Promoting the Use of Camellia

Masayuki Kanda†

Abstract

Camellia, a 128-bit block cipher developed jointly by NTT and Mitsubishi Electric Corporation, is an encryption algorithm with the world's highest level of security and performance. It has been selected as an ISO/IEC international standard cipher and an Internet standard cipher. This report provides an overview of Camellia and describes NTT's efforts to promote its use.

1. Camellia: Japan's representative cipher

Recognizing that cryptographic technology has become an important foundation of the information society, a worldwide movement is taking place to select secure encryption algorithms as standard and recommended ciphers based on strict evaluations performed by cryptographic researchers. Camellia has been recognized as the only cipher in the world having security and processing performance levels equivalent to AES (Advanced Encryption Standard), the standard cipher of the United States government. Like AES, Camellia has been selected as a next-generation international standard cipher by various standardization organizations and projects. Camellia is expected to be used on the international level as Japan's representative cipher.

This article provides an overview of Camellia, discusses the significance of its selection by standardization organizations and projects, and describes how NTT is working to promote the use of Camellia now and in the future.

2. Overview of Camellia

Camellia is a 128-bit block cipher*1 developed jointly by NTT and Mitsubishi Electric Corporation [1], [2]. As shown in **Fig. 1**, its design combines NTT's know-how on designing ciphers for high-speed software implementations (shown in blue), Mitsubishi Electric's world-renowned know-how on designing ciphers for compact and high-speed hardware implementations (red), and world-class cipher-security evaluation techniques*2 developed by both companies (yellow). Camellia uses a message-block length of 128 bits and supports secret keys of three different lengths: 128, 192, and 256 bits.

It has been proven mathematically that Camellia is secure against differential and linear cryptanalysis, which are known to be strong attacks against block ciphers. It has also been shown that Camellia is secure against other attacks. In addition, no obvious vulnerabilities have been found to date in numerous third-party evaluations conducted by cryptographic researchers throughout the world. Therefore, Camellia's expected security level in future (security margin) is in the world's top class. Camellia is expected to be more resistant to future unknown attacks than AES.

Another feature of Camellia is its excellent utility in diverse applications. Unlike AES, Camellia uses the same structure for encryption and decryption, which enables it to exhibit superior performance in

† NTT Information Sharing Platform Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: kanda.masayuki@lab.ntt.co.jp

*1 Block cipher: A block cipher, which encrypts data in fixed-length blocks, is a symmetric key encryption algorithm that uses the same secret key to encrypt and decrypt data. Since it achieves high-speed encryption processing, it is used widely in various applications such as communication sessions that deal with large-volume data, file encryption, and mobile terminal authentication.

*2 Cipher-security evaluation techniques: Methods of expressing an index of immunity against cryptanalytic attacks, e.g., differential cryptanalysis and linear cryptanalysis.

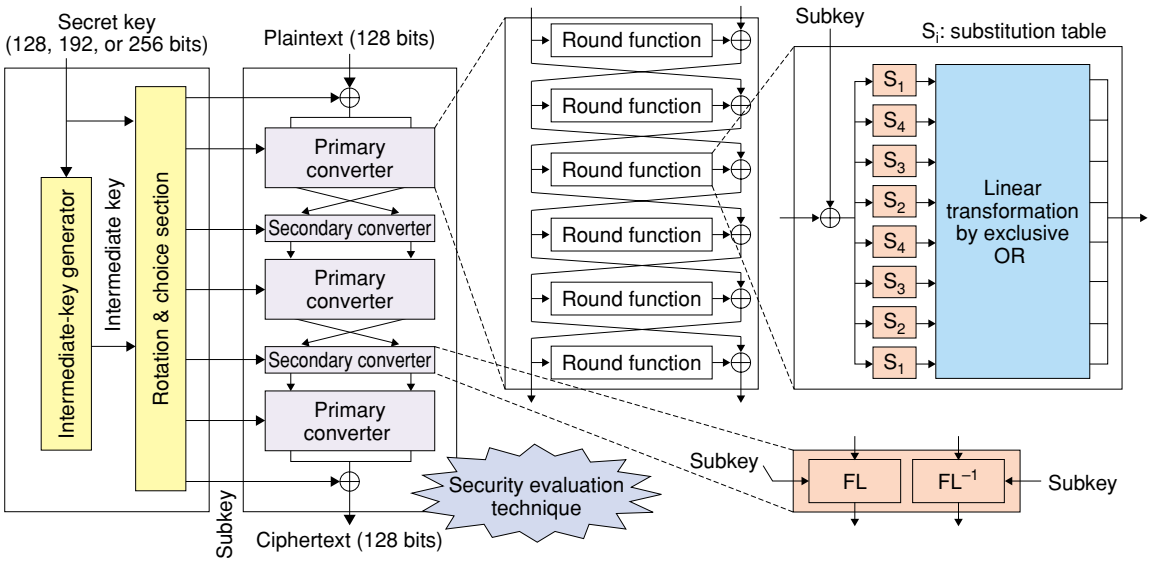

Fig. 1. Design of Camellia.

