Securing the Internet of Things in a Quantum World

Chi Cheng, Rongxing Lu, Albrecht Petzoldt, and Tsuyoshi Takagi

Currently, we rely on cryptographic algorithms such as elliptic curve cryptosystems (ECCs) as basic building blocks to secure the communication in the Internet of Things. However, public key schemes like ECC can be easily broken by the upcoming quantum computers. Due to recent advances in quantum computing, we should act now to make the IoT be prepared for the quantum world.

ABSTRACT

Currently, we rely on cryptographic algorithms such as elliptic curve cryptosystems (ECCs) as basic building blocks to secure the communication in the IoT. However, public key schemes like ECC can easily be broken by the upcoming quantum computers. Due to recent advances in quantum computing, we should act now to prepare the IoT for the quantum world. In this article, we focus on the current state of the art and recent developments in the area of quantum-resistant cryptosystems for securing the IoT. We first demonstrate the impacts of quantum computers on the security of the cryptographic schemes used today, and then give an overview of the recommendations for cryptographic schemes that can be secure under the attacks of both classical and quantum computers. After that, we present the existing implementations of quantum-resistant cryptographic schemes on constrained devices suitable for the IoT. Finally, we give an introduction to ongoing projects for quantum-resistant schemes that will help develop future security solutions for the IoT.

INTRODUCTION

The past decade has witnessed the steady development of the Internet of Things (IoT). As illustrated in Fig. 1, Gartner has estimated that by 2016 there will be 6.4 billion connected devices in use, and this number is further expected to hit 20.8 billion by 2020. The world population is believed to reach 7.6 billion by 2020, which means that on average each person in the world will have nearly 3 connected devices. Since these connected things, such as implantable medical devices and vehicles, play vital roles in our daily lives, strong security requirements for the IoT have become a must.

Generally, the main security goals for the IoT are confidentiality, integrity, and authentication [1]. Confidentiality guarantees that sensitive information cannot be leaked to unauthorized entities, while integrity prevents information from being modified en route, and authentication ensures that the communicating entities are indeed those they declare to be. As shown in Fig. 2, important communication protocols for the IoT include the IEEE 802.15.4 standard, the Constrained Application Protocol (CoAP), and the IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) standard. To achieve the aforementioned security goals for the IoT, these protocols use cryptographic primitives such as the Advanced Encryption Standard (AES) for confidentiality and integrity, and elliptic curve cryptosystems (ECCs), which include the Elliptic Curve Digital Signature Algorithm (ECDSA) for integrity and authentication and the Elliptic Curve Diffie-Hellman (ECDH) algorithm for exchanging keys used in AES [2].

However, recent advances in quantum computing threaten the security of the current IoT using these cryptographic schemes. Just as the security of Rivest, Shamir, and Adleman (RSA) and Diffie-Hellman (DH) key exchange schemes are based on the difficulty of solving some number-theoretic problems such as integer factorization and discrete logarithms, the security of the ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem. As early as 1994, mathematician Peter Shor of Bell Laboratories showed that quantum computers can solve the integer factorization problem and the (elliptic curve) discrete logarithm problems in an efficient way, sparking great research interest in quantum computing. Since then, quantum algorithms like Grover's search algorithm have been proposed, which provide significant speedup for many problems. Other examples include the quantum algorithms using the quantum Fourier transform, the quantum walk for solving searching problems, and adiabatic quantum computing for optimization problems. Besides that, much research is performed on how to design and build more powerful quantum computers with less resources to implement these algorithms [3].

It is still unclear when large-scale quantum computers will come into existence, but more and more scientists believe that we only need to overcome significant engineering obstacles. Based on recent advances in quantum computing, some scientists even claim that within 20 years our currently used public key infrastructures will become insecure because of the availability of large-scale quantum computers [4].

Even though there are quantum secure replacements for the cryptographic standards in use today, it will take a long time for the transition from currently used IoT systems to their quantum-resistant counterparts. Regarding the fact that we are at the very beginning of the standardization process for quantum resistant algorithms, and research on their application in the IoT is limited,

Digital Object Identifier:
10.1109/MCOM.2017.1600522CM

Chi Cheng is with China University of Geosciences (Wuhan) and Kyushu University; Rongxing Lu is with the University of New Brunswick; Albrecht Petzoldt and Tsuyoshi Takagi are with Kyushu University.

