Antoine Joux and Jacek Pomykała

Preface for the Number-Theoretic Methods in Cryptology conferences

https://doi.org/10.1515/jmc-2019-0111
Received Sep 01, 2020; accepted Sep 01, 2020

Number-Theoretic Methods in Cryptology (NutMiC) is a bi-annual series of conferences that was launched in 2017. Its goal is to spur collaborations between cryptographers and number-theorists and to encourage progress on the number-theoretic hard problems used in cryptology. The publishing model for the series is also mixing the traditions of the cryptography and number theory communities. Articles were accepted for presentation at the conference by a scientific commitee and were reviewed again at a slower pace for inclusion in the journal post-proceedings.

In 2019, the conference took place at the Institut de Mathématiques de Jussieu, Sorbonne University, Paris. The event was organized in collaboration with the international association for cryptologic research (IACR) and supported by the European Union's H2020 Program under grant agreement number ERC-669891. This support allowed us to have low registration costs and offer easy access to all interested researchers.

We were glad to have the participation of five internationally recognized invited speakers who greatly contributed to the success of the conference.

Nutmic 2019 Co-Chairs,

Antoine Joux and Jacek Pomykała

Program

The slides that were presented at the conference remain available on the website http://nutmic2019.imj-prg.fr/

Invited Talks:

1. **Cryptography for blockchains**
   Dan Boneh
2. **Cryptanalysis techniques in cryptography based on algebraic codes**
   Alain Couvreur
3. **Computing symbols in arithmetic**
   Hendrik Lenstra
4. **The computational supersingular isogeny problem**
   Alfred Menezes
5. **An elliptic finite field representation (d'après Guido Lido)**
   René Schoof

Antoine Joux: Nutmic 2019 Co-Chair, Fondation SU, IMJ, France
Jacek Pomykała: Nutmic 2019 Co-Chair, University of Warsaw, Poland

Curves 1 - Chair : Faruk Gologlu

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

Hash Functions - Chair: Janusz Szmidt

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

Constructions - Chair: Louis Goubin

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

Curves 2 - Chair: Tanja Lange

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

Integers - Chair: Piotr Sapiecha

1. **Integer factoring and compositeness witnesses2**
   Jacek Pomykała and Maciej Radziejewski
2. **A variant of the large sieve inequality with explicit constants**
   Maciej Grzeskowiak

Applications - Chair: Jacek Pomykała

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

Cryptanalysis - Chair: Aline Gouget

1. **Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem**
   Jean-Sebastien Coron and Agnese Gini
2. **Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem**
   Jung Hee Cheon, Wonhee Cho, Minki Hhan, Minsik Kang, Jiseung Kim and Changmin Lee

3. **On ideal lattices in multicubic fields**
   Andrea Lesavourey, Thomas Plantard and Willy Susilo

Program Committee

- Divesh Aggarwal, NUS, Singapore
- Xavier Boyen, Queensland University of Technology, Australia
- Chris Charnes, Institut für Angewandte Physik - Theorie, TU Darmstadt, Germany
- Nicolas Courtois, University College London, United Kingdom
- Ronald Cramer, CWI, Netherlands
- Andrzej Dąbrowski, University of Szczecin, Poland
- Gerhard Frey, University of Duisburg-Essen, Germany
- Faruk Gologlu, Charles University Prague, Czech Republic
- Louis Goubin, University of Versailles, France
- Aline Gouget, Gemalto, France
- Antoine Joux (co-chair), Fondation SU, IMJ, France
- Arjen Lenstra, EPFL, Switzerland
- Jerzy Kaczorowski, Adam Mickiewicz University, Poland
- Mieczysław Kula, University of Silesia, Poland
- Alexander May, Ruhr-Universität Bochum, Germany
- Ariane Mézard, Institut de Mathématiques de Jussieu, France
- Giacomo Micheli, Oxford University, UK
- Andrew Odlyzko, University of Minnesota, USA
- Alina Ostafe, University of New South Wales, Australia
- Andrzej Paszkiewicz, Military University of Technology Warsaw, Poland
- Jerzy Pejaś, West Pomeranian University of Technology, Poland
- Rene Peralta, NIST, USA
- Josef Pieprzyk, Data61, CSIRO, Sydney, Australia and Institute of Computer Science, PAN, Warsaw, Poland
- Jacek Pomykała (co-chair), University of Warsaw, Poland
- Olivier Ramaré, Aix Marseille Université , France
- Piotr Sapiecha, Warsaw University of Technology, Poland
- Igor Shparlinski, University of New South Wales, Australia
- Mariusz Skałba, University of Warsaw, Poland
- Janusz Szmidt, Military Communication Institute, Zegrze, Poland
- Frederik Vercauteren, KU Leuven, ESAT/COSIC, Belgium
- Vanessa Vitse, Université Grenoble Alpes, France
- Christine van Vredendaal, Eindhoven, Netherlands
- Huaxiong Wang, NTU, Singapore
- Chaoping Xing, NTU, Singapore
- Bartosz Źrałek, University of Warsaw, Poland