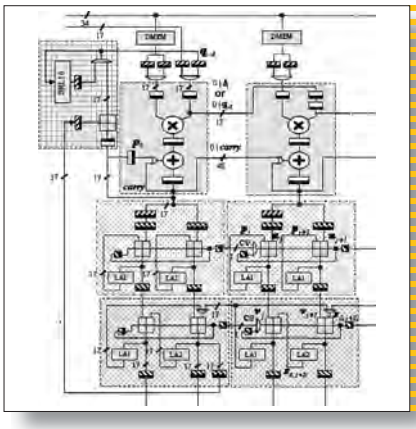
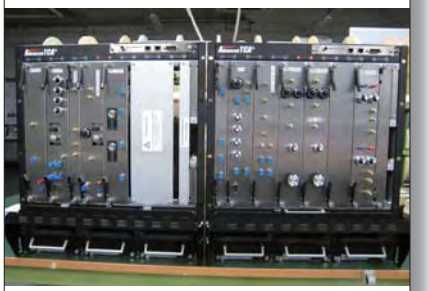
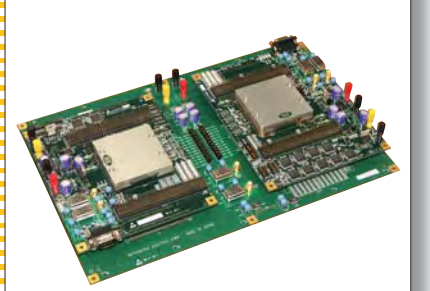
ISSN 1345-3041
MITSUBISHI ELECTRIC Jun. 2009 /Vol.126

ADVANCE

Information Security Technology







MITSUBISHI ELECTRIC
Changes for the Better

Jun. 2009 / Vol. 126
MITSUBISHI ELECTRIC ADVANCE
Information Security Technology

Cover Story

It is no exaggeration to state that not a day passes where encryption is not used in our daily life. This issue introduces various information security technologies supporting the safety and security of information systems, focusing on encryption technology and examples of its application.

• **Editorial Inquiries**
Makoto Egashira
Corporate Total Productivity Management
& Environmental Programs
Fax +81-3-3218-2465

• **Product Inquiries**
Information Technology R&D Center
Administration Dept.
Fax +81-467-41-2142

Mitsubishi Electric Advance is published on line quarterly (in March, June, September, and December) by Mitsubishi Electric Corporation.

CONTENTS

Technical Reports

Overview

Author: *Mitsuru Matsui**

Encryption technology is widely utilized in IT systems and products as an indispensable means for protecting personal privacy and corporate confidentiality. We are living in an age where it would be difficult to go about our daily activities without using any encryption even though it may not be directly visible.

The algorithms that support encryption technology are classified according to their properties into various types including common key block encryption, hash functions, and public key encryption. Encryption algorithms are organically integrated to support the security of information communication while sharing their role in the system.

Since 1995, we have developed common key block encryption algorithms, typified by MISTY and Camellia, and released their specifications to the public, and we have also promoted activities for their standardization in and outside Japan. Consequently, the International Organization for Standardization (ISO) currently adopts these encryption algorithms as world standards.

In the meantime, cryptanalysis studies aimed at evaluating the security of encryption algorithms have also made remarkable progress. Recent concerns have surfaced about the future security of some encryption systems currently in wide use, such as hash functions. Therefore, the current encryption system is globally shifting to a new cryptography system.

In addition, the mathematical security of encryption as well as the security of its implementation in both software and hardware must be considered in actual systems. In this respect, the point of contact between encryption technology and physics has widened.

Against this backdrop, Mitsubishi Electric is developing encryption algorithms and information security systems that combine high security against cryptanalysis with high practicality such as compact size and high speed. This issue provides a sampling of our efforts

**Information Technology R&D Center*

Current State and Future Trend of Encryption Technology

Author: *Mitsuru Matsui**

1. Introduction

A surprisingly long time has passed since encryption technology first came into use in our own backyard. Now, ciphers are used in many of the items that we carry around, such as cellular phones, cash cards, train tickets, mobile PCs, and electronic car keys. We live in an age where almost everyone uses encryption in their daily lives, often without even realizing it.

Looking back over the development of encryption technology, we can see that the purpose of using ciphers has extended from "confidentiality" for protecting confidential information to "authentication" for preventing spoofing and "integrity" for preventing forgery of information; and that today's processors and devices with lower power consumption and higher speed have greatly increased the potential for cryptographic application.

Meanwhile, the advances made in encryption technology also mean advances in cryptanalysis technology. The scientific community is presently engaged in research on cryptanalysis with the goal of identifying any problems in the current encryption systems. The consensus of encryption researchers is that advances made in cryptanalysis technology will mean advances in encryption technology.

Academia requires that encryption algorithms have universal and extremely high security. Therefore, the relationship between cryptanalysis in an academic sense and cryptanalysis in a specific practical application is not always self-evident. Serving as a bridge between them is an important role of encryption researchers in companies.

Recently, researchers pointed out that several widely used encryption systems are at risk of being compromised or deteriorating in security, which could affect the use of encryption from 2010 onward. This is the so-called "year 2010 encryption problem" under global discussion.

Against this backdrop, this paper focuses on the encryption systems currently used in our own backyard and discusses the present state of security evaluation from a practical viewpoint. Also presented is an overview of new encryption technologies currently attracting attention, and a summary of their significance from the viewpoint of convenience and security.

2. Security of Hash Functions

2.1 Hash Function

The hash function is a cryptographic component that finds a great number of applications such as for encrypted passwords, digital signatures, and random number generation. It is also referred to as a cryptographic hash function to clarify the use of encryption.

The role of the hash function is to receive data of an arbitrary length as input and "compress" it to generate a hash value of fixed length. Important security requirements for the hash function include one-wayness and collision resistance. One-wayness means that it is difficult to compute the input backwards from the output, and collision resistance means that it is difficult to detect two different input messages where the hash values are the same.

Figure 1 shows an example of using the hash function in a digital signature. A signer uses the hash

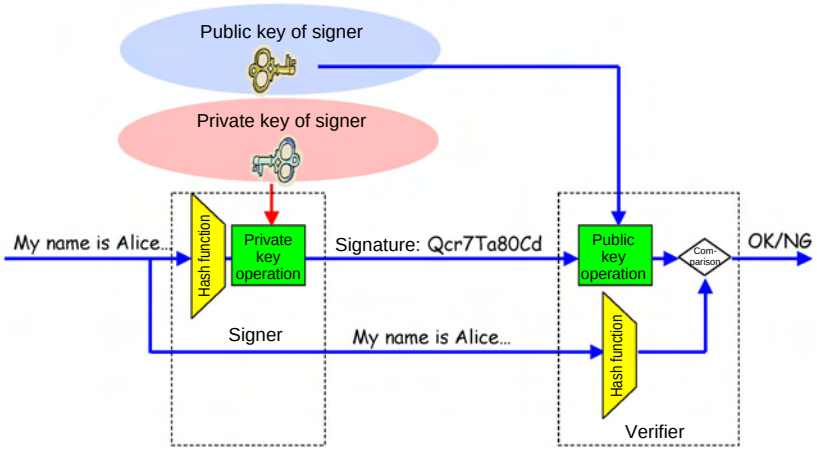


Fig. 1 Example of using the hash function in a digital signature

**Information Technology R&D Center*

function to process a message and then perform private key operation. In this case, the collision of hash functions can be disastrous. That is, the capability to compute two different messages, M and M', where Hash(M) = Hash(M') refers to the impossibility of the verifier being able to distinguish digital signature M from M.' Thus, collision resistance is a vital property of the hash function.

2.2 Examples of hash functions

The current most widely used hash function is U.S. Government Standard SHA-1[(1)]. Until SHA-1 was established, the MD series hash functions, MD4 and MD5, were in wide use. Even now, some applications use MD5 for the purpose of compatibility. However, as described in this section, the use of the MD series hash functions cannot be recommended in terms of security.

The hash length of SHA-1 is 160 bits. A newly established U.S. Government Standard, SHA-2, has a longer hash length. SHA-2 is the generic name for several hash functions, and individual algorithms are called SHA-256, SHA-384, and SHA-512 using the format in which the hash length follows the name.

2.3 Security problem of hash functions

It is generally known that the collision of hash functions with a hash length of n bits can be found by a computation amount of $2^{n/2}$. Thus, the upper limit of hash function security becomes $2^{n/2}$. However, it was recently found that the collision of some hash functions can be obtained by a computation amount that is smaller than $2^{n/2}$. Examples of actual collision of MD4 and MD5 in particular have been reported[(2)]. Although the collision of SHA-1 has not yet been reported, discovery is expected within one or two years.

Table 1 is a summary of the present state of security of hash functions. The step count here indicates the iteration count of the internal basic functions in the hash function. Since MD4 and MD5 collisions are easily found and the possibility of spoofing and forgery may actually arise in some applications, care must be taken and it is recommended that these hash functions not be used whenever possible.

Table 1 Present state of security of hash functions

	Hash length	Block length	Step count	Standard	Collision
MD4	128 bit	512 bit	48	RFC1320	×
MD5	128 bit	512 bit	64	RFC1321	×
SHA0	160 bit	512 bit	80		×
SHA1	160 bit	512 bit	80	FIPS180-2 ISO10118	Δ
SHA256	256 bit	512 bit	64	Same as the above	○
SHA512	512 bit	1024 bit	80	Same as the above	○

×: Many collisions have already been discovered.
Δ: High possibility that a collision will be discovered in the near future.
○: There is no indication that a collision will be discovered.

The computation amount for obtaining collision of SHA-1 is reported to be about 2^{63}[(3)], which is one hundred thousandth of its proper computation amount of 2^{80}. For SHA-0, the initial version of SHA-1, although its algorithm document differs in only one line from that of SHA-1 (specifically, SHA-1 requires one more rotation shift operation compared to SHA-0), it is already in a state in which collision is easily found. When this fact is taken into consideration, the risk of SHA-1 being compromised cannot be disregarded.

For SHA-2, the likelihood of the collision of algorithms being found has not yet been reported, and it is considered that there are no problems with SHA-2 even in an academic sense.

2.4 Future of hash functions

The U.S. National Institute of Standards and Technology (NIST), which establishes the Federal Information Processing Standards, recently announced that the use of SHA-1 for the purpose of digital signatures will be discontinued in 2010, and, consequently, a rapid shift from SHA-1 to SHA-2 is currently taking place. Even though SHA-2 does not presently pose a security problem, its structure is similar to that of SHA-1, and thus it is considered that hash functions with a new structure should eventually be standardized.

For this reason, NIST initiated a project in 2008 to select a government standard encryption ASH (Advanced Hash Standard) after SHA-2, and a new standard is expected around 2012. Therefore, the use of SHA-2 will continue only until the new standard is established.