0163-6804/17/$25.00 © 2017 IEEE

it is urgent to make significant efforts in securing IoT systems against possible attacks by quantum computers. Therefore, no matter whether we can predict the exact arrival time of large-scale quantum computers, we should act now to prepare IoT systems for the quantum world.

In this article, we focus on the current state of the art and recent developments in the area of quantum-resistant cryptosystems for securing the IoT. The structure of this article is as follows. In the next section we demonstrate the impacts of large-scale quantum computers on the security of the cryptographic schemes used today, and then give an overview of the recommendations for cryptographic schemes that can be secure under attacks of both classical and quantum computers. After that, we consider the implementations of quantum-resistant cryptographic schemes on constrained devices for the IoT. We give an introduction to ongoing projects and developments for post quantum cryptography that will help develop the future security solutions for the IoT, and conclude this article.

Impact of Quantum Computers on Current Cryptographic Algorithms

The existing cryptosystems used for securing the IoT can be divided into two groups: symmetric and asymmetric (or public key) cryptosystems. In a symmetric cryptosystem two parties share a common secret key, which is then used to encrypt and decrypt messages. On the other hand, an asymmetric cryptosystem makes use of two keys: a private key and a public key. Everybody can use the public key to encrypt messages, but only the owner of the private key can decrypt the ciphertexts. In the context of signature schemes, the private key is used to generate a signature for a document, while everyone can use the public key to check the validity of the signature.

Currently, the most well-known example of a symmetric cipher is the AES, which was selected and standardized in 2001 by the National Institute of Standards and Technology (NIST) via a public competition. AES allows messages to be encrypted with secret keys of length 128, 196, and 256 bits, which are denoted as AES-128, AES-196, and AES-256, respectively. Among them, AES-128 is the most widely deployed in securing the IoT. To date, the best known attack against AES is a brute force search covering all possible keys. Since Grover's algorithm speeds up this process dramatically using quantum computers, the key size of AES needs to be doubled. That is, in order to achieve a security level of 128 bits against attacks with quantum computers, we need an AES key size of 256 bits.

For a public key environment, hash functions, public key encryption schemes, signature schemes, and key exchange protocols are the basic building blocks. A hash function is a map that transforms data of arbitrary length to a hash value of small fixed length. Hereby, it should be difficult to find two different messages that map to the same hash value (collision resistance). Today, the most widely used hash functions are SHA-2 and SHA-3, which are members of the Secure Hash Algorithm (SHA) family selected by NIST. Depending on the output length, SHA-2 can be further divided into SHA-256, SHA-384, and SHA-512. According to NIST's recommendation, we also need to enlarge the output of hash functions to prevent attacks using Grover's algorithm.

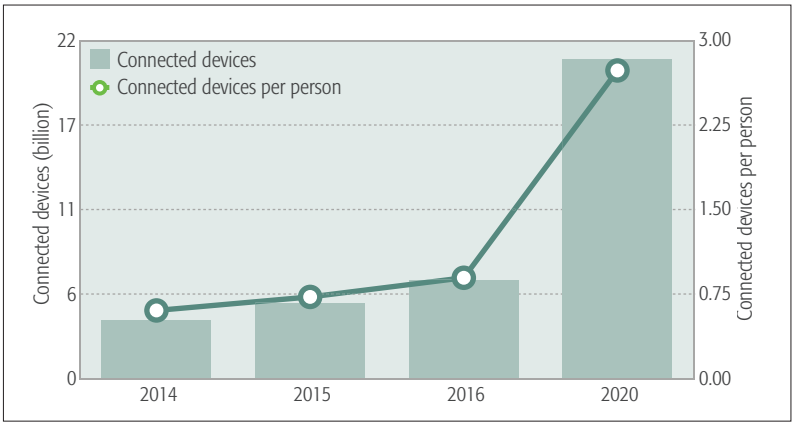

Figure 1. Number of connected devices in the IoT.

