

AVTCore
Internet-Draft
Intended status: Standards Track
Expires: December 07, 2013

W. Kim
J. Lee
D. Kim
J. Park
D. Kwon
NSRI
June 05, 2013

The ARIA Algorithm and Its Use with the Secure Real-time Transport
Protocol(SRTP)
draft-ietf-avtcore-aria-srtp-02

Abstract

This document describes the use of the ARIA block cipher algorithm within the Secure Real-time Transport Protocol (SRTP) for providing confidentiality for the Real-time Transport Protocol (RTP) traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP). It details three modes of operation (CTR, CCM, GCM) and a SRTP Key Derivation Function for ARIA.

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 December 07, 2013.

Copyright Notice

Copyright (c) 2013 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 | 2 |
| 1.1. | ARIA | 3 |
| 1.2. | Terminology | 3 |
| 2. | Cryptographic Transforms | 3 |
| 2.1. | ARIA-CTR | 3 |
| 2.2. | ARIA-GCM | 6 |
| 2.3. | ARIA-CCM | 9 |
| 3. | Key Derivation Functions | 11 |
| 4. | Security Considerations | 11 |
| 5. | IANA Considerations | 12 |
| 5.1. | SDES | 12 |
| 5.2. | DTLS-SRTP | 12 |
| 5.3. | MIKEY | 18 |
| 6. | References | 19 |
| 6.1. | Normative References | 19 |
| 6.2. | Informative References | 20 |
| Appendix A. | Test Vectors | 21 |
| A.1. | ARIA-CTR Test Vectors | 21 |
| A.1.1. | ARIA_128_CTR_HMAC_SHA1_80 | 21 |
| A.1.2. | ARIA_192_CTR_HMAC_SHA1_80 | 22 |
| A.1.3. | ARIA_256_CTR_HMAC_SHA1_80 | 23 |
| A.2. | ARIA-GCM Test Vectors | 23 |
| A.2.1. | ARIA_128_GCM | 24 |
| A.2.2. | ARIA_256_GCM | 24 |
| A.3. | ARIA-CCM Test Vectors | 24 |
| A.3.1. | ARIA_128_CCM | 25 |
| A.3.2. | ARIA_256_CCM | 25 |
| A.3.3. | ARIA_128_CCM_8 | 26 |
| A.3.4. | ARIA_256_CCM_8 | 26 |
| A.3.5. | ARIA_128_CCM_12 | 26 |
| A.3.6. | ARIA_256_CCM_12 | 27 |
| A.4. | Key Derivation Test Vector | 27 |
| A.4.1. | ARIA_128 | 28 |
| A.4.2. | ARIA_192 | 29 |
| A.4.3. | ARIA_256 | 30 |

1. Introduction

This document describes the use of the ARIA [RFC5794] block cipher algorithm in the Secure Real-time Transport Protocol (SRTP) [RFC3711]

for providing confidentiality for the Real-time Transport Protocol (RTP) [RFC3550] traffic and for the control traffic for RTP, the Real-time Transport Control Protocol (RTCP) [RFC3550].

1.1. ARIA

ARIA is a general-purpose block cipher algorithm developed by Korean cryptographers in 2003. It is an iterated block cipher with 128-, 192-, and 256-bit keys and encrypts 128-bit blocks in 12, 14, and 16 rounds, depending on the key size. It is secure and suitable for most software and hardware implementations on 32-bit and 8-bit processors. It was established as a Korean standard block cipher algorithm in 2004 [ARIAKS] and has been widely used in Korea, especially for government-to-public services. It was included in PKCS #11 in 2007 [ARIAPKCS]. The algorithm specification and object identifiers are described in [RFC5794].

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].

2. Cryptographic Transforms

Block ciphers ARIA and AES share common characteristics including mode, key size, and block size. ARIA does not have any restrictions for modes of operation that are used with this block cipher. We define three modes of running ARIA within the SRTP protocol, (1) ARIA in Counter Mode (ARIA-CTR), (2) ARIA in Counter with CBC-MAC Mode (ARIA-CCM) and (3) ARIA in Galois/Counter Mode (ARIA-GCM).