There is almost no application where its security is threatened because of the discovery of one SHA-1 collision, but the shift to a new hash function is required in systems where its validity must be guaranteed for a long time, such as for digital signatures.

Thus, for actual systems, the shift to a new hash function should be determined according to whether the system is affected by the recently discovered hash function collisions and the validity period of the system and data.

3. Security of Public Key Encryption

3.1 RSA encryption

Developed in the mid-1970s, RSA encryption is one of oldest and most widely used public key encryption technologies. Its security is based on the difficulty of a problem involving factorization into prime numbers, and if the key length (composite length) is increased, cryptanalysis should become exponentially difficult (factorization into prime numbers becomes difficult).

RSA encryption generally uses a key length of 1,024 bits, but 2,048 bits or more may be used in a particularly important system. The computation amount required for 1,024-bit composite factorization into prime numbers is about 2^{80}, or the same degree as the common key encryption of an 80-bit key and the security of a hash function with a hash length of 160 bits.

In RSA encryption, the computation amount required for encryption and decryption is proportional to the cube of the key length. That is, when the key length is doubled, the operation amount octuples. RSA encryption requires the generation of prime numbers each time a key is generated, and this computation amount is generally proportional to the fourth power of the key length. Thus, in an application requiring speed and a system that issues a large amount of digital certificates, the key length significantly affects the entire performance.

3.2 Present state of security of RSA encryption

The lower limit of the computation amount required for factorization into prime numbers is not known and even the fact that it is necessary for exponential time is not mathematically proven. However, factorization into prime numbers is a long-standing mathematical problem, and from the previous research findings, it is considered that factorization into prime numbers cannot be executed in polynomial time.

This indicates asymptotical evaluation or that the security increases dramatically when the key is lengthened, and does not guarantee the computation time of factorization into prime numbers when the key is fixed to a certain length. To determine the potential for individual composite factorization into prime numbers, researchers are continuously running experiments with multiple computers. As listed in Table 2, records have been broken one after another, with the current world record at 640 bits[4].

Table 2 History of world records for factorization into prime numbers

Number of bits of composite	Date that factorization into prime numbers was announced
430	April 10, 1996
463	February 2, 1999
512	August 22, 1999
530	April 1, 2003
576	December 3, 2003
633	May 9, 2005
640	November 2, 2005

From these results, it is difficult to predict when a 1,024-bit composite would be subjected to factorization into prime numbers, but it is considered that it will be about 2015 at the earliest. Thus, under the present circumstances, as with the hash function, it is recommended that the key length for RSA encryption be shifted to 2,048 bits for applications requiring long-term evidence to be secured, such as for digital signatures.

However, as previously described, it is not always easy to shift the key length for RSA encryption, since doubling the length significantly affects the application. As described below, it will become important to use a mechanism that extends the effectiveness of cryptographic processing to cope with this problem.

3.3 Identity-based encryption

Identity-based encryption, in which arbitrary information can be set in a public key, was advocated back in 1984. For many years after that, the specific construction of secure identity-based encryption was an unresolved problem. Eventually, around 2000, a system was invented that is practical and has proven security, possibly the ultimate solution[5][6]. Since then, active research and development has been underway around the world.

Table 3 lists the relationship between the public key and private key for RSA encryption, the elliptic curve cryptosystem, and identity-based encryption. The public key for RSA encryption and the elliptic curve cryptosystem appear on the left side of the relational expression and the private key for identity-based encryption appears on the left side. The essential advantage of identity-based encryption is that the relationship is one where computation can start with an arbitrary public key.

Table 3 Relationship between public key and private key in public key encryption

	Public key	Private key	Relationship between public key and private key
RSA encryption	N	P, q	$N = p \times q$ (p and q: Prime numbers) $\rightarrow$ N cannot be set to an arbitrary value.
Elliptic curve cryptosystem	y	x	$y = x \cdot P$ (dot: Multiplication of elliptic curve by scalars) (P: Common public information) $\rightarrow$ y cannot be set to an arbitrary value.
Identity-based encryption	y	x	$x = s \cdot y$ (dot: Multiplication of elliptic curve by scalars) (s: Secret known only by the center) $\rightarrow$ y can be set to an arbitrary value (= identity).

While one of the purposes of the digital certificate used in the current PKI framework is to prevent spoofing by guaranteeing the relationship between the public key and its owner, identity-based encryption has a breakthrough feature that prevents spoofing even without a certificate since the owner information is embedded in the public key itself.

Meanwhile, the PKI framework, which was stan-

dardized long ago, has a legal basis, is deeply integrated in our daily life, and the certificate has a revocation mechanism. Therefore, the role of identity-based encryption will depend on future applications; it will not be a rival of PKI. Although the products using identity-based encryption are still low in number, research and development towards higher-speed encryption is also making rapid progress and the application of identity-based encryption to embedded systems is expected.

4. Conclusion

This paper explained the present state of security of encryption algorithms and future prospects for encryption technology while giving specific examples. We have proceeded with a comprehensive approach to encryption technology from the development of block encryption and construction of public key encryption and PKI to participation in standardization. We have also been focusing on encryption implementation and quantum encryption application for a long time.

Approaches to individual technologies described here are discussed in the papers of this June 2009 issue. For details, refer to the relevant papers.

References

(1) "Secure Hash Standard," FIPS Publication 180-2, NIST (2002).
(2) X. Wang et al., "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD," Cryptology ePrint Archive 2004/199 (2004).
(3) X. Wang et al., "New Collision Search for SHA-1," CRYPTO 2005 Rump Session (2005).
(4) "RSA-640 is factored," RSA laboratories homepage, http://www.rsa.com/rsalabs/node.asp?id=2964
(5) K. Ohgishi, R. Sakai and M. Kasahara, "Basic consideration on ID key sharing scheme on elliptic curves," ISEC99-57 (1999).
(6) D. Boneh et al., "Identity-based encryption from the Weil pairing," CRYPTO 2001 (2001).

Development of ID-Based Encryption

Authors: *Katsuyuki Takashima** and *Tsutomu Sakagami**

1. Introduction

The recent development of ID-based encryption is attracting attention because it enables the use of ID information as a public key. After the concept of ID-based encryption was first proposed by Shamir in 1984[1], many years passed before a working system was implemented by Sakai and Kasahara using their ID-based key sharing scheme in 1999[2] and Boneh et al. in 2001[3] using their ID-based encryption algorithm with proven security. In ID-based encryption, an important role is played by pairing operation on elliptic curves. In this paper, Section 2 provides a technical overview of ID-based encryption; Section 3 introduces our efficient pairing operation method; and Section 4 discusses an experimental encrypted mail system.

2. ID-Based Encryption

Each ID-based encryption system needs an ID-based private key generator (PKG), which generates a private key for an arbitrary ID. It consists of four functions: "parameter generation function" and "private key generation function" utilized by the PKG, and "encryption function" and "decryption function" utilized by the users.

- The parameter generation function uses the bit length of the key as input data to generate system parameters for use throughout the system and a PKG private key.
- The private key generation function generates a user private key from ID information provided using the system parameters and the PKG private key.
- The encryption function generates ciphertext from plaintext using the system parameters and the ID.
- The decryption function generates plaintext from ciphertext using the system parameters and the user private key.

Note that the ID, an input to the encryption function, is the public key. In an ordinary public key encryption scheme, a public key certificate, which is the signature to the public key, is used to ensure the validity of the public key for the encryption. In ID-based encryption, however, a public key certificate is not required because any ID can be made into a public key, which increases the convenience of this method.

For ID-based encryption to work properly, the abovementioned four functions must satisfy the following two conditions:

1. Properly ciphertext can be decrypted to the original plaintext.
2. Any private key corresponding to any ID other than ID_1 cannot retrieve any information about plaintext corresponding to ciphertext addressed to ID_1.

The second condition is the security requirement against collusion attacks.

3. Improved Algorithm for Pairing operation on Elliptic Curves

While various schemes have been proposed to realize an ID-based encryption system as described in Section 2, all of the practical schemes are based on pairing operation on elliptic curves.

An elliptic curve E is defined by $Y^2 = X^3 + aX + b$ (where a and b are elements in a finite field). For points P and Q on the curve, algebraic addition P + Q is defined. Also, pairing operation on E is given as a bilinear map$(P,Q) \rightarrow e(P, Q)$ where e(P, Q) is in (an extension of) the finite field. In the following discussion, specific pairing called "Tate pairing e" is treated. One of the properties of pairing e is bilinearity, which is the most important characteristic for ID-based encryption and is expressed as:

$$e(uP, vQ) = e(P, Q)^{uv}$$

Due to this bilinearity, ID-based encryption and various other crypto applications can be used in practice.

Pairing operation largely consists of Miller's algorithm and final exponentiation. Extensive studies have been made to improve the efficiency of Miller's algorithm in relation to the selection of relevant parameters.

A commonly used Miller's algorithm is Algorithm 1. While a detailed explanation is not included here, computation according to Algorithm 1 is performed using lines l and v that appear in the addition and doubling algorithm on the elliptic curve.

Many reports have been published on the improved efficiency of the above algorithm. We have modified the method proposed by Scott[5] so that the security can be flexibly adjusted, using a specific curve $Y^2 = X^3 + b$ where $p \equiv 1 \pmod 3$ is the order of the finite field, which allows fast computation. This curve has the map $(x, y) \rightarrow (\beta x, y)$, where β is a primitive cubic root of 1. Using this map, faster computation can be achieved.

*Information Technology R&D Center

Algorithm 1 Miller's algorithm

Input: Points P and Q on E.

Output: Miller variable.

1: Select a point S on E.
2: $Q' \leftarrow Q + S$, $T \leftarrow P$.
3: $i \leftarrow \lfloor \log_2(r) \rfloor - 1$, $f \leftarrow 1$.
4: **while** $m \geq 0$ **do**
5: Calculate lines l and v for doubling T.
6: $T \leftarrow 2T$.
7: $f \leftarrow f^2 \frac{l(Q')v(S)}{v(Q')l(S)}$.
8: **If** the i-th bit of r is 1, **then**
9: Calculate lines l and v for adding T and P.
10: $T \leftarrow T + P$.
11: $f \leftarrow f \frac{l(Q')v(S)}{v(Q')l(S)}$
12: **end if**
13: $i \leftarrow i - 1$.
14: **end while**
15: Output f.

Fig. 1 Miller's algorithm

4. Prototype Encrypted Mail System

An experimental encrypted mail system was constructed applying the ID-based encryption scheme. We developed an ID-based private key generator (PKG) and encrypted mail client that is utilized by the users to transmit/receive encrypted mail. The experimental system makes it possible to transmit and receive encrypted mail without managing public key certificates or advance sharing of passwords. Implementation of this system is described in the following sections.

