

Séminaire IAA (IMATH) 2018-2019

mardi 02/10 : **Yssouf Dosso (IAA – UTLN)** - *Euclidean addition chains scalar multiplication on curves with one efficient endomorphism.*

mardi 6/11 : **Alejandro Giangreco (I2M – LAMU)** - *Cyclicity of the rational points group of abelian varieties over finite fields*

mardi 20/11 : **Yannick Téglia (THALES)** Starting Transition Towards Products Embedding Post-Quantum Cryptography

mardi 04/12 : **Jean-Marc Robert (IAA – UTLN)** *Cryptographie et ordinateur quantique 1*

mardi 11/12 : **Jean-Marc Robert (IAA – UTLN)** *Cryptographie et ordinateur quantique 2*

mardi 15/01 : **Jérémy Marrez (IAA – UTLN)** *Les systèmes de représentation adaptés polynomiaux (PMNS) et les racines de leur polynôme de réduction dans le corps $\mathbb{Z}/p\mathbb{Z}$.*

mardi 22/01 : **Jean-Marc Robert (IAA – UTLN)** *Cryptographie et ordinateur quantique 3*

mardi 05/02 : **Jean-Marc Robert (IAA – UTLN)** *Cryptographie et ordinateur quantique 4*

mardi 12/03 : **Elena Berardini (I2M- LAMU)** *Codes sur les surfaces abéliennes.*

mardi 26/03 : **Ilaria Zappatore (LIRMM - Montpellier)** *Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed Solomon Codes*