Guest Editors' Introduction to the Special Issue on Cryptographic Engineering in a Post-Quantum World: State of the Art Advances

Zhe Liu, *Senior Member, IEEE*, Patrick Longa, and Çetin Kaya Koç, *Fellow, IEEE*

THE vast majority of public-key cryptosystems currently in use is based on integer factorization and (elliptic curve) discrete logarithm problems, which are believed to be intractable with current computing technology. However, these hard problems can be solved in polynomial time by using Shor's algorithm (or one of its variants) on a quantum computer. Recent progress towards the development of a large-scale, fault-tolerant quantum computer has motivated the interest for post-quantum cryptography (a.k.a. quantum-safe or quantum-resistant cryptography) by governments, enterprises and the cryptography community. In April 2015, the National Institute of Standards and Technology (NIST) held a "Workshop on Cybersecurity in a Post-Quantum World" to discuss cryptographic algorithms for public-key based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. Four months later, the National Security Agency (NSA) published a report ("Cryptography Today") that announced a plan to transition to quantum-resistant algorithms in the near future. In this direction, NIST recently launched the so-called "Post-Quantum Cryptography Standardization" process, a multi-year effort aimed at selecting the next-generation of quantum-resistant public-key cryptographic algorithms for standardization. In particular, the call for proposals –due on November 30, 2017– requested candidate algorithms for key encapsulation mechanisms (KEM), public-key encryption and digital signatures. In total, NIST received 69 submissions. This record number of submissions (considering any of the open cryptographic competitions organized by NIST) closely reflects the remarkable interest in this area of cryptography.

This special issue aims at presenting state-of-the-art research in cryptographic engineering aspects of cryptographic systems that are currently believed to be secure against quantum computer cryptanalysis. This includes the performance and security evaluation of cryptographic systems in hardware and software platforms. The concrete goal of this special issue is to highlight new results in the design and analysis of cryptographic hardware and software implementations of post-quantum cryptography (PQC).

In the call for papers of this special issue we encouraged submissions about any of the competing families of PQC algorithms, such as code-based, hash-based, isogeny-based, lattice-based and multivariate cryptosystems, and covering all relevant aspects to cryptographic engineering, which include:

- Side-channel attacks and countermeasures for PQC.
- Hardware and software implementations of PQC.
- Hardware architectures of PQC systems.
- Cryptanalysis and cryptanalytic engines.
- Applications of PQC.

In response to this call for papers, we received 12 submissions, each of which was evaluated by at least three reviewers. Eventually 10 manuscripts have been selected to form this special issue of *IEEE Transactions on Computers*.

The (in alphabetic order of the authors) first paper, by Thomas Espitau, Pierre-Alain Fouque, Benoit Gérard, and Mehdi Tibouchi, reports on "Loop-Abort Faults on Lattice-Based Signatures and Key Exchange Protocols". The authors look in particular at fault attacks against implementations of lattice-based signatures and key exchange protocols. For signature schemes, the authors studied both in Fiat-Shamir type construction (particularly BLISS, but also GLP, PASS-Sign, and Ring-TESLA) and in hash-and-sign schemes (particularly the GPV-based scheme of Ducas-Prest-Lyubashevsky). For key exchange protocols, the authors studied the implementations of NewHope, Frodo, and Kyber. The authors present several fault attacks against those schemes that recover the entire key recovery with only a few faulty executions, show that those attacks can be mounted in practice based on concrete experiments in hardware, and discuss possible countermeasures against them.

Vincent Migliore, Guillaume Bonnoron, and Caroline Fontaine, "Practical Parameters for Somewhat Homomorphic Encryption (SHE) Schemes on Binary Circuits". The authors studied two famous Homomorphic encryption FV and SHIELD and provided a deep analysis of how to setup and size their parameters, to ensure both correctness and security. This paper aims to provide easy-to-use guidelines for implementation purposes. The authors gave a review of

- *Z. Liu is with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China. E-mail: zhe.liu@nuaa.edu.cn.*
- *P. Longa is with MSR Security and Cryptography group, Microsoft Research, WA 98052. E-mail: plonga@microsoft.com.*
- *Ç.K. Koç is with İstinye University, Istanbul 34010, Turkey, and with Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China, and also with the University of California Santa Barbara, Santa Barbara, CA 93106. E-mail: cetinkoc@ucsb.edu.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TC.2018.2869611

parameters extraction for FV and SHIELD with several explorations to evaluate parameters for various applications.

