Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2012

M. Katagi
S. Moriai
Sony Corporation
October 31, 2011

CLEFIA Cipher Suites for Transport Layer Security (TLS)
draft-katagi-tls-clefia-01

Abstract

This document specifies a set of cipher suites for the Transport Security Layer (TLS) protocol to support the CLEFIA encryption algorithm as a block cipher. CLEFIA is a lightweight block cipher and suitable for constrained devices.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document specifies cipher suites for the Transport Layer Security (TLS) [RFC5246] protocol to support the CLEFIA [RFC6114] encryption algorithm as a block cipher algorithm. The proposed ciphersuites include variants using the SHA-2 family of cryptographic hash functions [FIPS180-3] and Galois/Counter Mode (GCM) [GCM]. Elliptic Curve Cryptography (ECC) cipher suites and Pre-Shared Key (PSK) [RFC4279] cipher suites are also included.

1.1. CLEFIA

CLEFIA is a 128-bit blockcipher algorithm, with key lengths of 128, 192, and 256 bits, which is compatible with the interface of the Advanced Encryption Standard (AES) [FIPS-197]. The algorithm of CLEFIA was published in 2007 [FSE07]. Since AES was designed, cryptographic technologies have been advancing: new techniques on attack, design and implementation are extensively studied. CLEFIA is designed based on the state-of-the-art techniques on design and analysis of block ciphers. The security of CLEFIA has been scrutinized in the public community, and no security weaknesses have been reported so far.

CLEFIA is a general purpose blockcipher, and offers high performance in software and hardware. Especially, CLEFIA has an advantage in efficient hardware implementation over AES, Camellia, and SEED, which can be used in TLS. Its gate efficiency, which is defined as the ratio of speed to gate size, is superior to these ciphers [ISCAS08].

Standardization of CLEFIA in other organizations is in progress. CLEFIA is proposed in ISO/IEC 29192-2 [ISO29192-2] and the CRYPTREC project for the revision of the e-Government recommended ciphers list in Japan [CRYPTREC]. ISO/IEC 29192 is a standardization project of "LightWeight Cryptography (LWC)", which is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards and so on. LWC contributes to the security of the constrained devices connecting with IP.

The algorithm specification is described in RFC6114 [RFC6114]. Further information about CLEFIA, which includes design rationale, security evaluations, implementation results, and a reference code, is available from [CLEFIAWEB].

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in RFC2119 [RFC2119].

2. Proposed Cipher Suites

2.1. SHA-1 based Cipher Suites

The eight cipher suites use CLEFIA [RFC6114] in Cipher Block Chaining (CBC) mode with SHA-1 [FIPS180-3].

```
CipherSuite TLS_RSA_WITH_CLEFIA_128_CBC_SHA           = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_CBC_SHA       = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_CBC_SHA       = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_CBC_SHA       = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_CBC_SHA   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_CBC_SHA     = {TBD,TBD};
CipherSuite TLS_PSK_WITH_CLEFIA_128_CBC_SHA           = {TBD,TBD};
CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_CBC_SHA       = {TBD,TBD};
```

2.2. CBC + HMAC based Cipher Suites

The twenty cipher suites use CLEFIA in Cipher Block Chaining (CBC) mode with Hash-based Message Authentication Code (HMAC) with the SHA-2 family. Eight out of twenty use elliptic curves cryptography.

```
CipherSuite TLS_RSA_WITH_CLEFIA_128_CBC_SHA256        = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_128_CBC_SHA256     = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_128_CBC_SHA256     = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_RSA_WITH_CLEFIA_256_CBC_SHA384        = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_256_CBC_SHA384     = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_256_CBC_SHA384     = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};

CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_CBC_SHA256 = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_128_CBC_SHA256  = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_CBC_SHA256   = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_256_CBC_SHA384 = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_256_CBC_SHA384  = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_256_CBC_SHA384   = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
```