2.1. ARIA-CTR

Section 4.1.1 of [RFC3711] defines AES-128 counter mode encryption, which it refers to as "AES_CM". Section 2 of [RFC6188] defines "AES_192_CM" and "AES_256_CM" in SRTP. ARIA counter modes are defined in the same manner except that each invocation of AES is replaced by that of ARIA, and are denoted by ARIA_128_CTR, ARIA_192_CTR and ARIA_256_CTR respectively, according to the key lengths. The plaintext inputs to the block cipher are formed as in AES-CTR(AES_CM, AES_192_CM, AES_256_CM) and the block cipher outputs are processed as in AES-CTR.

When ARIA-CTR is used, it MUST be used only in conjunction with an authentication function. The ARIA-CTR crypto suites with HMAC-SHA1 as an authentication function are listed below. The authentication key length of all crypto suites is 20 octets.

| Name | Enc. Key Length | Auth. Tag Length |
|---------------------------|-----------------|------------------|
| ARIA_128_CTR_HMAC_SHA1_80 | 16 octets | 10 octets |
| ARIA_128_CTR_HMAC_SHA1_32 | 16 octets | 4 octets |
| ARIA_192_CTR_HMAC_SHA1_80 | 24 octets | 10 octets |
| ARIA_192_CTR_HMAC_SHA1_32 | 24 octets | 4 octets |
| ARIA_256_CTR_HMAC_SHA1_80 | 32 octets | 10 octets |
| ARIA_256_CTR_HMAC_SHA1_32 | 32 octets | 4 octets |

Table 1: ARIA-CTR Crypto Suites for SRTP/SRTCP

The parameters (from Table 2 to Table 7) in each crypto suite listed in Table 1 are described for use with the SDP Security Descriptions attributes [RFC4568].

| Parameter | Value |
|---------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 80 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |
| SRTCP authentication tag length | 80 bits |

Table 2: The ARIA_128_CTR_HMAC_SHA1_80 Crypto Suite

| Parameter | Value |
|---------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 32 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |

| | |
|---------------------------------|---------|
| SRTCP authentication tag length | 80 bits |
|---------------------------------|---------|

Table 3: The ARIA_128_CTR_HMAC_SHA1_32 Crypto Suite

| Parameter | Value |
|---------------------------------|------------------------------|
| Master key length | 192 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_192_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_192_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 80 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |
| SRTCP authentication tag length | 80 bits |

Table 4: The ARIA_192_CTR_HMAC_SHA1_80 Crypto Suite

| Parameter | Value |
|---------------------------------|------------------------------|
| Master key length | 192 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_192_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_192_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 32 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |
| SRTCP authentication tag length | 80 bits |

Table 5: The ARIA_192_CTR_HMAC_SHA1_32 Crypto Suite

| Parameter | Value |
|-------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |

| | |
|---------------------------------|--------------|
| Cipher (for SRTP and SRTCP) | ARIA_256_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 80 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |
| SRTCP authentication tag length | 80 bits |

Table 6: The ARIA_256_CTR_HMAC_SHA1_80 Crypto Suite

| Parameter | Value |
|---------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 112 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_CTR |
| SRTP authentication function | HMAC-SHA1 |
| SRTP authentication key length | 160 bits |
| SRTP authentication tag length | 32 bits |
| SRTCP authentication function | HMAC-SHA1 |
| SRTCP authentication key length | 160 bits |
| SRTCP authentication tag length | 80 bits |

Table 7: The ARIA_256_CTR_HMAC_SHA1_32 Crypto Suite

2.2. ARIA-GCM

GCM(Galois Counter Mode) [GCM][RFC5116] is a AEAD(authenticated encryption with associated data) block cipher mode. A detailed description of ARIA-GCM is defined similarly as AES-GCM found in [RFC5116][RFC5282].

