Specification of *Camellia* — a 128-bit Block Cipher Difference between Specifications

Kazumaro AOKI [†], Tetsuya ICHIKAWA [‡], Masayuki KANDA [†],
Mitsuru MATSUI [‡], Shiho MORIAI [†], Junko NAKAJIMA [‡], Toshio TOKITA [‡]

[†]Nippon Telegraph and Telephone Corporation, [‡]Mitsubishi Electric Corporation

September 26, 2001

The following information has been added to the specification document for CRYPTREC2000.

D Design Policy

This paper presents a 128-bit block cipher called *Camellia*, which was jointly developed by NTT and Mitsubishi Electric Corporation. Camellia supports 128-bit block size and 128-, 192-, and 256-bit key lengths, and so offers the same interface specifications as the Advanced Encryption Standard (AES). The design goals of Camellia are as follows.

High level of security. The recent advances in cryptanalytic techniques are remarkable. A quantitative evaluation of security against powerful cryptanalytic techniques such as differential cryptanalysis [BS93] and linear cryptanalysis [M94] is considered to be essential in designing any new block cipher. We evaluated the security of Camellia by utilizing state-of-art cryptanalytic techniques. We have confirmed that Camellia has no differential and linear characteristics that hold with probability more than 2^{-128}. Moreover, Camellia was designed to offer security against other advanced cryptanalytic attacks including higher order differential attacks [K95, JK97], interpolation attacks [JK97, A00], related-key attacks [B94, KSW96], truncated differential attacks [K95, MT99], boomerang attacks [W99], and slide attacks [BW99, BW00].

Efficiency on multiple platforms. As cryptographic systems are needed in various applications, encryption algorithms that can be implemented efficiently on a wide range of platforms are desirable, however, few 128-bit block ciphers are suitable for both software and hardware implementation. Camellia was designed to offer excellent efficiency in hardware and software implementations, including gate count for hardware design, memory requirements in smart card implementations, as well as performance on multiple platforms.

Camellia consists of only 8-by-8-bit substitution tables (s-boxes) and logical operations that can be efficiently implemented on a wide variety of platforms. Therefore, it can be implemented efficiently in software, including the 8-bit processors used in low-end smart cards, 32-bit processors widely used in PCs, and 64-bit processors. Camellia doesn't use 32-bit integer additions and

multiplications, which are extensively used in some software-oriented 128-bit block ciphers. Such operations perform well on platforms providing a high degree of support, e.g., Pentium II/III or Athlon, but not as well on others. These operations can cause a longer critical path and larger hardware implementation requirements.

The s-boxes of Camellia are designed to minimize hardware size. The four s-boxes are affine equivalent to the inversion function in the finite field GF(2^8). Moreover, we reduced the inversion function in GF(2^8) to a few GF(2^4) arithmetic operations. It enabled us to implement the s-boxes by fewer gate counts.

The key schedule is very simple and shares part of its procedure with encryption. It supports on-the-key subkey generation and subkeys are computable in any order. The memory requirement for generating subkeys is quite small; an efficient implementation requires about 32-byte RAM for 128-bit keys and about 64-byte RAM for 192- and 256-bit keys.

E Design Rationale

E.1 *F*-function

The design strategy of the F-function of Camellia follows that of the F-function of E2 [KMA+98]. The main difference between E2 and Camellia is the adoption of the 1-round (conservative) SPN (Substitution-Permutation Network), not the 2-round SPN, i.e. S-P-S. When the 1-round SPN is used as the round function in a Feistel cipher, the theoretical evaluation of the upper bound of differential and linear characteristic probability becomes more complicated, but the speed under the same level of "real" security is expected to be improved. See Section 6 for detailed discussions on security.

E.2 *P*-function

The design rationale of the P-function is similar to that of the P-function of E2. That is, for computational efficiency, it should be represented using only bytewise exclusive-ORs and for security against differential and linear cryptanalysis, its branch number should be optimal [KTM+99]. From among the linear transformations that satisfy these conditions, we chose one considering highly efficient implementation on 32-processors [AU00] and high-end smart cards, as well as 8-bit processors.

E.3 *s*-boxes

As the s-boxes we adopted functions affine equivalent to the inversion function in GF(2^8) for enhanced security and small hardware design.

It is well known that the smallest of the maximum differential probability of functions in GF(2^8) was proven to be 2^{-6}, and the smallest of the maximum linear probability of functions in GF(2^8) is conjectured to be 2^{-6}. There is a function affine equivalent to the inversion function in GF(2^8) that achieves the best known of the maximum differential and linear probabilities, 2^{-6}. We choose this kind of functions as s-boxes. Moreover, the high degree of the Boolean polynomial of every output bit of the s-boxes makes it difficult to attack Camellia by higher order differential attacks. The two affine functions that are performed at the input and output of the inversion function in GF(2^8) complicates

F Version Information

Camellia has been proposed in the following activities, where the proposed specification is exactly the same as the specification described in this document.

Papers

- Technical report of IEICE,
  K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia – A 128-bit Block Cipher", Technical Report ISEC2000-6, The Institute of Electronics, Information and Communication Engineers, 2000. (in Japanese).

- International Workshop SAC 2000
  K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design and Analysis —," In Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 2000, Proceedings, Lecture Notes in Computer Science 2012, pp.39-56, Springer-Verlag, 2001.