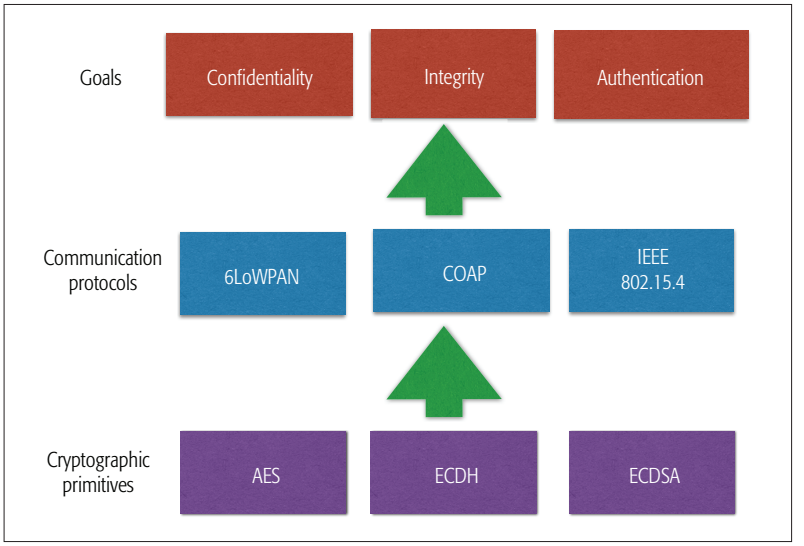

Figure 2. Current cryptographic primitives for securing communication in the IoT.

The impact of quantum attacks on the existing public key encryption and digital signature schemes is even more dramatic. The currently used cryptographic schemes for these purposes include RSA, the Digital Signature Algorithm (DSA), DH key exchange, and ECC, whose security is based on the hardness of certain number theoretic problems such as integer factorization and solving (elliptic curve) discrete logarithms. However, Shor's algorithm can solve these problems very efficiently on a quantum computer, which makes all these classical schemes insecure as soon as large quantum computers arrive.

To summarize, quantum computers have a great impact on the security of all cryptographic schemes used today. While for symmetric schemes and hash functions, it is relatively easy to prevent quantum attacks (increase key and output sizes respectively), public key schemes like RSA and ECC are completely broken (Table 1).

Therefore, we need to develop new schemes for public key encryption and signatures whose security is based on mathematical problems not affected by attacks using quantum computers. In

Algorithms	Purpose	Impact
AES	Symmetric encryption	Double the key size
SHA-2, SHA-3	Hash functions	Enlarge the output
RSA, ECC	Public key encryption and signature	Insecure
DH, ECDH	Key exchange	Insecure

Table 1. Impact of large-scale quantum computers.

Purpose	Type	Candidate algorithms
Symmetric encryption	Symmetric ciphers	AES-256, Salsa20
Public key encryption	Code-based	McEliece with binary Goppa
	Lattice-based	NTRUEncrypt
Public-key signature	Hash-based	XMSS, SPHINCS-256
	Multivariate-based	Rainbow, TTS, HFEv-
	Lattice-based	GPV, GLP, BLISS

Table 2. Initial recommendations for quantum-resistant algorithms.

the next section we give an overview of the existing candidates for this purpose.

Initial Recommendations for Quantum-Resistant Algorithms

To address the challenges in securing the IoT in the quantum world, we first need to know which kind of cryptographic primitives can be secure under the attacks of both classical and large-scale quantum computers. According to NIST [4], widely accepted quantum-resistant public key cryptosystems include hash-based signatures, code-based cryptosystems, multivariate polynomial-based cryptosystems, and lattice-based cryptosystems. The other recommendations given in [4] are based on the difficulty of the isogenies problem over supersingular elliptic curves and the conjugacy search problem in braid groups.

The first code-based cryptosystem was proposed by McEliece in 1978 and is a public key encryption scheme based on an error correcting code called Goppa code. The basic idea of the McEliece scheme can be described as follows: A message is encrypted into a codeword with some added errors, and only the private key holder can remove the errors and recover the original message. After nearly four decades, the McEliece scheme has withstood all proposed attacks [5, 6]. In particular, there is no quantum attack known that breaks the McEliece cryptosystem.

The construction of hash-based signatures employs only hash functions, and therefore minimizes the security requirements for building digital signature schemes. The first hash-based signature scheme was proposed by Merkle, who used a binary hash tree to construct the signatures. The Extended Merkle Signature Scheme (XMSS) is an improved version of Merkle's signature scheme, which reduces the signature size and requires weaker security assumptions [7]. A common requirement of the hash-based signature schemes is the need to record information about previously signed messages, which is called "state." This can lead to problems when signatures are generated on several devices since these devices have to be synchronized after each signature generation. To avoid this, a stateless hash-based signature scheme called SPHINCS has been proposed, which can be described as a multi-tree version of XMSS [8].

