Cryptography and Communications (2019) 11: 363–365
https://doi.org/10.1007/s12095-019-00356-8

EDITORIAL

Editorial: Special Issue on Mathematical Methods for Cryptography

Lilya Budaghyan[1] · Chunlei Li[1] · Matthew G. Parker[1]

Published online: 19 February 2019

Information processing by electronic devices leads to a multitude of security relevant challenges many of which can be solved with the help of cryptography. Modern cryptography is based on and uses mathematical methods some of which have been specifically developed for cryptographic applications while many of them are taken from the classical mathematical canon. The present special issue is dedicated to mathematical methods for cryptography.

In September 2017, we invited leading specialists from twelve different countries all over the world to Svolvar, Lofoten, Norway, for an event[1] celebrating the 70th birthday of Prof. Tor Helleseth from the University of Bergen, a well-known Norwegian scientist who has made a considerable contribution to the fields of coding theory, sequence design, Boolean functions, finite fields and mathematical cryptography. Contributed talks were also presented at the workshop. All speakers have been invited to submit a paper (on the subject of their talk or on another subject connected to mathematical methods for cryptography). All received submissions were thoroughly reviewed and eleven papers, described below, have been accepted after revision.

Linear cryptanalysis is a well-known statistical method that makes use of nonrandom behavior of linear approximations to distinguish a block cipher from a random family of permutations. Due to its effectiveness, different variants and extensions of linear cryptanalysis

[1]Information on MMC 2017 workshop can be found on the webpage https://people.uib.no/chunlei.li/workshops/MMC

This special issue is dedicated to the 70th Birthday of Tor Helleseth

This article is part of the Topical Collection on *Special Issue: Mathematical Methods for Cryptography*

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Chunlei Li
Chunlei.Li@uib.no

Matthew G. Parker
Matthew.Parker@uib.no

[1] Department of Informatics, University of Bergen, PO Box 7803, 5020 Bergen, Norway

have appeared in the literature. In the paper "Affine Linear Cryptanalysis", Kaisa Nyberg proposes a new variant of linear cryptanalysis, where she adopts a new chi square distinguisher using correlations of linear approximations that form an affine subspace in the linear space of all linear approximations and demonstrates a clear advantage of the new method over the known multi-dimensional linear cryptanalysis methods.

In their paper "Decomposition of Permutations in a Finite Field" Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen describe a method to decompose a permutation of finite fields into a sequence of quadratic or cubic permutations with the aim of efficient implementation of complex S-boxes in hardware. They, together with Kerem Varici in "Constructions of S-boxes with uniform sharing", consider the construction of S-boxes with desired threshold implementation sharings from smaller ones and also investigate the self-equivalency of constructed S-boxes.

The efficiency of a secret sharing scheme is traditionally measured by its complexity. In "Secret sharing on large girth graphs" László and Péter Ligeti investigate graph-based secret sharing schemes and present an explicit family of d-regular graphs with largest possible complexity and arbitrarily large girth.

The Learning with Errors (LWE) problem and its more efficient ring-based variants Ring-LWE have turned out to be an amazingly versatile basis for cryptographic constructions, particularly for post-quantum cryptography. Error distribution plays a central role in the security of LWE-based encryption constructions. In their paper "Error Analysis of Weak Poly-LWE Instances", Yao Chen, Benjamin M. Case, Shuhong Gao, and Guang Gong present a general algebraic method to derive the mapped error distribution with a formula and show that their method can apply to a broader range of parameters as well as non-Gaussian error distributions, which can identify a broader class of weak cases of LWE instances.

Patrick Felke in "On the Security of Biquadratic C* Public-Key Cryptosystems and its Generalizations", investigates the complexity in attacking multivariate-based cryptosystems and shows that security requirements on biquadratic C^* and its generalizations lead to impractical key sizes for applications.

The paper "Factorization Using Binary Decision Diagrams" by Håvard Raddum and Srimathi Varadharajan presents a different approach to the integer factorization problem by applying operations on binary decision diagrams. The complexity of the proposed approach is also analyzed.

Exponential sums are a celebrated tool on analytical number theory, combinatorics, sequence design, coding theory, and cryptography. Kloosterman sums are a particular type of exponential sum with rather interesting intrinsic properties. Victor A. Zinoviev in "On classical Kloosterman sums" surveys the known results on classical Kloosterman sums during the last decades, including the distinctness, divisibility properties, moments and zeros of such sums and their connections with cryptographic functions, elliptic and modular curves and error-correcting codes.

In the paper "Computing the Number of Finite Field Elements with Prescribed Absolute Trace and Co-trace", Assen I. Bojilov, Lyubomir Y. Borissov and Yuri L. Borissov investigate the problem of determining the number of finite field elements with prescribed absolute trace and co-trace by converting them to certain circulant matrix formed by Kloosterman sums.

Over the years Niho exponents have appeared to be an important source in constructing optimal and good objects in different areas. The paper "A survey on the applications of Niho exponents" by Nian Li and Xiangyong Zeng surveys recent progress on the applications

of Niho exponents in sequence design, cryptography and coding theory and proposes some open problems in this direction.

The errors in flash memories can be modeled as a type of unbalanced error. Torleiv Kløve in "Codes of length two correcting single errors of limited size" considers single-error-correcting linear codes of length two over integers modulo $\mathbb{Z}_q$ and shows the existence of this kind of code for sufficiently large integer q.

We thank all the authors of these papers for their nice contributions, and also the large number of reviewers whose careful reading of the papers have ensured the high standard of this special issue.