Leading-edge Cryptography

● Takeshi Shimoyama ● Kazuya Takemoto ● Arnab Roy ● Avradip Mandal

Cryptography, a fundamental information security technology, is used in diverse aspects of daily life including digital TV broadcasting, digital money, and mobile phones. It is no exaggeration to say that the history of cryptography is the history of cryptanalysis. Even ciphers said to be absolutely safe have eventually become exposed to risks (become compromised) due to the discovery of new cryptanalysis methods or rapid advances in computers and networks, which has led, in turn, to the development of new encryption techniques. This paper describes recent developments in cryptography with a focus on activities at Fujitsu Laboratories. It also introduces technology for correctly determining the lifetime of a cipher considering advances in cryptanalysis and a new encryption technique having novel functions not found in conventional ciphers. Finally, it explains quantum cryptography, which is said to be the ultimate unbreakable cipher.

1. Introduction

Today, with a wide variety of devices connected to the network and information moving back and forth over the Internet, large volumes of data are being created on a daily basis. This information is of various types, from information that will lose its value soon after its creation to information that will affect individuals and society in a semi-permanent manner. Some of this information is highly confidential and highly sensitive in nature, and there is a strong demand for techniques that can reliably protect this type of information. Cryptography has come to be used as one technical means of protecting such data.

The history of cryptography began with the classical ciphers of the Roman era. Then, in medieval Europe, the use of multiple substitution tables led to the development of a much stronger cipher called the *tabula recta*. The evolution of cryptography continued with the development of mechanical cryptography in World War II and complex cryptographic algorithms implemented by computer programs in the current era. Of these ciphers, those that have been used from classical to modern times are no longer valid in today's age of advanced science and technology. Nevertheless, those ciphers made the most of the then state-of-the-art techniques, and in this sense, it can be said that they are a mirror of their times.

Current cryptography is exemplified by RSA, an evolutionary public-key cryptosystem developed in 1977. This system was a major breakthrough in cryptography as it made the cryptographic key public. It uses advanced number theory to eliminate the need to deliver a secret key securely, which had been the shortcoming of previous systems. It is now a fundamental technology in today's information society. Thinking about how a cipher developed 10–20 years ago has now become a mainstream technology, we might say that today's state-of-the art ciphers may help us to predict the future state of cryptography and society using it. Fujitsu Laboratories is thus researching and developing novel encryption technologies.

In this paper, we begin by describing modern cryptanalysis, the lifetime of ciphers, which can be derived from the power of cryptanalysis, and the cipher lifecycle. Next, we focus on the functional aspects of cryptography and describe "Relational Hash," a cryptographic primitive that can greatly reduce the labor associated with key management, which is essential. It is an encryption technology with new functions that were difficult to achieve in past schemes. Finally, we

describe quantum cryptography, which is considered to be the ultimate cipher in that it overcomes the problem facing previous ciphers—eventual deciphering.

2. Cryptanalysis, cipher life, and lifecycle

2.1 Types of ciphers and balance between cipher strength and performance

Cryptography plays an important role in several information systems supporting today's information society including the Internet, mobile phones, digital broadcasting, and digital money. Most of these information systems are achieved using some combination of elemental cryptographic techniques, which include symmetric-key cryptosystems, public-key cryptosystems, and hash functions. A major issue in the construction of a safe and practical information system is selecting a combination of ciphers that will achieve a good balance between safety and performance. Taking, for example, security in an information system, the entire system is no stronger than its most vulnerable component. This tells us that even a single vulnerability is not acceptable in the ciphers selected for various types of information security applications. At the same time, the safety of a cipher is not permanent—a cipher will eventually be compromised as cryptanalysis progresses and/or computing power increases. Furthermore, using a cipher that's stronger than needed in part of a system is wasteful in terms of computer resources or electric power since the cipher will not contribute much to the security of the entire system. Thus, when choosing a cipher for each part of a system, it is important to carefully consider how strong it is and how long it can be used.