The European research group PQCRYPTO has given initial recommendations with specific parameters for quantum-resistant schemes, and we summarize their results in Table 2.

The security of multivariate polynomial-based cryptosystems is based on the difficulty of solving a system of multivariate quadratic (degree 2) equations over a finite field, which is proved to be an NP-hard problem. Depending on the field size used in the system, the multivariate polynomial-based schemes can be divided into small field ones, which include signature schemes such as Unbalanced Oil and Vinegar (UOV), Rainbow, and TTS, and big field ones such as Hidden Field Equations (HFE) [6]. As a variant of HFE, the HFEv- scheme is very useful due to its efficiency and ability to produce the shortest signatures among all existing multivariate polynomial-based schemes.

Previously, lattices were regarded as an important tool in breaking cryptographic schemes. However, starting with Ajtai's pioneering work on using lattices to construct cryptographic systems, numerous works have been done in this area [9]. In 1998, Hoffstein, Pipher, and Silverman proposed NTRUEncrypt (also known as NTRU), a lattice-based public key encryption algorithm that has attracted a lot of attention due to its efficiency and compact keys. Currently, the security of lattice-based cryptosystems mainly depends on the hardness of two problems: the short integer solution (SIS) problem and the learning with errors (LWE) problem, as well as their corresponding variants over rings, the ring-SIS problem and the ring-LWE problem. The advantage of cryptosystems based on the ring-SIS problem and ring-LWE problem is that they are more efficient and significantly reduce the key size compared to schemes based on the non-ring versions of the corresponding problems. Stele and and Steinfeld have proposed a variant of NTRUEncrypt, which can be proven to be secure under the ring-LWE assumption. Another hot topic in lattice-based cryptography is the design of lattice-based signature schemes, which include schemes based on preimage sampleable functions such as GPV, schemes based on the decisional ring-LWE problem such as GLP, and schemes based on the ring-SIS problem such as BLISS.

Quantum-Resistant Cryptographic Schemes on Constrained Devices and Networks

The IoT cannot become reality without the help of various kinds of constrained devices, which not only help us collect and gather information from nature, our households, and factories, but also process and even act on this information. As defined in [10], constrained devices refer to small

devices with limited resources in CPU, memory, and power. These limited resources bring special challenges for the cryptographic schemes used to secure constrained devices in the IoT. Since some of these devices may be used for decades, we should make them secure against long-term attacks. ECC with appropriate parameters is regarded as a solution to this problem. However, devices using ECC become insecure as soon as quantum computers appear. Therefore, the design and implementation of quantum-resistant cryptographic algorithms for constrained IoT devices are of vital importance.

Lattice-based and multivariate polynomial-based algorithms have shown their efficiency in providing quantum-resistant security for constrained devices. In [11] the signature scheme BLISS is implemented on a 32-bit ARM Cortex-M4F microcontroller with 1024 kB flash memory, taking 35.3 ms for signing and 6 ms for verification to achieve 128-bit security. In [12], the implementations of a ring-LWE-based encryption scheme, RLWEenc, and BLISS are conducted on an Atmel ATxmega128A1 microcontroller, which is equipped with an 8-bit CPU running at 32 MHz and a 128-kB flash memory. Specifically, in order to achieve security levels higher than 156 bits, it takes 68 ms for Ring-LWE encryption and 18.8 ms for decryption. For 128-bit security, BLISS needs 329 ms for signing and 88 ms for verification.

For multivariate polynomial-based cryptosystems, in [13] implementations of enhanced TTS (enTTS) and Rainbow are also done on an 8-bit Atmel ATxmega128A1 microcontroller. It is shown that the enTTS needs 66.9 ms for signing and 962.2 ms for verification, respectively, for a 128-bit security level. At the same time, for Rainbow it costs 257.1 ms for signing and 288.0 ms for verification. Since the two implementations in [12, 13] are done on the same 8-bit microcontroller, we list their results in Table 3, which compares the different implementations regarding key and signature sizes as well as the running times for signature generation and verification (for a security level of 128 bits).

