Jung Hee Cheon, Kristin Lauter, and Donggeon Yhee

Preface to the First Annual MathCrypt Proceedings Volume

<https://doi.org/10.1515/jmc-2020-0060>

Execution date: Apr 08, 2020

In 2017, we decided to start the annual series of MathCrypt Workshops in order to encourage more mathematicians and computational number theorists to propose and work on hard problems in cryptography. This is the first volume of papers from our first annual MathCrypt conference hosted at Crypto 2018, on August 19, 2018 in Santa Barbara. We were motivated to launch this series of workshops to attract more mathematicians to work on hard problems in cryptography. There is a gap in the publishing culture between mathematics and computer science which we hope to bridge with this effort. Mathematicians primarily recognize publications in journals, whereas cryptographers almost always publish their results quickly in proceedings volumes of conferences which are the most prestigious venues for the research area. Many mathematicians are not accustomed to the model of submitting a paper by the conference deadline, presenting the work at the conference, and publishing in the proceedings volume. We wanted to provide a regular annual venue for mathematicians to contribute to the cryptographic research community at this accelerated pace, and the Journal of Mathematical Cryptology was an ideal place and a willing partner to create this opportunity.

We are at a point in time where it is increasingly important for mathematicians to be involved in cryptography research, as we set out to determine the next generation of cryptographic systems based on hard math problems which can withstand attacks from a quantum computer once it is built. In 2017, NIST launched a 5-year international competition to determine post-quantum cryptosystems (PQC). MathCrypt can play a complementary role by encouraging mathematicians to work on and publish attacks on new proposals, including both preliminary results and also even results which represent the failure of a certain approach to effectively attack a new system. This creates the culture of sharing information on approaches which have been tried and their measure of success. Currently there is such a high bar for publishing papers with new attacks. Attacking the underlying hard math problems in cryptography is an extremely challenging endeavor, and so the incentives are not aligned to encourage new researchers and young researchers to work and commit themselves to this direction. The opportunity to publish intermediate results in venues like MathCrypt should help to de-risk this endeavor and encourage more mathematician to pursue these research directions.

The MathCrypt proceedings volumes are also intended as a place to publish proposals for new cryptographic systems based on new ideas for hard math problems. The post quantum era provides both an opportunity and a challenge to mathematicians to create new systems based on new ideas. When an idea for a hard math problem is first proposed, it can be hard to evaluate the long-term potential in the span of a few weeks during a short review cycle. Thus more established venues may be reluctant to accept such papers in their highly competitive process since they could be viewed as a risk if they are found to be weak proposals within a relatively short time span. MathCrypt provides a forum and community for discussion and publication of new proposals.

Significant funding opportunities exist, for example in the US with the National Science Foundation (NSF) SaTC cybersecurity program, and proposals for new systems and mathematical cryptography research directions may be good candidates for support from federal grants. In fact, a Program Officer from NSF spoke at the first MathCrypt workshop in August and encouraged participants to apply to the NSF SaTC program for potential support for their research.

Kristin Lauter: Microsoft Research, United States of America; Email: klauter@microsoft.com

Jung Hee Cheon, Donggeon Yhee: Seoul National University, Korea

The founders of MathCrypt, Jung Hee Cheon and Kristin Lauter, acted as Program Chairs, and were joined by Jintai Ding to form the Organizing Committee. We are excited at the success of the first edition of the conference, which had 30 submitted papers and more than 70 registered participants. The one-day workshop included 16 talks and a poster session, representing 11 accepted papers and 5 extended abstracts. The program and full list of accepted papers are below. Often the small room was packed to overflowing with an audience of more than 100 researchers, at times sitting on the floor. The program committee worked hard to evaluate the 30 submissions and did an outstanding job of selecting many papers worthy of presentation or publication. The program committee also provided guidance after the workshop on small updates to be made for next year's conference. The Program Chairs are particularly grateful to Donggeon Yhee for his editorial help in handling the papers and producing this volume. We hope MathCrypt will continue to be a successful conference and a prestigious venue for presentation of important mathematical results in cryptography which are published together in volumes of the Journal of Mathematical Cryptology.