4.1 PKG

For ID-based encryption, the keystone of the system is PKG. It plays an essential role in the overall operation of the ID-based encryption system including distribution of the system parameters pkeyPKG to users and generation of user private keys. In our experimental system, considering recent business network environments such as the use of firewalls and proxy servers, the http/https scheme is used as the protocol for encrypted mail clients to access the PKG. In addition, considering the need for complex data communication between the encrypted mail client and the PKG using http/https, SOAP is used as the protocol for inter-application communication. Since the http/https protocol is used as the low-level protocol, PKG is implemented as a servlet on the Web-based application server.

4.2 Encrypted mail client

Outlook 2003 is used as the encrypted mail client, because of its expandability with add-on features and our previous experience with feature expansion. Low-level library software is written in C/C++, and high-level GUI programs are in VB.

4.3 Data communication between PKG and mail client

The data format for communication between PKG and the mail client is defined using XML because SOAP over http/https is used as the low-level protocol.

4.4 Encrypted mail data

Encrypted mail transmitted from the encrypted mail client is formatted using Mitsubishi's proprietary capsular scheme. This capsular data format, which has long been studied at our laboratory, allows not only data encryption but the definition of usage restrictions on the received data (printable or not, copy/paste allowed or not, etc.).

4.5 Future prospects

Since ID-based encryption is a new encryption scheme, related standards are still under consideration by the IETF, including the method for distributing system parameters from PKG to the client, and how to transfer a private key from PKG to the client. The IETF is considering the Cryptographic Message Syntax (CMS) used in the Secure/Multipurpose Internet Mail Extension (S/MIME) with additional data format for ID-based encryption (see Reference (4)). Although our own scheme is used in the current implementation, we intend to develop a system that allows us to propose standardization to the IETF and that conforms to the standards.

5. Conclusion

Regarding ID-based encryption that uses ID information as the public key and allows easy introduction of public key encryption function, we proposed an improved algorithm and presented an experimental encrypted mail system.

References

(1) A. Shamir, "Identity-based cryptosystems and signature schemes," Crypto 84, pp. 47-53, Springer Verlag, 1985.
(2) K. Ohgishi, R. Sakai and M. Kasahara, "Basic consideration on ID key sharing scheme on elliptic curves," IEICE Technical Report, ISEC99-57, pp. 37-42, 1999.
(3) D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," Crypto 2001, pp. 213-229, Springer Verlag, 2001.

(4) IETF Internet Draft "Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the Cryptographic Message Syntax (CMS)."

(5) K. Takashima, "Scaling security of elliptic curves with fast pairing using efficient endomorphisms," IEICE Trans. on Fundamentals, Vol. E90-A, No. 1, pp. 152-159, Jan. 2007.

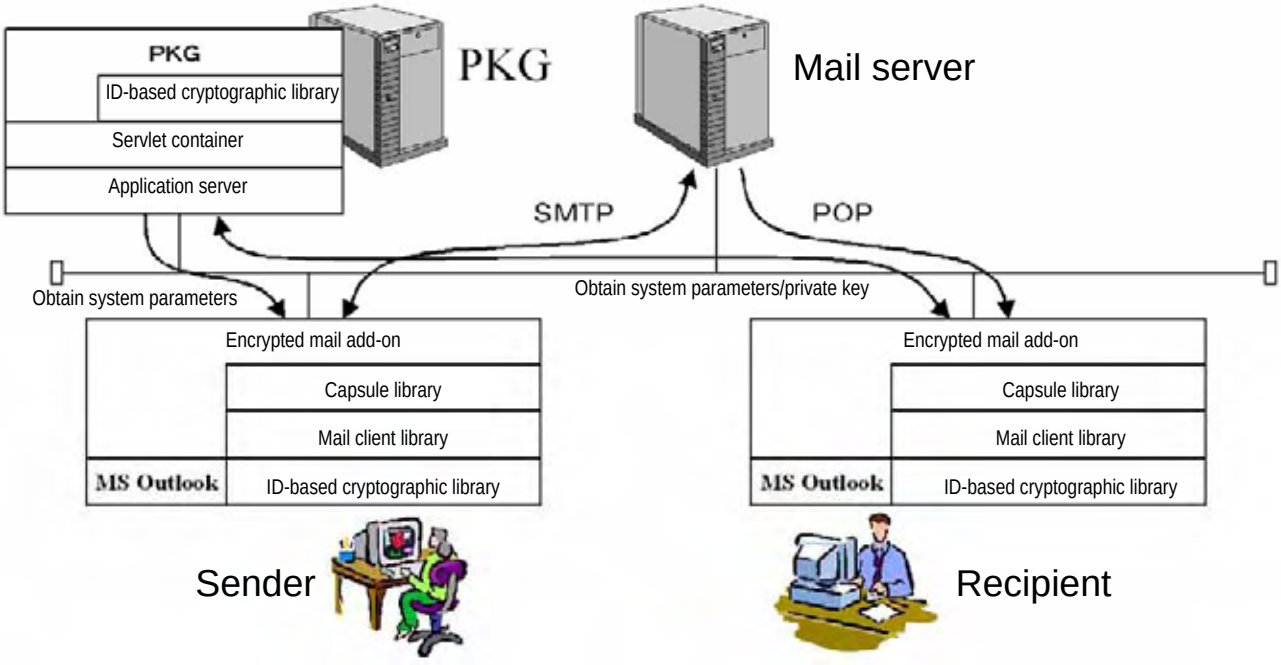


Fig. 2 Configuration of prototype ID-based encryption system

Research Activities in Quantum Cryptography and Security Analysis

Authors: *Toshio Hasegawa** and *Toyohiro Tsurumaru**

1. Introduction

Quantum cryptography is a technology that ensures ultimate security[1]. Compared to current cryptography that could be defeated by the development of an ultra high-speed computer, quantum cryptography ensures secure communication because it is based on the fundamental physical laws. Among the various quantum information technologies, the most extensive research is being conducted on quantum cryptography, including the development of experimental equipment, field tests, and discussions on proposals of new theoretical schemes. This paper outlines the domestic and overseas trends in research and development on quantum cryptography and presents our achievements and current efforts toward its practical application. The security analysis of quantum cryptography, which is attracting an increasing amount of attention, is also discussed.

2. Research and Development Trends

In experiments with quantum cryptography, phase modulation is often used as the coding method. In this case, an interferometer is configured (for example, a Mach-Zehnder type) and the interference effects are detected by a photon detector. In actual communication experiments, careful and improved preparation such as higher interferometer stability is required. Typical optical schemes include a one-way setup where the light source is placed on the sending side and the detector on the receiving side, and a two-way setup ("plug & play" system) where the light source and detector are both placed on the same side and the photons traverse the same path twice to compensate for fluctuation. In the "plug & play" system, when transmitting from Bob (the recipient) to Alice (the sender), fluctuating path lengths and polarization shifts in the optical fiber is compensated by that of the returning signal reflected by the Faraday mirror, resulting in a stable system. This high stability has made the plug & play system the mainstream until now. However, since the light source and the detector are both placed on the receiving side in this system, scattered light from the light source becomes a high-intensity input, which may increase the error rate and can be an obstacle for long-distance transmission. In addition, this system is vulnerable to one type of implementation attack (so-called "Trojan horse attack"), which creates a security issue. For these reasons, the one-way setup is more advantageous for longer-distance experiment and has been widely used in recent experiments. In this case, however, active compensation such as an optical path adjustment is required to maintain the stability of the interferometer.

Quantum cryptography experiments using optical fiber have been actively conducted, with several reports being published including one on a long-distance experiment over 100 km conducted at Toshiba Research Europe Ltd.[2] Field experiments between two remote points have also been conducted using existing optical fiber cables, including a 67-km experiment by the University of Geneva[3], a 96-km experiment by Mitsubishi Electric[4], and a 125-km experiment by the University of Science and Technology of China (USTC)[5]. Table 1 shows representative field experiments between two remote points using the Bennett-Brassard 1984 protocol (BB84 protocol, the de facto standard).

In the field test, it is important to establish synchronization between the transmitting and receiving equipment and achieve stability. The timing of photon detection must be adjusted to within an accuracy of several hundred picoseconds, which requires optical and timing synchronization as essential functions. For effective use of the transmission line, it is desirable to achieve syn-

Table 1 Representative quantum cryptographic system experiments using optical fiber
(Field test between two remote points)

Research institute (year)	Optical scheme	Wavelength (μm)	Transmission distance (km)	Error rate QBER (%)	Raw key transmission rate (bps)
Geneva (2002)	P&P	1.55	67 (Field)	6*	150*
Mitsubishi (2004)	P&P	1.55	96 (Field)	9.9	8.2
USTC (2004)	One-way	1.55	125 (Field)	6	–
Toshiba R.E. (2005)*	One-way	1.3/1.55	20.3 (Field)	0.87*	430*

* Experiment with average photon number of 0.2, double the ordinary case.

**Information Technology R&D Center*

chronization by sending a clock synchronization signal of high intensity, together with a quantum signal at the single-photon level. When this high-intensity clock synchronization signal is transmitted through an optical fiber along with the very weak quantum signal using a wavelength division multiplexing (WDM) technique, the technical challenge is to achieve high-isolation wavelength separation.

Progress in security analysis also continues, accompanied by proposals for new quantum cryptographic schemes. Formerly, the BB84 protocol and weak laser beam were used for most quantum cryptographic experiments at research institutes. However, this system is vulnerable to certain attacks called PNS (photon number splitting) attacks, which limits the transmission distance to less than 25 km if strict security standards are applied. To mitigate this drawback, it was, until recently, acceptable in the worldwide academic community to apply imperfect standards to practical quantum cryptography, which is that "a weak laser beam having an average photon number of 0.1 or less is assumed to be a single photon." Underlying such an assumption was an implicit common understanding: to achieve unconditional security for long-distance transmission, it is essential to have a strict single photon source, but this is difficult to realize. As a result, giving priority to the completion of a quantum cryptographic system, a weak laser has meanwhile been used for the light source to accelerate research on the detector, optical system and other elements. Once a low-cost single photon source eventually becomes available, it can be integrated into the system at any time.

This situation has changed greatly over the last several years since the "decoy method," an improved BB84 protocol, was proposed. With this method, unconditional security is achieved for long-distance transmission using a weak laser beam without a single photon source. With these developments, mainstream research is shifting its focus toward efficiently implementing an unconditionally secure quantum cryptographic system.