In the next section, we take a look at RSA as a standard cipher and describe the results of a cryptanalysis experiment evaluating its strength in terms of the computational complexity of breaking it. We also describe a method for evaluating cipher strength taking into account the performance of the world's most powerful supercomputers extrapolated into the future.

2.2 Computational complexity of cipher breaking and safety evaluation

RSA encryption technology has come to be used by all sorts of systems as standard technology for achieving a public-key cryptosystem. The safety of this encryption technology has been reevaluated a number of times during its life for various types of attacks, and its parameters have been upgraded each time so that it could safely be used into the present.

The continued use of a cipher requires the guarantee that it cannot be broken for all practical purposes even with leading-edge technology and high-performance computers. Cryptography and cryptanalysis are therefore inextricably linked. In other words, the setting of safety parameters based on leading-edge cryptography and cryptanalysis technologies becomes the theoretical basis for guaranteeing the strength of a cipher. In this way, cryptanalysis is not simply used to find a hole in a cipher—it also serves to close up holes prior to an actual attack and to present appropriate methods of using the cipher and means of avoiding vulnerabilities. Additionally, if cipher compromising progresses as expected, a new technology needs to be developed beforehand, and various strength and performance evaluations must be performed. This approach ensures a smooth transition to new ciphers and makes for a stable cipher lifecycle, all of which is tied to sustaining a safe information society.

A reasonable approach to evaluating the strength of RSA encryption is to focus on prime factorization, which is the basis for safe usage. The general number field sieve (GNFS) is the most efficient prime factorization algorithm at present.[1)] Proposed by Lenstra in 1990, GNFS has held all world records in recent years in terms of prime-factorization size for general composite numbers. This algorithm returns a result by executing a four-step procedure:

1) Polynomial selection,
2) Sieve processing,
3) Linear algebra calculation, and
4) Square root calculation.

Of these, step 2), sieve processing, is the most difficult portion of the algorithm from both theoretical and practical points of view. To determine the actual computational complexity of prime factorization, one has to actually perform prime factorization. In the case of RSA, however, there is no way in which 2048-bit prime factorization used as standard can be performed in a realistic time (the current record for prime factorization is 768 bits). This situation has resulted in the adoption of methods that perform only part of the prime factorization process to calculate the entire computational

complexity using world-record algorithms and experimental equipment.

In Japan, the Cryptography Research and Evaluation Committees (CRYPTREC) establishes government-recommended ciphers for constructing a safe e-Government. Its annual report includes the computational complexity required for breaking a cipher and the time period for which the cipher can be safely used for bit numbers of 1024, 1536, and 2048, which are used as standard by RSA encryption.[2] The foundation for these results is the computational complexity of sieve processing calculated experimentally in a uniform environment. The complexity and time period values take into account progress in cipher-breaking algorithms, and the report provides a variety of other evaluation values. Moreover, in addition to the experimentally calculated values, the following formula for evaluating the theoretical computational complexity of GNFS can be used to evaluate the computational complexity of cipher breaking for bit numbers other than those used in the experiment.[3]

$$L_N(s, c) = \exp\left(c\,(\log(N)^s \log(\log(N))^{1-s}\right)$$

In examining the safety of a cipher, improvements in computing power are also an important consideration. Computing power will continue to progress, so calculations have to be based not on computing power at present but on the power that is expected in the future. Here, as evaluation indices, we can use data taken from the TOP500 performance rankings for the world's most powerful supercomputers.[4] This performance data can be used to predict future supercomputer performance and to infer when the world's most powerful supercomputer that can break RSA encryption within one year will appear (**Figure 1**).

The compromise timetable taking into account RSA key length and improvements in computing power is shown in **Table 1** together with symmetric-key cryptosystem strengths.

3. Relational Hash scheme—further evolution of cryptographic functions

In recent years, cryptography has been evolving toward ciphers having a variety of functions going beyond simply data concealment, which has been their main function. In this section, we describe this expansion of functions leading toward applications that could not be achieved with previous cryptographic techniques.