The Transport Layer Security (TLS) protocol provides a good solution for Internet security, achieving both confidentiality and authentication. Meanwhile, CoAP, which is safeguarded by the Datagram Transport Layer Security (DTLS) protocol, has been designed for the IoT, especially for constrained devices. Just as TLS is designed to secure applications based on the Transmission Control Protocol (TCP), DTLS is based on the User Datagram Protocol (UDP). In [14], the authors have optimized the implementation of DTLS over CoAP for the IoT. Their implementations are based on ECC and conducted on a platform named MagoNode, which features the Atmel Atmega128RFA1 with a 2.4 GHz low-power transceiver for the IEEE 802.15.4 standard.

However, both TLS and DTLS need to be updated to resist attacks using quantum computers. The work in [15] moved forward toward this goal by providing ciphersuites for TLS, in which the security of the key exchange protocol is based on the ring-LWE problem. Thus, an intriguing problem is whether the latticed-based key exchange schemes work well for DTLS over CoAP. Furthermore, in [15] only the key exchange scheme is quantum resistant. Therefore, another interesting problem is the performance of both TLS and DTLS if all the components are replaced by the aforementioned quantum-resistant cryptographic schemes.

Schemes	Key size private (kB)	Key size public (kB)	Signature size (bit)	Time sign (ms)	@32 MHz verify
BLISS	2	7	7,680	329	88
enTTS	12.7	229.5	704	66.9	962.2
Rainbow	95.4	132.7	632	257.1	288.0

Table 3. Performance and parameters of BLISS, Rainbow, and enTTS (128-bit security).

Ongoing Projects and Developments

We summarize ongoing projects and developments that will help develop the future security solutions for the IoT. The research on quantum-resistant cryptography, which is known as "post-quantum cryptography," is active, and has attracted much attention from government, industry, and academia. Two recent announcements by the U.S. National Security Agency (NSA) and NIST have indicated the increasing necessity for transitions to quantum-resistant schemes [4]. In August 2015, NSA declared its plan to turn to quantum-resistant algorithms on its website. Just recently, at PQCrypto 2016, a leading conference for post-quantum cryptography held in February 2016, NIST announced its plan for a public call for quantum-resistant schemes, leading the way to new public key standards.

The European Commission has also promoted the research on post-quantum cryptosystems. A European research group, PQCRYPTO, has been funded by the European Union Horizon 2020 project, and is conducting research on post-quantum cryptography for small devices, the Internet, and the cloud. Another project supported by Horizon 2020 is SAFEcrypto, which focuses on practical and physically secure post-quantum cryptographic solutions in protecting satellite and public safety communication systems, as well as preserving the privacy of data collected by the government.

Besides that, a research project called CryptoMathCREST, which is supported by the Japan Science and Technology Agency, aims to study the mathematical problems underlying the security of post-quantum cryptography, and implement cryptosystems based on these problems to evaluate their performance in the real world.

Conclusion

Recent advances in quantum computing have demonstrated the urgency of developing quantum-resistant algorithms for securing communication in the IoT. In this article, we have shown the impacts of large-scale quantum computers on the security of the cryptographic schemes widely used today, followed by an overview of the recommendations for cryptographic schemes that can be secure under the attacks of both classical and quantum computers. After that, the recent implementations of quantum-resistant cryp-

The research on quantum resistant cryptography, which is known as "post-quantum cryptography," is active and has attracted much attention from government, industry, and academia. Two recent announcements by the U.S. National Security Agency and NIST have indicated the increasing necessity for transitions to quantum-resistant schemes.

tographic schemes for constrained devices have been introduced. Although ongoing projects are taking steps to develop new quantum-resistant security solutions for the IoT, more work is needed to prepare the IoT system for the quantum world.

Acknowledgments

The work presented in this article was supported in part by the National Natural Science Foundation of China under Grant nos. 61301166, 61672029, 61363069, and 61662016, the Fundamental Research Funds for the Central Universities, China University of Geosciences (Wuhan) (Grant Nos. CUGL150831, CUGL150416), and the JSPS KAKENHI, Grant Nos. 26.04347 and 15F15350.

