Standardization Trends on Cryptographic Algorithms and Protocols in ISO/IEC JTC 1 SC 27 WG 2

Keita Xagawa, Ryo Kikuchi, Atsunori Ichikawa, and Takayuki Miura

Abstract

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 Subcommittee 27 has developed and standardized methods, technologies, and guidelines for information security and privacy. Working Group 2 (WG 2) is responsible for the development and standardization of cryptographic and other security mechanisms. We introduce the latest standardization trends of cryptographic algorithms and protocols in WG 2.

Keywords: lightweight encryption, anonymous signature, elliptic curve cryptography, secret sharing, secure multiparty computation

1. Overall introduction to ISO/IEC JTC 1 SC 27 WG 2

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 (JTC 1) Subcommittee 27 (SC 27) is a standards body dealing with methods, technologies, and guidelines concerning information security and privacy protection. Working Group 2 (WG 2) deals with cryptographic and other security mechanisms. We discuss various methods, from basic encryption methods (e.g., blockciphers and hash functions) to advanced protocols (e.g., anonymous authentication and secure multiparty computation).

2. Lightweight encryption (ISO/IEC 29192 series and ISO/IEC 18033-7)

The performance of a cryptographic mechanism can be measured using various indicators such as computation time, latency, the power consumed, area of hardware implementation, and memory size used for computation. If a device runs on battery, low-power encryption is required, and if it runs in high-transmission environments, less computation time is required. If a device runs in environments where real-time performance is important, such as sensors in the human body, vehicles, and robots in factories, low-latency encryption is required. Lightweight cryptography refers to cryptography that is used in such environments and is “lighter” than existing standardized cryptography with certain indicators. Research on lightweight cryptography began in the early 2000s, and is still active in light of recent safety requirements for devices and trends in Internet of Things.

ISO/IEC has also established the ISO/IEC 29192 series, which summarize lightweight cryptography, and ISO/IEC 29167 series, which define cryptographic technology for radio frequency identification. The US National Institute of Standards and

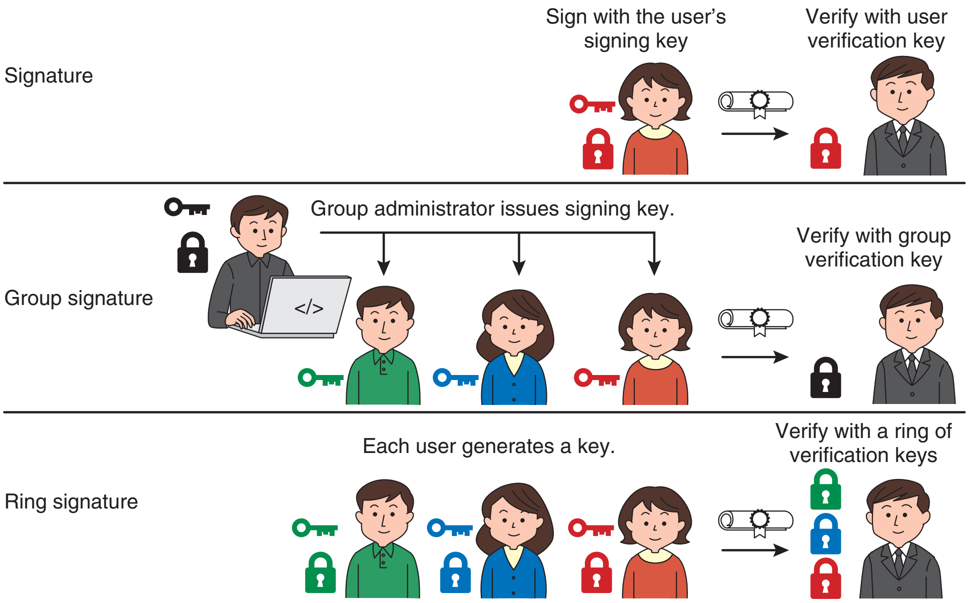

Signature
Sign with the user's signing key
Verify with user verification key
Group signature
Group administrator issues signing key.
</>
Verify with group verification key
Ring signature
Each user generates a key.
Verify with a ring of verification keys

Fig. 1. Anonymous signature.

Technology (NIST) has been studying lightweight cryptography since 2014 and called for applications in 2018. The selection process (Round 2) is now in progress, which involves decreasing the number of candidates. Cryptography Research and Evaluation Committees (CRYPTREC) in Japan also studies lightweight cryptography and published the summary "CRYPTREC Cryptographic Technology Guidelines (lightweight cipher)" [1] in 2017.