3.1 Problem of secret key management

For example, let's assume the existence of a database holding the fingerprints of known criminals. This database should not be easy to access by members of the organization holding the database, so it will be necessary to protect it by some means such as encryption. On the other hand, the database needs to be used for fingerprint matching of suspects in criminal investigations, so the conventional approach has been to temporarily decrypt the encrypted data to enable the matching to be carried out. Today, however, with importance being attached to the need for privacy in the handling of databases, it has become necessary to

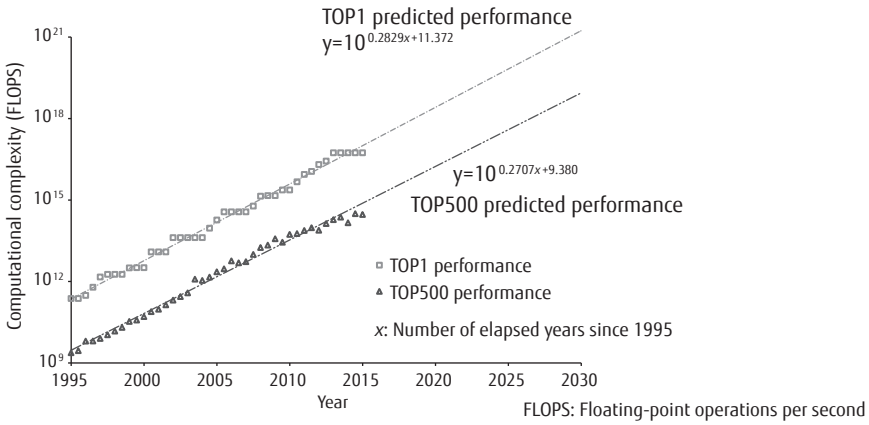


Figure 1
Predicted performance of supercomputers using TOP500 data.

Table 1
Cipher strength evaluation and compromise timetable.

Cipher strength (bits)	Symmetric-key cryptosystem strength	Public-key cryptosystem (RSA) key length (bits)	Compromise timetable
52 or less	DES	512	–
56	–	696	1995
60	–	768	2000
64	2TDES	850	2004
72	–	1024	2013
80	–	1219	2021
92	–	1536	2035
108	–	2048	2052
112	3TDES	2206	2056
128	AES-128	2832	2074
192	AES-192	6281	2143
256	AES-256	11393	2213

conceal the data itself when matching fingerprints. Is this really possible?

The use of homomorphic encryption described in the paper "Anonymization and Encryption Technologies to Protect Privacy of Personal Data," also in this special issue, is one solution to this problem, but it is not a complete answer. This is because the results of matching in homomorphic encryption are also encrypted, so getting those results requires decoding using a secret key. However, this secret key can also be used to decode the database itself, which means that the data is not concealed at all as far as the investigative officer in possession of the secret key is concerned.

A new encryption technology that can fundamentally solve this problem is the "Relational Hash" cryptographic primitive.[5] Given the values of two different hash functions, Relational Hash enables the relationship between the input values to those functions to be determined while concealing those values. Another feature of this technology is that data cannot be decoded even with the secret key possessed by the investigative officer. Of course, as a cipher, Relational Hash satisfies various safety requirements such as one-wayness, twin one-wayness, and unforgeability. It also features the ability to obtain appropriate search results even for input exhibiting fluctuations whenever data is gathered as in the case of biometric information.

3.2 Related technologies

Deterministic hash functions such as the well-known MD5 and SHA-3 functions have the property of data one-wayness in which encryption calculations are easy but the reverse operation is extremely difficult. However, a hash function of this type produces the same hash value for the same plaintext. As a result, the relationship between the plaintext and the hash value can be surmised through analogical reasoning solely on the basis of that hash value, so it cannot be said that deterministic hash functions are sufficiently safe in such equality-checking applications. In contrast, a technology called "probabilistic hash functions"[6),7)] solves the problem of a unique hash value for the same plaintext, but it suffers from severe constraints with respect to usable plaintexts and is not especially user friendly. In any case, probabilistic hash functions targeting fluctuating data such as biometric information convert the hash value of that data into a completely unrelated random value, which means that hash functions of this type are ineffective for such applications.