The internet draft [I-D.ietf-avtcore-srtp-aes-gcm] describes the use of AES-GCM with SRTP. The use of ARIA-GCM with SRTP is defined the same as that of AES-GCM except that each invocation of AES is replaced by ARIA.

The ARIA-GCM algorithms in Table 8 may be used with SRTP and SRTCP:

| Name | Enc. Key Length | Auth. Tag Length |
|-------------------|-----------------|------------------|
| AEAD_ARIA_128_GCM | 16 octets | 16 octets |
| AEAD_ARIA_256_GCM | 32 octets | 16 octets |

| | | |
|----------------------|-----------|-----------|
| AEAD_ARIA_128_GCM_8 | 16 octets | 8 octets |
| AEAD_ARIA_256_GCM_8 | 32 octets | 8 octets |
| AEAD_ARIA_128_GCM_12 | 16 octets | 12 octets |
| AEAD_ARIA_256_GCM_12 | 32 octets | 12 octets |

Table 8: ARIA-GCM Crypto Suites for SRTP/SRTCP

The parameters (from Table 9 to Table 14) in each crypto suite listed in Table 8 are described for use with the SDP Security Descriptions attributes [RFC4568].

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_GCM |
| AEAD authentication tag length | 128 bits |

Table 9: The AEAD_ARIA_128_GCM Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_GCM |
| AEAD authentication tag length | 128 bits |

Table 10: The AEAD_ARIA_256_GCM Crypto Suite

| Parameter | Value |
|------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |

| | |
|--------------------------------|--------------|
| Cipher (for SRTP and SRTCP) | ARIA_128_GCM |
| AEAD authentication tag length | 64 bits |

Table 11: The AEAD_ARIA_128_GCM_8 Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2^{48} packets |
| Default key lifetime (SRTCP) | 2^{31} packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_GCM |
| AEAD authentication tag length | 64 bits |

Table 12: The AEAD_ARIA_256_GCM_8 Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2^{48} packets |
| Default key lifetime (SRTCP) | 2^{31} packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_GCM |
| AEAD authentication tag length | 96 bits |

Table 13: The AEAD_ARIA_128_GCM_12 Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2^{48} packets |
| Default key lifetime (SRTCP) | 2^{31} packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_GCM |
| AEAD authentication tag length | 96 bits |

Table 14: The AEAD_ARIA_256_GCM_12 Crypto Suite

2.3. ARIA-CCM

CCM(Counter with CBC-MAC) [RFC3610][RFC5116] is another AEAD block cipher mode. A detailed description of ARIA-CCM is defined similarly as AES-CCM found in [RFC5116] [RFC6655] [I-D.ietf-avtcore-srtp-aes-gcm].

The internet draft [I-D.ietf-avtcore-srtp-aes-gcm] describes the use of AES-CCM with SRTP. The use of ARIA-CCM with SRTP is defined the same as that of AES-CCM except that each invocation of AES is replaced by ARIA.

The ARIA-CCM algorithms in Table 15 may be used with SRTP and SRTCP:

| Name | Enc. Key Length | Auth. Tag Length |
|----------------------|-----------------|------------------|
| AEAD_ARIA_128_CCM | 16 octets | 16 octets |
| AEAD_ARIA_256_CCM | 32 octets | 16 octets |
| AEAD_ARIA_128_CCM_8 | 16 octets | 8 octets |
| AEAD_ARIA_256_CCM_8 | 32 octets | 8 octets |
| AEAD_ARIA_128_CCM_12 | 16 octets | 12 octets |
| AEAD_ARIA_256_CCM_12 | 32 octets | 12 octets |

Table 15: ARIA-CCM Crypto Suites for SRTP/SRTCP

The parameters (from Table 16 to Table 21) in each crypto suite listed in Table 15 are described for use with the SDP Security Descriptions attributes [RFC4568].