WG 2 is responsible for the ISO/IEC 29192 series for various lightweight cryptographic mechanisms. The standard is divided into lightweight blockcipher (Part 2), lightweight stream cipher (Part 3), lightweight hash function (Part 5), lightweight message authentication code (MAC) (Part 6), and so on. ISO/IEC 29192-6 (Lightweight MAC) was published in 2019 and contains Chasky-12 and LightMAC, in which NTT is involved, proposed from Japan.

The standardization of tweakable blockcipher as ISO/IEC 18033-7 began in 2020. This standard will contain [2] Deoxys-BC in Deoxys, which is one of the lightweight ciphers selected by CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness), and SKINNY, in which NTT is involved.

3. Anonymous signature (ISO/IEC 20008 series)

Digital signatures are a basic technology used in various fields. The signer generates a signing key and verification key and publishes the verification key. The signer then generates a signature on the document using the signing key, and the verifier verifies the document and signature with the verification key.

When we look at a document and signature, we know which signer signed it. Thus, when a digital signature is used as an authentication, it is possible to know which verification-key owner carried out the authentication.

Some applications require that signers remain anonymous. For this purpose, a technique called anonymous signature has been studied. The ISO/IEC 20008 series deal with anonymous signatures (**Fig. 1**).

3.1 Group signature (ISO/IEC 20008-2)

In the group-signature scheme proposed in 1991, the group administrator issues a signing key to each user. A user signs the document with the signing key, and the verifier verifies the document and signature with the group's verification key. In this case, the verifier only knows that the signer belongs to the group. This protects the anonymity of the user. The standardization of group signatures began around 2010 as ISO/IEC 20008-2 and was published as a standard in 2013.

3.2 Ring signature (ISO/IEC 20008-3)

In the ring-signature scheme proposed in 2001, each user has a signing key and verification key. The user signs the document with a signing key along with other verification keys. The verifier verifies the set of verification keys (called a ring), document, and signature.

In this case, the verifier only knows that the signer is the owner of one of the verification keys in the ring. This also protects the anonymity of the user. Compared with group signatures, it is less centralized because it does not require a group administrator.

In 2020, ISO/IEC 20008-3 started to standardize ring signatures in response to decentralization and certain blockchains incorporating them as a technology for achieving anonymity in electronic cash. NTT has also been conducting research and development (R&D) of ring signatures since the early 2000s, and actively providing suggestions and feedback.

4. Elliptic curve for pairing (ISO/IEC 15946-5)

Public-key cryptography is based on mathematical problems. For example, Diffie and Hellman's paper [3], which advocated public key cryptography, describes a key-exchange method based on the discrete logarithm problem. Then, around 1985, the construction of public key cryptography based on the discrete logarithm problem on elliptic curves was proposed. It was found that the sizes of the key and ciphertext could be made smaller than those of the usual discrete logarithm problem, and R&D advanced. Around 2000, it was discovered that by using the pairing function defined on an elliptic curve, one could construct novel cryptosystems (identity-based encryption, efficient threshold encryption, etc.) that were not possible before.

WG 2 has been standardizing elliptic curve cryptography, and from 1999 to 2004 this cryptography was compiled as the ISO/IEC 15946 series. Elliptic curve cryptography-based key establishment was later re-classified in ISO/IEC 15946-3 as another standard, and elliptic curve cryptography-based signatures were reclassified in 15946-2, -4 as signature standard. ISO/IEC 15946-1, which defines the terminology of elliptic curve cryptography, and ISO/IEC 15946-5, which describes how to construct elliptic curves and pairing functions, remain.

Kim (then at NTT) and Barbulescu in 2016 proposed an algorithm for solving the discrete logarithm problem on elliptic curves suitable for pairing functions [4]. This algorithm solves the discrete logarithm problem faster than other algorithms, which degrade the security levels of conventional elliptic curves. With the advent of this algorithm, the security evaluation and selection of new elliptic curves have been carried out among researchers and developers.

In WG 2, the security level of the elliptic curves in ISO/IEC 15946-5 has also declined, and in 2018, discussions began on revising the standards to improve the security levels of elliptic curves. The review, selection, and parameter setting of elliptic curves suitable for pairing are being discussed, and standardization is planned from 2021 to 2022. In response to the proposal of this analysis algorithm, NTT is also conducting research on a new elliptic curve [5] and actively contributing to discussions at WG 2.

5. Secret sharing (ISO/IEC 19592 series)

Secret sharing divides data to be kept secret into fragments (called 'shares') with proper encoding. Individual shares do not leak the original data, but if sufficient shares are gathered, then one can recover the original data even if some shares are lost (**Fig. 2**).