Other related technologies include "Fuzzy Extractors" such as fuzzy vault,[8)] fuzzy commitment,[9)] and secure sketch.[10),11)] These serve as authentication techniques using biometric information or as technology for protecting biometric information templates. Regardless of their purpose, they protect only registered information. However, they do not protect data at the time of authentication, so safety is an issue. Boyen[12)] attempted to solve this problem by remote biometric authentication, referred to as "zero storage," but data

exchange in this case is very difficult, resulting in a less than practical technology.

Another related technology is Multi-Input Functional Encryption (MIFE).[13] It enables the calculation of value that would otherwise be obtainable only by operations on the target plaintexts from the corresponding ciphertexts. However, the values that can be computed are limited, and some forms of processing such as proximity calculation (proximity of two values) are particularly difficult.

3.3 Relational Hash mechanism

In this section, we describe the mechanism underlying the Relational Hash scheme, which makes it possible to determine whether two input plaintexts satisfy a relation while concealing the original data through the use of hash functions. For example, given a set of three values x, y, z consisting of 0,1, we describe a construction to determine whether the relation $x+y=z$ holds.

- Key generation

For a given security parameter, we consider pairing operator e on groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ of prime order q.

We extract elements $\mathbf{g}_0$ from $\mathbb{G}_1$ and $\mathbf{h}_0$ from $\mathbb{G}_2$ and extract random $n+1$ elements $<a_i>_{i=1}^{n+1}$ and $<b_i>_{i=1}^{n+1}$ from $\mathbb{Z}_q^*$. Now, defining $\mathbf{g}_i=\mathbf{g}_0^{a_i}$, $\mathbf{h}_i=\mathbf{h}_0^{b_i}$, we determine the public keys to be used in hash calculation as follows:

$$pk_1 := <\mathbf{g}_i>_{i=0}^{n+1},\ pk_2 := <\mathbf{h}_i>_{i=0}^{n+1},\ pk_R := \sum_{i=1}^{n+1} a_i b_i.$$

- Hash function 1

Given plaintext $x=<x_i>_{i=1}^{n}$ consisting of 0,1 and public key $pk_1 := <\mathbf{g}_i>_{i=0}^{n+1}$, the hash value is determined as follows:

$$hx := (\mathbf{g}_0^{r},\ <\mathbf{g}_i^{(-1)^{x_i} r}>_{i=1}^{n},\ \mathbf{g}_{n+1}^{r}),$$

where $r \in \mathbb{Z}_q^*$ is a randomly sampled value.

- Hash function 2

Similarly, given plaintext $y=<y_i>_{i=1}^{n}$ consisting of 0,1 and public key $pk_2 := <\mathbf{h}_i>_{i=0}^{n+1}$, the hash value is determined as follows:

$$hy := (\mathbf{h}_0^{s},\ <\mathbf{h}_i^{(-1)^{y_i} s}>_{i=1}^{n},\ \mathbf{h}_{n+1}^{s}),$$

where $s \in \mathbb{Z}_q^*$ is a randomly sampled value.

- Verify algorithm

Given the two hashes $hx=<hx_i>_{i=0}^{n+1}$ and $hy=<hy_i>_{i=0}^{n+1}$ and the quantity $z=<z_i>_{i=1}^{n}$, this algorithm checks whether the following equality holds:

$$e(hx_0, hy_0)^{pk_R} = e(hx_{n+1}, hy_{n+1}) \prod_{i=1}^{n} e(hx_i, hy_i)^{(-1)^{z_i}}.$$

(algorithm completed)

3.4 Relational Hash application

In this section, we describe a method for testing the proximity of two sets of data as an especially convenient function of the Relational Hash scheme. Specifically, we use hash values to determine whether the value set x, y satisfies the relation $\mathrm{dist}(x, y)<\delta$. Here, $\mathrm{dist}(x, y)$ refers to the Hamming distance, and δ denotes a positive integer less than n. This type of processing is expected to provide a safer way of achieving biometric authentication on servers (**Figure 2**).