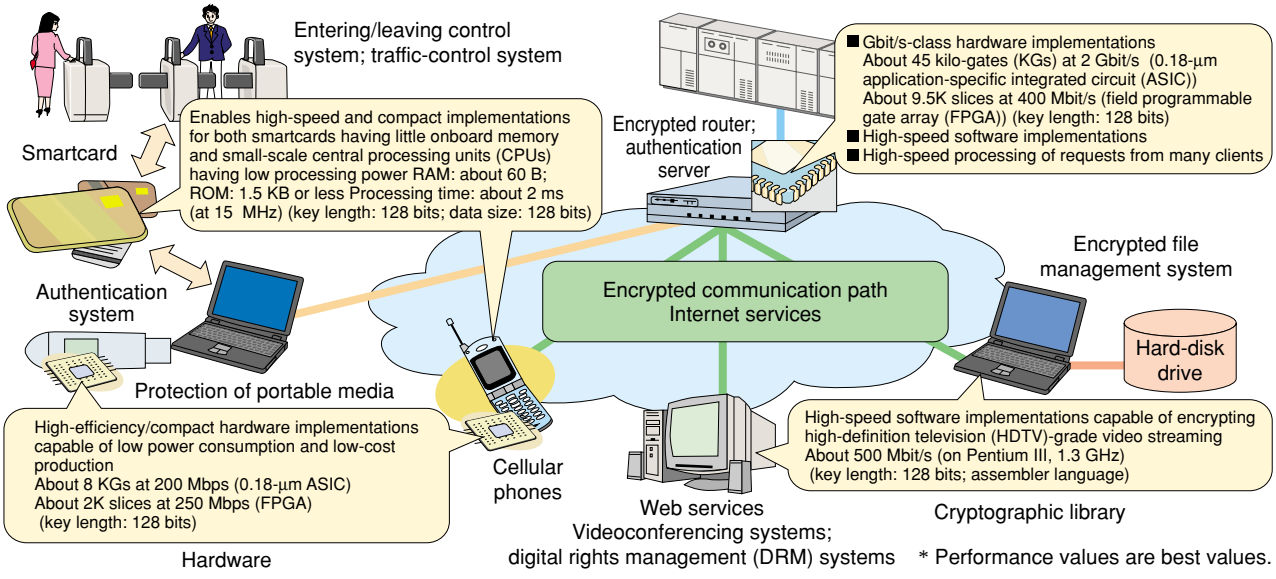

Fig. 2. Camellia's high-efficiency processing.

smartcards that have a little onboard memory and in other compact hardware devices. Specifically, Camellia can be used to achieve high-speed encryption processing on a variety of platforms from low-cost smartcards to personal computers and server systems by using software implementations that use instruction sets and ROM/RAM (read-only memory, random access memory) sizes applicable to the application environments in question. In this way, Camellia has been shown to achieve processing speeds from four to five times faster than Triple DES and at least twice as fast as FEAL-32X. It can also be used to achieve high-speed processing in hardware implementations.

Moreover, it can be used to construct the world's smallest implementation of a 128-bit block cipher (with a circuit scale under 8000 gates) with a processing efficiency at the highest level in this class. As shown in **Fig. 2**, Camellia achieves high-efficiency processing by flexibly adapting the implementation to the application and circumstances. Camellia is the best choice in these typical software implementations and two hardware implementations, which have different priorities for performance, memory, and cost.

3. Camellia's inclusion among standard and recommended ciphers

Besides international cryptography societies, NTT has submitted proposals for using Camellia to the European Union's project for selecting recommended ciphers (NESSIE: New European Schemes for Signatures, Integrity, and Encryption) and Japan's project for selecting recommended ciphers for e-government (CRYPTREC: Cryptography Research and Evaluation Committees) [3]. In this way, NTT received thorough and objective evaluations of Camellia from researchers throughout the world over a period of several years. For example, the evaluation performed at NESSIE determined that "Camellia has many similarities to AES, so much of the analysis for AES is also applicable to Camellia. It is also the case that the NESSIE project did not find an attack on either AES or Camellia." For this reason, Camellia was the only 128-bit block cipher selected as an EU recommended cipher out of ten submitted ciphers [4].

