Séminaire IAA (IMATH)
2021-2022

mardi 9/11 : **Ali Issa (IAA – UTLN)** - *Polynômes d'uniformité différentielle maximale*.

mardi 23/11 **Philippe Langevin (IAA – UTLN)** - *Asymptotically optimal Boolean functions*

mardi 7/12 : **Stéphane Ballet (I2M – AMU) -** *Sur la complexité scalaire des algorithmes de Chudnovsky*

mardi 11/01 : **Yoann MARQUER** (en visio) - *The Interleaved Ladders: securing algorithms against side-channel and fault-injection attacks*

mardi 25/01 : **Jean-Marc Robert (IAA – UTLN)** : *Fast modular multiplications.*

mardi 22/02 : **Maxime Bombar (INRIA - LIX)** (en visio) *On codes, and learning with errors over function fields*

mardi 08/03 : **GOY Guillaume (CEA – LETI)** (en visio) – *Estimating the strenght of horizontal correlation attacks in the hamming weight leakge model : a side-channel analysis on HQC KEM*

mardi 22/03 : ~~**Elena Berardini (Université d'Eindhoven) :** *Curves on Frobenius classical surfaces in the projective space over finite fields*~~

mardi 05/04 : **réunion d'équipe.**

mardi 26/04 : **Elena Berardini (Université d'Eindhoven)** (en visio) : *Curves on Frobenius classical surfaces in the projective space over finite fields* (à confirmer)

mardi 10/05 : TBA

mardi 24/05 : TBA

mardi 7/06 : TBA