

IEEE Transactions on Computers Special Section on Cryptographic Engineering in a Post-Quantum World

Guest editors

Çetin Kaya Koç, University of California Santa Barbara, USA

Zhe Liu, University of Waterloo, Canada

Patrick Longa, Microsoft Research, USA

Supervising TC Associate Editor

Çetin Kaya Koç, University of California Santa Barbara, USA

Schedule

- Deadline for submissions: May 31, 2017
- First decision (accept/reject/revise): September 4, 2017
- Submission of revised papers: October 30, 2017
- Notification of final decision: December 4, 2017
- Publication issue: The first half of 2018

The vast majority of public-key cryptosystems currently in use (e.g., RSA, Diffie-Hellman and Elliptic Curve Cryptography) is based on integer factorization and 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 quantum computer has motivated the interest for post-quantum cryptography (a.k.a. quantum-safe cryptography) by both government and cryptography communities.

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. More recently, NIST published a draft (“Report on Post-Quantum Cryptography”) that details NIST's current understanding about the status of quantum computing and post-quantum cryptography and outlines NIST's initial plan for standardization in this space. According to this plan, it is expected that standardization of the selected algorithm(s) begin after a period of 3-5 years following the initial submission deadline on November 2017. Under the light of this major effort, a fundamental question that arises is: how well suited is the cryptography of the future for designing the internet of the future?

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).

It is expected that contributed submissions place emphasis on computing issues in general and on engineering and architecture design aspects of security in particular. Pure theoretical papers lacking architecture design aspects and related evaluations (and comparisons) will not be considered

Topics of interest include (but are not limited to):

- Code-based, hash-based, isogeny-based, lattice-based, multivariate, non-abelian cryptography and other PQC methods and their implementations
- 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

The submitted papers must describe original research which is not published nor currently under review by other journals or conferences.

For extended versions of conference or workshop papers, it is required that submissions have at least 50% of new content and should include a list of changes. All submissions will be peer-reviewed for originality, significance, technical soundness, practical contribution, and clarity of reporting.

Authors are invited to submit manuscripts to Transactions on Computers (TC) at <https://mc.manuscriptcentral.com/tc-cs>. Guidelines concerning the submission process, LaTeX and Word templates can be found at <https://www.computer.org/web/tc/author>. Submission deadline should be observed. Please address all correspondence regarding this Special Section to the Guest Editors using TCPQC@cs.ucsb.edu. While submitting through ScholarOne, please select the option "Special Section on PQC". As per TC policies, only full length papers (10-16 pages, double column) can be submitted to special sections.