Special Issue AMC:

Title : Secure Implementations of Post-Quantum Cryptographic Algorithms and Mathematical Approaches

The security of digital communications is backed by cryptographic algorithms.
Recently, novel algorithms, known as "Post Quantum Cryptography" (PQC), have been promoted.
Their adoption affects basic trust foundations such as key exchange, data signature and information encryption.

PQC algorithms are based on underlying problems which are hard to solve both by quantum and classical computers.
This leads to two tracks of work: the assurance in their rationale, and the security in the way they are implemented.

Regarding the first point, it is on good tracks, as several competitions and standardization initiatives have been launched.
For instance, some hash-based signature schemes are already available as IETF RFC and it is taken for granted that some lattice-based and code-based algorithms will make it as standards.

In this special issue, we aim to tackle the second point.
Indeed, PQC algorithms must be ready to be implemented in products which shall not be attackable using side-channel information.
These weaknesses are now well understood, as there are even some certification schemes in place (Common Criteria, ISO/IEC 17825, etc.).
But the application of countermeasures to side-channel attacks on PQC algorithms is still at its infancy.
They deserve a more formal processing, based on implementation of specific algorithmic protections.

The techniques employed in cryptographic algorithms protection against side-channels is nourished by several mathematical fields.
For instance, randomization and coding are used as building blocks for side-channel resistance, and error correcting codes are leveraged for fault attack detection.

We therefore welcome contributions of side-channel attacks protection, applied to PQC.
Original works, mathematically-oriented, are welcomed, on the following topics:

- Constant-time PQC algorithms
- Masking schemes for PQC algorithms
- Error detection schemes for PQC algorithms
- Countermeasures at PQC primitive level
- Leakage resilient schemes applied to PQC algorithms
- White-box or obfuscated implementations of PQC

Timeline:
- Publicity : 16 November
- Submission of papers: 1st March 2022
- Notification : 15 June 2022
- Publication : November 2022

Guest editors:

1. Sylvain Guilley (sylvain.guilley@secure-ic.com)

Sylvain Guilley is General Manager and CTO at Secure-IC, a French company offering security for embedded systems.
Secure-IC's flagship product is the multi-certified \textsc{Securyzr} integrated Secure Element (iSE).
Sylvain is also professor at TELECOM-Paris, research associate at \'Ecole Normale Sup\'erieure (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS, Beijing).
His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal / mathematical methods.
Since 2012, he organizes the PROOFS workshop (\url{http://www.proofs-workshop.org/2020/}), which brings together researchers whose objective is to increase the trust in the security of embedded systems.
Sylvain is also lead editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of non-invasive testing tools), and ISO/IEC 24485 (White Box Cryptography).
He is leading the topic ``High Level Principles for Design \& Architecture" in the editing team of TR68 (Singapore, Standards Development Organisation), and is member of the French BNA (Bureau de Normalisation de l'Automobile).
Sylvain is associate editor of the Springer Journal of Cryptography Engineering (JCEN).
He has co-authored 250+ research papers and filed 40+ invention patents.
He is member of the IACR, the IEEE and senior member of the CryptArchi club.
He is an alumnus from \'Ecole Polytechnique and TELECOM-Paris.

2. Youssef Souissi (youssef.souissi@secure-ic.com)

Youssef Souissi is a Business Line Director at Secure-IC, a French company offering security for embedded systems.
After getting his engineering diploma in computer science and micro-electronics in Tunisia, he obtained a master of engineering degree in embedded systems architecture and security from Ecole Nationale Supérieure des Mines de Saint-Etienne, followed by a PhD thesis from Télécom Paristech in France. His thesis research mainly focused on the ways of evaluating cryptographic embedded systems through side-channel and fault injection analyses.
He has had several roles in Secure-IC as the head of the Threat Analysis bu-

siness line in charge of the Hardware and Software security evaluation for embedded systems. Currently, he is leading Think Ahead business line for security research and innovation.
His research interests regard all the scope of cyber security ranging from specification and code level to system and end-user device security levels. This includes for instance pre-silicon vulnerability detection, silicon countermeasures, hardware Trojans, CPU cyber protection, AI for security and Post-quantum cryptography.