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_CCM |
| AEAD authentication tag length | 128 bits |

Table 16: The AEAD_ARIA_128_CCM Crypto Suite

| Parameter | Value |
|-----------|-------|
|-----------|-------|

| | |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_CCM |
| AEAD authentication tag length | 128 bits |

Table 17: The AEAD_ARIA_256_CCM Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_CCM |
| AEAD authentication tag length | 64 bits |

Table 18: The AEAD_ARIA_128_CCM_8 Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_CCM |
| AEAD authentication tag length | 64 bits |

Table 19: The AEAD_ARIA_256_CCM_8 Crypto Suite

| Parameter | Value |
|------------------------------|------------------------------|
| Master key length | 128 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_128_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_128_CCM |

| | |
|--------------------------------|---------|
| AEAD authentication tag length | 96 bits |
|--------------------------------|---------|

Table 20: The AEAD_ARIA_128_CCM_12 Crypto Suite

| Parameter | Value |
|--------------------------------|------------------------------|
| Master key length | 256 bits |
| Master salt length | 96 bits |
| Key Derivation Function | ARIA_256_CTR_PRF (Section 3) |
| Default key lifetime (SRTP) | 2 ⁴⁸ packets |
| Default key lifetime (SRTCP) | 2 ³¹ packets |
| Cipher (for SRTP and SRTCP) | ARIA_256_CCM |
| AEAD authentication tag length | 96 bits |

Table 21: The AEAD_ARIA_256_CCM_12 Crypto Suite

3. Key Derivation Functions

Section 4.3.3 of [RFC3711] defines the AES-128 counter mode key derivation function, which it refers to as "AES-CM PRF". Section 3 of [RFC6188] defines the AES-192 counter mode key derivation function and the AES-256 counter mode key derivation function, which it refers to as "AES_192_CM_PRF" and "AES_256_CM_PRF" respectively. The ARIA-CTR PRF is defined in a same manner except that each invocation of AES replaced by that of ARIA. According to the key lengths of underlying encryption algorithm, ARIA-CTR PRFs are denoted by "ARIA_128_CTR_PRF", "ARIA_192_CTR_PRF" and "ARIA_256_CTR_PRF". The usage requirements of [RFC6188][I-D.ietf-avtcore-srtp-aes-gcm] regarding the AES-CM PRF apply to the ARIA-CTR PRF as well. The PRFs for ARIA crypto suites with SRTP are defined by ARIA-CTR PRF of the equal key length with the encryption algorithm (see Section 2). SRTP_ARIA_128_CTR_HMAC, SRTP_AEAD_ARIA_128_GCM, and SRTP_AEAD_ARIA_128_CCM MUST use the ARIA_128_CTR_PRF Key Derivation Function. SRTP_ARIA_192_CTR_HMAC MUST use that ARIA_192_CTR_PRF Key Derivation Function. And SRTP_ARIA_256_CTR_HMAC, SRTP_AEAD_ARIA_256_GCM, and SRTP_AEAD_ARIA_256_CCM MUST use the ARIA_256_CTR_PRF Key Derivation Function.

4. Security Considerations

At the time of writing this document no security problem has been found on ARIA (see [TSL]).

The security considerations in [RFC3610] [GCM] [RFC3711] [RFC5116] [RFC6188] [I-D.ietf-avtcore-srtp-aes-gcm] apply to this document as well.