2.3. GCM based Cipher Suites

The twenty cipher suites use the same asymmetric key algorithms as those in the previous section but use the authenticated encryption modes defined in TLS 1.2 [RFC5246] with CLEFIA in GCM [GCM].

```
CipherSuite TLS_RSA_WITH_CLEFIA_128_GCM_SHA256          = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_128_GCM_SHA256       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_128_GCM_SHA256       = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_RSA_WITH_CLEFIA_256_GCM_SHA384          = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_256_GCM_SHA384       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_256_GCM_SHA384       = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};

CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_GCM_SHA256  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_128_GCM_SHA256   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_GCM_SHA256    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_128_GCM_SHA256     = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_256_GCM_SHA384  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_256_GCM_SHA384   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_256_GCM_SHA384    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_256_GCM_SHA384     = {TBD,TBD};
```

2.4. PSK based Cipher Suites

The fourteen cipher suites describe PSK cipher suites. The first eight cipher suites use the CLEFIA in CBC mode with HMAC with the SHA-2 family and the next six cipher suites use CLEFIA in GCM.

```
  CipherSuite TLS_PSK_WITH_CLEFIA_128_CBC_SHA256        = {TBD,TBD};
  CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
  CipherSuite TLS_RSA_PSK_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
  CipherSuite TLS_ECDHE_PSK_WITH_CLEFIA_128_CBC_SHA256  = {TBD,TBD};
  CipherSuite TLS_PSK_WITH_CLEFIA_256_CBC_SHA384        = {TBD,TBD};
  CipherSuite TLS_DHE_PSK_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
  CipherSuite TLS_RSA_PSK_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
  CipherSuite TLS_ECDHE_PSK_WITH_CLEFIA_256_CBC_SHA384  = {TBD,TBD};

  CipherSuite TLS_PSK_WITH_CLEFIA_128_GCM_SHA256        = {TBD,TBD};
  CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_GCM_SHA256    = {TBD,TBD};
  CipherSuite TLS_RSA_PSK_WITH_CLEFIA_128_GCM_SHA256    = {TBD,TBD};
  CipherSuite TLS_PSK_WITH_CLEFIA_256_GCM_SHA384        = {TBD,TBD};
  CipherSuite TLS_DHE_PSK_WITH_CLEFIA_256_GCM_SHA384    = {TBD,TBD};
```

```
     CipherSuite TLS_RSA_PSK_WITH_CLEFIA_256_GCM_SHA384    = {TBD,TBD};
```

3. Cipher Suite Definitions

3.1. Key Exchange

The RSA, DHE_RSA, DH_RSA, DHE_DSS, DH_DSS, ECDH, DH_anon, and ECDHE key exchanges are performed as defined in RFC5246 [RFC5246].

3.2. Cipher

The CLEFIA_128_CBC cipher suites use CLEFIA [RFC6114] in CBC mode with a 128-bit key and 128-bit Initialization Vector (IV); the CLEFIA_256_CBC cipher suites use a 256-bit key and 128-bit IV.

AES-authenticated encryption with associated data algorithms, AEAD_AES_128_GCM and AEAD_AES_256_GCM are described in RFC5116 [RFC5116]. AES GCM cipher suites for TLS are described in RFC5288 [RFC5288]. AES and CLEFIA share common characteristics, including key sizes and block length. CLEFIA_128_GCM and CLEFIA_256_GCM are defined according to those characteristics of AES.

3.3. Hash and PRFs

3.3.1. Hash and PRFs prior to TLS 1.2

The cipher suites ending with _SHA use HMAC-SHA1 as the MAC algorithm.

When used with TLS versions prior to TLS 1.2 (TLS 1.0 [RFC2246] and TLS 1.1 [RFC4346]), the PRF is calculated as specified in the appropriate version of the TLS specification.