Angshuman Karmakar, Sujoy Sinha Roy, Oscar Reparaz, Frederik Vercauteren, and Ingrid Verbauwhede, "Constant-Time Discrete Gaussian Sampling". The authors propose a constant-time implementation of the Knuth-Yao random walk algorithm for performing constant-time discrete Gaussian sampling. The authors express the generated sample as a function of the input random bits as the random walk is dictated by a set of input random bits. The implementation expresses the unique mapping of the input random-bits to the output sample-bits as a Boolean expression of the random-bits. We use bit-slicing to generate multiple samples in batches and thus increase the throughput of the constant-time sampling manifold. Experiments on an Intel i7-Broadwell processor show that the proposed method can be as much as 2.4 times faster than the constant-time implementation of cumulative distribution table based sampling and consumes exponentially less memory than the Knuth-Yao algorithm with shuffling for a similar level of security.

Wei Dai, William Whyte, and Zhenfei Zhang, "Optimizing Polynomial Convolution for NTRUEncrypt". The authors study all know attacks against the NTRUEncrypt parameter set and show that it delivers 256 bits of security against classical attacker and 128 bits of security against quantum attacks. Further, the authors present a parameter-dependent optimization using a tailored hierarchy of multiplication algorithms as well as the Intel AVX2 instructions, and show that this optimization is constant-time. Implementation shows that the proposed method is two to three times faster than the reference implementation of NTRUEncrypt.

Xinwei Gao, Jintai Ding, Lin Li, and Jiqiang Liu, "Practical Randomized RLWE-Based Key Exchange Against Signal Leakage Attack". The authors propose a new randomized RLWE-based keyexchange protocol. The proposed lightweight approach incorporates an additional ephemeral public error term into key exchange materials to resist the attack. With the same attack, the proposed protol shows that the signal value of the protocol is indistinguishable from uniform random, therefore, the attack no longer works. Further, the authors explain how the attack fails, present 200-bit classic and 80-bit quantum secure parameter choice, efficient implementations, comparisons and discussion. Benchmark shows the proposed protocol truly efficient and even faster than related vulnerable protocols.

Brian Koziel, Reza Azarderakhsh, and Mehran Mozaffari-Kermani, "A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography". The authors present a high-performance and scalable architecture for isogeny-based cryptosystems. In particular, they use the architecture in a fast, constant-time FPGA implementation of the quantum-resistant supersingular isogeny Diffie-Hellman (SIDH) key exchange protocol. The authors implementing at 83, 124, 168, and 252-bit quantum security levels, and shows that the architecture is scalable. Further, the implementation completes the SIDH protocol 2 times faster than performance-optimized software implementations and 1.34 times faster than the previous best FPGA implementation, both running a similar set of formulas.

Thomas Ricosset and Carlos Aguilar-Melchor, "CDT-Based Gaussian Sampling: From Multi to Double Precision". The authors first study the exist tight bound and show that it can be used to bound the precision requirement in Gaussian sampling to the IEEE 754 floating-point standard double precision for usual lattice-based signature parameters by using a modified cumulative distribution table (CDT), which reduces the memory needed by CDT-based algorithms and makes the constant-time implementation faster and simpler. Futher, the authors apply this approach to a variable-center variant of the CDT algorithm which occasionally requires the online computation of the cumulative distribution function.

Armando Faz-Hernández, Julio López, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez, "A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol". The authors present several algorithmic optimizations targeting both elliptic-curve and field arithmetic operations aiming to accelerate the SIDH runtime performance. The authors introduce in the context of the SIDH protocol a more efficient approach for calculating the elliptic curve operation $P + [k]Q$. Our strategy achieves a factor 1.4 speedup compared with the popular variable-three-point ladder algorithm regularly used in the SIDH shared secret phase. Moreover, profiting from precomputation techniques the proposed algorithm yields a factor 1.7 acceleration for the computation of this operation in the SIDH key generation phase. Furhter, the authors present an optimized evaluation of the point tripling formula, and discuss several algorithmic and implementation techniques that lead to faster field arithmetic computations.