Furthermore, as the only 128-bit block cipher in the world having the same level of security and processing performance as AES, Camellia has joined AES on the lists of various standard and recommended ciphers, as shown in **Fig. 3**. Its selection as an ISO/IEC international standard cipher and Internet standard cipher is especially significant [5].

3.1 ISO/IEC international standard cipher

Based on the results of evaluations conducted in a similar manner to those of NESSIE and CRYPTREC, ISO/IEC standardized a set of ciphers recognized internationally as secure and efficient in the first formal ISO/IEC international standard cipher (ISO/IEC18033 series). Camellia, AES, and SEED (developed by Korea Information Security Agency (KISA)) are the only 128-bit block ciphers included in ISO/IEC18033-3 and are thus destined to become next-generation standards.

3.2 Internet standard ciphers

The only ciphers that can be formally used on the Internet are those that have been selected by IETF (Internet Engineering Task Force) as Internet standard ciphers. As a result, protocols for secure com-

Standardization organization	Type of standardized ciphers	Japanese block ciphers	Overseas block ciphers
NESSIE	EU recommended ciphers	Camellia	AES
		MISTY 1	—
		—	SHACAL-2
CRYPTREC	Recommended ciphers for e-government in Japan	Camellia, Cipherunicorn-A, Hierocrypt-3, SC2000	AES
		Cipherunicorn-E, Hierocrypt-L1, MISTY 1	3-key Triple DES
ISO/IEC	ISO/IEC international standard ciphers (ISO/IEC18033-3)	Camellia	AES, SEED
		MISTY 1	Triple DES, CAST-128
IETF (Japanese first)	SSL/TLS standard ciphers	Camellia (RFC4132)	AES, SEED
		—	Triple DES, IDEA, RC2
	XML standard ciphers	Camellia (RFC4051)	AES
		—	Triple DES
	S/MIME standard ciphers	Camellia (RFC3657)	AES, SEED
		—	Triple DES, CAST-128, IDEA, RC2, RC5
	IPsec standard ciphers	Camellia (RFC4312)	AES, SEED
		—	Triple DES, CAST-128, IDEA, RC5, Blowfish
TV-Anytime Forum Server-type broadcast standards	Bi-direction metadata delivery protection ciphers	Camellia	AES
		—	—
	Copyright-management/ information-protection ciphers	Camellia	AES
		MULTI-2	Triple DES
ETSI European Telecommunications Standards Institute	Bi-direction metadata delivery protection ciphers	Camellia	AES
		—	—

* Ciphers in blue indicate standard or approved ciphers for government use

128-bit block ciphers 64-bit block ciphers

Fig. 3. Standardization of symmetric key block ciphers.

munications on the Internet such as SSL/TLS (secure sockets layer, transport layer security) and S/MIME (secure multipurpose Internet mail extensions) are currently using Triple DES and RC4 as standard ciphers. Ciphers that have not been established as Internet standard ciphers cannot be used on the Internet even if they have been selected by other organizations. Its selection for SSL/TLS makes Camellia the first Japanese-produced cipher to be approved for use as a standard Internet cipher. It is also the first Japanese-produced cipher to be formally used to construct a variety of services and systems for Internet use.

4. Toward next-generation ciphers

The relationships in international cipher standardization are shown in **Fig. 4**. Although Camellia, AES, and SEED have been selected as 128-bit block ciphers that should become standard implementations on the international level and on the Internet, SEED is limited to a key length of 128 bits and is more technically restricted than Camellia and AES. Moreover, even though Camellia and AES have different encryption structures, they have equivalent processing performance, so they can be used in parallel without a drop in processing performance. Thus, we can easily create countermeasures against the encryption scheme becoming compromised by using multiple ciphers, e.g., using both Camellia and AES together. Furthermore, while it is true that many ciphers are being proposed by other vendors in Japan, Camellia is the only Japanese cipher to have been approved as an international standard cipher, which gives it an overwhelming competitive edge among Japanese-produced ciphers.

