Recent Trends in Cryptographic Technology

Yuichi Murata[†]*, Atsushi Kanai, Ichizo Nakamura, and Masayuki Kanda*

Abstract

This article describes recent technology trends and standardization activities in the field of cryptography and explains measures that are being taken to deal with the problem of encryption algorithms being compromised in the future.

1. Classification of cryptographic techniques and technology trends

Cryptographic technology is becoming an indispensable platform technology for information security as digital technology and the Internet continue to expand. It is being used in a variety of ways in diverse situations. For example, symmetric-key encryption, public-key encryption, and hash functions are currently being used as cryptographic techniques to achieve encryption (concealment), authentication, and digital-signature functions (**Fig. 1**). For the future, advanced research on cryptography is working to develop an even wider range of applications such as multi-party protocols[*1], ID-based encryption, secure circuit evaluation[*2], and quantum cryptography, which is based on the principles of quantum mechanics.

1.1 Symmetric-key encryption

Cryptanalysis methods for symmetric-key encryption, especially block ciphers, developed rapidly in the 1990s, and cipher design methods and techniques for evaluating the security of encryption algorithms consequently underwent drastic changes. As a result, block ciphers that were developed before and after the mid-1990s were designed in substantially different ways from the viewpoint of security. Specifically, 64-bit block ciphers (such as Triple DES[*3] and MISTY1) were developed in the early 1990s while 128-bit block ciphers (such as Camellia and AES (Advanced Encryption Standard)) were developed around 2000 incorporating the latest design guidelines. It is therefore being recommended internationally that a transition be made from 64-bit block ciphers to 128-bit block ciphers because the latter have not only significantly better security but also higher processing speeds.

1.2 Public-key encryption

The RSA scheme has come to be the most widely used cipher in recent years. The root of its security lies in the difficulty posed by the mathematical problem of factoring a number having many digits, so a series of factorization experiments has been conducted to gauge its security. In 2005, a 663-bit composite number was successfully factored. At present, the RSA scheme is commonly used with a key length of 1024 bits or longer, and while security is not consid-

[†] NTT Information Sharing Platform Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: murata.yuichi@lab.ntt.co.jp

[*1] Multi-party protocol: A protocol that enables "operation of encrypted data" and "execution of encrypted operation logics" only when at least K participants out of the total of N participants cooperate. In general, the level of security becomes higher as K increases.

[*2] Secure circuit evaluation: A technology that enables arbitrary operation on encrypted data without decryption. Based on the multiparty protocol theory, secure circuit evaluation is guaranteed to be cryptologically secure.

[*3] Triple-DES: An advanced version of the Data Encryption Standard.

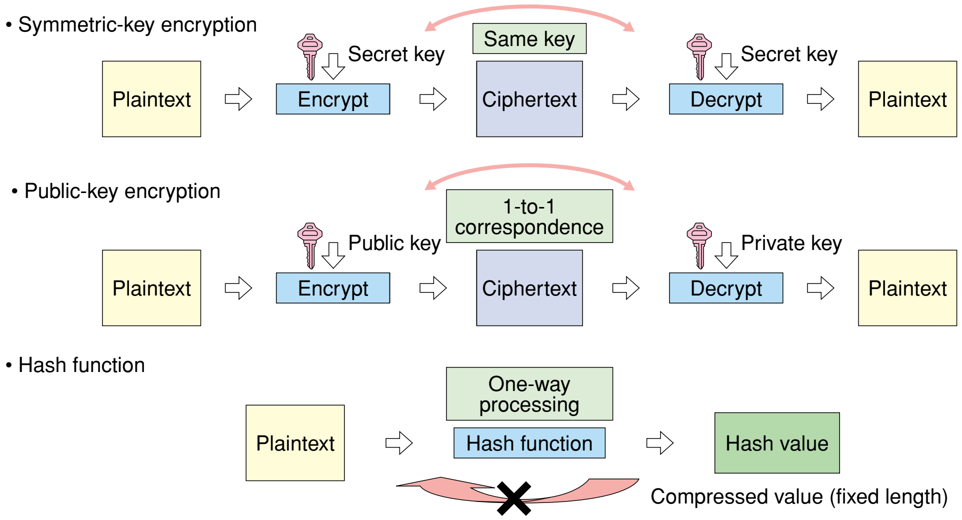


Fig. 1. Basic mechanisms of symmetric-key encryption, public-key encryption, and hash functions.

ered to be an actual problem, discussions on migrating to a 2048-bit key to improve security have begun.