To construct this Relational Hash, we prepare a $(n, k, 2\delta+1)$ linear error correcting code and denote the encoding and decoding algorithms of the linear code as Encode and Decode. Here, $\mathrm{weight}(x)$ is the Hamming weight of x. The following expression holds if error vector e satisfies $\mathrm{weight}(e)<\delta$.

$$\mathrm{Decode}(\mathrm{Encode}(m)+e) = m$$

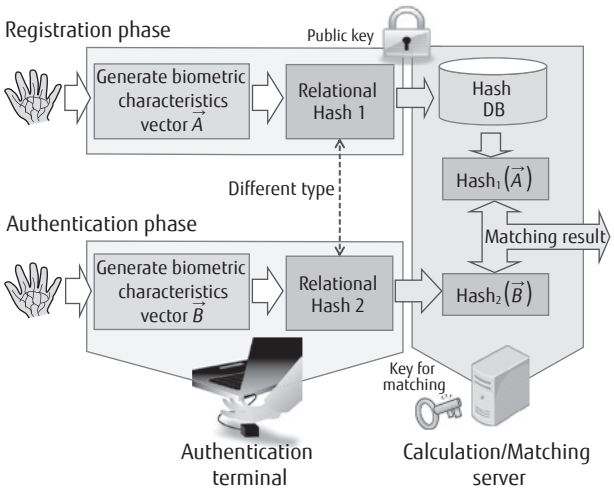


Figure 2
Application of Relational Hash cryptographic primitive to biometric authentication.

Furthermore, if weight(e)>δ, Decode outputs the symbol $\perp$. This application is carried out using the following procedure.

• Key generation

For the above linear code, construct a Relational Hash for linearity consisting of KeyGenLinear, HashLinear_1, HashLinear_2, and VerifyLinear. Denoting the output of KeyGenLinear as pk_{lin}, the public key is determined as follows:

$$pk := (\text{Encode}, \text{Decode}, pk_{lin}).$$

• Hash function 1

Let $hx := (hx_1, hx_2)$ for plaintext x and random number r.

$$hx_1 := x + \text{Encode}(r)$$
$$hx_2 := \text{HashLinear}_1(pk_{lin}, r)$$

Hash function 2 is defined in the same way.

• Verify algorithm

Verification is carried out as follows for the two hash values $hx := (hx_1, hx_2)$, $hy := (hy_1, hy_2)$.

Compute $z := \text{Decode}(hx_1 + hy_1)$. If Decode returns the symbol $\perp$, output "reject," indicating that $\text{dist}(\text{Encode}(z), hx_1 + hy_1) > \delta$ and complete the process. Otherwise, output

$$\text{VerifyLinear}(pk_{lin}, hx_2, hy_2, z).$$

(algorithm completed)

It can be mathematically proven that this algorithm with appropriately set parameters satisfies 80-bit security, corresponding to a sufficient level of strength, while having a practical level of processing performance as a security primitive. This is another major feature of this algorithm.

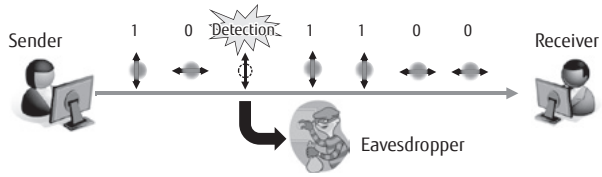
4. Quantum cryptography —safe cryptographic communications of the future

