PROGRAMME JC2

Journées Codage & Cryptographie

02 - 06 novembre 2020 #15

VISIOCONFERENCE

LUNDI 02 NOVEMBRE

09:30	Chair : Vanessa Vitse	
	Jean Kieffer	Calcul d'isogénies à partir d'équations modulaires en genre 2
	Simon Masson	Verifiable Delay Functions from Supersingular Isogenies and Pairings
10:30	Arthur Lavice	Multiplication over extension fields for Pairing-based Cryptography: an Hardware Point of view
10:45	*Pause 15 minutes*	
	Sulamithe Tsakou	Attaque par calcul d'indices sur les Jacobiennes de courbes hyperelliptiques munies d'endomorphismes
	Youssef El Housni	Optimized and secure pairing-friendly elliptic curve suitable for one layer proof composition
11:00	Andy Russon	The quest for an exception-free windowing elliptic curve scalar multiplication
	Chair : Sonia Belaïd	
	Loïc Masure	Vers une meilleure compréhension de l'apprentissage profond appliqué aux attaques par observation
11:40	Nicolas Bordes	High-order private multiplication in characteristic two revisited
11:50	*Pause 10 minutes*	
	Lucas Barthelemy	Toward an Asymmetric White-Box Proposal
12:30	Adel Hamdi	Blind Functional Encryption

MARDI 03 NOVEMBRE

09:30	Chair : Christina Boura	
	Paul Huynh	Feistel case: when the boomerang comes back
	Baptiste Lambin	Linearly equivalent S-boxes and the Division Property
10:30	Victor Mollimard	Efficient Search for Optimal Diffusion Layers of Generalized Feistel Networks
10:45	*Pause 15 minutes*	
	Durand Amaury	Codes duaux des codes de Reed-Solomon lin□earis□es dans le cadre differentiel
	Florette Martinez	QMDS codes with minimal length
11:00	Maxime Bros	An Algebraic Attack on Rank Metric Code-Based Cryptosystems
	Chair : Claire Delaplace	
	Katharina Boudgoust	On the classical hardness of Module-LWE: the linear rank case
11:40	Charbel Saliba	Key exchange based on Ring-LWE using Barnes-Wall lattices
11:50	*Pause 10 minutes*	
	André Schrottenloher	Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm
12:30	Yixin Shen	Better Quantum Algorithms for Subset-Sums

MERCREDI 04 NOVEMBRE

10:00	AG du GT C2

UMR IRISA

JEUDI 05 NOVEMBRE

09:30	Chair : Eleonora Guerrini	
	Weiqiang Wen	Faster Enumeration-based Lattice Reduction: Root Hermite Factor k^(1/(2k)) in Time k^(k/8 + o(k))
	Gabrielle De Micheli	Discrete logarithm algorithms in pairing-relevant finite fields
10:30	**Andrea Lesavourey**	Retrieving short generators of principal ideals in real Kummer extensions
10:45	*Pause 15 minutes*	
	Antonio Florez Gutierrez	Improving the key recovery in linear cryptanalysis: An application to PRESENT
	Olivier Bernard	Twisted PHS: Using the product formula to solve Approx-SVP on ideal lattices
11:00	**Guillaume Kaim**	Post-quantum e-voting scheme
	Chair : Aurore Guillevic	
	Isabella Panaccione	The Power Error Locating Pairs algorithm
11:40	**Matthieu Lequesne**	On the security of subspace subcodes of Reed-Solomon codes for public key encryption
11:50	*Pause 10 minutes*	
	Aude Le Gluher	Complexité asymptotique fine du crible algébrique
12:30	**Manon Bertin**	Understanding the complexity of an algebraic attack on the superdetermined DAGS system

VENDREDI 06 NOVEMBRE

09:15	Chair : Malika Izabachène	
	Ida Tucker	Bandwith efficient threshold ECDSA
	Chloé Hébant	Linearly-Homomorphic Signatures and Scalable Mix-Nets
	Rémi Clarisse	Efficacité globale des protocoles à base de couplage
10:35	**Laura Brouilhet**	Round-Optimal Constant-Size Blind Signatures
10:45	*Pause 10 minutes*	
	Céline Duguet	Zero-knowledge proofs for MLS
	Abbass Madi	A secure approach for Neural Networks using Homomorphic Encryption and Verifiable Computation
11:00	**Florian Caullery**	Exploring Parallelization Strategies for SPHINCS+
	Chair : Sihem Mesnager	
	Simon Abelard	Un algorithme (plus) rapide pour calculer des espaces de Riemann-Roch
11:40	**Sarah Bordage**	Interactive Oracle Proof of Proximity for Products of Reed-Solomon Codes
11:50	*Pause 10 minutes*	
	Ilaria Zappatore	Enhancing simultaneous rational function reconstruction with errors: adaptive error correction capability and new bounds for applications
12:30	**Jade Nardi**	Explicit construction and parameters of projective toric codes

JC2 2020

UMR IRISA