One cipher that has been attracting attention recently uses elliptic curve cryptography. This is a public-key encryption scheme based on the discrete logarithm problem of elliptical curves. The elliptic curve encryption scheme can achieve a level of security equivalent to that of the RSA scheme while using a shorter key, so it offers faster processing. Some examples of elliptic curve encryption schemes are NTT's PSEC-KEM and ECDSA.

1.3 Hash functions

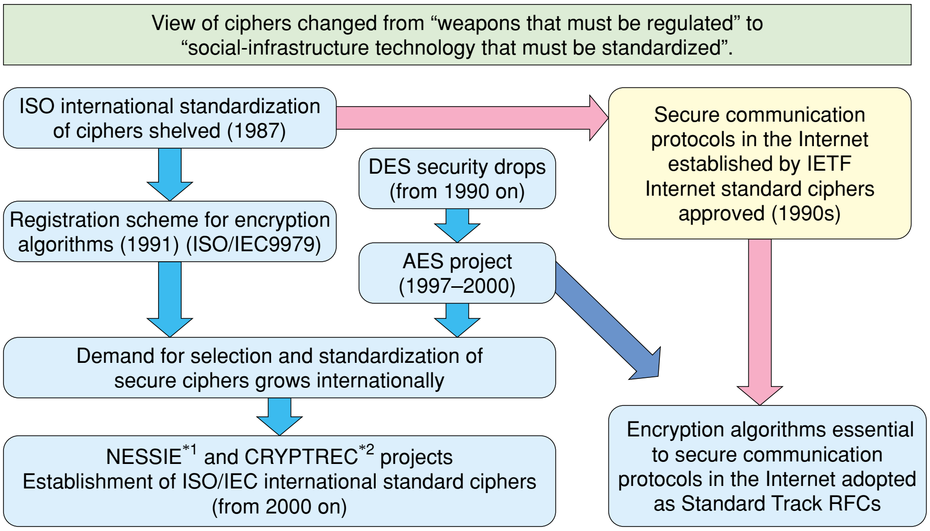
A hash function is actually a compression function that takes a message of any length and outputs compressed data of a fixed length (hash value). It can be used, for example, in the generation of message authenticators and in the preprocessing of digital signatures. One important property of hash functions is that collision cannot easily occur among messages subjected to hashing (collision-free generation). This means that it is difficult to find two different messages with the same hash value and that message falsification or alteration is impossible for all practical purposes. However, attacks on hash functions began to escalate in 2004, and in February 2005, it became clear that the collision-free state of the SHA-1 hash function could not be satisfied against attacks under certain conditions. Besides being a standard hash function for the United States government, SHA-1 is currently the most widely used hash function in the world. The best way to go about making a transition from SHA-1 to a replacement has become an important international issue.

2. Standardization trends in cryptographic technology

In the 1980s, ciphers were regulated as weapons of war in the USA. There were strict export controls on encryption systems, and encryption schemes were excluded from being targets of ISO international standardization. However, the explosive growth of the Internet has made international cooperation on the use of encryption essential. Cryptography is now being viewed as a social-infrastructure technology that must be standardized. Moreover, from 2000 to 2002, projects for selecting standard government ciphers and recommended ciphers were conducted in the USA, Europe, and Japan, and their selections have apparently been accepted as international standard ciphers by ISO/IEC. There is also a move toward using newly developed and secure encryption algorithms in security protocols at the Internet Engineering Task Force (IETF) (**Fig. 2**).

2.1 ISO/IEC international standard ciphers

ISO/IEC (International Organization for Standardization & International Electrotechnical Commission) has been managing a registration scheme for encryption algorithms (ISO/IEC9979) since 1991, but until recently, it had not been drafting international standards for cryptographic algorithms. However, an increasing demand for standardization led to


View of ciphers changed from "weapons that must be regulated" to "social-infrastructure technology that must be standardized".
ISO international standardization of ciphers shelved (1987)
Registration scheme for encryption algorithms (1991) (ISO/IEC9979)
DES security drops (from 1990 on)
AES project (1997–2000)
Demand for selection and standardization of secure ciphers grows internationally
NESSIE*1 and CRYPTREC*2 projects Establishment of ISO/IEC international standard ciphers (from 2000 on)
Secure communication protocols in the Internet established by IETF Internet standard ciphers approved (1990s)
Encryption algorithms essential to secure communication protocols in the Internet adopted as Standard Track RFCs

*1 NESSIE: New European Schemes for Signatures, Integrity, and Encryption
*2 CRYPTREC: Cryptography Research and Evaluation Committees

Fig. 2. Changes in cipher standardization.