Since the original confidential information is not leaked from the shares, it can be used to prevent leakage of sensitive information. Usually, shares are kept by several people, and when a secret is needed, the shares are brought together for restoration of the secret. It is also a key technology for secure multiparty computation, which is described later. Because data can be recovered even if some shares are lost, it can also be used as a distributed data-storage technology or data-recovery technology in the event of data loss due to machine crash or disaster.

Since Shamir and Blakley's independent proposal of secret sharing in 1979, many schemes have been proposed. There are various differences such as safety, division method, and restoration method, and appropriate secrecy distribution must be selected in accordance with the usage scenario. If the same method is used, there may be differences depending on the implementation.

In 2014, the ISO/IEC 19592 series started the standardization of secret sharing. NTT has been active in the standardization of secrecy sharing in ISO/IEC, leading the development of the standard as an editor and contributing significantly to its publication in 2017. We contribute to the selection of easy-to-handle secret sharing by feeding back the knowledge obtained from NTT's research on secret sharing and secure multiparty computation and development of various products (secret sharing technology Trust-SS, distributed storage SHSS (Super High-speed Secret

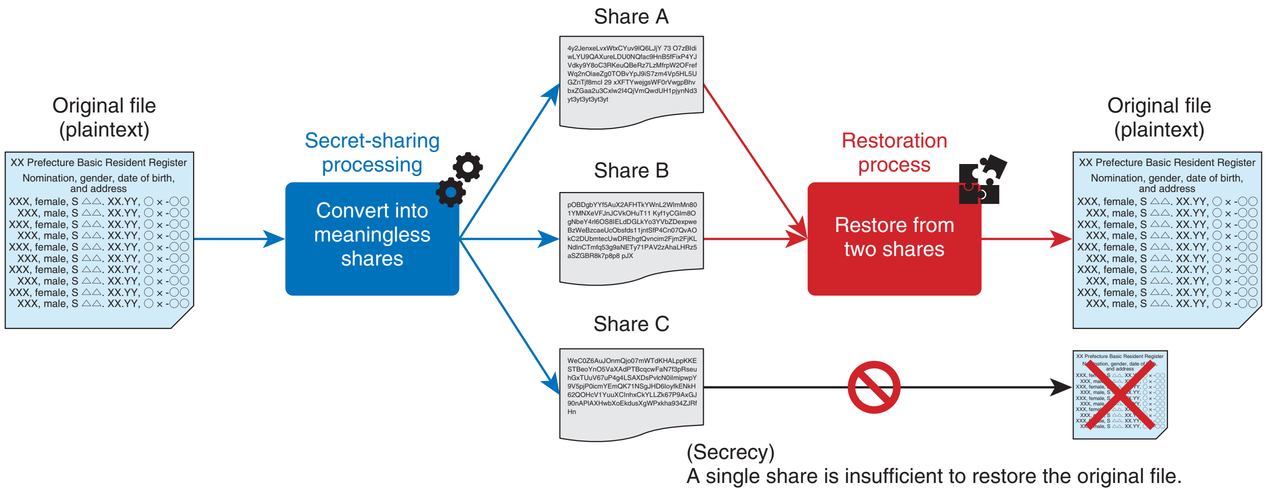
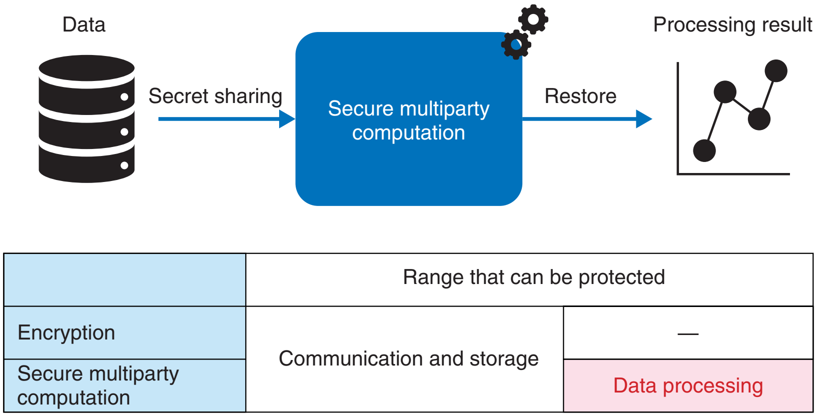

Original file
(plaintext)
XX Prefecture Basic Resident Register
Nomination, gender, date of birth, and address
Secret-sharing processing
Convert into meaningless shares
Share A
Share B
Share C
Restoration process
Restore from two shares
Original file
(plaintext)
(Secrecy)
A single share is insufficient to restore the original file.