5. Future developments

As the importance of Camellia is expected to grow, NTT is increasing its efforts to promote its use not only as an NTT cipher but also as Japan's representative cipher. In 2001, NTT launched a non-exclusive royalty-free licensing system of Camellia's essential patents under the principle of mutual reciprocity, targeting mainly enterprises that develop products that incorporate Camellia. This approach was taken as part of NTT's role as a leader in developing a low-cost and secure information society and with the aim of promoting NTT's "brand image" as a developer.

Camellia has already been implemented in a number of system integration projects mainly in public and government systems, and cryptographic libraries and other products using Camellia from NTT Software, and Camellia-based anti-information-leakage systems from NTT-AT (NTT Advanced Technology) have been put on the market. Camellia has also been chosen for several non-NTT commercial products such as the Authentication BOX Server from Oi Electric Co., Ltd. Plans are also being made to expand the lineup of NTT Group products that incorporate Camellia, such as the eLWISE card from NTT Communications and hardware products from NTT Electronics Corporation (NEL). There are also plans to incorporate Camellia in facility systems and integrated products manufactured by leading vendors by the end of this fiscal year. Development work for this is now in progress at various companies. Plans are also being made to use Camellia for information protec-

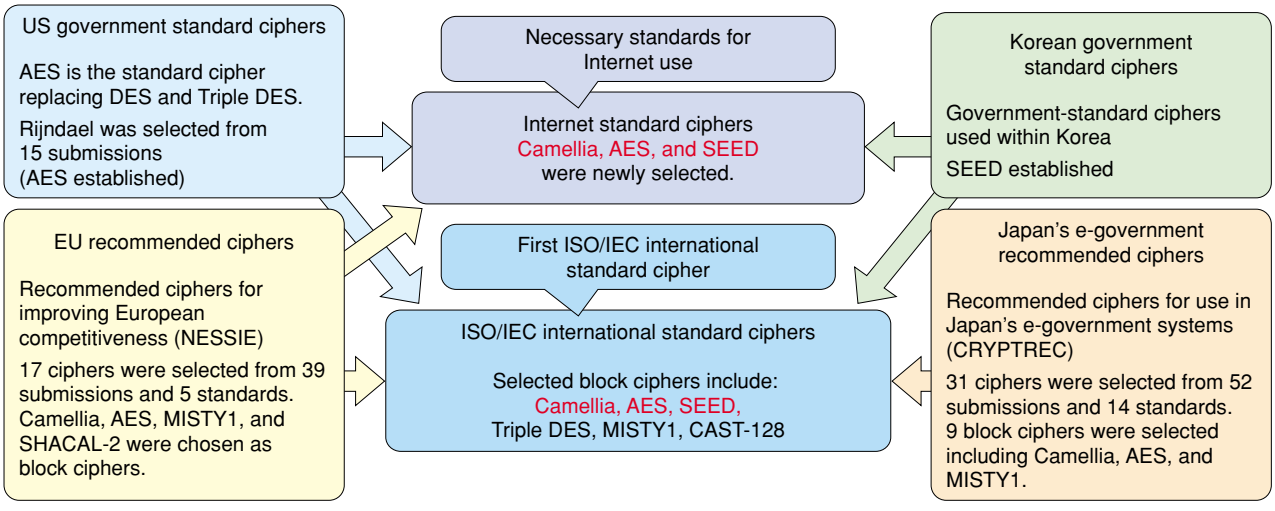

Fig. 4. Relationships in international cipher standardization.

tion in online games from leading video-game developers. Thus, other vendors besides NTT and Mitsubishi Electric are also working to get products that use Camellia on the market as soon as possible. The widespread use of Camellia in a variety of services should lead to the use of Camellia at more and more of the popular sites familiar to general users.

The selection of Camellia as an ISO/IEC international standard cipher and Internet standard cipher should also contribute to the spread of Camellia by encouraging the provision of source code to open-source communities such as OpenSSL and the inclusion of Camellia products in the products of various leading venders.

References

[1] http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html

[2] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "The 128-Bit Block Cipher Camellia," IEICE transactions on fundamentals, Vol. E85-A No.1, 2001.

[3] M. Kanda, T. Matsumoto, T. Kaneko, and H. Imai, "Recent Evaluation Process and Standardization of Cryptographic Primitives," Information Processing, Vol. 45, No. 11, 2004 (in Japanese).

[4] https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf

[5] Y. Murata, A. Kanai, I. Nakamura, and M. Kanda, "Recent Trends in Cryptographic Technology," NTT Technical Review, Vol. 4, No. 2, pp. 37-42, 2006 (this issue).

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 the Institute of Electronics, Information and Communication Engineers of Japan and the Information Processing Society of Japan.