Table 1. ISO/IEC18033 international standard ciphers.

Technical category		Cipher name	
Public-key encryption (ISO/IEC18033-2)		PSEC-KEM (NTT), ACE-KEM, ECIES-KEM, HIME(R), RSA-KEM, RSA-OAEP	
Symmetric-key encryption	Block ciphers (ISO/IEC 18033-3)	128-bit block ciphers	Camellia (NTT/Mitsubishi Electric), AES, SEED
		64-bit block ciphers	CAST-128, MISTY1, Triple DES
	Stream ciphers (ISO/IEC 18033-4)	MUGI, SNOW, (MULTI-S01 in appendix)	

a change in policy in 1999, resulting in the first selection of ISO/IEC international standard ciphers (ISO/IEC18033). These ciphers were selected by comparing the results of security and performance evaluations performed by third-party institutions in the public sector. The selected ciphers included Camellia and PSEC-KEM (**Table 1**). Incidentally, when ISO/IEC18033 was established, it was decided to discontinue ISO/IEC9979.

2.2 IETF

At IETF, encryption algorithms judged to be essential for secure communication protocols in the Internet such as SSL/TLS (secure sockets layer, transport layer security) and IPsec (Internet protocol security) are designated as Standard Track RFCs (requests for comment). Camellia as well as AES and SEED have been added as new ciphers for Standard Track RFC designation. These ciphers coincide with the 128-bit block ciphers selected by ISO/IEC18033. They are regarded as being the mainstream ciphers of the future, including the world of the Internet.

IETF has also set up a hash-function working group in response to the compromising of the SHA-1 hash function. This working group will discuss ways of changing how hash functions are used in the various protocols established by the IETF.

3. Trends in compromised encryption algorithms

The development of AES as a replacement for Triple DES, the successful factoring of a 663-bit composite number, and the successful attack on the SHA-1 hash function in recent years all signify that the security and future operation of encryption technologies now in use as *de facto* standards might be in jeopardy.

In the USA, the National Institute of Standards and Technology (NIST) has the responsibility to terminate the use of cryptographic algorithms used in government systems before they become seriously compromised and to initiate a transition to other ciphers deemed to be secure. It has established a policy that calls for a change in *de facto* ciphers by 2010 as a means of dealing with this situation. NIST has also issued a number of official guidelines in this regard starting with Special Publication 800-57 "Recommendation for Key Management" in August 2005 [1]. This publication lists cryptographic technologies that should be used in US government systems over the medium and long term. It also describes a scale of security of cryptographic techniques called "equivalent security" and states how most cryptographic algorithms currently in use as *de facto* standards possess "80-bit security". It recommends that the use of these algorithms be terminated by the end of 2010.

In short, it has been decided that cryptographic algorithms in US government systems having 80-bit security are insufficient over the medium and long term and that they should be replaced by algorithms having a security level of 112 bits or higher (**Figs. 3 and 4**).

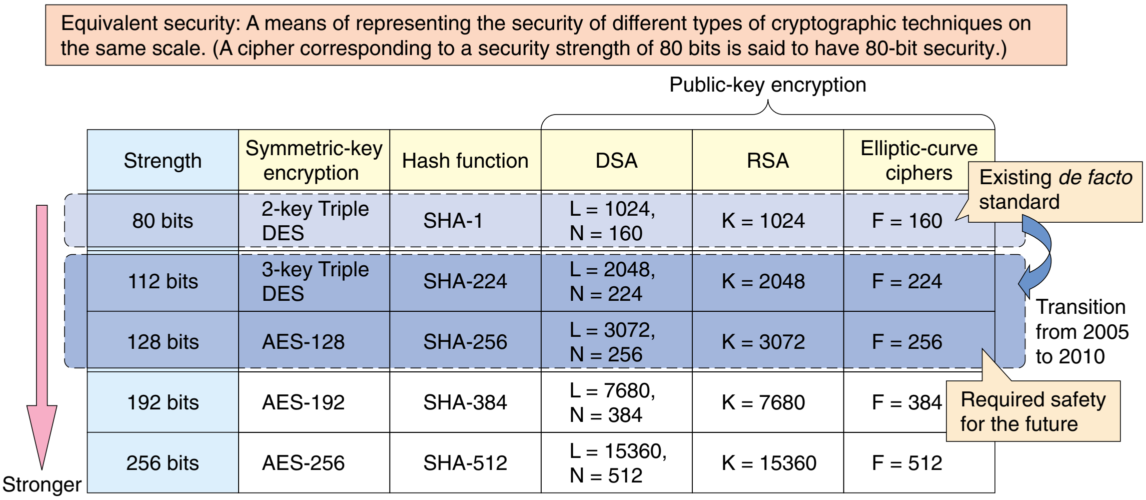
3.1 NIST trends in symmetric-key encryption