The basic setup for the decoy method is the same as that for the BB84 protocol except that Alice, the sender, changes the intensity of each light pulse intentionally and randomly. In addition, the distribution of light intensity will not be disclosed until Bob, the recipient, receives the light. Under this condition, Eve, the eavesdropper, is forced to attack without any knowledge about the intensity distribution. Therefore, if an attack is made, Bob finds statistical inconsistency in the signal detection rate. This enables accurate detection of the abovementioned PNS attacks and thus achieves more secure quantum cryptography. The unconditional security of the decoy method has been theoretically proved, and the achievable long distance is estimated to be approx. 140 km. In fact, an approx. 100-km optical fiber experiment and 144-km free space experiment have already been reported.

To achieve secure and long-distance implementation with equipment simpler than the decoy method, a "differential phase shift scheme" (DPSQKD protocol) has been proposed. The equipment setup for this protocol is the same as that for a conventional optical communication scheme (DPSK scheme), resulting in a relatively low-cost system configuration. The basic idea is that quantum mechanical effects clearly appear because of the extremely low light intensity, and thus the system can be used for quantum cryptography. The greatest difference from the BB84 protocol in terms of security is that the bit information of the private key is coded into multiple light pulses, and thus the effect from eavesdropping appears in multiple light pulses and is easy to detect. The proposers initially claimed that this system can provide communication distance and speed exceeding that of the decoy method. However, they did not rigorously prove system security and discussed it only within the limited conditions of "individual attacks." Based on such evaluation, they reported their experimental results and claimed the world's longest distance of 100 to 200 km. After that, as a result of rigorous security analysis conducted by Mitsubishi Electric, it was found that the quantum cryptography in these experiments was not secure and that the communication distance using the DPSQKD protocol only reached 95 km[6] in practical experimental setups which are commonly used today. Since this scheme was found to be unsuitable for long-distance communication, discussion is now focused on the security of high-speed communication over short distances.

3. Research and Development at Mitsubishi Electric

3.1 Activities up to 2005

In 1999, Mitsubishi Electric started R&D activities of quantum cryptography, and in 2000, in collaboration with Hokkaido University, successfully conducted experiments on short-wavelength (830 nm) quantum cryptographic communication[7]. In 2001, Mitsubishi was awarded a 5-year commission under the NICT (National Institute of Information and Communications Technology) Project I entitled "Research and Development on Quantum Cryptography," together with NEC and the University of Tokyo. In this project, Mitsubishi was responsible for "single photon generation," "single photon detection," "random number generation" and "technology for the quantum cryptographic key distribution system." Since then, our achievements include 1,550-nm high-performance single-photon detectors (dark count probability of approx. 10^{-6}, detection efficiency of approx. 20%) and experiments using these

detectors on an 87-km long-distance quantum cryptographic communication system[8] in 2002, and practical field experiments using the existing 96 km of optical fiber between Osaka and Kyoto in 2004[4]. In the final year of the project, we also developed and functionally tested WDM quantum cryptographic equipment using 4 wavelengths to achieve higher speed. In addition to these achievements, Mitsubishi Electric also proposed a "circular-type quantum key distribution scheme" in the area of new optical scheme protocol studies, and conducted experiments on the proposed system to demonstrate transmission speed faster than that in conventional methods as well as multi-user communication capability[9]. Mitsubishi Electronic has actively participated in international exhibitions (ITU Telecom World 2003, 2006; RSA Conference 2005 Japan, etc.), presenting our quantum cryptographic system and quantum encrypted secure voice telephone / videophones as practical application examples.

3.2 Research and development for practical application

In 2006, we were awarded a 5-year commission under the NICT Project II entitled "Research and Development for Practical Applications of Quantum Cryptography." In this project, we have been working on the development of high-speed and high-stability quantum transmission technology, and key management and security evaluation technology, which will be required to realize a quantum cryptographic network. The quantum cryptographic equipment under development has a practical performance target: communication distance of 50 km and speed of 1 Mbps, and the following features: (1) Time-division transmission of the classical signal and the quantum signal (the classical signals are high intensity pulses, that is, they have a light strength similar to those used in conventional optical communications, and they carry the system clock information and the information to compensate for fluctuation in the polarization. On the other hand, the quantum signals are extremely weak laser pulses at the single-photon level which carry secret key bits.) (2) High-speed equipment with light source repetition rate at the GHz level, and transmission distance of several dozen km using BB84, decoy, or DPSQK quantum cryptographic protocol.

3.3 Development of multiplex transmission of quantum and classic signals

The key technology is the separation of multiplexed quantum and classical signals using time-division multiplexing. Specifically, we have developed and implemented a method to compensate for environmental temperature change and polarized state fluctuation, which is achieved through synchronized gate control and feedback control by monitoring the clock and polarized state information contained in the classical signal. A very weak light at the single photon level is used for the quantum cryptographic communication, whereas a high-intensity signal at the classical optical level is used for the control of the communication equipment. The conventional way to provide a transmission line for this classical signal is to use a physically separated line or to separate the classic and quantum signals using WDM on a physically common line. However, the former poses a problem with facility cost, and the latter involves the difficult issue of separating the quantum and classical signals. Therefore, we are striving to develop such equipment that transmits and separates quantum and classical signals by WDM and time-division multiplexing (TDM) on a physically common transmission line. The equipment using TDM utilizes the classical control signals to compensate for the optical fiber propagation characteristics (polarized state fluctuation, etc.) and to transmit the clock signal. We also plan to transmit path control information with a view to networking applications.

3.4 Development of high-speed optical system equipment

Combining the multiplex transmission of quantum and classical signals and the high-speed single-photon detection technologies, we studied an experimental optical system required to achieve one of the final objectives of 1 Mbps at 50 km (see Fig. 1). This equipment features high-speed quantum cryptography using applicable protocol based on the BB84, decoy or DPSQKD protocol, light source repetition rate at the GHz level, and transmission distance of several dozen km. We also studied circuit-board partitioning by system functions that provides efficient configuration of the optical and electronic control system. Specifically, we further divided the transmitting and receiving functions and adopted AdvancedTCA to configure the circuit-board modules. The quantum and classical light sources are designed using DWDM CW DFB laser modules with wavelength of 1550.918 nm (classical signal) and 1549.315 nm (quantum signal), and driving frequency up to v = 1 GHz. To separate wavelength-multiplexed signals, DWDM DEMUX is designed for channel isolation between two signals of 80 dB or greater, which will be tested in the experimental system to determine if the weak quantum signal is accurately separated from the strong classical signal.

3.5 Security analysis technology

In parallel with the experiments, Mitsubishi Electric has also been conducting theoretical studies on system security. Recent achievements, as described at the end of Section 2, include a proposal related to a new attack

method against DPSQKD protocol and security analysis results based on the proposal[6]. Theoretical study is also being conducted in collaboration with Hokkaido University on the decoy method, and, in 2007, we developed a new mathematical analysis method that precisely estimates the upper and lower bounds of the "yield" parameter[10]. This achievement is expected to further enhance the communication distance and speed of the decoy method.

Theoretical studies have also been conducted on general quantum cryptographic protocols including authentication and signature not limited to quantum key distribution. Achievements in this area include quantum bit-string commitment[11].

4. Summary and Future Prospects

In this paper, we presented research and development trends and Mitsubishi Electric's achievements and current R&D status on quantum cryptography. We also described the security analysis technology. Such theoretical analysis is important because quantum cryptography carries meaning only when its security is theoretically proven, and also for promoting steady and efficient development of actual quantum cryptographic equipment. Even today, the search for a new method continues and in addition to the decoy method and DPSQKD protocol as presented in this paper, new protocols such as the six-state protocol and continuous-variable protocol are being proposed. However, proof of security has not kept pace with new proposals, and protocols that are proven to have unconditional security are in the minority. It is important to understand the trend in security analysis and we will continue to strive toward our own research goals.

Part of this work was supported by the project "Research and Development on Quantum Cryptography" of National Institute of Information and Communications Technology as part of Ministry of Internal Affairs and Communications of Japan's program.

References

(1) Edited by Sasaki et al., Quantum Information Communication, Optronics Co., Ltd. (2006)
(2) C. Gobby et al., Appl. Phys. Lett. 84, 19, 10 (2004)
(3) D. Stucki et al., New J. Phys. 4, 41 (2002)
(4) T. Hasegawa et al., CLEO/Europe-EQEC2005, EH3-4, Munich (2005)
(5) X. Mo et al., Opt. Lett. 30, 2632 (2005)
(6) T. Tsurumaru, Phys. Rev. A 75, 062319 (2007)
(7) T. Hasegawa et al., IEICE E85-A No. 1, 149 (2002)
(8) T. Hasegawa et al., CLEO/QELS2003, QTuB1, Baltimore (2003)
(9) T. Nishioka et al., IEEE PTL 14, 4 (2002)
(10) T. Tsurumaru et al., Phys. Rev. A 77, 022319 (2008)
(11) T. Tsurumaru, Phys. Rev. A 71, 012313 (2005) and 74, 042307 (2006)

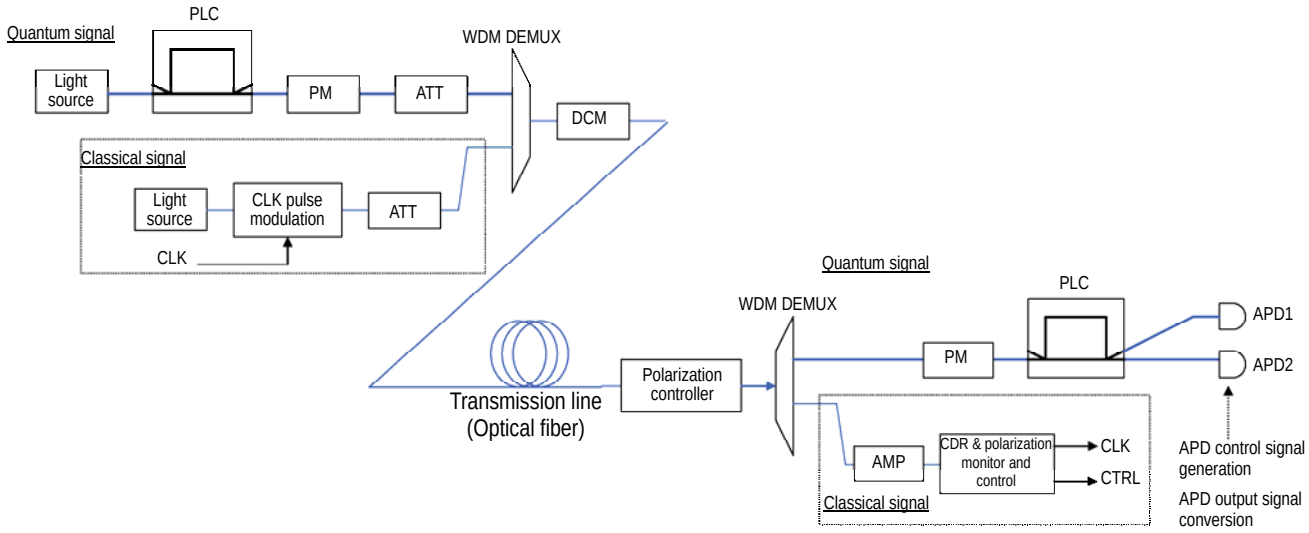


Fig. 1 Basic configuration of the quantum cryptographic system under development

PLC: planar light circuit, PM: phase modulator, ATT: optical attenuator, CLK: clock, WDM MUX: wavelength division multiplexing, DCM: dispersion compensation module, AMP: optical amplifier, CDR: clock data recovery, APD: avalanche photodiode

Hardware Implementation of Cryptographic Algorithm

Author: *Daisuke Suzuki**

1. Introduction

Extensive research has been conducted on the hardware implementation of high-speed public key cryptosystems represented by RSA cryptography. In particular, various circuit architectures have been proposed for the processing of Montgomery multiplication(1). The Virtex-4 series and Spartan-3A DSP series released by Xilinx, Inc., a FPGA vendor, are equipped with a functional block (instead of a conventional multiplication unit) as a hardware macro, and they support dynamic changes in multiple-pattern multiplicative summation (henceforth called the "digital signal processing (DSP) function"). Some applications of this DSP function have already been reported, such as fast finite impulse response (FIR) filters and image processors; however, we believe that no cryptographic algorithms using this function have yet been reported, with the exception of the simple usage of such. This paper describes a modular exponentiation processing method and circuit architecture that can derive the maximum performance from this DSP function.

