Security and Communication Networks

Special Issue on
Secure and Efficient Implementation of Postquantum Cryptography and Its Applications

CALL FOR PAPERS

Information and communication networks, including wired, wireless, and optical transmission platforms, require robust security protocols to protect the transmitted data. These protocols are constructed on the basis of cryptographic primitives such as encryption, digital signature, cryptographic hash, and message authentication. The security of these cryptographic primitives has been based on either computational or mathematical hardness of the underlying problems over classical binary computers. However, the recent remarkable advances in realization of quantum computers by, for example, Google and IBM, and efficient quantum algorithms are raising questions on the existing cryptographic algorithms. As a result, extensive research on quantum-resistant cryptographic algorithms is being performed by many researchers. The open call for proposals for new postquantum cryptography standards by the National Institute of Standards and Technology (NIST) in December 2016 is also accelerating the research of postquantum cryptographic algorithms.

In the era of transition from classical computers to quantum computers, however, we face the issue that new postquantum algorithms should also work effectively on classical computers and be compatible with the existing infrastructure. In other words, postquantum algorithms should be effectively realized in current devices including PCs, servers, GPUs, smart devices, and even sensor nodes. In addition, the new network environments including the internet of things require the implementation of secure primitives on low-end resource-constrained devices. Because most of these devices have relatively simple structures and operating mechanisms, naïve implementation of cryptographic primitives may be vulnerable to side channel attacks such as timing analysis, power analysis, and electromagnetic analysis. Therefore, we need efficient and side-channel resistant implementation of postquantum cryptography considering the new environments. We also need robust security protocols that work effectively with the new cryptographic algorithms.

To pave the way for the new era, we solicit contributions examining secure and efficient implementations of postquantum cryptographic algorithms on nonquantum classical architectures and their applications to the current infrastructure. Papers will be peer-reviewed and selected based on the quality and relevance to the special issue.

Potential topics include but are not limited to the following:

- Efficient implementation of lattice-based cryptosystems
- Efficient implementation of code-based cryptosystems
- Efficient implementation of multivariate cryptosystems
- Efficient implementation of isogeny-based cryptosystems
- Efficient implementation of hash-based signatures
- Side channel attacks and countermeasures
- Fault attacks and countermeasures
- Security protocols based on postquantum cryptographic algorithms
- Applications of postquantum cryptographic algorithms

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/seip/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Mun-Kyu Lee, Inha University, Incheon, Republic of Korea
mklee@inha.ac.kr

Guest Editors
Dong-Guk Han, Kookmin University, Seoul, Republic of Korea
christa@kookmin.ac.kr

Hani M. Alzaid, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
hmalzaid@kacst.edu.sa

Chong Hee Kim, Brightsight, Delft, Netherlands
kim@brightsight.com

Submission Deadline
Friday, 6 April 2018

Publication Date
August 2018