Publication 46-3 of the Federal Information Processing Standards (FIPS46-3) authorized the use of DES and Triple DES as standard ciphers for the US government. The validity of this publication expired in May 2005, so DES was discontinued and the importance of Triple DES was reduced, as described in SP800-67. Standard ciphers for the US government are now grouped in AES FIPS 197, and the plan is to promote the use of AES vigorously. The use of 128-bit block ciphers is expected to become common on the international level as well. Special Publication 800-67 also calls for the discontinuation of 2-key Triple-DES by the end of 2010.

3.2 NIST trends in hash functions

In response to the announcement of an attack method for SHA-1 in February 2005, it was decided that the US government standard on hash functions should undergo a transition from SHA-1 to SHA-224/256/384/512 (collectively called SHA-2). The plan is to discontinue the use of SHA-1 as a government standard by 2010.

A workshop on hash functions was held in October



Equivalent security: A means of representing the security of different types of cryptographic techniques on the same scale. (A cipher corresponding to a security strength of 80 bits is said to have 80-bit security.)

			Public-key encryption		
Strength	Symmetric-key encryption	Hash function	DSA	RSA	Elliptic-curve ciphers
80 bits	2-key Triple DES	SHA-1	L = 1024, N = 160	K = 1024	F = 160
112 bits	3-key Triple DES	SHA-224	L = 2048, N = 224	K = 2048	F = 224
128 bits	AES-128	SHA-256	L = 3072, N = 256	K = 3072	F = 256
192 bits	AES-192	SHA-384	L = 7680, N = 384	K = 7680	F = 384
256 bits	AES-256	SHA-512	L = 15360, N = 512	K = 15360	F = 512

Stronger
Existing *de facto* standard
Transition from 2005 to 2010
Required safety for the future

L = size of p (public key); N = size of q (private key); K = size of n; F = size of order n of base-point G

From NIST Guidelines SP800-57 "Recommendation for Key Management" [1].

Fig. 3. Equivalent security of encryption algorithms.

