	Monday 08/10	Tuesday 09/10	Wednesday 10/10	Thursday 11/10	Friday 12/10
09:00 - 10:00	**Magalie Bardet**	**Ben Smith** Pre- and post-quantum Diffie--Hellman	**Matthieu Rivain**	**Olivier Blazy** Cryptographie implicite, comment faire plus en révélant moins.	**Marine Minier** Utilisation de la programmation par contraintes pour la recherche d'attaques différentielles à clés liées contre l'AES.
	PAUSE CAFÉ	PAUSE CAFÉ	PAUSE CAFÉ	PAUSE CAFÉ	PAUSE CAFÉ
10:30 - 11:30	**X. Bonnetain, M. Naya-Plasencia and A. Schrottenloher.** Cryptanalyse quantique de l'AES (et effets secondaires). **B. Lambin.** Variants of the AES key-schedule for better truncated differential bounds. **D. Coggia, A. Canteaut and C. Boura.** On subspace trails cryptanalysis.	**N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta and G. Zémor**. LRPC codes : new decoding algorithm and applications. **I. Zappatore**. Error polynomial linear system solving by simultaneous polynomial reconstruction of interleaved Reed-Solomon codes. **K. Carrier and J.-P. Tillich**. Near collisions search and generic decoding.	**O. Blazy, L. Brouilhet and D. H. Phan**. Anonymous identity based encryption with traceable identities. **C. Qian, B. Libert and T. Peters**. Logarithmic-size ring signatures with tight security from the DDH assumption. **I. Tucker, G. Castagnos and F. Laguillaumie**. Chiffrement fonctionnel sans restriction pour le calcul de produits scalaires modulo un nombre premier.	**G. Kaim**. Lattice-based (partially) blind signature without abort. **R. Titiu, B. Libert and D. Stehlé**. Adaptively secure distributed PRFs from LWE. **P. Bert**. From identification using rejection sampling to signatures via the Fiat-Shamir transform.	**M. Zuber**. Privacy-preserving classification using an encrypted neural network with FHE. **A. Dupin, D. Pointcheval and C. Bidan**. On the leakage of corrupted garbled circuits. **J. Lavauzelle**. Preuves cryptographiques pour le stockage en ligne : modèles et construction.
	PAUSE	PAUSE	PAUSE	PAUSE	FIN - REPAS - BUS - TRAIN
11:40 - 12:20	**Y. Aono, P. Q. Nguyen and Y. Shen**. Quantum lattice enumeration. **A. Pellet-Mary**. Approx-SVP in ideal lattices with pre-processing.	**A. Le Gluher and P.-J. Spaenlehauer.** Une approche géométrique pour le calcul d'espaces de Riemann-Roch : algorithme et complexité. **L. Grémy.** Higher dimensional sieving for the number field sieve algorithms.	**J. Kieffer**. Towards practical key exchange from isogeny graphs. **X. Bonnetain and A. Schrottenloher**. Submerging CSIDH.	**S. Masson**. Cocks-Pinch pairing-friendly curves of embedding degrees five and seven and ate pairing computation. **M. Trimoska, S. Ionica and G. Dequen**. Time-memory trade-offs for parallel collision search algorithms.	
	DÉJEUNER	DÉJEUNER	DÉJEUNER	DÉJEUNER	
	LIBRE !				
17:00 - 18:00	**C. Hébant, D. H. and D. Pointcheval**. Evaluating boolean formulae on encrypted data with applications to group testing and machine learning. **D. Lucas, C. Pernet, P. Lafourcade, J.-G. Dumas, J.-B. Orfila, M. Puys and J. Lopez-Fenner**. Secure multi-party matrix multiplication based on Strassen-Winograd algorithm. **A. Nitulescu**. Efficient protocols for integrity in the cloud.	**A. Bauer, H. Gilbert, G. Renault and M. Rossi**. On the security of NewHope key encapsulation mechanisms against key mismatch oracle attacks. **J.-C. Deneuville, P. Gaborit, Q. Guo and T. Johansson**. Ouroboros-E: an efficient lattice-based key-exchange protocol. **G. Eberhart**. Optimising a secure signature scheme based on module-SIS/LWE.	**A. Couvreur, M. Lequesne and J.-P. Tillich**. Recovering short secret keys of RLCE encryption scheme in polynomial time. **T. Debris-Alazard and J.-P. Tillich**. Deux attaques contre des schémas se fondant sur les codes en métrique rang : RankSign et un chiffrement basé sur l'identité. **T. Richmond, B. Gérard, A. Heuser and A. Legay**. Side-channel information eakage of the syndrome computation in code-based cryptography.	**C. Chaigneau**. Key-recovery attacks on full Kravatte. **D. Mercadier and P.-E. Dagand**. Usuba, optimizing and trustworthy bitslicing compiler. **J.-F. Couchot and S. Contassot-Vivier**. Canonical form and automatic generation of Gray Codes in N-cubes: application to PRNG.	
	PAUSE	PAUSE	PAUSE	PAUSE	
18:10 - 18:50	**A. Grospellier and A. Krishna.** Estimation numérique du threshold des codes expanseurs quantiques. **V. Vasseur.** Estimating the QCMDPC decoding failure rate.	**L. Perrin and A. Canteaut**. On CCZ-equivalence, extended-affine equivalence, and function twisting. **F. Sibleyras**. The missing difference problem, and its applications to counter mode encryption.	AG du GT C2	**L.-S. Didier, F.-Y. Dosso and P. Véron**. Efficient and secure modular operations using the Adapted Modular Number System. **N. Coxon**. Fast transforms over finite fields of characteristic two.	
20:00	DINER	DINER	DINER	DINER	