4.1 Latent risks in modern ciphers

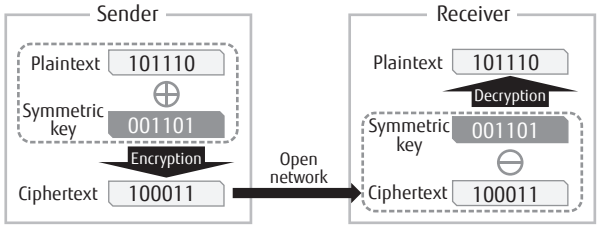
As described above in the section "Cryptanalysis, cipher life, and lifecycle," a modern cipher can be used to keep information secret by appropriately setting cipher strength on the basis of predicted advances in cryptanalysis. On the other hand, the impossibility of cipher breaking beyond the lifetime of a cipher cannot necessarily be guaranteed. Consequently, to convey information that needs to be protected over a relatively long period of several tens of years or more such as genetic information, the need is felt for more advanced cryptography. Furthermore, if a quantum-gate type of quantum computer capable of massively parallel computing can be achieved, RSA encryption based on prime factorization can be broken in polynomial time by Shor's algorithm.[14] Thus, to deal effectively with such a latent risk, there will be a need in the future for absolutely unbreakable cryptography independent of computing power.

4.2 Overview of quantum cryptography

Quantum cryptography is essentially cryptographic communications technology that guarantees unconditional security by combining two key technologies: cryptographic key transmission capable of detecting eavesdropping using the quantum properties of single photons, and a single-use key cipher proven to be "information theoretically secure" (one-time pad). The basic mechanism of quantum cryptography is shown in **Figure 3**. The former technology, called quantum key distribution (QKD), is being actively researched at institutions throughout the world toward practical application. The most standard QKD protocol



a) Quantum key distribution (transmit and share cryptographic key as random number sequence one photon at a time)



b) Encryption using a one-time pad (encrypted communications using a shared random number sequence as a symmetric key)

Figure 3
Mechanism of quantum cryptography.

is BB84,[15] which uses the polarization or phase of single photons to carry the random number sequence that serves as the basis of a cryptographic key. A single photon cannot be divided into smaller components, so it cannot be partially stolen. Moreover, if an eavesdropper attempts to copy key information, the state of that photon will change in accordance with the uncertainty principle of quantum mechanics. A legitimate user can detect such eavesdropping and discard the affected information, enabling the remaining random numbers to be safely shared as a secret key.

Quantum key distribution based on the BB84 protocol requires a single-photon source (SPS) for emitting photons one at a time with arbitrary timing. However, SPS devices are not easy to develop, so most verification experiments today make use of weak coherent pulses (WCPs) in which laser light has been significantly weakened. The use of WCPs, however, presents a problem in that multiple photons are frequently generated simultaneously, a situation that can facilitate eavesdropping. In other words, an eavesdropper who steals only one photon from a group of photons and forwards the rest to the receiver can prevent eavesdropping from being detected. Consequently, as transmission distance lengthens (as the transmission loss of the optical fiber increases), the sender must weaken the laser's output light to lower the probability of generating multiple photons. This, however, makes the ratio of detector noise to the optical signal large at an early stage, preventing the generation of a cryptographic key (dashed line in **Figure 4**).

A modified version of the BB84 protocol (decoy method) was therefore proposed to deal with this problem.[16] This version, which is now widely used, artificially mixes in several types of weak light (decoy light) with intensities different than those of the WCPs for use in detecting eavesdropping. The decoy method suppresses the drop in the key generation rate compared to using simple WCPs and thus enables the transmission distance to be significantly extended (dashed-dotted line in Figure 4). On the other hand, equipment configuration and key extraction processing become more complicated, so maintaining security requires that careful attention be paid to the management and operation of that equipment, which is an issue in itself. In contrast, an ideal SPS achieves the highest transmission performance in theory (solid line in Figure 4), and since it generates only one photon per pulse, it can also greatly simplify key processing and equipment setup. Finally, it can provide a provable, high level of security based on quantum mechanics.

4.3 1.5-μm-band SPS and QKD system

As part of the Creation of Innovation Center for Advanced Interdisciplinary Research Areas Program, a Ministry of Education, Culture, Sports, Science and Technology (MEXT) project for developing innovative systems, Fujitsu Laboratories, Professor Yasuhiko Arakawa of The University of Tokyo, and NEC Corporation joined forces in a three-way collaboration to develop a high-performance SPS in the 1.5-μm-band and a long-distance single-photon QKD system incorporating that SPS.