5. IANA Considerations

5.1. SDP

Security description [RFC4568] defines SRTP "crypto suites". In order to allow SDP to signal the use of the algorithms defined in this document, IANA is requested to add the below crypto suites to the "SRTP Crypto Suite Registrations" created by [RFC4568], at time of writing located on the following IANA page: <http://www.iana.org/assignments/sdp-security-descriptions/sdp-security-descriptions.xml#sdp-security-descriptions-3> [1]

```
srtp-crypto-suite-ext = "ARIA_128_CTR_HMAC_SHA1_80"/
                        "ARIA_128_CTR_HMAC_SHA1_32"/
                        "ARIA_192_CTR_HMAC_SHA1_80"/
                        "ARIA_192_CTR_HMAC_SHA1_32"/
                        "ARIA_256_CTR_HMAC_SHA1_80"/
                        "ARIA_256_CTR_HMAC_SHA1_32"/
                        "AEAD_ARIA_128_GCM"      /
                        "AEAD_ARIA_256_GCM"      /
                        "AEAD_ARIA_128_GCM_8"    /
                        "AEAD_ARIA_256_GCM_8"    /
                        "AEAD_ARIA_128_GCM_12"   /
                        "AEAD_ARIA_256_GCM_12"   /
                        "AEAD_ARIA_128_CCM"      /
                        "AEAD_ARIA_256_CCM"      /
                        "AEAD_ARIA_128_CCM_8"    /
                        "AEAD_ARIA_256_CCM_8"    /
                        "AEAD_ARIA_128_CCM_12"   /
                        "AEAD_ARIA_256_CCM_12"   /
srtp-crypto-suite-ext
```

5.2. DTLS-SRTP

DTLS-SRTP [RFC5764] defines a DTLS-SRTP "SRTP Protection Profile". In order to allow the use of the algorithms defined in this document in DTLS-SRTP, IANA is requested to add the below crypto suite to the "DTLS-SRTP Protection Profiles" created by [RFC5764], at time of writing located on the following IANA page: <http://www.iana.org/assignments/srtp-protection/srtp-protection.xml#srtp-protection-1> [2]

```
SRTP_ARIA_128_CTR_HMAC_SHA1_80 = {TBD,TBD}
SRTP_ARIA_128_CTR_HMAC_SHA1_32 = {TBD,TBD}
```

```

SRTP_ARIA_192_CTR_HMAC_SHA1_80 = {TBD,TBD}
SRTP_ARIA_192_CTR_HMAC_SHA1_32 = {TBD,TBD}
SRTP_ARIA_256_CTR_HMAC_SHA1_80 = {TBD,TBD}
SRTP_ARIA_256_CTR_HMAC_SHA1_32 = {TBD,TBD}
SRTP_AEAD_ARIA_128_GCM = {TBD,TBD}
SRTP_AEAD_ARIA_256_GCM = {TBD,TBD}
SRTP_AEAD_ARIA_128_GCM_8 = {TBD,TBD}
SRTP_AEAD_ARIA_256_GCM_8 = {TBD,TBD}
SRTP_AEAD_ARIA_128_GCM_12 = {TBD,TBD}
SRTP_AEAD_ARIA_256_GCM_12 = {TBD,TBD}
SRTP_AEAD_ARIA_128_CCM = {TBD,TBD}
SRTP_AEAD_ARIA_256_CCM = {TBD,TBD}
SRTP_AEAD_ARIA_128_CCM_8 = {TBD,TBD}
SRTP_AEAD_ARIA_256_CCM_8 = {TBD,TBD}
SRTP_AEAD_ARIA_128_CCM_12 = {TBD,TBD}
SRTP_AEAD_ARIA_256_CCM_12 = {TBD,TBD}

```

The following list indicates the SRTP transform parameters for each protection profile. The parameters `cipher_key_length`, `cipher_salt_length`, `auth_key_length`, and `auth_tag_length` express the number of bits in the values to which they refer. The `maximum_lifetime` parameter indicates the maximum number of packets that can be protected with each single set of keys when the parameter profile is in use. All of these parameters apply to both RTP and RTCP, unless the RTCP parameters are separately specified.

