Nutmic 2019 Program

Monday, June 24th

9h-9h30: **Welcome Coffee**

9h30-9h45: **Introduction**

9h45-10h45: Invited Talk - **Alain Couvreur**
Cryptanalysis techniques in cryptography based on algebraic codes

10h45-11h45: Session 1 - **Curves 1 -** *Chair: Faruk Gologlu*
- Claire Delaplace and Alexander May.
  Can we Beat the Square Root Bound for ECDLP over F(p^2) via Representations?
- Kazuhiro Yokoyama, Masaya Yasuda, Yasushi Takahashi and Jun Kogure.
  Complexity Bound on Semaev's Naive Index Calculus Method for ECDLP

14h30-15h30: Invited Talk - **Dan Boneh**
Cryptography for blockchains

15h30-16h: **Coffee Break**

16h-17h: Session 2 - **Hash functions -** *Chair: Janusz Szmidt*
- Hayley Tomkins, Monica Nevins and Hadi Salmasian.
  New Zémor-Tillich Type Hash Functions Over GL2(F_(p^n))
- Wouter Castryck, Thomas Decru and Benjamin Smith.
  Hash functions from superspecial genus-2 curves using Richelot isogenies

Tuesday, June 25th

9h00-10h00: Invited Talk - **Alfred Menezes**
The computational supersingular isogeny problem

10h-10h30: **Coffee Break**

10h30-12h: Session 3 - **Constructions -** *Chair: Louis Goubin*
- Eric Brier, Houda Ferradi, Marc Joye and David Naccache.
  New Number-Theoretic Cryptographic Primitives
- Carl Bootland, Wouter Castryck, Alan Szepieniec and Frederik Vercauteren.
  A Framework for Cryptographic Problems from Linear Algebra
- Christina Boura, Nicolas Gama, Mariya Georgieva and Dimitar Jetchev.
  CHIMERA: Combining Ring-LWE-based Fully Homomorphic Encryption Schemes

Free Afternoon

Wednesday, June 26th

9h00-10h00: Invited Talk - **Hendrik Lenstra**
Computing symbols in arithmetic

10h-10h30: **Coffee Break**

10h30-12h: Session 4 - **Curves 2 -** *Chair: Tanja Lange*

- Leonardo Colò and David Kohel.
  Orienting supersingular isogeny graphs
- Taechan Kim and Mehdi Tibouchi.
  Equidistribution Among Cosets of Elliptic Curve Points in Intervals
- Ronal Pranil Chand and Maheswara Rao Valluri.
  Elliptic Curves in Generalized Huff's Model

14h30-15h30: Session 5 - **Integers -** *Chair: Piotr Sapiecha*

1. Jacek Pomykała and Maciej Radziejewski. *Integer factoring and compositeness witnesses*
2. Maciej Grzeskowiak. *A variant of the large sieve inequality with explicit constants*

15h30-16h: **Coffee Break**

16h-17h: Session 6 - **Applications -** *Chair: Jacek Pomykała*

3. Marc Joye. *ECC Against Fault Attacks: The Ring Extension Method Revisited*
4. Giovanni Di Crescenzo, Matluba Khodjaeva, Delaram Kahrobaei and Vladimir Shpilrain.
   Delegating a Product of Group Exponentiations with Application to Signature Schemes

19h: Conference Dinner

Thursday, June 27th

9h00-10h00: Invited Talk - **René Schoof**
An elliptic finite field representation (d'après Guido Lido)

10h-10h30: **Coffee Break**

10h30-12h: Session 7 - **Cryptanalysis -** *Chair: Aline Gouget*

- Jean-Sebastien Coron and Agnese Gini.
  Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem
- Jung Hee Cheon, Wonhee Cho, Minki Hhan, Minsik Kang, Jiseung Kim and Changmin Lee.
  Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem
- Andrea Lesavourey, Thomas Plantard and Willy Susilo.
  On ideal lattices in multicubic fields