2. Processing Method

Montgomery multiplication is a high-speed processing method for modular exponentiation, which is heavily used in the field of public key cryptosystems. While Montgomery multiplication has many variations, we chose a processing method described in Ref. (2) and expanded its processing unit and flow. We also enhanced the FPGA hardware macros to provide more efficient usability. Figure 1 shows this processing method, which features the following three key improvements.

First improvement: For each multiple-length addition operation, additions for 2 blocks (34 bits) are performed in one loop, whereas each multiple-length multiplication operation is performed in a half loop count (αr/2). This improvement, with the DSP48 being operated at the maximum frequency and other user logics at half frequency, eases the timing constraint on the circuits that are configured without using hardware macros, and allows the configuration of realistic circuits, while maintaining overall throughput. Second: By introducing branching control, Algorithm 1 can be processed in pipeline without any stalling in the process flow. Third: The number of DSP48 units used, α, is fixed in this algorithm, and thus the same circuit can be used for input of different bit lengths.

Algorithm 1 Montgomery Multiplication for Virtex-4

Setting: radix: $2^k(=2^{17})$, delay parameter : $d(=1)$, no. of DSP48s : $\alpha(=17)$, $2 < M < 2^h$ ($h \in \{512, 1024, 1536, 2048\}$), $\gcd(M,2) = 1$, $(-MM' \bmod 2^{k(d+1)}) = 1$, $\tilde{M} = (M' \bmod 2^{k(d+1)})M$, $0 \le A, B \le 2\tilde{M}$, $h' = h + k(d+1) + 1$ no. of words at A and B: $n = \lceil h'/k \rceil$, no. of words processed by one DSP48 : $r = 2\lceil(\lceil n/\alpha \rceil)/2\rceil$ ($r \in \{2,4,6,8\}$), $A = \sum_{j=0}^{\alpha r-1}(2^k)^j a_j$, $B = \sum_{j=0}^{n+d}(2^k)^j b_j$, $M'' = \sum_{j=0}^{\alpha r-1}(2^k)^j m_j$, $S_i = \sum_{j=0}^{\alpha r-1}(2^k)^j s_{(i,j)}$, $a_j, b_j, m_j, s_{(i,j)} \in \{0, 1, \cdots, 2^k - 1\}$, $a_j = b_j = 0$ for $j \ge n$ and $m_j = 0$ for $j \ge \lceil h/k \rceil$.
Input: A, B, M''
Output: $\mathrm{MM}(A,B) = S_{n+3} \equiv ABR^{-1} \bmod M$, $0 \le S_{n+3} \le 2\tilde{M}$

```
1: S_0 := 0; q_{-1} := 0;
2: for i = 0 to n + 1 do
3:    carry := 17'b0; cv := 1'b0; cs := 1'b0;
      /* Multiple-length multiplication: MUL_AB */
4:    for j = 0 to αr − 1 do
5:       carry||p_j := b_i a_j + carry;
6:    end for
      /* Multiple-length multiplication: MUL_MQ */
7:    for j = 0 to αr − 1 do
8:       if j = 0 then
9:          carry||v_0 := q_{i−d} m_j + p_0;
10:      else
11:         carry||u_j := q_{i−d} m_j + carry;
12:      end if
13:   end for
      /* Calculation q_i: ADD_V0S1 */
14:   q_{i+1} := v_0 + s_{(i,1)};
      /* Multiple-length addition: ADD_PU */
15:   for j = 0 to αr/2 − 1 do
16:      if j = 0 then
17:         cv||v_1||v_0 := (p_1||17'b0) + (u_1||v_0);
18:      else
19:         cv||v_{2j+1}||v_{2j} := (p_{2j+1}||p_{2j}) + (u_{2j+1}||u_{2j}) + cv;
20:      end if
21:   end for
      /* Multiple-length addition: ADD_VS */
22:   for j = 0 to αr/2 − 1 do
23:      cs||s_{(i+1,2j+1)}||s_{(i+1,2j)} := (v_{2j+1}||v_{2j}) +
                                             (s_{(i,2j+2)}||s_{(i,2j+1)}) + cs;
24:   end for
25: end for
26: S_{n+3} := S_{n+2}||s_{(n+1,0)};
27: return S_{n+3};
```

Fig. 1 Montgomery multiplication algorithm for Virtex-4

3. Hardware Configuration

Figure 2 shows the basic circuit that performs each processing task of Algorithm 1. Input A and M" are entered every 34 bits (2 blocks) at a time from left to right and stored in each specified DMEM. Only A is updated for each Montgomery multiplication. DMEM is implemented using a single port memory. Once a_j ($0 \le j$

*Information Technology R&D Center

≤ r–1) is stored in the leftmost DMEM, the circuit connected to it begins processing according to Algorithm 1. The DSP48 that performs multiplication of the least significant block (MUL_AB and MUL_MQ) switches the calculation type depending on whether the carry bit is on or off.

ADD_PU is performed by the circuit consisting of the adders and LA1s (Latency Adjuster) shown at the center in Fig. 2. First, two blocks of the result from MUL_AB calculation are provided at the same time from the DSP48 and entered into the adder at the negative edge of the clock (clk1). At this time, by resetting all other inputs to zero, the calculation result from MUL_AB is stored in LA1 as it is. Then the calculation result from MUL_MQ is added to the calculation result from MUL_AB already stored in LA1. At this time, the difference between the input timing of MUL_AB and MUL_MQ is r/2 cycle. Carry propagation from the addition is one of two cases: propagation to the same adder or to the next adder. For the circuit shown in Fig. 2, a flip-flop to store the carry is implemented for each case to improve the timing.

The circuit shown at the bottom in Fig. 2 performs ADD_VS calculation. This circuit performs simultaneous addition of two blocks, $s_{(i, 2j + 1)}$ and $s_{(i, 2j + 2)}$, which are respectively provided from LA1 and LA2 at the timing when the calculation result is provided from ADD_PU. For more details about the hardware configuration, see Ref. (3).

4. Hardware Performance

This section describes the characteristics of a prototype circuit for modular exponentiation based on the Montgomery multiplication circuit shown in Fig. 2. In Table 1, a comparison is made between the results of the circuit placed and routed using XC4VFX12-10SF363 as the target device and the previous research results. To the best of our knowledge, this is the world's fastest processing performance for a modular exponentiation using FPGA. This circuit can be implemented on FPGA having the smallest logic scale among the Virtex-4 series. In addition, modular exponentiation from 512 to 2048 bits can be performed on the same circuit, providing high scalability.

Table 1 Characteristics of prototype circuit and comparison with previous research results

Architecture	Proposed method	Reference[4]	Reference[5]
Target device	XC4VFX12-10	XC2V3000-6	XC40250XV
Scalability	Y	N	N
512 bit MEX time	0.26 ms (max)	0.59 ms (avr)	2.93 ms (max)
512 bit MEX area	3937 slices + 17 DSP48	8235 slices + 32 multipliers	3413 slices
1024 bit MEX time	1.71 ms (max)	2.33 ms (avr)	11.95 ms (max)
1024 bit MEX area	3937 slices + 17 DSP48	14334 slices + 62 multipliers	6636 slices

* MEX: Modular exponentiation

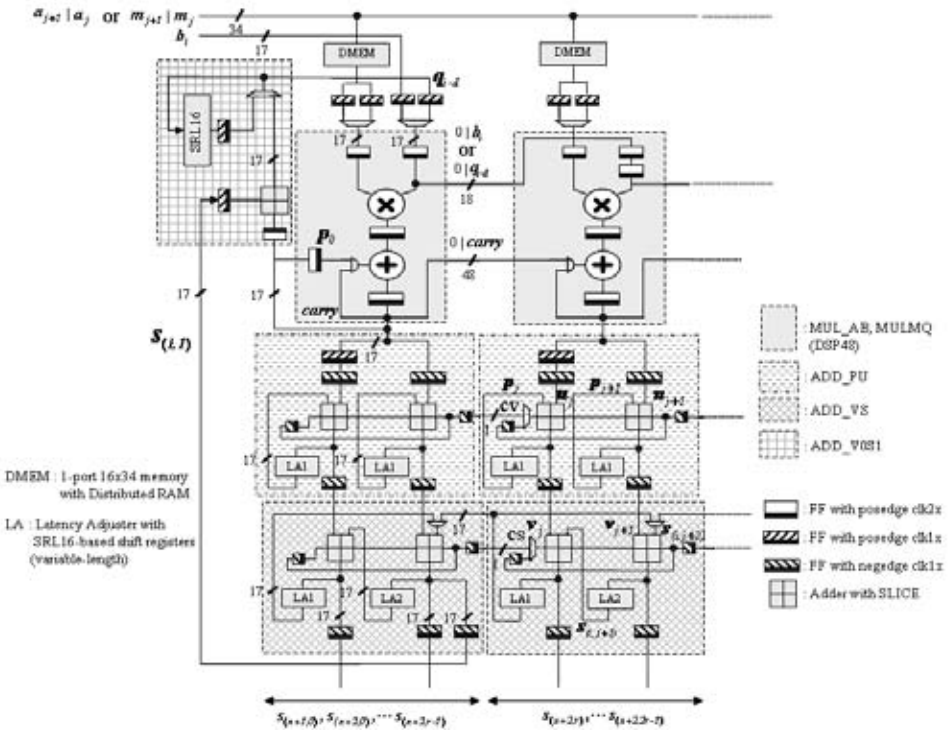


Fig. 2 Montgomery multiplication circuit

5. Conclusion

This paper presented hardware implementation technology for cryptographic algorithms using an example of high-speed hardware for public key cryptosystems. In addition to this example, we have also developed block cipher and stream cipher circuits, a hash function circuit, and other hardware setups required for the construction of security systems. We will strive to develop fully optimized applications using these hardware implementation technologies.

