Séminaire IAA (IMATH)
2017-2018

mardi 10/10 : **Julien Eynard (IAA – UTLN)** - *Arithmétiques efficaces pour schémas de chiffrement (complètement) homomorphes.*

mardi 24/10 : **Amine El Mrabet (Paris VIII) -** *Implémentation efficace de la multiplication de Montgomery sur FPGA.*

mardi 14/11 : **Anastasiia Volkova (AriC - ENS Lyon)** - *Algorithmique de l'implementation fiable de filtres numériques.*

mardi 21/11 **Elise Barelli (LIX)***, Short McEliece key from algebraic geometry codes with automorphism.*

mardi 28/11 : **Laurent Gremy (ENS LYON)** *: Computing discrete logarithms in GF(p^5) and GF(p^6): a focus on the relation collections.*

mardi 05/12 **Nadia El Mrabet (EMSE)** - *Implémentation de couplage en utilisant les bases AMNS.*

mardi 12/12 **Alexandre Wallet (LIP - ENS LYON) -** *The point decomposition problem in Jacobian varieties.*

mardi 19/12 **Vincent Grosso (UCL)** *Attaques par canaux cachés et algorithmes d'énumération.*

mardi 23/01 **Elena Berdardini (I2M)** - *Codes sur les surfaces abéliennes.*

mardi 20/02 **Jean-Christophe Deneuville (INSA)** - *Échange de clé et chiffrement basés sur les codes, une nouvelle approche.*

mardi 06/02 : **Kevin Atighehchi (Université de Caen)** – *Arbres de hachage.*

mardi 20/03 *:* **Philippe Langevin (IAA – IMATH)** – *Quelques conjectures sur* les *fonctions booléennes.*

mardi 27/03 *:* **Loubna Ghammam (GREYC – EMSE - Monastir) –** *Utilisation des couplages en Cryptographie.*

mardi 17/03 : **Jean-Marc Robert -** *Enhanced Digital Signature using Splitted Digit Exponent Representation.*

mardi 03/04. : **Tania Richmond (INRIA, IRISA Rennes)** - *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs.*

mardi 19/06 : **Gregor Leander (Ruhr University Bochum)** - *Invariant Subspace Attacks on Lightweight Block Ciphers .*