Cryptography and Communications
https://doi.org/10.1007/s12095-021-00502-1

Special issue from mathematics to embedded devices

Yves Aubry[1,2] · Pierre Barthélémy[2] · Nadia El Mrabet[3]

Accepted: 3 June 2021Published online: 05 August 2021

Mathematics Subject Classification (2010) 94A60 · 94A15 · 11G20 · 14G50 · 11R58 · 11Y16 · 68P15 · 68P25 · 94C10 · 94C12

Cryptography embraces many facets starting from deep pure Mathematics to the implementation of low-level primitives. The aim of the international conference YACCRYPTED (Yet Another Conference on CRYPTography and Embedded Devices) in May 2020 was to bring together actors of these different fields, namely mathematicians from academic research institutes and researchers in companies.

The present Special Issue contains original research articles reflecting these different points of view. All the papers sent were thoroughly reviewed and seven papers, described below, have been accepted after revision.

In cryptography, a hash function is a mathematical process that converts a data of arbitrary length into another encrypted one of fixed length. In "Hashing to elliptic curves of j-invariant 1728", Dimitrii Koshelev generalizes the simplified Shallue–van de Woestijne–Ulas (SWU) method of a deterministic finite field mapping $h : \mathbb{F}_q \to E_a(\mathbb{F}_q)$ to the case of any elliptic $\mathbb{F}_q$-curve $E_a : y^2 = x^3 - ax$ of j-invariant 1728. In comparison with the (classical) SWU method, the simplified SWU method allows to avoid one quadratic residuosity test in the field $\mathbb{F}_q$, which is a quite painful operation in cryptography with regard to timing attacks.

Efficient multiplication on finite fields is important to produce efficient implementation of a cryptographic protocol based on a finite field arithmetic. In "Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields", Stéphane

✉ Yves Aubry
yves.aubry@univ-tln.fr

Pierre Barthélémy
p.barthelemy@univ-amu.fr

Nadia El Mrabet
nadia.el-mrabet@emse.fr

1 Institut de Mathématiques de Toulon, Toulon, France

2 Institut de Mathématiques de Marseille, Marseille, France

3 Mines de Saint-Étienne, Saint-Étienne, France

Ballet, Alexis Bonnecaze and Thanh-Hung Dang propose several constructions for the original multiplication algorithm of D.V. and G.V. Chudnovsky in order to improve its scalar complexity. They highlight the set of generic strategies who underlay the optimization of the scalar complexity, according to parameterizable criteria. As an example, they apply this analysis to the construction of type elliptic Chudnovsky-Chudnovsky multiplication algorithms for small extensions.

The protection of data and files in the dematerialised structure should be provided by a cryptographic protocol. In "On the privacy of a code-based single-server computational PIR scheme", Sarah Bordage and Julien Lavauzelle show that the single-server computational PIR protocol proposed by Holzbaur, Hollanti and Wachter-Zeh in 2020 is not private, in the sense that the server can recover in polynomial time the index of the desired file with very high probability. The attack relies on the following observation. Removing rows of the query matrix corresponding to the desired file yields a large decrease of the dimension over $\mathbb{F}_q$ of the vector space spanned by the rows of this punctured matrix. Such a dimension loss only shows up with negligible probability when rows unrelated to the requested file are deleted.

Side-channel attacks are powerfull attacks that use the information leakage of a cryptographic protocol during its execution. Several countermeasures exist and masking is one of them. In "Categorizing All Linear Codes of IPM over $\mathbb{F}_{2^8}$", Wei Cheng, Sylvain Guilley and Jean-Luc Danger present an Inner Product Masking resisting to side channel attacks. Inner Product Masking (IPM) is a generalization of several masking schemes including Boolean one to protect cryptographic implementation against side-channel analysis. The core competitiveness of IPM is that it provides higher side-channel resistance than Boolean masking with the same number of shares. In this paper, they follow the coding theoretic approach and categorize all linear codes of IPM with two shares over the finite field $\mathbb{F}_{2^8}$ in terms of side-channel resistance.

Considering the resistance to side channel attacks, in "Monomial Evaluation of Polynomial Functions Protected by Threshold Implementations – With an Illustration on AES", Simon Landry, Yanis Linge, and Emmanuel Prouff combine two previous methods to propose a more efficient threshold implementation (TI). On several aspects, TI may be seen as an extension of another classical side-channel countermeasure, called masking, which is essentially based on the sharing of any internal state of the processing into independent parts (also called shares). When specifying such a scheme to secure a cryptographic implementation, as e.g. the AES block cipher, the challenging part is to minimise both the number of steps (or cycles) and the consumption of randomness. Here, the authors propose a new TI which does not consume fresh randomness and which is efficient (in terms of cycles) for classical block ciphers. As an illustration, they develop their proposal for the AES.

Machine learning and deep learning algorithms are increasingly considered as potential candidates to perform black box side-channel security evaluations. Inspired by the literature on machine learning security, in "How to Fool a Black Box Machine Learning Based Side-Channel Security Evaluation", Charles-Henry Bertrand Van Ouytsel, Olivier Bronchain, Gaëtan Cassiers and François-Xavier Standaert highlight that it is easy to conceive implementations for which such black box security evaluations will incorrectly conclude that recovering the key is difficult, while an informed evaluator / adversary will reach the opposite conclusion.

Integrated Circuits (ICs) are sensible to a wide range of (passive, active, invasive, non-invasive) physical attacks. In this context, Hardware Trojans (HTs), that are malicious modifications of a circuit by an untrusted manufacturer, are one of the most challenging

threats to mitigate. In “A Stealthy Hardware Trojan based on a Statistical Fault Attack”, Charles Momin, Olivier Bronchain and François-Xavier Standaert propose a stealthy HT instance leading to successful and hidden Statistical Fault Attacks (SFA). More precisely, the faults are injected when the chip in running under condition for which metastabilty occurs (i.e. with an increased clock frequency), leading to the apparition of faults at random positions within the target implementation.

Through the diversity of the topics covered, the theoretical and practical approaches of these papers are being deployed to address a number of matters raised today by Cryptography. We hope that this Special Issue will foster interest from both the mathematical and cryptographic communities.