Sujoy Sinha Roy, Kimmo Jarvinen, Jo Vliegen, Frederik Vercauteren, and Ingrid Verbauwhede, "HEPCloud: An FPGA-Based Multicore Processor for FV Somewhat Homomorphic Function Evaluation". The authors present an FPGA based hardware accelerator, named HEPCloud, for homomorphic evaluations of medium depth functions which has applications in cloud computing. The proposed HEPCloud architecture supports the polynomial ring based homomorphic encryption scheme FV for a ring-LWE parameter set of dimension 215, modulus size 1,228-bit, and a standard deviation 50. The processor of HEPCloud is composed of multiple parallel cores. To achieve fast computation time for such a large parameter-set, various optimizations in both algorithm and architecture levels are performed. First, the authors optimize the BRAM access, use a fast Barrett like polynomial reduction method, optimize the cost of CRT, and design a fast divide-and-round unit. Further, they implement HEPCloud on a medium-size Xilinx 14 Virtex 6 FPGA board ML605 board and measure its on-board performance.

Silvan Streit and Fabrizio De Santis, "Post-Quantum Key Exchange on ARMv8-A: A New Hope for NEON Made Simple". The authors present constant-time and vector-optimized implementations of NEWHOPE and NEWHOPE-SIMPLE for ARMv8-A 64-bit processors which target high-speed 8 applications. The proposed architecture is implemented in a growing number of smart phone and tablet processors, and features powerful 128-bit SIMD operations provided by the NEON engine. Further, the authors propose the use of three alternative modular reduction methods.

We would like to express our sincere gratitude to all authors who submitted their work to this special issue. We

also would like to thank the anonymous reviewers for their invaluable help in evaluating and judging the submissions. Further on, it is our pleasure to thank the Editor-in-Chief Paolo Montuschi for his continuous help and support with all our organizational questions in connection with this special section.

Zhe Liu
Patrick Longa
Çetin Kaya Koç
Guest Editors

Zhe Liu received the PhD degree from the Laboratory of Algorithmics, Cryptology and Security (LACS), University of Luxembourg, Luxembourg. He is a professor with Nanjing University of Aeronautics and Astronautics, China. His PhD thesis has received the prestigious FNR Awards 2016 – Outstanding PhD Thesis Award for his contributions in cryptographic engineering on IoT devices. He is the recipient of ACM China SIGSAC Rising Star Award and Honorable Mentions for ACM China Rising Star Award in 2017. His research interests include computer arithmetic and cryptographic engineering. He has co-authored more than 70 research peer-reviewed journal and conference papers. He is a senior member of the IEEE.

Patrick Longa received the MSc degree in electrical engineering from the University of Ottawa, in 2007 and the PhD degree in electrical and computer engineering from the University of Waterloo, in 2011. He is a cryptography researcher and engineer with the MSR Security and Cryptography group at Microsoft Research, Redmond. During his time at Waterloo, he was a member of the Center for Applied Cryptographic Research (CACR) and the Laboratory for Side-Channel Security of Embedded Systems. He is co-designer of the elliptic curve Four$\mathbb{Q}$, the signature scheme Schnorr$\mathbb{Q}$ and the post-quantum schemes SIKE, FrodoKEM and qTESLA, and is the author of numerous high-performance cryptographic libraries including FourQlib, SIDH and LatticeCrypto. His research interests mainly involve elliptic curve and pairing-based cryptography, post-quantum cryptography, efficient algorithmic design, high-performance implementation of cryptographic primitives, and side-channel attacks and countermeasures.

Çetin Kaya Koç received the PhD degree in electrical and computer engineering from the University of California Santa Barbara, in 1988. His research interests include electronic voting, cyber-physical security, cryptographic hardware and embedded systems, elliptic curve cryptography and finite fields, and deterministic, hybrid and true random number generators. He is the co-founder of the Cryptographic Hardware and Embedded Systems Conference, and the founding editor-in-chief of the *Journal of Cryptographic Engineering*. He has also been in the editorial boards of the *IEEE Transactions on Computers* (2003-now) and the *IEEE Transactions on Mobile Computing* (2003-2007). He is the author and co-author of the about 200 articles three books in computer science and cryptography. He was elected as and IEEE fellow for his contributions to cryptographic engineering in 2007. Currently, he has appointments at İstinye University (Istanbul, Turkey), Nanjing University of Aeronautics and Astronautics (Nanjing, China), and University of California Santa Barbara. He is a fellow of the IEEE.