The configuration of a 1.5-μm-band quantum dot SPS is shown in **Figure 5**. The use of a nanometer-size semiconductor nanocrystal, i.e., a quantum dot, is a common method for generating single photons. Irradiating a quantum dot generates an electron-hole pair that emits a photon when recombined. The authors have devised a means of forming a fine parabolic structure, an "optical horn," around a quantum dot to raise the efficiency of extracting photons from the outside of the substrate.[17]

An important index of SPS performance is $g^{(2)}(0)$, which indicates the degree to which the generation of

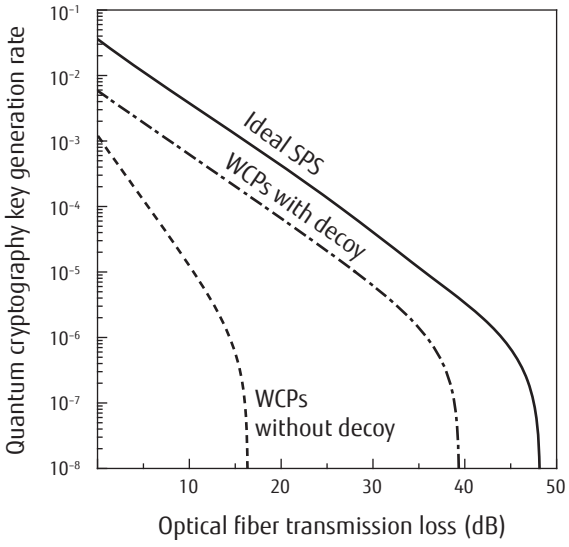


Figure 4
Quantum cryptography key generation rate versus transmission loss.

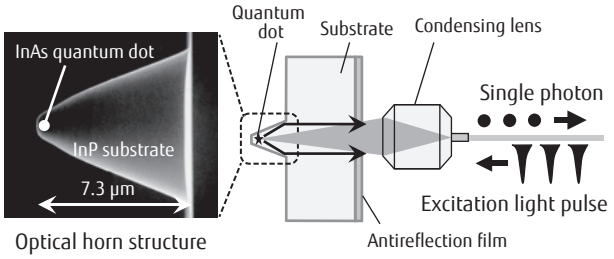


Figure 5
1.5-μm band quantum dot SPS.

multiple photons can be suppressed. In essence, the $g^{(2)}(0)$ index indicates the purity of single photons: for a WCP, $g^{(2)}(0)=1$, while for an ideal SPS, $g^{(2)}(0)=0$. Thus, a lower value of this index means less generation of multiple photons and the operation of QKD at longer distances. A QKD verification experiment using a 1.5-μm-band SPS achieved transmission distances of up to 50 km.[18] One reason for this was that the value for $g^{(2)}(0)$ was relatively high at 0.055. More recently, the authors succeeded in suppressing the generation of multiple photons by compressing the excitation pulse irradiating the quantum dot, resulting in $g^{(2)}(0)=0.002$, which is less than 1/25 the previous value.[18] Converting this to a simultaneous photon generation rate gives a value of 1/1,000,000 per pulse, which is currently the highest level of single-photon purity. Furthermore, a transmission experiment incorporating this high-purity SPS in a QKD system based on an ultra-low-noise superconducting single-photon detector showed that safe key transmission can be performed up to 120 km, the longest distance for a single-photon method.[19] This system can thus cover major cities in the Tokyo regional area, and as such, it represents a milestone toward the realization of an urban secure network in which eavesdropping is impossible.

5. Conclusion

In this paper, we introduced leading-edge cryptography and described, in particular, technology for correctly assessing the lifetime of a cipher taking into account progress in cryptanalysis, a new encryption technology having novel functions not found in existing ciphers, and quantum cryptography, the ultimate unbreakable cipher.

