cycliques tordus** Martin Scotti – **On the lower bound for the length of minimal codes** Virginio Fratianni – **The Dual and the Hull code in the framework of the two generic constructions** Charles Meyer-Hilfiger - **Rigorous Foundations for Dual Attacks in Coding Theory** Bastien Pacifico – **Une approche pour introduire la localité dans les codes AG généralisés** Rakhi Pratihar - **Generalized rank weights and Betti numbers**	17h30-18h30 **Table ronde** – Politique, cryptographie et nouvelles régulations	17h – 18h30 Lucas Ottow – **Calculs distribués sécurisés sur polynômes et applications à Private Set Intersection et problèmes connexes** Dinh Duy Nguyen – **Verifiable Decentralized Multi-Client Functional Encryption for Inner Product** River Moreira Ferreira – **Toward Threshold UOV** Agathe Beaugrand – **Private intersection-sum and ZK-proof of shuffle** Jules Maire – **Efficient Zero-Knowledge Arguments and Digital Signatures via Sharing Conversion in the Head** Thomas Lavaur – **Modular zk-Rollup On-Demand**	
		20h30 AG C2		