Cryptogr. Commun. (2018) 10:1–3
https://doi.org/10.1007/s12095-017-0269-y

# Editorial: Special issue on recent trends in cryptography

**Tor Helleseth[1] · Bart Preneel[2]**

Published online: 25 November 2017


As our society becomes ever more dependent on digital technologies, cryptography becomes increasingly important to secure data while it is being stored, transferred and processed. In the field of cryptography there is a strong crossfertilization between new applications and innovative research results. The 13 contributions in this special issue of "Recent Trends on Cryptography" encompass a wide range of recent research; we believe that this collection offers an interesting snapshot of research that is appealing to experts in the field but also to a broader audience. Collectively these papers illustrate the diverse range of issues that are presently being investigated in the field of cryptography.

The paper by Michael Scott "Missing a trick: Karatsuba variations" takes the reader for a tour through different versions of Karatsuba multiplication. This is of considerable interest for efficient implementations of public-key cryptography and in particular for Elliptic Curve Cryptography. The author discusses an interesting variant called "arbitrary-degree" Karatsuba (ADK).

In the paper "Backtracking-assisted multiplication", Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache and Hang Zhou describe a new multiplication algorithm, particularly suited to lightweight microprocessors. This leads to improvements when one of the operands is known in advance.

Homomorphic encryption is an important research topic since it allows to compute on sensitive data whilst it stays encrypted. A challenging problem is the security of

This article is part of the Topical Collection on *Recent Trends in Cryptography*
Guest Editors: Tor Helleseth and Bart Preneel

✉ Tor Helleseth
Tor.Helleseth@uib.no

Bart Preneel
Bart.Preneel@esat.kuleuven.be

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

[2] imec-COSIC KU Leuven, Department of Electrical Engineering - ESAT, Kasteelpark Arenberg 10 Bus 2452, 3001 Leuven, Belgium

these schemes. In their paper "Cryptanalysis of a homomorphic encryption scheme", Sonia Bogos, John Gaspoz and Serge Vaudenay present three attacks on a homomorphic encryption scheme earlier proposed by Zhou and Wornell.

The paper "Security of BLS and BGLS signatures in a multi-user setting" by Marie-Sarah Lacharité provides a security analysis of several signature schemes in the multi-user setting: this corresponds to a realistic scenario in which multiple users are employing the scheme. The schemes analyzed are Boneh-Lynn-Shacham (BLS) signatures and variants and a variant of the aggregate signature scheme by Gentry-Boneh-Shacham (BGLS).

In their paper on "Generic attacks with standard deviation analysis on A-Feistel schemes", Valérie Nachef, Jacques Patarin and Emmanuel Volte consider attacks on schemes based on classical Feistel schemes using one or two affine permutations. The results indicate that A-Feistel schemes are more secure than normal Feistel schemes.

Brett Hemenway and Rafail Ostrovsky propose in "Efficient robust secret sharing from expander graphs" a novel secret sharing construction based on expander graphs; this scheme permits new trade-off between efficiency and share size resulting in smaller share sizes. The construction identifies users as nodes in the expander graph, where each player only checks the neighbours in the expander graph.

The paper by Éloi de Chérisey, Sylvain Guilley, Annelie Heuser and Olivier Rioul entitled "On the optimality and practicability of mutual information analysis in some scenarios" studies mutual information analysis (MIA) as a side-channel distinguisher and analyzes its effectiveness in a setting where the exact probabilities are replaced by online estimations of the probability distribution.

The paper by Gregory G. Rose "KISS: A bit too simple" illustrates how an efficient random number generator (KISS) can be cryptographically insecure if it is used for a different purpose than originally intended, for example as a stream cipher.

In the paper "Searchable symmetric encryption over multiple servers", Geong Sen Poh, Moesfa Soeheila Mohamad and Ji-Jian Chin consider the problem of searching over encrypted data that has been distributed over many servers. Their main aim is to maintain privacy of a subset of the data even if the decryption key for one server is leaked.

The paper "On generating invertible circulant binary matrices with a prescribed number of ones" by Tomáš Fabšič, Otokar Grošek, Karol Nemoga and Pavol Zajac first studies how to generate invertible binary matrices with a prescribed number of ones in a direct and efficient way. Thereafter, it considers applications of the algorithms to generate matrix blocks in the QC-LDPC McEliece cryptosystem.

In the paper by Christian Forler, Eik List, Stefan Lucks and Jakob Wenzel "POEx: A beyond-birthday-bound-secure on-line cipher" an on-line cipher called POEx is proposed that allows for single pass encryption. The design is based upon an XTX tweakable $n$-bit block cipher construction and it is shown to have beyond birthday security, that is, the security bound does not become void when $2^{n/2}$ inputs are processed.

In the area of block cipher cryptanalysis, Tingting Cui, Huaifeng Chen, Long Wen and Meiqin Wang present statistical integral distinguishers on two block ciphers. Their paper, entitled "Statistical Integral Attacks on CAST-256 and IDEA", describes a 29-round key recovery attack of CAST-256 and a 4.5-round attack on IDEA.

It has been proposed that a blockchain can be used as a source of randomness. The paper by Cécile Pierrot and Benjamin Wesolowski "Malleability of the blockchain's entropy", investigates the extent the entropy of a blockchain can be manipulated by an adversary with limited computing power and a limited budget.

This special issue was preceded by an international workshop in cryptography, Arctic Crypt 2016, held in Longyearbyen, Svalbard, Norway at 78° north. After the workshop all

participants with an accepted paper (20 out of 40) were invited to submit their paper to this special issue of the Journal "Cryptography and Communications". The 16 submissions that were received were again thoroughly reviewed using the high reviewing standard of the journal and the 13 papers in this volume are the results of this selection process. We would like to thank all authors for their excellent submissions and all reviewers whose careful reading and constructive comments have ensured that this special issue is of a high scientific standard.

Tor Helleseth and Bart Preneel