As described at the beginning of the paper, encryption technologies that are now mainstream were developed several tens of years ago, so the leading-edge technologies introduced here may likewise come into practical and widespread use several tens of years from now. It should be pointed out, however, that these leading-edge encryption technologies developed by Fujitsu Laboratories are the result of diverse research achievements over many years. Such an approach drives Fujitsu's mission of constructing an infrastructure for a safe information society now and into the future. It is hoped that the technologies described in this paper will become the basis for safe systems in the future.

The research described in the section titled "4. Quantum cryptography—safe cryptographic communications of the future" was carried out with support provided by the Creation of Innovation Center for Advanced Interdisciplinary Research Areas Program of the Ministry of Education, Culture, Sports, Science and Technology (MEXT).

References

1) A. Lenstra et al.: The Number Field Sieve, STOC 1990, pp. 564–572, ACM, 1990.
2) CRYPTREC: CRYPTREC Report 2014. Information-technology Promotion Agency (IPA), National Institute of Information and Communications Technology (NICT), 2014.3.
3) M. Yasuda et al.: On the Strength Comparison of the ECDLP and the IFP. SCN2012, pp. 302–325, 2012.
4) TOP500 Supercomputer Sites. *http://top500.org*
5) A. Mandal and A. Roy: Relational Hash: Probabilistic Hash for Verifying Relations, Secure against Forgery and More. CRYPTO 2015, volume 9215 of LNCS, pp. 518–537. Springer, August 2015.
6) R. Canetti: Towards realizing random oracles: Hash functions that hide all partial information. CRYPTO'97, volume 1294 of LNCS, pp. 455–469. Springer, August 1997.
7) R. Canetti et al.: Perfectly one-way probabilistic hash functions (preliminary version). In 30th ACM STOC, pp. 131–140. ACM Press, May 1998.
8) A. Juels et al.: A fuzzy vault scheme. Cryptology ePrint Archive, Report 2002/093, 2002.
9) A. Juels et al.: A fuzzy commitment scheme. In ACM CCS 99, pp. 28–36. ACM Press, November 1999.
10) Y. Dodis et al.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. EUROCRYPT 2004, volume 3027 of LNCS, pp. 523–540. Springer, May 2004.
11) Y. Dodis et al.: Correcting errors without leaking partial information. 37th ACM STOC, pp. 654–663. ACM Press,

May 2005.
12) X. Boyen: Reusable cryptographic fuzzy extractors. ACM CCS 04, pp. 82–91. ACM Press, October 2004.
13) S. Goldwasser et al.: Multi-input functional encryption. EUROCRYPT 2014, volume 8441 of LNCS, pp. 578–602. Springer, May 2014.
14) P. W. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26, pp. 1484–1509 (1997).
15) C. H. Bennett et al.: Quantum Cryptography: Public Key Distribution and Coin Tossing. IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175–179 (1984).
16) H.-K. Lo et al.: Decoy State Quantum Key Distribution. Phys. Rev. Lett., 94, 230504 (2005).
17) K. Takemoto et al.: An optical horn structure for single-photon source using quantum dots at telecommunication wavelength. J. Appl. Phys., 101, 081720 (2007).
18) K. Takemoto et al.: Transmission Experiment of Quantum Keys over 50 km Using High-Performance Quantum-Dot Single-Photon Source at 1.5 μm Wavelength. Appl. Phys. Exp., 3, 092802 (2010).
19) K. Takemoto et al.: Quantum Key Distribution over 120 km Using Ultrahigh Purity Single-Photon Source and Superconducting Single-Photon Detectors. Sci. Rep., 5, 14383 (2015).

Takeshi Shimoyama
Fujitsu Laboratories Ltd.
Mr. Shimoyama is currently engaged in the research of cryptography.

Kazuya Takemoto
Fujitsu Laboratories Ltd.
Mr. Takemoto is currently engaged in the research of quantum information processing technology.

Arnab Roy
Fujitsu Laboratories of America, Inc.
Mr. Roy is currently engaged in the research of cryptography.

Avradip Mandal
Fujitsu Laboratories of America, Inc.
Mr. Mandal is currently engaged in the research of cryptography.