References

(1) Montgomery, P.L.: Modular Multiplication without Trial Division. Mathematics of Computation, Vol. 43, No. 170, pp. 519-521, 1985.
(2) Orup, H.: Simplifying quotient determination in high-radix modular multiplication, Proc. of the 12th Symposium on Computer Arithmetic, pp. 193-199, 1995.
(3) Suzuki, D.: How to Maximize the Potential of FPGA Resources for Modular Exponentiation. CHES 2007, LNCS, Vol. 4727, pp. 272-288, 2007.
(4) Blum, T., Paar, C.: High-Radix Montgomery Modular Exponentiation on Reconfigurable Hardware, IEEE Transactions on Computers, Vol. 50, No. 7, pp. 759-764, 2001.
(5) Tang, S.H., Tusi, K.S., Leong P.H.W.: Modular Exponentiation using Parallel Multipliers, FPT 2003, pp. 52-59, 2003.

Performance Evaluation of Block Encryption Algorithms on Core 2

Authors: *Junko Nakajima** and *Mitsuru Matsui**

1. Introduction

This paper presents the high-speed software encryption technique, "bit-slice implementation," on Intel's new Core 2 processor, which is its first micro-architecture platform. Until now, the performance of leading-edge processors has been evaluated and compared by implementing encryption algorithms and various benchmark tests. From the standpoint of encryption implementation, it is important to study the best implementation method together with platform migration because the execution speed of the same program can change completely depending on the architecture.

In 1997, Biham proposed bit-slice implementation, where multiple blocks are processed in parallel by assuming a single software instruction with n-bit-long registers as n-sets of hardware logic gates. Therefore, when this method is used to implement an encryption algorithm on a small-sized hardware and target processor with many registers, faster speed is expected. This method has an additional advantage of providing security against side-channel attacks such as cache attacks because there is no need to refer to the tables depending on the key value.

Until now, bit-slice implementation has demonstrated its effectiveness on reduced instruction set computer (RISC) processors, whereas PC (x86) processors are considered to be unsuitable for this implementation because of the increased frequency of memory access due to few available registers, resulting in a bottleneck to the execution speed. This time, we focused on the new feature of the Core 2, that is, the significantly enhanced single instruction multiple data (SIMD) instructions compared to the Pentium 4 and Athlon 64, which is expected to improve the performance of bit-slice implementation. Consequently, we studied the software implementation and speed-up techniques of block encryption schemes (MISTY, KASUMI, AES, and Camellia) taking into account the processor architecture in a 128-bit environment.

2. Core 2 Architecture

To reduce power consumption, the design concept of the Core 2's architecture was shifted to increasing scalability rather than frequency, resulting in 14 pipeline stages. This number is less than half that of the conventional Pentium 4 core (Prescott core). Decoding is now performed online, similar to the Pentium III, not using the trace cache. The Core 2 has also enhanced the fusion functions used in the Pentium M, and fused μ-ops have become quite similar to the macro-operation of the Athlon 64.

Table 1 shows a listing of instruction latency and throughput obtained by experiment. It is evident from this table that the throughput of logic operation instructions, which was below 2 μ-ops/cycle with the x64 instructions of the Pentium 4, is now improved to 3 μ-ops/cycle with the Core 2; and the latencies of right shift and left/right rotate instructions, which were extremely long with the Pentium 4, are now much improved with the Core 2. In addition, for the XMM instructions, throughputs of register-to-register move and logic operation instructions are improved from 1 to 3; and the latencies are also improved, achieving nearly the same performance as x64 instructions. In contrast, the greatest performance bottleneck for the Core 2 seems to be caused by the instruction fetch being limited to 16 bytes per cycle. To speed up a program, certain techniques are required, such as making the instruction length as short as possible.

Table 1 Instruction latency and throughput

Processor	Pentium4 561	Athlon64 3500+	Core2 Duo E6400
Operand type	64-bit general registers		
mov reg,[mem]	4, 1	3, 2	3, 1
mov reg,reg	1, 3	1, 3	1, 3
add reg,reg	1,2.88	1, 3	1, 3
xor/and/or reg,reg	1, 7/4	1, 3	1, 3
shr reg,imm	7, 1	1, 3	1, 2
shl reg,imm	1, 7/4	1, 3	1, 2
ror/rol reg,imm	7, 1/7	1, 3	1, 1
Operand type	128-bit XMM registers		
movaps xmm,[mem]	-, 1	-, 1	-, 1
movaps xmm, xmm	7, 1	2, 1	1, 3
paddb/w/d xmm,xmm	2, 1/2	2, 1	1, 2
paddq xmm,xmm	5, 2/5	2, 1	1, 1
xorps/andps xmm,xmm	2, 1/2	2, 1	1, 3
psllw/d/q xmm,imm	2, 2/5	2, 1	2, 1
pslldq xmm,imm	4, 2/5	2, 1	2, 1
punpcklbw/wd/dq xmm,xmm	2, 1/2	2, 1	4, 1/2
punpcklqdq xmm,xmm	3, 1/2	1, 1	1, 1
pmovmskb reg,xmm	-, 1/2	-, 1	-, 1

3. MISTY and KASUMI

KASUMI is a 64-bit block encryption algorithm used as the standard in the Universal Mobile Telecommunications System (UMTS) / Global System for Mobile

*Information Technology R&D Center

Communications (GSM). The design of KASUMI is based on MISTY and because its structure is suited for hardware, faster speed by using bit-slice implementation can be expected. The left side of Fig. 1 shows the FI function of KASUMI, and the right-hand side shows that the number of instructions required by the FI function can be reduced by an equivalent transformation. Both MISTY and KASUMI have two kinds of S-boxes, S7 and S9, within the dominant inner function FI. While MISTY has three S-boxes (S7 – S9 – S7), KASUMI has two of each kind, for a total of four S-boxes, resulting in a difference in the total number of table references (KASUMI = 96, MISTY = 76), which becomes the defining factor for KASUMI's slower encryption speed compared to MISTY. On the contrary, KASUMI's key scheduling time is much shorter than the encryption time because bit-slice implementation does not require any shift/rotate operations. Bit-slice implementation of KASUMI provides an encryption speed 4 times faster and key scheduling speed at least 30 times faster than with normal implementation (Table 2).

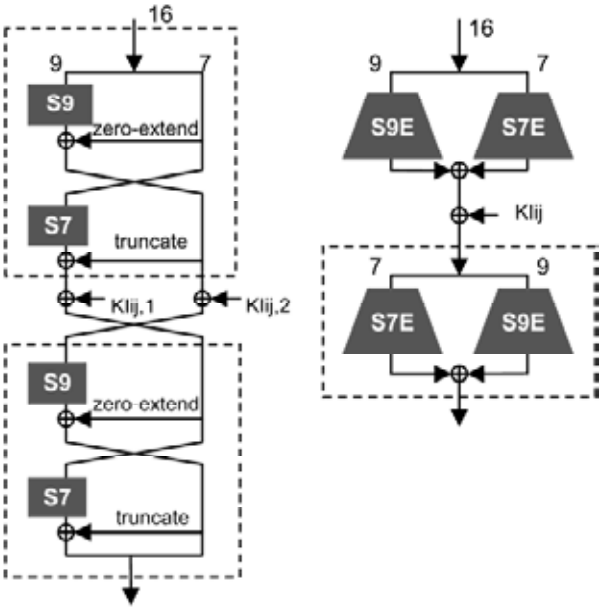


Fig. 1 Equivalent forms of the FI function of KASUMI

Table 2 Implementation performance of KASUMI and MISTY1

Processor	Pentium4		Athlon64		Core2	
KASUMI						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/blk	241	300	241	272	**74**	290
Cy/byte	30.1	37.5	30.1	34.0	**9.25**	36.3
Inst/cycle	0.71	1.69	0.71	1.86	**2.31**	1.75
Cy/Keysch	8	104	7	64	**2**	78
MISTY1						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/block	185	234	195	203	**59**	214
Cy/byte	23.1	29.3	24.4	25.4	**7.38**	26.8
Inst/cycle	0.72	1.82	0.68	2.10	**2.26**	1.99
Cy/Keysch	57	244	57	240	**16**	178

4. AES and Camellia

Both AES and Camellia use linearly equivalent S-boxes for the inversion functions of GF (2^8). The number of instructions for this calculation has a dominant influence on the overall calculation speed. From the standpoint of bit-slice implementation, the smallest S-box we are aware of uses subfields, where the inversion functions of GF (2^8) are configured by the operations of GF (2^4), and the operations of GF (2^4) is in turn configured by the operations of GF (2^2)[5]. In the case of bit-slice, there are approx. 200 instructions for one S-box, and considering that AES and Camellia respectively refer to the S-box 160 and 144 times per one block, the total processing amount for the S-box, e.g. for 128 blocks of parallel processing, would be 250 and 225 instructions per one block, respectively, which accounts for approx. 70% of the overall instructions. A performance comparison between the Core 2 and Pentium 4 in normal implementation shows that the Core 2 requires a slightly smaller cycle count per block, but a comparison with the Athlon 64 still shows a significant performance difference.

The reason for the difference is that the Athlon 64 can perform 64-bit memory read operations twice per cycle compared to only once per cycle for the Core 2. In contrast, in the case of bit-slice implementation using 128-bit XMM registers, the effect of enhanced SIMD instructions for the Core 2 becomes evident. This implementation provides more than 50% faster speed compared to that with normal implementation, and performance that is twice as fast as that with bit-slice implementation using 64-bit general registers, which directly reflects the register size being doubled from 64 bits to 128 bits. Considering that the speed of the Pentium 4 and Athlon 64 with bit-slice implementation is 50% slower than with normal implementation, the performance improvement of the Core 2 SIMD instructions is remarkable. Until now, Camellia's performance has never approached that of AES on any platform in normal implementation, but the implementation results for Camellia show that with the two-block parallel imple-

Table 3 Implementation performance of AES and Camellia with 128-bit key

Processor	Pentium4		Athlon64		Core2	
AES						
Style	BS	Sing	BS	Sing	BS	Sing
Cy/blk	491	256	560	170	**147**	232
Cy/byte	30.7	16.0	35.0	10.6	**9.19**	14.5
Inst/cycle	0.80	1.18	0.70	2.74	**2.66**	2.00
Camellia						
Style	BS	Doubl	BS	Doubl	BS	Doubl
Cy/blk	467	457	510	175	**135**	208
Cy/byte	29.2	28.6	31.9	10.9	**8.44**	13.0
Inst/cycle	0.72	0.94	0.65	2.46	**2.47**	2.07
Format conversion						
Cy/blk	41.5		28.1		15.4	
Cy/byte	2.59		1.76		0.96	
Inst/cycle	0.72		1.06		1.96	

mentation on the Core 2, Camellia (Table 3; Double) surpasses AES (Single). With bit-slice implementation, Camellia is faster than AES on any processor, which is mostly attributed to the fact that Camellia has 16 units fewer S-boxes.