3.3.2. Hash and PRFs for TLS 1.2

The hash algorithms and pseudorandom function (PRF) algorithms for TLS 1.2 [RFC5246] SHALL be as follows:

a) The cipher suites ending with _SHA256 use HMAC-SHA-256 [RFC2104] as the MAC algorithm, The PRF is the TLS PRF [RFC5246] with SHA-256 [FIPS180-3] as the hash function,
b) The cipher suites ending with _SHA384 use HMAC-SHA-384 [RFC2104] as the MAC algorithm, The PRF is the TLS PRF [RFC5246] with SHA-384 [FIPS180-3] as the hash function.

3.4. PSK cipher suites

PSK cipher suites for TLS are described in RFC4279 [RFC4279], RFC4785 [RFC4785], RFC5487 [RFC5487], and RFC5489 [RFC5489].

4. Security Considerations

The security of CLEFIA algorithm has been scrutinized in the public community since the algorithm was proposed, but no security weaknesses have been reported so far.

The cipher suites with SHA-1 are included in this document for interoperability with TLS prior to 1.2. NIST SP 800-131A describes that SHA-1 for non-digital signature applications (including HMAC-SHA-1) is acceptable; no security risk is currently known. The use of SHA-1 for digital signature generation by US Federal government agencies is allowed through 2013, but the user must accept some risk [SP800-131A]. SHA-1 may be used for digital signature verification in legacy-use, but there may be risk in doing so. Methods for mitigating this risk should be considered [SP800-131A].

For other security considerations, please refer to the security considerations in previous RFCs ([RFC4279], [RFC4785], [RFC5116], [RFC5288], [RFC5289], [RFC5487], and [GCM]). These apply to this document as well.

5. IANA Considerations

IANA is requested to allocate (has allocated) the following numbers in the TLS Cipher Suite Registry:

```
CipherSuite TLS_RSA_WITH_CLEFIA_128_CBC_SHA             = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_CBC_SHA         = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_CBC_SHA         = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_CBC_SHA         = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_CBC_SHA     = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_CBC_SHA       = {TBD,TBD};
CipherSuite TLS_PSK_WITH_CLEFIA_128_CBC_SHA             = {TBD,TBD};
CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_CBC_SHA         = {TBD,TBD};

CipherSuite TLS_RSA_WITH_CLEFIA_128_CBC_SHA256          = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_128_CBC_SHA256       = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_128_CBC_SHA256       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_CBC_SHA256      = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_CBC_SHA256      = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_CBC_SHA256      = {TBD,TBD};
CipherSuite TLS_RSA_WITH_CLEFIA_256_CBC_SHA384          = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_256_CBC_SHA384       = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_256_CBC_SHA384       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_256_CBC_SHA384      = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_256_CBC_SHA384      = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_256_CBC_SHA384      = {TBD,TBD};

CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_CBC_SHA256  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_128_CBC_SHA256   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_128_CBC_SHA256     = {TBD,TBD};
CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_256_CBC_SHA384  = {TBD,TBD};
CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_256_CBC_SHA384   = {TBD,TBD};
CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};
CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_256_CBC_SHA384     = {TBD,TBD};

CipherSuite TLS_RSA_WITH_CLEFIA_128_GCM_SHA256          = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_128_GCM_SHA256       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_128_GCM_SHA256       = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
CipherSuite TLS_RSA_WITH_CLEFIA_256_GCM_SHA384          = {TBD,TBD};
CipherSuite TLS_DHE_RSA_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
CipherSuite TLS_DH_RSA_WITH_CLEFIA_256_GCM_SHA384       = {TBD,TBD};
CipherSuite TLS_DHE_DSS_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
CipherSuite TLS_DH_DSS_WITH_CLEFIA_256_GCM_SHA384       = {TBD,TBD};
CipherSuite TLS_DH_anon_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
```

```
    CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_128_GCM_SHA256  = {TBD,TBD};
    CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_128_GCM_SHA256   = {TBD,TBD};
    CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_128_GCM_SHA256    = {TBD,TBD};
    CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_128_GCM_SHA256     = {TBD,TBD};
    CipherSuite TLS_ECDHE_ECDSA_WITH_CLEFIA_256_GCM_SHA384  = {TBD,TBD};
    CipherSuite TLS_ECDH_ECDSA_WITH_CLEFIA_256_GCM_SHA384   = {TBD,TBD};
    CipherSuite TLS_ECDHE_RSA_WITH_CLEFIA_256_GCM_SHA384    = {TBD,TBD};
    CipherSuite TLS_ECDH_RSA_WITH_CLEFIA_256_GCM_SHA384     = {TBD,TBD};

    CipherSuite TLS_PSK_WITH_CLEFIA_128_CBC_SHA256          = {TBD,TBD};
    CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_CBC_SHA256      = {TBD,TBD};
    CipherSuite TLS_RSA_PSK_WITH_CLEFIA_128_CBC_SHA256      = {TBD,TBD};
    CipherSuite TLS_ECDHE_PSK_WITH_CLEFIA_128_CBC_SHA256    = {TBD,TBD};
    CipherSuite TLS_PSK_WITH_CLEFIA_256_CBC_SHA384          = {TBD,TBD};
    CipherSuite TLS_DHE_PSK_WITH_CLEFIA_256_CBC_SHA384      = {TBD,TBD};
    CipherSuite TLS_RSA_PSK_WITH_CLEFIA_256_CBC_SHA384      = {TBD,TBD};
    CipherSuite TLS_ECDHE_PSK_WITH_CLEFIA_256_CBC_SHA384    = {TBD,TBD};

    CipherSuite TLS_PSK_WITH_CLEFIA_128_GCM_SHA256          = {TBD,TBD};
    CipherSuite TLS_DHE_PSK_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
    CipherSuite TLS_RSA_PSK_WITH_CLEFIA_128_GCM_SHA256      = {TBD,TBD};
    CipherSuite TLS_PSK_WITH_CLEFIA_256_GCM_SHA384          = {TBD,TBD};
    CipherSuite TLS_DHE_PSK_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
    CipherSuite TLS_RSA_PSK_WITH_CLEFIA_256_GCM_SHA384      = {TBD,TBD};
```

