Introduction for Embedded Platforms for Cryptography in the Coming Decade

We are excited to roll out this special issue on Embedded Platforms for Cryptography in the Coming Decade. We believe cryptography is on the brink of becoming an essential, central element in embedded systems, and here is why.

The Internet has enabled a society where information access is instantaneous, ubiquitous, and complete. This has especially affected the embedded systems, integrated around us in everything we touch and use. We keep our roads safe, our factories running, and our homes warm and powered thanks to embedded systems. Their global connectivity is unavoidable because of the complexity of the problems they address—think, for example, about traffic and airspace control or smart grid. However, that connectivity brings enormous security and privacy risks. Of course, there are policies and regulations, but those are for the people that abide by them. In a globally connected world, policy will need the support of a technological basis.

Cryptography is that technological basis. It is the workhorse to connect embedded systems in a secure manner to the global Internet society. Cryptography has truly changed the world in the past 40 years, and it will continue to do so. Public-key cryptography has helped us to create the electronic equivalent of signatures, vital in verifying the authenticity of data. Hash operations help us to detect minute modifications—malicious or not—in electronic documents and to generate universal digital currencies. Standard modes of symmetric encryption allow us to transmit arbitrarily long information confidentially, anywhere in the world.

Yet, this is only the start of an even bigger revolution fueled by ubiquitous, global connectivity. In the shadow of the race for connectivity, there is an equally fast-paced race for computing technology. Faster and more power-efficient computing means that the scale of cryptographic computations increases drastically: we use longer key sizes to ramp up security, we deploy more advanced protocols, and we rely on more advanced algorithms. There are entirely new, quantum-based computing technologies on the horizon that require a revision of the fundamental cryptographic technologies already in use. Indeed, the classic so-called trapdoor problems that underpin public-key cryptography will need to be replaced before new quantum computers become available. And finally, entirely new applications of cryptography are emerging into practical use. We see novel, elegant methods to handle a person's privacy, and new solutions to entrust the handling of confidential data to an untrusted server. Cryptography is becoming a science in the same way as ad hoc computer programming has evolved into computer science.

With this special issue, we aimed to present the impact of these rapid changes in cryptographic technology on embedded computing platforms. In the Call for Papers, we wrote: "However, this is not your father's cryptography, and its efficient implementation needs new research efforts. It is based on different mathematical structures, novel transformations and data organizations, and in many cases its computational complexity is significantly higher than that of traditional cryptographic operations."

We received 18 manuscripts in response to our Call for Papers. After a two-stage review process, we selected the five manuscripts that are included in this special issue. In addition, we recommended three papers for publication as a regular article in ACM

DOI: http://dx.doi.org/10.1145/2745710

Transactions on Embedded Computing Systems. The process of review and revision was handled as follows. Initially, all manuscripts were assigned to at least three different reviewers. After this first review stage, the guest editors held a face-to-face meeting. Ten articles were selected for a second review, and eight articles were rejected. All review iterations were regarded as requiring "major revision," which meant that the revised articles were returned to the original reviewers for verification. Nine revised articles were received for a second review. After the second review iteration, one article was rejected based on the second-round comments. Of the final set of eight articles, we selected five to form the special issue, while three were recommended for a regular issue. This selection was made considering the coherence in topics of these articles, and the planned publication timeline of the special issue.

As some of the submissions were coauthored by the guest editors, special attention was given to handling conflict of interest. When a conflict of interest was identified, the article in question was handled in a separate, private review account by the guest editors that did not have the conflict of interest. Final decisions on these papers were made by the guest editors with no conflict of interest, in concurrence with the editor-in-chief. By enforcing a two-stage review policy (with mandatory major revision), we ensured that the accepted articles maintained the highest quality.

The five articles that appear in this special issue present the embedded implementation of novel cryptographic schemes based on either lattices or codes. These two forms of cryptography are regarded as the most promising quantum-safe techniques. They appear to provide resistance against known attacks from quantum-computing algorithms. For each cryptosystem, we present one overview article, followed by one or more implementation- and optimization-oriented articles.

In "Practical Lattice-Based Digital Signature Schemes," Howe et al. present a comprehensive survey on how one can generate digital signatures using lattice-based cryptography. They also indicate future research opportunities and open problems.

The second article is "On Constrained Implementation of Lattice-Based Cryptographic Primitives and Schemes on Smart Cards." Jalili et al. discuss the optimization of lattice-based cryptography for constrained smart-card platforms. They present one of the first results that confirm the feasibility of executing lattice-based cryptographic signatures on very restricted microcontroller platforms, and they explain the main computational bottlenecks in these algorithms.

The article by Aysu et al., "The Future of Real-Time Security: Latency-Optimized Lattice-Based Digital Signatures," considers the problem of response time (latency) when generating a signature. In an embedded context, where an application often only needs a single signature at a time, latency optimization is crucial, and the article describes techniques to achieve this requirement.

The article "Implementing QC-MDPC McEliece Encryption" by von Maurich et al. describes the design and implementation of a code-based cryptographic system that uses Quasicyclic Moderate-Density Parity-Check (QC-MDPC) codes in combination with the McEliece encryption system. Their design demonstrates a practical, lightweight implementation of a code-based cryptosystem.

Finally, in "Optimized and Scalable Coprocessor for McEliece with Binary Goppa Codes," Massolino et al. present a hardware implementation of the McEliece encryption system using binary Goppa codes. Their results are twice as fast and twice as compact as the best published result to date.

We hope you will enjoy these articles and their relevance to secure embedded computing platforms. Cryptography is a fast-moving, exciting field that generates challenging design specifications for the world of embedded computing. The TECS community has contributed to the wireless revolution by their efforts to design compact and efficient digital signal processing architectures. We wish to encourage the TECS community to

contribute to securing the connected revolution, by looking for better ways to guarantee security and trust.

Finally, we would like to thank the contributing authors and especially the numerous reviewers that contributed to this special issue. Peer review is a cornerstone of scientific progress, and its duties lie within the community itself. Thank you very much for all your efforts.

March 2015

Patrick Schaumont
Virginia Tech, USA

Maire O'Neill
Queen's University Belfast, United Kingdom

Tim Güneysu
Ruhr University Bochum, Germany

Guest Editors