SRTP_ARIA_128_CTR_HMAC_SHA1_80

```

cipher:                ARIA_128_CTR
cipher_key_length:    128 bits
cipher_salt_length:   112 bits
maximum_lifetime:    2^31 packets
key derivation function: ARIA_128_CTR_PRF
auth_function:        HMAC-SHA1
auth_key_length:      160 bits
auth_tag_length:      80 bits

```

SRTP_ARIA_128_CTR_HMAC_SHA1_32

```

cipher:                ARIA_128_CTR
cipher_key_length:    128 bits
cipher_salt_length:   112 bits
maximum_lifetime:    2^31 packets
key derivation function: ARIA_128_CTR_PRF
auth_function:        HMAC-SHA1
auth_key_length:      160 bits
SRTP auth_tag_length: 32 bits
SRTCP auth_tag_length: 80 bits

```

SRTP_ARIA_192_CTR_HMAC_SHA1_80

cipher: ARIA_192_CTR
cipher_key_length: 192 bits
cipher_salt_length: 112 bits
maximum_lifetime: 2³¹ packets
key derivation function: ARIA_192_CTR_PRF
auth_function: HMAC-SHA1
auth_key_length: 160 bits
auth_tag_length: 80 bits

SRTP_ARIA_192_CTR_HMAC_SHA1_32

cipher: ARIA_192_CTR
cipher_key_length: 192 bits
cipher_salt_length: 112 bits
maximum_lifetime: 2³¹ packets
key derivation function: ARIA_192_CTR_PRF
auth_function: HMAC-SHA1
auth_key_length: 160 bits
SRTP auth_tag_length: 32 bits
SRTCP auth_tag_length: 80 bits

SRTP_ARIA_256_CTR_HMAC_SHA1_80

cipher: ARIA_256_CTR
cipher_key_length: 256 bits
cipher_salt_length: 112 bits
maximum_lifetime: 2³¹ packets
key derivation function: ARIA_256_CTR_PRF
auth_function: HMAC-SHA
auth_key_length: 160 bits
auth_tag_length: 80 bits

SRTP_ARIA_256_CTR_HMAC_SHA1_32

cipher: ARIA_256_CTR
cipher_key_length: 128 bits
cipher_salt_length: 112 bits
maximum_lifetime: 2³¹ packets
key derivation function: ARIA_256_CTR_PRF
auth_function: HMAC-SHA1
auth_key_length: 160 bits
SRTP auth_tag_length: 32 bits
SRTCP auth_tag_length: 80 bits

SRTP_AEAD_ARIA_128_CCM

cipher: ARIA_128_CCM
cipher_key_length: 128 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 128 bits
auth_function: NULL
auth_key_length: N/A

auth_tag_length: N/A
 key derivation function: ARIA_128_CTR_PRF
 maximum_lifetime: at most 2^{31} SRTCP packets and
 at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_CCM

cipher: ARIA_256_CCM
 cipher_key_length: 256 bits
 cipher_salt_length: 96 bits
 aead_auth_tag_length: 128 bits
 auth_function: NULL
 auth_key_length: N/A
 auth_tag_length: N/A
 key derivation function: ARIA_256_CTR_PRF
 maximum_lifetime: at most 2^{31} SRTCP packets and
 at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_128_CCM_8

cipher: ARIA_128_CCM
 cipher_key_length: 128 bits
 cipher_salt_length: 96 bits
 aead_auth_tag_length: 64 bits
 auth_function: NULL
 auth_key_length: N/A
 auth_tag_length: N/A
 key derivation function: ARIA_128_CTR_PRF
 maximum_lifetime: at most 2^{31} SRTCP packets and
 at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_CCM_8

cipher: ARIA_256_CCM
 cipher_key_length: 256 bits
 cipher_salt_length: 96 bits
 aead_auth_tag_length: 64 bits
 auth_function: NULL
 auth_key_length: N/A
 auth_tag_length: N/A
 key derivation function: ARIA_256_CTR_PRF
 maximum_lifetime: at most 2^{31} SRTCP packets and
 at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_128_CCM_12

cipher: ARIA_128_CCM
 cipher_key_length: 128 bits
 cipher_salt_length: 96 bits
 aead_auth_tag_length: 96 bits
 auth_function: NULL
 auth_key_length: N/A

auth_tag_length: N/A
key derivation function: ARIA_128_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_CCM_12