6. Acknowledgements

We would like to thank Shoichi Sakane for providing valuable comments.

7. References

7.1. Normative References

[FIPS180-3] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-3, October 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", April 2006, <http://csrc.nist.gov/publications/drafts/Draft-NIST_SP800-38D_Public_Comment.pdf>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, January 2007.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, August 2008.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, March 2009.

[RFC6114] Katagi, M. and S. Moriai, "The 128-Bit Blockcipher CLEFIA", RFC 6114, March 2011.

7.2. Informative References

[CLEFIAWEB]
Sony Corporation, "The 128-bit blockcipher CLEFIA", <http://www.sony.net/clefia>.

[CRYPTREC]
Cryptography Research and Evaluation Committees, "the revision of the e-Government Recommended Ciphers List", <http://www.cryptrec.go.jp/>.

[FIPS-197]
National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[FSE07] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and T. Iwata, "The 128-bit Blockcipher CLEFIA", proceedings of Fast Software Encryption 2007 - FSE 2007, LNCS4593, pp.181-195, Springer-Verlag, 2007.

[ISCAS08] Sugawara, T., Homma, N., Aoki, T., and A. Satoh, "High-performance ASIC implementations of the 128-bit block cipher CLEFIA", ISCAS 2008, pp.2925-2928, IEEE, 2008.

[ISO29192-2]
ISO/IEC 29192-2, "Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers", <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[SP800-131A]
National Institute of Standards and Technology, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", SP 800-131A,

January 2011, <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>.

Authors' Addresses

Masanobu Katagi
Sony Corporation

Phone: +81-3-5448-3701
Fax: +81-3-5448-6438
Email: Masanobu.Katagi@jp.sony.com

Shiho Moriai
Sony Corporation

Phone: +81-3-5448-3701
Fax: +81-3-5448-6438
Email: Shiho.Moriai@jp.sony.com