cryptography

MDPI

Editorial

Cryptography: A New Open Access Journal

Kwangjo Kim

Editor-in-Chief of Journal of Cryptography, School of Computing, Korea Advanced Institute of Science and Technology (KAIST), Yuseong-gu, Daejoen 305-701, Korea; kkj@kaist.ac.kr; Tel.: +82-42-350-3550; Fax: +82-42-350-7750

Received: 2 February 2016; Accepted: 2 February 2016; Published: 15 February 2016

Cryptography has very long history, from ancient ciphers, such as Ceaser cipher, machine (or rotor) cipherx during WWI and WWII, and modern ciphers, which play a fundamental role in providing Confidentiality, Integrity, and Authentication services during transmission, processing, and storage of the sensitive data over the open or public networks. In 1949, Shannon [1], known as the father of information theory, introduced the seminal idea to construct secure block cipher using iterating cryptographically weak and simple functions, such as confusion and diffusion, as many times, even though each functions are popularly used in classical ciphers and are easily cryptanalyzed by ciphertext-only attacks. Based on Shannon's idea, DES (Data Encryption Standard) was developed in 1977 by the joint team of IBM and NSA as NIST (National Institute of Standards and Technology) requested the standard block ciphers to protect unclassified Federal data in the USA. DES is 64-bit plaintext and 56-bit key, of which security depends on Kerckhoff's principle—any secure system must be secure even if the system can be completely known to attackers, except for the secret key. NIST believed that DES could not be broken by key-exhaustive search attacks, which requires 2^{56} operations. However, Biham and Shamir [2], in 1990, suggested the very clever DC (Differential Cryptanalysis), which utilizes the probabilistic significant distribution of bit-by-bit Exclusive Oring between subsets of plaintext and ciphertext iteratively. They found that the complexity to break DES using DC requires 2^{47} operations. In 1992, Matsui [3] developed a more sophiscated breaking method of DES than DC, called LC(Linear Cryptanalysis), which requires 2^{43} operations by utilizing probabilistic significant distribution between linear subsum of plaintext and ciphertext. This is a dramatic contribution to the breaking of DES in the sense that DC and LC require less complexity than a key-exhaustive search attack. Due to these notorious attacks, DES was deleted from the federal standard, and changed to use DES 3-times to increase the size of the key to a 112-bit for 128-bit block cipher. In 1999, Kocher *et al.* [4] introduced a very poweful attacking method called SCA (Side Channel Attack) by monitoring the timing or the power consumption during an encrypting operation to derive a part of the secret key with 100% accuracy, correctly embedded into the secure device. The designer must check the security of a block cipher from this type of powerful attack, in addition to the complexity of a key-exhaustive search attack. NIST changed the policy for standard algorithms by announcing a call-for-algorithm, all over the world, in 1997. After a three-year public debate, AES (Advanced Encryption Standard) [5] was chosen from the Rijndael block cipher with variable key size from 128-bit to 256-bit in 2000. AES was proved to be secure against DC and LC. In 2000, Berson [6] gave the IACR (International Association for Cryptologic Research) distinguished lecture entitled "Cryptography Everywhere" at Asiacrypt2000:

> *"The past twenty years have seen cryptography move from arcane to commonplace, from difficult to easy, from expensive to cheap. Many influences are at work. These include:the professionalization of cryptographers, in which the IACR has played a significant role; the creation of textbooks and of courses; the steady growth of computational power delivered by the operation of Moore's Law; the algorithmic advances made by cryptographic researchers and engineers; the rise of e-commerce and wireless infrastructures which have a seemingly endless appetite for cryptographic services; the entry of many young people into the field; and the easing of government export controls."*

In 1976, Diffie and Hellman [7] proposed the seminal idea to generate a common secret key over the public channel, between any two parties in a network, by exchanging their public keys to other party derived from their private keys. This was the historical birth of PKC (Public Key Cryptosystem), of which security depends on the difficult problems from the number theory. If public parameters, including the public keys are known (or public) to any one, the complexity to derive the corresponding private key is computationally difficult, even if using the best-known algorithms by massively parallel digital computers. The security of DH (Diffie Hellman) key distribution depends on DLP (Discrete Logarithm Problem). In 1978, RSA (Rivest, Shamir and Adelmann) [8] extended DH's idea to construct a one-way trapdoor function under the composite number, which is a product of large prime numbers. The security of RSA depends on the computational difficulty of IFP (Integer Factorization Problem). DLP and IFP are found to have almost similar sub-exponential complexity. PKC can provide a digital signing capability to make secure transactions over a pubic network to be feasible, such as secure electronic payment, secure electronic voting, auctions, *etc.* Miller [9] and Koblitz [10], coincidently, suggested the idea to use an elliptic curve instead of a number field in 1985 and 1987, respectively. This was the birth of Elliptic Curve Cryptosystem (ECC) which uses 1/6 key size of RSA to guarantee the equivalent security.