cipher: ARIA_256_CCM
cipher_key_length: 256 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 96 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_256_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_128_GCM

cipher: ARIA_128_GCM
cipher_key_length: 128 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 128 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_128_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_GCM

cipher: ARIA_256_GCM
cipher_key_length: 256 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 128 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_256_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_128_GCM_8

cipher: ARIA_128_GCM
cipher_key_length: 128 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 64 bits
auth_function: NULL
auth_key_length: N/A

auth_tag_length: N/A
key derivation function: ARIA_128_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_GCM_8

cipher: ARIA_256_GCM
cipher_key_length: 256 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 64 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_256_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_128_GCM_12

cipher: ARIA_128_GCM
cipher_key_length: 128 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 96 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_128_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

SRTP_AEAD_ARIA_256_GCM_12

cipher: ARIA_256_GCM
cipher_key_length: 256 bits
cipher_salt_length: 96 bits
aead_auth_tag_length: 96 bits
auth_function: NULL
auth_key_length: N/A
auth_tag_length: N/A
key derivation function: ARIA_256_CTR_PRF
maximum_lifetime: at most 2^{31} SRTCP packets and
at most 2^{48} SRTP packets

Note that these SRTP Protection Profiles do not specify an `auth_function`, `auth_key_length`, or `auth_tag_length` because all of these profiles use AEAD algorithms, and thus do not use a separate `auth_function`, `auth_key`, or `auth_tag`. The term `aead_auth_tag_length` is used to emphasize that this refers to the authentication tag provided by the AEAD algorithm and that this tag is not located in the authentication tag field provided by SRTP/SRTCP.

5.3. MIKEY

[RFC3830] and [RFC5748] define encryption algorithms and PRFs for the SRTP policy in MIKEY. In order to allow the use of the algorithms defined in this document in MIKEY, IANA is requested to add the below crypto suites to the "MIKEY Security Protocol Parameters SRTP Type 0 (Encryption algorithm)" and to add the below PRF to the "MIKEY Security Protocol Parameters SRTP Type 5 (Pseudo Random Function)" created by [RFC3830], at time of writing located on the following IANA page <http://www.iana.org/assignments/mikey-payloads/mikey-payloads.xml#mikey-payloads-26> [3]

| SRTP Enc. alg | Value |
|---------------|-------|
| ARIA-CTR | TBD |
| ARIA-CCM | TBD |
| ARIA-GCM | TBD |

Default session encryption key length is 16 octets.

| SRTP PRF | Value |
|----------|-------|
| ARIA-CTR | TBD |

MIKEY specifies the algorithm family separately from the key length (which is specified by the Session Encryption key length) and the authentication tag length (specified by AEAD authentication tag length [I-D.ietf-avtcore-srtp-aes-gcm]).

| | Encryption Algorithm | Encryption Key Length | AEAD Auth. Tag Length |
|---------------------------|----------------------|-----------------------|-----------------------|
| SRTP_ARIA_128_CTR_HMAC_80 | ARIA-CTR | 16 octets | 80 bits |

