Call for Papers

ACM Transactions on Embedded Computing Systems
Special Issue

Association for Computing Machinery

Advancing Computing as a Science & Profession

Embedded Platforms for Cryptography in the Coming Decade

Cryptography has made great strides in capability and variety over the past few years, enabling a broad range of new applications and extending the reach of security deep into the embedded world. A few examples include lightweight primitives that provide information security for a fraction of the energy and cost of traditional primitives; lattice-based crypto-engines that provide an alternative to public-key operations in a post-quantum-computing world; cryptographic sponges that can be configured as universal crypto-kernels; anonymous signatures that support electronic cash in portable, compact form factors; and homomorphic primitives and zero-knowledge proofs that allow privacy-friendly interaction of devices with the all-knowing cloud. These novel forms of cryptography will drive the embedded information infrastructure, and they will become a necessity to mix and merge our virtual life with our real life in a trustworthy and scalable manner.

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. For several primitives, such as for post-quantum cryptography and homomorphic computing, the optimal implementation strategies are still an open area of research. Furthermore, threats against these novel forms of cryptography, such as side-channel analysis or fault injection, are unexplored.

This special issue of ACM Transactions on Embedded Computing Systems solicits state-of-the-art research results and surveys in embedded system engineering for these novel cryptographic primitives. The issue will cover both hardware and software implementations for performance-optimized, resource-constrained, energy-efficient platforms. Of special interest are implementations that demonstrate novel applications for cryptographic primitives.

A few examples of topics of interest for the special issue include:

- Post-quantum Primitives for Constrained Platforms (RFID, microcontroller)
- Lattice-based Cryptography in Embedded Platforms
- Embedded Implementations that interact with the Homomorphic Cloud
- Custom-instruction Extensions and Hardware Primitives for Post-quantum Cryptography
- Performance Comparisons and Benchmarks for Multi-party Computation
- Privacy-friendly Cryptography in Embedded Platforms
- Privacy-friendly Car Electronics and Public-transport Infrastructure
- Implementations of Electronic Cash
- Implementations of Electronic Passports
- Hardware Acceleration of Privacy-friendly Cryptographic Primitives
- Implementations of Unified Cryptographic Primitives (eg Authenticated Encryption)
- Implementations of Leakage-resilient Cryptography

The special issue specifically seeks novel, non-traditional implementations of cryptography, and novel, non-traditional threat analysis. Submissions that discuss standard encryption schemes such as based on AES, RSA or ECC, are considered out of scope. Likewise, implementation attacks on traditional targets (standard block ciphers) are considered out of scope.

Guest Editors

Patrick Schaumont
ECE Department
Virginia Tech
Blacksburg VA 24060
schaum@vt.edu

Máire O'Neill
CSIT
Queen's University Belfast
Belfast, United Kingdom
m.oneill@ecit.qub.ac.uk

Tim Güneysu
Dept. of EE and IT
Ruhr University Bochum
Bochum, Germany
tim.gueneysu@rub.de

Timeline

- Submission: July 1, 2014
- Reviews Returned: October 1, 2014
- Revisions: November 1, 2014
- Publication: First Quarter 2015