Guest Editors' Introduction

Special Issue on Postquantum Cryptography for Internet of Things

Shivam Bhasin and Anupam Chattopadhyay
Nanyang Technological University
Singapore 639798

Swarup Bhunia
University of Florida
Gainesville, FL 32611 USA

Tim Güneysu
Ruhr-University Bochum
44801 Bochum, Germany

A TIME FRAME of 10–15 years is predicted by many researchers for the widespread deployment of quantum computers. They are poised to break all mainstream public-key cryptographic schemes, which are currently used in many industrial control networks, public key infrastructures (PKIs), and blockchain-based technologies in the supply chain. In 2014, the National Institute of Standards and Technology (NIST) suggested that a quantum computer capable of breaking RSA cryptosystem could be built by 2030. The National Security Agency (NSA) warned in 2015 that progress in quantum computing has reached a point that organizations should start deploying encryption algorithms designed to withstand attacks performed on quantum computers. Since 2020, there has been a final recommendation from NIST for stateful hash-based signatures and a total of seven finalists for public-key encryption, key encapsulation mechanisms, and digital signatures. Two prominent requirements to enable a smooth transition from current cryptographic algorithms, such as RSA and ECC, to postquantum algorithms are implementation security and acceptable performance. This is especially true for resource-constrained devices, specifically, edge computing devices in Internet of Things (IoT) systems deployed in several application domains, such as, industrial networks, smart and critical infrastructures, banking, e-health, and transportation. This transition, generally termed crypto agility, underscores an urgent need for evaluating postquantum cryptographic implementations on IoT platforms for physical security and performance, including the integration of such implementations in current protocols and systems.

Digital Object Identifier 10.1109/MDAT.2024.3400894
Date of current version: 29 August 2024.

In this issue

With this backdrop, we solicited excellent research articles from around the world on the topic of postquantum cryptography (PQC). Out of a total of 15 manuscript submissions, four papers were accepted after a thorough editorial review process. A summary of these works is provided below for the curious readers.

Moraitis et al. [A1] explore the efficient implementation of NIST finalist PQC candidate with side-channel attack resistance. The work reports the most efficient field-programmable gate array (FPGA)-based implementation of this algorithm, including resistance to deep-learning-based side-channel attacks.

Yao et al. [A2] study the performance bottleneck posed by PQC digital signatures when establishing the identity of IoT devices in security protocol and data model (SPDM). A variant of the protocol is

introduced that does away with signature and uses KEM instead. Corresponding performance studies as well as security analyses are presented.

Beckwith et al. [A3] juxtapose two different lattice-based digital signature schemes in a quantum-safe era with the possible application to IoT platforms. Efficient accelerator designs are proposed considering the tight area and power budgets for such devices.

Chattopadhyay et al. [A4] present a summary of quantum threats as well as classical algorithmic/implementation-level threats to public-key cryptographic primitives. Subsequently, state-of-the-art practices for IoT security are discussed to outline the roadmap for future IoT platforms.

We sincerely hope that you enjoy reading this special issue, and we would like to thank all authors and reviewers for their tremendous efforts and contributions in producing these high-quality articles. We also take this opportunity to thank *IEEE Design&Test* Editor-in-Chief Partha Pratim Pande, the editorial board, and the entire editorial staff for their encouragement and assistance in delivering this special issue. ■

Appendix: Related Articles

[A1] M. Moraitis et al., "Securing CRYSTALS-Kyber in FPGA using duplication and clock randomization," *IEEE Des. Test*, vol. 41, no. 5, pp. 7–16, Sep./Oct. 2024, doi: 10.1109/MDAT.2023.3298805.

[A2] J. Yao, A. Hlayhel, and K. Matusiewicz, "Post quantum KEM authentication in SPDM for secure session establishment," *IEEE Des. Test*, vol. 41, no. 5, pp. 17–26, Sep./Oct. 2024, doi: 10.1109/MDAT.2023.3292998.

[A3] L. Beckwith, D. T. Nguyen, and K. Gaj, "Hardware accelerators for digital signature algorithms Dilithium and FALCON," *IEEE Des. Test*, vol. 41, no. 5, pp. 27–35, Sep./Oct. 2024, doi: 10.1109/MDAT.2023.3305156.

[A4] A. Chattopadhyay et al., "Quantum-safe Internet of Things," *IEEE Des. Test*, vol. 41, no. 5, pp. 36–45, Sep./Oct. 2024, doi: 10.1109/MDAT.2024.3408748.

Shivam Bhasin is a principal research scientist and the program manager (cryptographic engineering) at the Center for Hardware Assurance, Temasek Laboratories, Nanyang Technological University, Singapore 639798. His research interests include embedded security, trusted computing, and secure designs. Bhasin has a master's in security of integrated systems and applications from Mines Saint-Etienne, Saint-Étienne, France, and a PhD in electronics and communication from Telecom ParisTech, Paris, France.

Anupam Chattopadhyay is interested in application-specific architecture, electronic design automation, and security. Chattopadhyay has a BE from Jadavpur University, Kolkata, India, an MSc from ALaRI, Lugano, Switzerland, and a PhD from RWTH Aachen University, Aachen, Germany. He is a Senior Member of ACM and IEEE.

Tim Güneysu is a full professor and the head of the chair of security engineering at Ruhr-Universität Bochum, 44801 Bochum, Germany. He is also affiliated with the Cyber Physical Systems (CPS) Division of the German Research Center for Artificial Intelligence (DFKI), 28359 Bremen, Germany. His primary research interests include secure design and low-level engineering of systems, with a focus on advanced and quantum-secure cryptographic implementations, processor security, and hardware security.

Swarup Bhunia is a professor of electrical and computer engineering at the University of Florida, Gainesville, FL 32611 USA. His research interests include hardware and systems security, energy-efficient electronics, and edge intelligence. Bhunia has an MTech from the Indian Institute of Technology (IIT) at Kharagpur, Kharagpur, India, and a PhD in electrical engineering from Purdue University, West Lafayette, IN, USA.

■ Direct questions and comments about this article to Swarup Bhunia, University of Florida, Gainesville, FL 32611 USA; swarup@ece.ufl.edu.