Standardization

- ISO 18033
- NESSIE
- IETF
  The followings were submitted as Internet-Drafts.
  - J. Nakajima and S. Moriai,"A Description of the Camellia Encryption Algorithm" `<draft-nakajima-camellia-02.txt>`
  - S. Moriai,"Addition of the Camellia Encryption Algorithm to TLS" `<draft-ietf-tls-camellia-01.txt>`

G Object Identifier

The object identifier of Camellia is described in the Internet-Draft, " A Description of the Camellia Encryption Algorithm ". The following is extracted from the document.

The Object Identifier for Camellia in Cipher Block Chaining (CBC) mode is as follows:

- 128-bit key length, CBC mode
```
id-camellia128-cbc OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) 392 200011 61 security(1)
 algorithm(1) symmetric-encryption-algorithm(1) camellia128-cbc(2) }
```
- 192-bit ke length, CBC mode
```
id-camellia192-cbc OBJECT IDENTIFIER ::=
{ iso(1) member-body(2) 392 200011 61 security(1)
algorithm(1) symmetric-encryption-algorithm(1) camellia192-cbc(3) }
```

- 256-bit key length, CBC mode
  `id-camellia256-cbc OBJECT IDENTIFIER ::=`
  `{ iso(1) member-body(2) 392 200011 61 security(1)`
  `algorithm(1) symmetric-encryption-algorithm(1) camellia256-cbc(4) }`

H Applications and Products

Camellia can be used for all applications of symmetric block ciphers. In particular, it is suitable for secure communications and authentication.

Camellia can be implemented efficiently on a wide range of platforms, including software implementations on 32-bit/64-bit CPUs and low-end/high-end smart cards, and compact and high-speed hardware implementations on ASICs and FPGAs.

Most of the information about applications of Camellia can be found at `http://www.security.melco.co.jp/`

References

[A00] K. Aoki. Practical Evaluation of Security against Generalized Interpolation Attack. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E83-A, No. 1, pp. 33–38, 2000. (A preliminary version was presented at SAC'99).

[AU00] K. Aoki and H. Ueda. Optimized Software Implementations of E2. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E83-A, No. 1, pp. 101–105, 2000. (The full paper is available on `http://info.isl.ntt.co.% linebreak[3]jp/e2/RelDocs/`).

[B94] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *Journal of Cryptology*, Vol. 7, No. 4, pp. 229–246, 1994. (The extended abstract was appeared at EUROCRYPT'93).

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[BW99] A. Biryukov and D. Wagner. Slide Attacks. In L. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 245–259, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

[BW00] A. Biryukov and D. Wagner. Advanced Slide Attacks. In S. Vaudenay, editor, *Advances in Cryptology — EUROCRYPT2000*, Volume 1807 of *Lecture Notes in Computer Science*, pp. 589–606, Berlin, Heidelberg, New York, 2000. Springer-Verlag.

[JK97] T. Jakobsen and L. R. Knudsen. The Interpolation Attack on Block Cipher. In E. Biham, editor, *Fast Software Encryption — 4th International Workshop, FSE'97*, Volume 1267 of *Lecture Notes in Computer Science*, pp. 28–40, Berlin, Heidelberg, New York, 1997. Springer-Verlag.

[K95] L. R. Knudsen. Truncated and Higher Order Differentials. In B. Preneel, editor, *Fast Software Encryption — Second International Workshop*, Volume 1008 of *Lecture Notes in Computer Science*, pp. 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[KMA+98] M. Kanda, S. Moriai, K. Aoki, H. Ueda, M. Ohkubo, Y. Takashima, K. Ohta, and T. Matsumoto. A New 128-bit Block Cipher ***E2***. Technical Report ISEC98-12, The Institute of Electronics, Information and Communication Engineers, 1998. (in Japanese).

[KSW96] J. Kelsey, B. Schneier, and D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In N. Koblitz, editor, *Advances in Cryptology — CRYPTO'96*, Volume 1109 of *Lecture Notes in Computer Science*, pp. 237–251. Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[KTM+99] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta. A Strategy for Constructing Fast Round Functions with Practical Security against Differential and Linear Cryptanalysis. In S. Tavares and H. Meijer, editors, *Selected Areas in Cryptography — 5th Annual International Workshop, SAC'98*, Volume 1556 of *Lecture Notes in Computer Science*, pp. 264–279, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

[M94] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, Volume 765 of *Lecture Notes in Computer Science*, pp. 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994. (A preliminary version written in Japanese was presented at SCIS93-3C).

[MT99] M. Matsui and T. Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2. In L. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 71–80, Berlin, Heidelberg, New York, 1999. Springer-Verlag. (Japanese version was presented at SCIS99.).

[W99] D. Wagner. The Boomerang Attack. In L. R. Knudsen, editor, *Fast Software Encryption — 6th International Workshop, FSE'99*, Volume 1636 of *Lecture Notes in Computer Science*, pp. 156–170, Berlin, Heidelberg, New York, 1999. Springer-Verlag.

Errata

- C.2.7 The equation to calculate using only four tables, SP_1, SP_2, SP_3, and SP_4, has be corrected.
- Section D,E,F,G, and H have been added.