When we generate a digital signature of arbitrary length for a message, we need to compress the message, using the cryptographically hash function. Merkle and Damgard suggested an efficient contruct collision resistant hash function from collision-resistant one-way compression function. In 1995, NIST adopted the standard of hash function SHA-1, which was cryptoraphically secure for 10 years. In 2004, Wang *et al.* [11] found an efficient algorithm to find a collision of previous hash functions. In 2009, Steven *et al.* [12] showed how to make a rogue certificate of any issued certificate if the MD (Message Digest) 5 hash function is used to generate the digital signature. NIST was very anxious of these kinds of collision attacks and intitiated the SHA-3 project [13], very similar as AES in 2007. Many proposals for SHA-3 candiates were submitted in 2008. The finalist of SHA-3 was Keccak [14], which can meet all the security requirements of SHA-3 and has a very unique sponge function.

The cryptographic protocols that makes some agreements or decisions between two parties or multiple parties over the Internet using cryptosystems and hash fuctions provides key management, authentication, verification, and identification protocols into the practice. The security of the cryptographic protocols must be proved in detail under some theoretical assumptions before practical use.

In 1984, Shor [15] proposed a polynomial time algorithm to solve IFP or DLP if the attackers have access to quantum computers, which have quite different computing architectures compared to digital computers. If a quantum computer, with a sufficient number of qubits, could operate without succumbing to noise and other quantum decoherence phenomena, Shor's algorithm could be used to break PKC, such as the widely-used RSA or ECC. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum computer algorithms. It has also facilitated research on new cryptosystems, which are secure from quantum computers, collectively called post-quantum cryptography or quatum-safe cryptography.

Nowdays, new types of secure or private protocols are becoming practical. New types of cyber businesses are available. Every day, we can enjoy cryptography to send a secure message over SNS (Social Network Service) to your friends, to secure financial transactions over the Internet, *etc.* Everyone can understand that security and privacy, as well as cryptography, are everywhere.

There is a strong demand to apply cryptographic techniques to, not only ICT (Information Communication Technologies), but also merged applications ith ICT, such as smart cars, smart embedded devices , smart grids, service robots, *etc.*

Cryptography (ISSN 2410-387X) was established to provide a state-of-the-art forum for original results in all areas of modern cryptography, we focus mainly on areas that include, but are not limited to:

- Theory of Cryptography
  - Secret-key cryptography
  - Public-key cryptography
  - Hash Functions
  - Cryptanalysis
  - Cryptographic Protocols
  - Quantum Safe Cryptography
- Practice of Cryptography
  - Cryptographic Hardware/Engineering
  - Applied Cryptography
  - Secure Smart System/Device
  - Digital Forensics
  - Digital Rights Management

Cryptography is a fully open access, peer-reviewed journal that covers a broad range of topics related to cryptography and is published by MDPI, based in Basel, Switzerland. Open access provides several advantages, including free access via the web for anyone interested, rapid publication, literature is immediately released in open access format and the published material can be re-used without obtaining permission after citation, and the long-term impact of the journal will be high. Additionally, all submissions will be published online in open access, free of charge until the end of 2017, after peer review.

On behalf of the Editorial Board, I encourages researchers worldwide to contribute papers to *Cryptography*. Any suggestions about our journal or proposals for Special Issues are welcome.

References

1. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Biham, E.; Shamir, A. *Differential Cryptanalysis of the Data Encryption Standard*; Springer: Berlin, Germany, 1993.
3. Matsui, M. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology—EUROCRYPT '93*; Springer: Berlin, Germany, 1993; pp. 386–397.
4. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Advances in Cryptology—CRYPTO' 99*; Springer: Berlin, Germany, 1999; pp. 388–397.
5. Announcing the Advanced Encryption Standard (AES). Available online: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (accessed on 1 February 2016).
6. Berson, T. Cryptography everywhere. In *Advances in Cryptology—ASIACRYPT 2000*; Okamoto, T., Ed.; Lecture notes in Computer Science 1976; Springer: Berlin, Germany, 2000.
7. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
8. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
9. Miller, V.S. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology—CRYPTO '85 Proceedings*; Springer: Berlin, Germany, 1985; pp. 417–426.
10. Koblitz, N. Elliptic Curve Cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
11. Wang, X.; Feng, D.; Lai, X.; Yu, H. Collisiond for hash functions, MD4, MD5, HAVAL-128 and Ripend. Available online: http://ivanlef0u.fr/repo/madchat/crypto/papers/199.pdf (accessed on 1 February 2016).
12. Stevens, M.; Sotirov, A.; Appelbaum, J.; Lenstra, A.; Molnar, D.; Osvik, D.A.; de Weger, B. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In *Advances in Cryptology—CRYPTO 2009*; Springer: Berlin, Germany, 2009; pp. 55–69.
13. NIST. Computer Security Division, SHA-3 Competition. Available online: http://csrc.nist.gov/groups/ST/hash/sha-3/ (accessed on 1 February 2016).

14. Bertoni, G.; Daemen, J.; Peeters, M.; van Assche, G. The KECCAK Sponge Function Family. Available online: http://keccak.noekeon.org/ (accessed on 1 February 2016).
15. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *26*, 1484–1509. [CrossRef]