Bit-slice operations are performed in special data format, which necessitates format conversion to maintain compatibility. This conversion requires the repositioning of all data bits and hence considerable computation time, which was one of the factors hindering practical application of the bit-slice technique. This time, bit-slice implementation on the Core 2 has achieved the performance of one cycle or less per byte, which is much faster than with normal implementation even when pre- and post-format-conversion time is added.

5. Conclusion

In this paper, the superior performance of Intel's latest processor, Core 2, in particular its SIMD instructions, was described from the viewpoint of bit-slice implementation of block encryption algorithms. It was clearly shown that AES performance with bit-slice implementation on a PC processor is higher than that with normal implementation. This fact, together with the security advantage of the bit-slice technique against implementation attacks such as cache attacks, may create a turning point in discussions on the application of public key cryptography (such as usage mode).

References

(1) M. Matsui: New encryption algorithm MISTY (1997)
(2) 3GPP TS 35.202 v6.1.0: 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification (2005)
(3) K. Aoki, et al.: The 128-Bit Block Cipher Camellia (2002)
(4) Federal Information Processing Standards Publication 197: Advanced Encryption Standard (2002)
(5) M. Matsui: How Far Can We Go on the x64 Processors? (2006)

Information Security for Mitsubishi Digital CCTV System MELOOKμ

Authors: *Teruyoshi Yamaguchi*, Hironobu Abe** and *Tomohiro Ueda***

1. Introduction

Mitsubishi Electric has developed a new digital closed-circuit television (CCTV) system MELOOKμ featuring the simple introduction of a video surveillance system, and an easy-to-use video information management system. MELOOKμ not only records and displays high-definition images, but also protects against eavesdropping of stored images through the use of Mitsubishi Electric's encryption technology MISTY. This paper presents the security features of MELOOKμ.

1. Mitsubishi Digital CCTV System MELOOKμ

1.1 Configuration of MELOOKμ

The digital CCTV system MELOOKμ consists of a mega-pixel recorder, up to eight mega-pixel cameras, and up to eight units of DIGITAL MELOOK series network cameras. The mega-pixel recorder is connected with these cameras to collect, store and display video images. The mega-pixel cameras are directly connected to the mega-pixel recorder, whereas the DIGITAL MELOOK series network cameras are connected to the recorder via a switching hub. Video images stored in the recorder can be copied to DVDs as required. (Fig. 1)

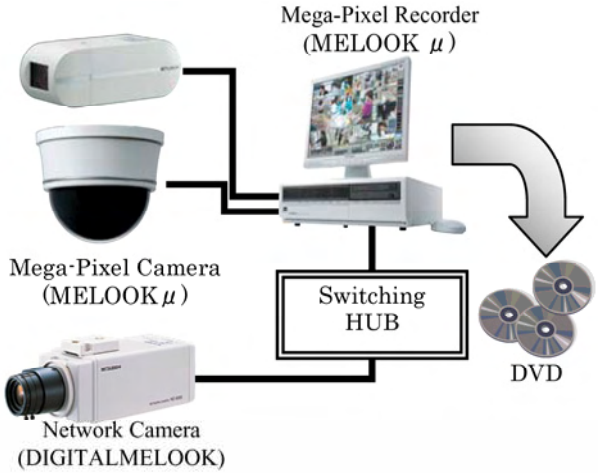


Fig. 1 Mitsubishi digital CCTV system MELOOKμ

1.2 Security features of MELOOKμ

MELOOKμ encrypts captured video images in real time before storing them to protect the accumulated data. When encrypted video images are displayed, they are decrypted in real time. They are copied to DVD or other media as encrypted. Since the video images are encrypted when stored, they cannot be directly viewed with an ordinary file viewer unless a legitimate method is used. As a result, even if a DVD or HDD is stolen, the stored video information is protected. (Fig. 2)

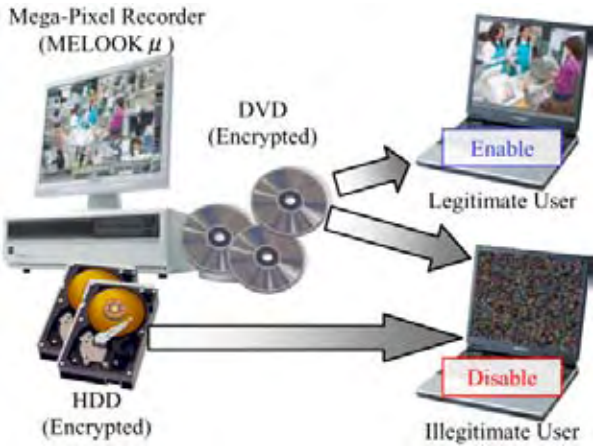


Fig. 2 Image data encryption in MELOOKμ

In addition, the mega-pixel recorder performs user authentication to control access. The access control function restricts user's operations. Access to the DVD data is available by proprietary viewer software, which is included when the video images are copied to DVD. User authentication is also performed when a DVD is played back. (Fig. 3)

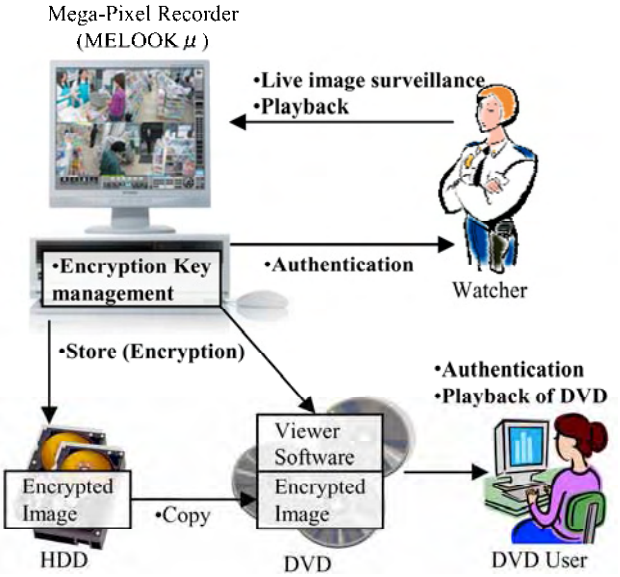


Fig. 3 Security functions in MELOOKμ

**Information Technology R&D Center **Communication Networks Center*

2. Security Technologies in MELOOKμ

2.1 Encrypted storage

In a digital CCTV system, a large amount of video data captured by camera must be stored and displayed at a high speed. MELOOKμ encrypts mega-pixel quality (SXVGA, Super Extended Video Graphics Array) video data for storage, and decrypts it for display. As a consequence, high-speed encryption and decryption are required.

The MELOOKμ requires a cryptographic performance of 80Mbps[1] at maximum. In addition, MELOOKμ must perform other processing tasks besides cryptographic processing. Therefore, the load of cryptographic processing should be kept as low as possible. Generally, it is necessary to use dedicated hardware to meet these requirements.

To realize low-cost cryptographic equipment by achieving hardware-level performance using a software process, Mitsubishi Electric has developed a new cryptographic algorithm, BROUILLARD, which belongs to the MISTY family and provides both high-speed processing and sufficient security.

BROUILLARD achieves high-speed and secure operation by means of random access within a large memory space. BROUILLARD realizes an encryption speed of 8 Gbps through implementation on the Pentium 4 (3 GHz).

MELOOKμ applies BROUILLARD to realize an encryption speed of 80 Mbps through software.

2.2 Encryption key management

The mega-pixel recorder encrypts and accumulates video image data in mass storage, and strictly controls the key information used for encryption as well as provides authorized users with easy-to-use key information.

The mega-pixel recorder randomly generates image encryption key when the system is initially booted up, and thus the probability that two recorders have identical key is extremely low. With this mechanism, video images encrypted on a certain recorder cannot be opened on other recorders. The image encryption key generated in this manner is encrypted by multiple parameters and stored in multiple non-volatile areas. The encryption keys stored in the non-volatile areas are all encrypted and thus secure against illegal extraction of data from non-volatile areas.

When the mega-pixel recorder is booted up in a normal mode, encrypted image encryption key is retrieved from the system area and decrypted. Using the decrypted image encryption key, the video images are actually encrypted.

When a user copies their images to DVD, the encrypted image encryption key, encrypted images, and viewer software are copied. When the DVD is replayed, the viewer software is activated, and then the password is entered. If the entered password is correct, the image encryption key is decrypted, then the encrypted images are decrypted and played back. If the password is invalid, the image encryption key cannot be decrypted, inhibiting the playback of encrypted images. (Fig. 4)

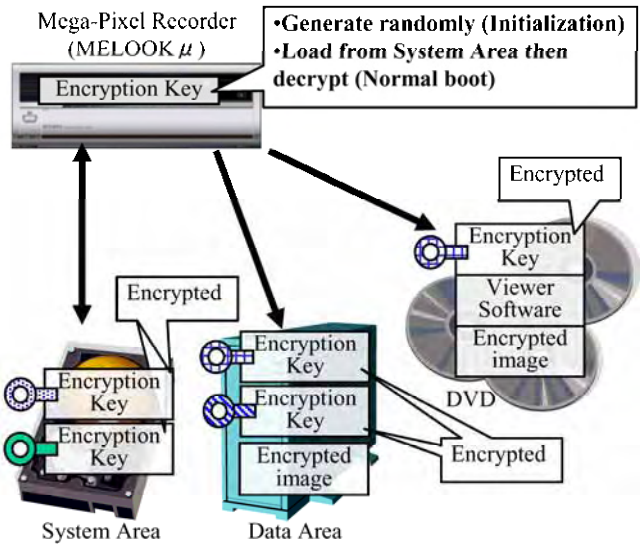


Fig. 4 Encryption key management in MELOOKμ

2.3 User authentication

The mega-pixel recorder performs access control by verifying the password provided by the user.

Table 1 shows the user levels and operations permitted for each level. Assistant level allows only live image surveillance. Manager level allows, in addition to live image surveillance, playback of accumulated images, and camera manipulation. Owner level is the highest authorization level and allows changes to various settings and copying of DVDs. Operations at the assistant level do not require a password, whereas operations at the manager and owner levels require password verification.