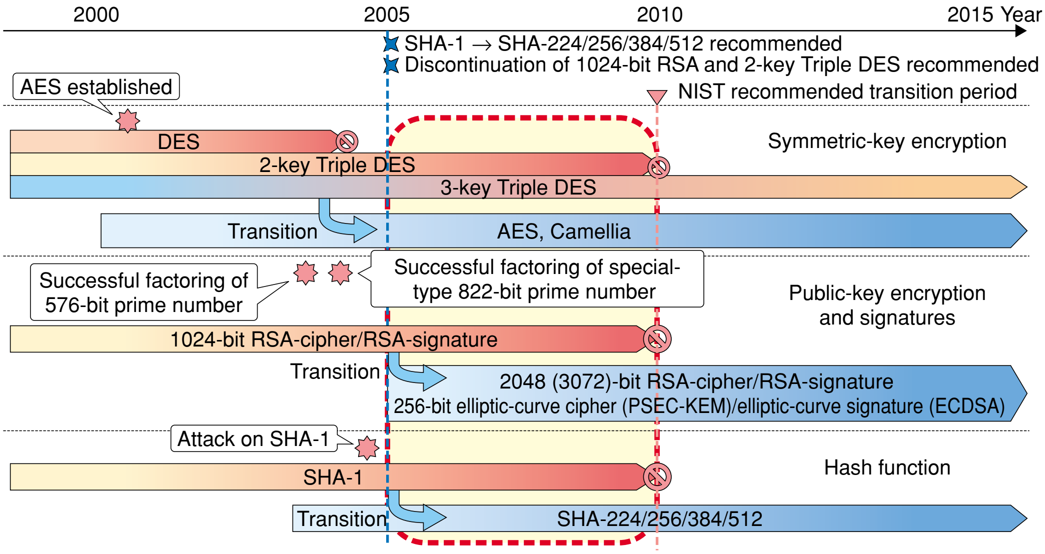

2000
2005
2010
2015 Year
SHA-1 → SHA-224/256/384/512 recommended
Discontinuation of 1024-bit RSA and 2-key Triple DES recommended
NIST recommended transition period
AES established
DES
2-key Triple DES
3-key Triple DES
Symmetric-key encryption
Transition
AES, Camellia
Successful factoring of 576-bit prime number
Successful factoring of special-type 822-bit prime number
Public-key encryption and signatures
1024-bit RSA-cipher/RSA-signature
Transition
2048 (3072)-bit RSA-cipher/RSA-signature
256-bit elliptic-curve cipher (PSEC-KEM)/elliptic-curve signature (ECDSA)
Attack on SHA-1
SHA-1
Hash function
Transition
SHA-224/256/384/512

Fig. 4. Trends in compromised encryption algorithms.

2005 under the sponsorship of NIST. The topics discussed there included SHA-2 security evaluations, plans for migrating from SHA-1 to SHA-2, and the need to make a call for proposals for developing new hash functions. The results of this workshop point to a transition from SHA-1 to SHA-2 and new hash functions.

3.3 NIST trends in public-key encryption and digital signatures

NIST points out that 1024-bit RSA encryption, RSA signatures, and DSA and 160-bit ECDSA all have the same level of security as SHA-1 (80-bit security). It is recommending that the former make a transition to a key length of 2048 bits and the latter to a key length of around 256 bits by 2010.

Moreover, for digital signatures having 80-bit security, guidance is being provided on the handling of applications that require a fixed verification period. For example, SP800-78 [2] states that the generation of digital signatures should be prohibited at the end of 2008 and that only signature verification should be used for a two-year period ending in 2010.

4. Future outlook

The compromising of cryptographic algorithms in recent years has made many of the cryptographic algorithms currently used as *de facto* standards the target for a future transition. The US government, in particular, has set forth a policy that calls for the transition of current cryptographic algorithms by 2010. It will therefore be necessary to select, in the most appropriate way based on outside trends, the cryptographic techniques that are to be used not only in newly developed systems but also in existing systems whose use is expected to continue after 2010.

At the same time, cutting-edge research on quantum cryptography is progressing in many countries to provide a scheme that is immune to compromise even if powerful quantum computers are made in the future. NTT is proposing quantum public-key encryption based on the NP-complete problem as a secure public-key encryption scheme that can be used even in an era of quantum computers. Research and development in this area is moving forward at NTT Laboratories.

References

[1] http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf
[2] http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

Yuichi Murata

Senior Research Engineer, Information Security Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in information science from Tokyo Institute of Technology, Tokyo in 1989. He joined NTT Laboratories in 1989. He has been engaged in R&D of application systems for information security. He is a member of the Information Processing Society of Japan (IPSJ) and the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Atsushi Kanai

Project Manager, Information Security Project, NTT Information Sharing Platform Laboratories.

He received the B.S., M.S., and Ph.D. degrees in information science from Tohoku University, Miyagi in 1979, 1982, and 2000, respectively. Since 1982, he has been working at NTT Laboratories. His current research interests include software design methodology, software development environments, Web application technologies, and information security. He is a member of IPSJ and IEICE.

Ichizo Nakamura

Senior Research Engineer, Supervisor, Information Security Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electrical engineering from Keio University, Kanagawa, in 1984 and 1986, respectively. Since 1986, he has been working at NTT Laboratories. His current research interests include RFID and information security. He is a member of IEICE.

Masayuki Kanda

Senior Research Engineer, Information Security Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electronic engineering from Tokyo Institute of Technology, Tokyo in 1991 and 1993, respectively. He received the Ph.D. degree in information engineering from Yokohama National University, Kanagawa in 2002. He joined NTT Laboratories in 1993. In 2002, he was temporarily transferred to the Telecommunication Advancement Organization of Japan. He has been engaged in the design and cryptanalysis of block ciphers and security protocols and in the promotion of Camellia. He is a member of IEICE and IPSJ.