Fig. 2. Secret sharing.



	Range that can be protected	
Encryption	Communication and storage	—
Secure multiparty computation		Data processing

Fig. 3. Secret multiparty computation.

Sharing), secure multiparty computation technology “Sanshi®”) using secret sharing.

NTT’s products effectively use three secret-sharing schemes. ISO/IEC 19592-2, published in 2017, specifies five secret-sharing schemes, including these three [6]. In addition, standardization of secure multiparty computation based on secret sharing has recently started.

6. Secure multiparty computation (ISO/IEC 4922 series)

Secure multiparty computation is a technique to execute computations with encrypted data. General encryption protects data communication and storage. Secure multiparty computation can also protect the data-computation process. By using secure multiparty computation, analysis work using personal data of individuals and trade secrets of companies does not leak data and enables “not look inside” operation (**Fig. 3**). This will enable not only safer data processing but also new integrated analysis that transcends the boundaries of companies and industries by bringing together data that have been difficult to disclose to other organizations.

NTT is conducting R&D of secure multiparty computation using secret-sharing technology. That is, data are converted into shares by secret sharing then passed to the servers, which execute the computation without having to restore the original data from the shares. In addition to NTT, various companies, universities, and research institutes are conducting and competing in R&D on secure multiparty computation.

In 2020, the ISO/IEC 4922 series started the standardization of secure multiparty computation. ISO/IEC 4922-1 will be the general standard for secure multiparty computation, and ISO/IEC 4922-2 will be the standard for secure multiparty computation based on secret sharing. NTT is actively leading the creation of standards as editors of both.

7. Future development

NTT will contribute to the development of international standards for cryptographic technology and protocols on the basis of our R&D expertise.

References

[1] CRYPTREC, "CRYPTREC Cryptographic Technology Guidelines (lightweight cipher)," Mar. 2017 (in Japanese).
https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

[2] The British Standards Institution, "ISO/IEC JTC 1/SC 27 N 20359, ISO/IEC NP 18033-7 Information technology - Security techniques - Encryption algorithms - Part 7: Tweakable block ciphers,"
https://standardsdevelopment.bsigroup.com/projects/9020-03695#/section

[3] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Inf. Theory, Vol. 22, No. 6, pp. 644–654, Nov. 1976.

[4] T. Kim and R. Barbulescu, "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case," Proc. of the 36th International Cryptology Conference (CRYPTO 2016), Part I, Vol. 9814, pp. 543–571, Santa Barbara, USA, Aug. 2016.

[5] Y. Kiyomura, A. Inoue, Y. Kawahara, M. Yasuda, T. Takagi, and T. Kobayashi, "Secure and Efficient Pairing at 256-bit Security Level," Proc. of the 15th International Conference on Applied Cryptography and Network Security (ACNS 2017), pp. 59–79, Kanazawa, Japan, July 2017.

[6] Press release issued by NTT on Nov. 23 (in Japanese).
https://www.ntt.co.jp/news2017/1710/171023a.html

Keita Xagawa

Scientist, NTT Secure Platform Laboratories.

He received a B.S. from Kyoto University and an M.S. and D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2010. He is presently engaged in research on cryptography and information security in NTT Secure Platform Laboratories. His research focus is on provable security and analysis in cryptography. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and International Association for Cryptologic Research (IACR). He has been an expert in ISO/IEC JTC 1/SC 27/WG 2 since 2018.

Ryo Kikuchi

Research Engineer, NTT Secure Platform Laboratories.

He received a B.E., M.E., and Ph.D. from Tokyo Institute of Technology in 2008, 2010, and 2015. Since 2010, he has been with NTT. His research focus is on cryptography and privacy-preserving data analysis. He has been an expert in ISO/IEC JTC 1/SC 27/WG 2 since 2013 and was a visiting researcher at the National Statistics Center from 2016 to 2019.

Atsunori Ichikawa

Research Engineer, NTT Secure Platform Laboratories.

He received a B.E. and M.E. from Tokyo Institute of Technology in 2015 and 2017. Since 2017, he has been with NTT. His research focus is on cryptography and oblivious data structures. He has been an expert in ISO/IEC JTC 1/SC 27/WG 2 since 2020.

Takayuki Miura

Research Engineer, NTT Secure Platform Laboratories.

He received a B.E. and M.E. from The University of Tokyo in 2017 and 2019. Since 2019, he has been with NTT. His research focus is on cryptography and machine learning security. He has been an expert in ISO/IEC JTC 1/SC 27/WG 2 since 2020.