On behalf of the Editors,

Jung Hee Cheon (Seoul National University)

Kristin Lauter (Microsoft Research)

Donggeon Yhee (Seoul National University)

Accepted Papers

1. **Self-dual DeepBKZ for finding short lattice vectors** Masaya Yasuda (Kyushu University)
2. **Designing Efficient Dyadic Operations for Cryptographic Applications** Gustavo Banegas (Technische Universiteit Eindhoven); Paulo S. L. M. Barreto (UW Tacoma); Edoardo Persichetti (Florida Atlantic University); Paolo Santini (Universita' Politecnica delle Marche)
3. **Characterizing overstretched NTRU attacks** Gabrielle De Micheli; Nadia Heninger; Barak Shani (University of Pennsylvania)
4. **Multiparty Non-Interactive Key Exchange and More from Isogenies on Elliptic Curves** Dan Boneh (Stanford University); Darren Glass (Gettysburg College); Daniel Krashen (University of Georgia Athens); Kristin Lauter (Microsoft Research); Shahed Sharif (California State University San Marcos); Alice Silverberg (University of California Irvine); Mehdi Tibouchi (NTT Corporation); Mark Zhandry (Princeton University)
5. **Recovering Secrets From Prefix-Dependent Leakage** Houda Ferradi (NTT Corporation); Rémi Géraud (École normale supérieure); Sylvain Guilley (Telecom ParisTech); David Naccache (École normale supérieure); Mehdi Tibouchi (NTT Corporation)
6. **New Techniques for SIDH-based NIKE** David Urbanik; David Jao (University of Waterloo)
7. **Quasi-subfield polynomials and the Elliptic Curve Discrete Logarithm Problem** Ming-Deh A. Huang (University of Southern California); Michiel Kisters (University of California, Irvine); Christophe Petit (University of Birmingham); Sze Ling Yeo (Institute for Infocomm Research (I2R) and Nanyang Technical University); Yang Yun
8. **A signature scheme from the finite fields isomorphism problem** Jeffrey Hoffstein (Brown University); Joseph H. Silverman (Brown University); William Whyte (OnBoard Security); Zhenfei Zhang (OnBoard Security)
9. **Efficiently processing complex-valued data in homomorphic encryption** Carl Bootland (KU Leuven); Wouter Castryck (KU Leuven and UGent); Ilia Iliashenko (KU Leuven); Frederik Vercauteren (KU Leuven)
10. **A polynomial quantum space attack on CRS and CSIDH** David Jao; Jason LeGrow; Christopher Leonardi; Luiz Ruiz-Lopez (University of Waterloo)
11. **Flattening NTRU for evaluation key free homomorphic encryption** Yarkın Doröz (New Jersey Institute of Technology)

Program

New Mathematical Objects

Chair: Jung Hee Cheon

A signature scheme from the finite fields isomorphism problem

Zhenfei Zhang

Designing Efficient Dyadic Operations for Cryptographic Applications

Gustavo Banegas

An improvement to the quaternion analogue of the L-isogeny path problem

Spike Smith

Recursive MDS Matrices Over Quotient Rings

Abhishek Kesarwani, Sumit Kumar Pandey, Santanu Sarkar

Elliptic Curves and Isogeny-based Cryptography

Chair: Kristin Lauter

Multiparty Non-Interactive Key Exchange and More from Isogenies on Elliptic Curves

Dan Boneh

New Techniques for SIDH-based NIKE

David Urbanik

A polynomial quantum space attack on CRS and CSIDH

Jason LeGrow

Quasi-subfield polynomials and the Elliptic Curve Discrete Logarithm Problem

Michiel Kusters

LWE and Ring-LWE

Chair: Dan Boneh

Self-dual DeepBKZ for finding short lattice vectors

Masaya Yasuda

Characterizing overstretched NTRU attacks

Gabrielle De Micheli

On the Hardness of Decisional Ring-LWE with Bounded Number of Samples

Barak Shani

FHE and DL

Chair: Jintai Ding

Flattening NTRU for evaluation key free homomorphic encryption

Yarkin Doröz

Efficiently processing complex-valued data in homomorphic encryption

Ilya Iliashenko

Efficient Fully Homomorphic Encryption Scheme

Shuhong Gao

Recovering Secrets From Prefix-Dependent Leakage

Rémi Géraud

Program Committee

- Martin Albrecht
- Lily Chen
- Chen-Mou Cheng
- Jung Hee Cheon (Co-Chair)
- Jintai Ding
- Pierre-Alain Fouque
- David Hyeon
- Sorina Ionica
- Antoine Joux
- Kristin Lauter (Co-Chair)
- Hyangsook Lee
- Arjen Lenstra
- Dongdai Lin
- Alexander May
- Alfred Menezes
- Michele Mosca
- Christophe Petit
- Joachim Rosenthal
- San Ling
- Igor Shparlinski
- Joseph Silverman
- Fang Song
- Katherine Stange
- Damien Stehle
- Ron Steinfeld
- Rainer Steinwandt
- Tsuyoshi Takagi
- Mehdi Tibouchi
- Vinod Vaikuntanathan
- Aaram Yun