INTERNET-DRAFT
TLS Working Group
Expires November 2001

S. Moriai
Nippon Telegraph and Telephone Corporation

May 2001

Addition of the Camellia Encryption Algorithm to TLS

<draft-ietf-tls-camellia-01.txt>

Status of this Memo

Abstract

This document proposes the addition of new cipher suites to the TLS protocol 1.0 to support the Camellia encryption algorithm as a bulk cipher algorithm. Please send comments on this document to the TLS mailing list.

1. Introduction

This document proposes the addition of new cipher suites to the TLS protocol 1.0 [4] to support the Camellia encryption algorithm as a bulk cipher algorithm. This proposal provides a new option for bulk cipher algorithms.

Camellia is a block cipher with 128-bit block size and 128-, 192-, and 256-bit key sizes, i.e. the same interface specifications as the Advanced Encryption Standard (AES). The algorithm description is in [1][3]. Efficiency on both software and hardware platforms is a remarkable characteristic of Camellia in addition to its high level of security. It is confirmed that Camellia provides strong security

against differential and linear cryptanalysis. An optimized implementation of Camellia in assembly language can encrypt on a Pentium III (1.13GHz) at the rate of 471 Mbits per second. In addition, a distinguishing feature is its small hardware design. The hardware design, which includes the parts for key schedule, encryption and decryption, occupies only 9.66K gates using a 0.35um CMOS ASIC library, which is in the smallest class among all existing 128-bit block ciphers as far as we know [2].

2. Cipher Suites

We propose the new cipher suites below following the AES ciphersuites.

```
CipherSuite TLS_RSA_WITH_CAMELLIA_128_CBC_SHA      = { 0x00,0x41 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x42 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA   = { 0x00,0x43 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x44 };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x45 };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA  = { 0x00,0x46 };

CipherSuite TLS_RSA_WITH_CAMELLIA_256_CBC_SHA      = { 0x00,0x47 };
CipherSuite TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x48 };
CipherSuite TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA   = { 0x00,0x49 };
CipherSuite TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4A };
CipherSuite TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4B };
CipherSuite TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA  = { 0x00,0x4C };
```

Note: The above numeric definitions for Cipher Suites have not yet been registered. The numeric definitions follow the numbers given in the CipherSuite of the TLS standard.

3. CipherSuite Definitions

CipherSuite	Is Exportable	Key Exchange	Cipher	Hash
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		RSA	CAMELLIA_128_CBC	SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA		DH_DSS	CAMELLIA_128_CBC	SHA
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA		DH_RSA	CAMELLIA_128_CBC	SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA		DHE_DSS	CAMELLIA_128_CBC	SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		DHE_RSA	CAMELLIA_128_CBC	SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA		DH_anon	CAMELLIA_128_CBC	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		RSA	CAMELLIA_256_CBC	SHA
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA		DH_DSS	CAMELLIA_256_CBC	SHA
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA		DH_RSA	CAMELLIA_256_CBC	SHA
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA		DHE_DSS	CAMELLIA_256_CBC	SHA

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE_RSA	CAMELLIA_256_CBC	SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	DH_anon	CAMELLIA_256_CBC	SHA

Cipher	Type	Key Material	Expanded Key Material	Effective Key Bits	IV Size	Block Size
CAMELLIA_128_CBC	Block	16	16	128	16	16
CAMELLIA_256_CBC	Block	32	32	256	16	16

Note: Key Exchange Algorithms and Hash Functions are defined in TLS.

4. Security Considerations

Security considerations except Camellia are discussed in [4]. The security of Camellia is evaluated by utilizing state-of-the-art cryptanalytic techniques. We confirmed that Camellia has no differential and linear characteristics that hold with probability more than 2^(-128), which means that it is extremely unlikely that differential and linear attacks will succeed against Camellia. Moreover, Camellia was designed to offer security against other advanced cryptanalytic attacks including higher order differential attacks, interpolation attacks, related-key attacks, truncated differential attacks, and so on [3].

5. Intellectual Property Statement

Mitsubishi Electric Corporation (Mitsubishi Electric) and Nippon Telegraph and Telephone Corporation (NTT) have pending applications or filed patents which are essential to Camellia. License policy for these essential patents declared formally by NTT and Mitsubishi Electric will be available on the IETF page of Intellectual Property Rights Notices.

References

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita ``Specification of Camellia --- a 128-bit Block Cipher'', 2000. http://info.isl.ntt.co.jp/camellia/

[2] 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'', 2000. http://info.isl.ntt.co.jp/camellia/

[3] 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.

[4] T. Dierks, and C. Allen, ``The TLS Protocol Version 1.0'', RFC 2246, January 1999.

Author's Addresses

Shiho Moriai
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka, 239-0847, Japan
Phone: +81-468-59-2007
FAX: +81-468-59-3858
Email: shiho@isl.ntt.co.jp