References

[1] S. Sicari *et al.*, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, 2015, pp. 146–64.
[2] J. Granjal, E. Monteiro, and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 3, 2015, pp. 1294–1312.
[3] T. Monz *et al.*, "Realization of a Scalable Shor Algorithm," *Science*, vol. 351, no. 6277, 2016, pp. 1068–70.
[4] NIST, *Report on Post-Quantum Cryptography*, NISTIR 8105 DRAFT; http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf, accessed Oct. 4, 2016.
[5] A. Daniel *et al.*, "Initial Recommendations of Long-Term Secure Post-Quantum Systems"; http://pqcrypto.eu.org/docs/initial-recommendations.pdf, accessed Oct. 4, 2016.
[6] J. Buchmann *et al.*, "Post-Quantum Cryptography: State of the Art," *The New Codebreakers*, Springer, 2016, pp. 88–108.
[7] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS-A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions," *Post-Quantum Cryptography*, Springer, 2011, pp. 117–29.
[8] D. J. Bernstein *et al.*, "SPHINCS: Practical Stateless Hash-Based Signatures," *Advances in Cryptology--EUROCRYPT 2015*, Springer, 2015, pp. 368–97.
[9] C. Peikert, "A Decade of Lattice Cryptography," *Cryptology ePrint Archive*, Rep. 2015/939, 2015, http://eprint.iacr.org/2015/939.pdf, accessed Oct. 4, 2016, 2016.
[10] C. Bormann *et al.*, "Terminology for Constrained-Node Networks," IETF RFC 7228, DOI 10.17487/RFC7228, May 2014; http://www.rfc-editor.org/info/rfc7228, accessed Oct. 4, 2016.
[11] T. Oder *et al.*, "Beyond ECDSA and RSA: Lattice-Based Digital Signatures on Constrained Devices," *51st Annual ACM Design Automation Conf. 2014*, San Francisco, CA, June 1–5, 2014.
[12] T. Pöppelmann, T. Oder, and T. Güneysu, "High-Performance Ideal Lattice-Based Cryptography on ATxmega 8-Bit Microcontrollers," *Progress in Cryptology-LATINCRYPT 2015*, Springer, 2015, pp. 346–65.
[13] P. Czypek *et al.*, "Efficient Implementations of MQPKS on Constrained Devices," *Cryptographic Hardware and Embedded Systems 2012*, Springer, 2012, pp. 374–89.
[14] A. Capossele *et al.*, "Security as a CoAP Resource: An Optimized DTLS Implementation for the IoT," *2015 IEEE ICC*, 2015, pp. 549–54.
[15] J. Bos *et al.*, "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem," *2015 IEEE Symp. Security and Privacy*, 2015, pp. 553–70.

Biographies

Chi Cheng [M'15] (chengchizz@gmail.com) received his B.S. and M.S. degrees in mathematics from Hubei University in 2003 and 2006, respectively, and his Ph.D. degree in information and communication engineering from Huazhong University of Science and Technology in 2013. He is currently an associate professor in the School of Computer Science, China University of Geosciences, Wuhan, China, and a JSPS postdoctoral researcher at Kyushu University, Japan. His research interests include applied cryptography and network security.

Rongxing Lu (rlu1@unb.ca) has been an assistant professor at the Faculty of Computer Science, University of New Brunswick, Canada, since August 2016. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from May 2013 to August 2016. His research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy. He currently serves as the Secretary of IEEE ComSoc CIS-TC.

Albrecht Petzoldt (albrecht.petzoldt@gmail.com) received a Diploma in mathematics from FAU Erlangen-Nürnberg in 2008, and a Ph.D. in computer science in 2013 at the Technical University of Darmstadt (TU Darmstadt), Germany. He is currently working as a Japan Society for the Promotion of Science (JSPS) postdoctoral researcher at Kyushu University. His main research interests are multivariate cryptography and post-quantum digital signature schemes.

Tsuyoshi Takagi (takagi@imi.kyushu-u.ac.jp) received his B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively, and his Ph.D. from TU Darmstadt in 2001. He is currently a professor in the Institute of Mathematics for Industry at Kyushu University. His current research interests are information security and cryptography. He has received the DOCOMO Mobile Science Award in 2013, IEICE Achievement Award in 2013, and JSPS Prize in 2014, and is a Program Chair of PQCrypto 2016.