Table 1 User's authority and available operations

Authority	Available operations	Password
Lv.1 (Assistant)	•Live image surveillance	Unnecessary
Lv.2 (Manager)	•Live image surveillance •Playback •Camera manipulation	Necessary
Lv.3 (Owner)	•Live image surveillance •Playback •Camera manipulation •Configuration •Copy to DVD	Necessary

[1] Including both encryption and decryption

A password for DVD playback is defined when the owner copies video images to DVD. When the DVD is played back, the specified password must be entered to play back the video images.

A manager level or owner level password can be changed after it is authenticated at each proper level.

3. Conclusions

This paper introduced the security features of the Mitsubishi digital CCTV system, MELOOKμ. In the future, MELOOKμ is expected to be equipped with additional features including Web distribution functions, and backup HDD expansion capability.

Our Efforts in PKI Technologies

Authors: *Satoshi Takeda*, Tadakazu Yamanaka** and *Hideyuki Miyohara***

1. Introduction

A digital signature is an effective means of authenticating the identity of an electronic document's author or preventing the illegal alteration of an electronic document. The digital signature can be verified through a digital certificate, which is valid for a maximum period of five years, as defined by the law. However, many electronic documents must be stored for longer than 5 years, as in the case of receipts and financial statements that have a legally required retention period of 7 years. As a consequence, an issue arises when the 5-year validity period for a digital certificate has expired, and the digital signature cannot be verified.

Long-term signature technology ensures the validity of a digital signature even after the certificate's period of validity. This technology is standardized by the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI). The Next Generation Electronic Commerce Promotion Council of Japan (ECOM) proposed the standardization of long-term signature formats under the Japanese Industrial Standards (JIS), and it was officially announced as a JIS standard in March 2008. ECOM formulated a long-term signature profile and conducted interoperability tests based on the formulated profile and involving multiple vendors. Meanwhile, the Japanese Association of Healthcare Information Systems Industry (JAHIS) is developing a guideline and working on the standardization of electronic archiving and digital signatures for healthcare documents to ensure the interoperability of healthcare information systems.

Mitsubishi Electric has been participating in the ECOM and JAHIS committees and is actively involved in the formulation of a long-term signature profile and interoperability tests. This paper presents the details and development status of some of Mitsubishi Electric's efforts in Public Key Infrastructure (PKI) technologies, including standardization activities at ECOM and JAHIS.

2. Trend of Standardization

2.1 Long-term signature format

Digital signature technology allows authentication of a signer's document, where a digital signature is generated using a digital certificate and corresponding private key issued by the user's trusted Certificate Authority (CA), and verification is performed using the digital certificate and public key. The digital signature can be verified by confirming that it is within the valid period of the digital certificate and has not been invalidated. To ensure the validity of a digital signature, it is necessary to prove that it existed when the signer's document was created. The creation time of a digital signature can be set as one of the attributes of the signature. However, the time set will be the time information provided by the equipment that generates the electronic signature, which may create a reliability issue. It is also necessary to be able to check the validity of the signature even after the certificate expires or is invalidated. To deal with these issues, the following requirements must be satisfied:

- Identify the time when the signature was applied.
- Identify the evidence information required for re-verification.
- Enable the detection of illegal alteration of electronically signed document and information required for re-verification.
- Retain electronically signed document and information required for re-verification, with the detection of illegal alteration enabled.

The long-term signature format satisfies the above requirements, and ensures the validity of a digital signature "even after the digital certificate has expired, or even if the old encryption algorithm has been compro-

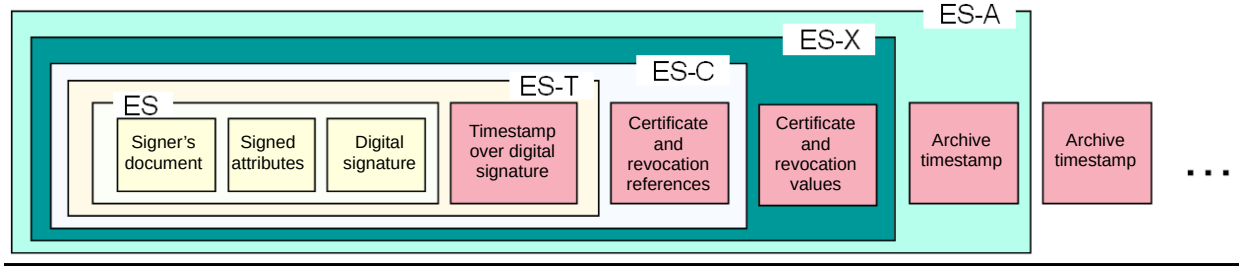


Fig. 1 Long-term signature format

**Information Technology R&D Center **Information Security Consulting & Supporting Center*

mised." As shown in Fig. 1, in addition to the signer's document and digital signature (ES), the long-term signature format data includes a timestamp over the digital signature that indicates the signing time (ES-T), certificate and revocation references for the digital certificate and revocation information (ES-C), certificate and revocation values used as verification information for the digital signature and the timestamp over the digital signature (ES-X), and an archive timestamp (ES-A). The timestamp data proves "when" the signer's document was signed; and the issuing agency in Japan secures the reliability of timestamps using the certification system. As long as an archive timestamp is affixed using an uncompromised encryption algorithm, the validity period of the digital signature can be extended. The authenticity of the data can be proven for a long term by verifying the consistency of the digital signature, timestamp over the digital signature, and digital certificate and revocation data included in the long-term signature format.

The long-term signature uses the advanced format of either Cryptographic Message Syntax (CMS) or Extensible Markup Language (XML), referred to as CAdES (CMS Advanced Electronic Signatures) or XAdES (XML Advanced Electronic Signatures), respectively, and published as standards RFC 5126[1], ETSI TS 101 733[2], and ETSI TS 101 903[3].

2.2 JIS Standards for long-term signature profile

ECOM has been working on standardizing the profile for the long-term signature format as described in the previous section. During their activities, ECOM exchanged information and opinions with ETSI to establish consistency between the profiles developed by ECOM and the profiles specified by ETSI, and then developed JIS drafts for the long-term signature profiles, which were eventually published as JIS X 5092[4] and JIS X 5093[5].

2.3 Activities by JAHIS

JAHIS is working to promote standardization in the field of healthcare systems, including the standardization of electronic archiving and digital signatures to ensure the interoperability of healthcare information systems.

In the guideline developed by JAHIS, the digital certificate for Healthcare PKI (HPKI), developed by the Ministry of Health, Labour and Welfare, is recommended as the digital certificate to be used for digital signatures on electronically archived medical records. According to the policy for the HPKI certificate, since the qualification data is described in the digital certificate, the hcRole attribute can be used as an extended certificate field. An important feature of this certificate is that the person who is verifying the certificate can use hcRole to determine if the signer is a licensed medical doctor or a management representative of a medical institution, such as a hospital director.

With regard to the validity of a certificate, in order to indicate that the digital signature was valid at the time that it was timestamped, it is specified that the authenticity of the information required to verify the certificate, such as the certificate and revocation values on a certificate 'pass' (CRL/ARL), must be maintained during the certificate retention period; and the recommended format to be used is the long-term signature format specified in the previously mentioned JIS standards. It is also specified that the signer prepares the ES-A format for documents to be personally retained, and the ES-T format for documents to be externally submitted.

3. Our Efforts

3.1 Interoperability tests according to the JIS draft for ECOM long-term signature profile

From 2006 to 2007, ECOM conducted "Interoperability tests according to the JIS draft for long-term signature profiles." Eighteen companies including Mitsubishi Electric participated in the tests, in cooperation with three companies that offer the service of issuing timestamps. The interoperability tests consist of the following two kinds of tests:

(1) Off-line test to verify long-term signature format

ECOM prepared the long-term signature data, verification data, and set-up data conforming to the JIS draft for long-term signature profiles. Products or prototypes of participating companies performed off-line verification of the validity of the long-term signature data. The verification results were checked to determine if they matched ECOM's assumptions.

(2) Product matrix interoperability test

Data prepared by the products (prototypes) of participating companies was verified using other companies' products, and the implementation of data generation functions and verification functions was checked to determine if they were in conformance with the JIS draft for long-term signature profiles. ECOM prepared the verification data and set-up data, and timestamps were provided using the timestamp agencies of the three cooperating companies.

Mitsubishi Electric participated in the interoperability tests to confirm that both of our proprietary CAdES and XAdES libraries were in conformance with the JIS draft for long-term signature profiles. As the first step in the test, conformity of the long-term signature format data prepared by other companies was checked using Mitsubishi's libraries. In parallel, we also prepared long-term signature format data, and confirmed that our

data was properly verified using the other companies' verification mechanisms. With these results, both our CAdES and XAdES libraries were confirmed to be in conformance with the JIS draft for long-term signature profiles.

3.2 Office add-on: long-term signature application

For the purpose of creating long-term signatures directly from an application program for preparing electronic documents, we used our long-term signature libraries to develop an Office Add-on for long-term signature application for Microsoft Office® (Note 1) 2007.

The Office Add-on for long-term signature application has the capability to construct and verify ES-T format data that is recommended in the JAHIS guideline for application to documents for external submission. It can create CAdES data as a PDF document and XAdES data as an OpenXML document. These functions are used to create a PDF document, generate a signature for the PDF document, and affix a timestamp in the case of CAdES data; they also generate a signature for an OpenXML document created using the Office application, and affix a timestamp in the case of XAdES data; and create ES-T format data for either CAdES or XAdES data.

Until now, a document prepared using an Office application was printed out on paper, and then the paper document was sealed and stored. In contrast, by using the Office Add-on for long-term signature application, a long-term signature format can be constructed and verified on the Office application, allowing preparation and storage of electronic documents having legal force equivalent to the paper document. As a result, a reduction in paper consumption and administrative costs, as well as time costs, is expected by using emails and file servers for real-time data communications and data sharing.

4. Conclusion

The Office Add-on for long-term signature application has wide-ranging relevance including in the healthcare field and for digital signatures on mandatory archive documents. We will further strive to integrate the long-term signature library into existing applications, enabling long-term signature generation on various products.

References

(1) RFC 5126: CMS Advanced Electronic Signatures (CAdES) (2008)
(2) ETSI TS 101 733 V1.7.4: CMS Advanced Electronic Signatures (CAdES) (2008)
(3) ETSI TS 101 903 V1.3.2: XML Advanced Electronic Signatures (XAdES) (2006)
(4) JIS X 5092: Long term signature profiles for CMS advanced electronic signatures (CAdES) (2008)
(5) JIS X 5093: Long term signature profiles for XML advanced electronic signatures (XAdES) (2008)

Note 1: The Microsoft and Microsoft Office logo are registered trademarks of Microsoft Corporation in the United States and other countries.


MITSUBISHI ELECTRIC CORPORATION