| | | | |
|---------------------------|----------|-----------|----------|
| SRTP_ARIA_128_CTR_HMAC_32 | ARIA-CTR | 16 octets | 32 bits |
| SRTP_ARIA_192_CTR_HMAC_80 | ARIA-CTR | 24 octets | 80 bits |
| SRTP_ARIA_192_CTR_HMAC_32 | ARIA-CTR | 24 octets | 32 bits |
| SRTP_ARIA_256_CTR_HMAC_80 | ARIA-CTR | 32 octets | 80 bits |
| SRTP_ARIA_256_CTR_HMAC_32 | ARIA-CTR | 32 octets | 32 bits |
| SRTP_AEAD_ARIA_128_GCM | ARIA-GCM | 16 octets | 128 bits |
| SRTP_AEAD_ARIA_128_CCM | ARIA-CCM | 16 octets | 128 bits |
| SRTP_AEAD_ARIA_128_GCM_12 | ARIA-GCM | 16 octets | 96 bits |
| SRTP_AEAD_ARIA_128_CCM_12 | ARIA-CCM | 16 octets | 96 bits |
| SRTP_AEAD_ARIA_128_GCM_8 | ARIA-GCM | 16 octets | 64 bits |
| SRTP_AEAD_ARIA_128_CCM_8 | ARIA-CCM | 16 octets | 64 bits |
| SRTP_AEAD_ARIA_256_GCM | ARIA-GCM | 32 octets | 128 bits |
| SRTP_AEAD_ARIA_256_CCM | ARIA-CCM | 32 octets | 128 bits |
| SRTP_AEAD_ARIA_256_GCM_12 | ARIA-GCM | 32 octets | 96 bits |
| SRTP_AEAD_ARIA_256_CCM_12 | ARIA-CCM | 32 octets | 96 bits |
| SRTP_AEAD_ARIA_256_GCM_8 | ARIA-GCM | 32 octets | 64 bits |
| SRTP_AEAD_ARIA_256_CCM_8 | ARIA-CCM | 32 octets | 64 bits |

+=====+

Figure 1: Mapping MIKEY parameters to AEAD algorithm

6. References

6.1. Normative References

- [GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST SP 800-38D, November 2007.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.
- [RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.
- [RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.
- [RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, July 2006.

- [RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.
- [RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, August 2008.
- [RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.
- [RFC6188] McGrew, D., "The Use of AES-192 and AES-256 in Secure RTP", RFC 6188, March 2011.
- [RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, July 2012.

6.2. Informative References

- [ARIAKS] Korean Agency for Technology and Standards, "128 bit block encryption algorithm ARIA - Part 1: General (in Korean)", KS X 1213-1:2009, December 2009.
- [ARIAPKCS] RSA Laboratories, "Additional PKCS #11 Mechanisms", PKCS #11 v2.20 Amendment 3 Revision 1, January 2007.
- [I-D.ietf-avtcore-srtp-aes-gcm] McGrew, D. and K. Igoe, "AES-GCM and AES-CCM Authenticated Encryption in Secure RTP (SRTP)", draft-ietf-avtcore-srtp-aes-gcm-06 (work in progress), May 2013.
- [RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.
- [RFC5748] Yoon, S., Jeong, J., Kim, H., Jeong, H., and Y. Won, "IANA Registry Update for Support of the SEED Cipher Algorithm in Multimedia Internet KEYing (MIKEY)", RFC 5748, August 2010.
- [RFC5794] Lee, J., Lee, J., Kim, J., Kwon, D., and C. Kim, "A Description of the ARIA Encryption Algorithm", RFC 5794, March 2010.

[TSL] Tang, X., Sun, B., Li, R., Li, C., and J. Yin, "A meet-in-the-middle attack on reduced-round ARIA", The Journal of Systems and Software Vol.84(10), pp. 1685-1692, October 2011.

Appendix A. Test Vectors

All values are in hexadecimal.

A.1. ARIA-CTR Test Vectors

Common values are organized as follows:

| | |
|------------------------|--|
| Rollover Counter: | 00000000 |
| Sequence Number: | 315e |
| SSRC: | 20e8f5eb |
| Authentication Key: | f93563311b354748c97891379553063116452309 |
| Session Salt: | cd3a7c42c671e0067a2a2639b43a |
| Initialization Vector: | cd3a7c42e69915ed7a2a263985640000 |
| RTP header: | 8008315ebf2e6fe020e8f5eb |
| RTP Payload: | f57af5fd4ae19562976ec57a5a7ad55a 5af5c5e5c5fdf5c55ad57a4a7272d572 62e9729566ed66e97ac54a4a5a7ad5e1 5ae5fdd5fd5ac5d56ae56ad5c572d54a e54ac55a956afd6aed5a4ac562957a95 16991691d572fd14e97ae962ed7a9f4a 955af572e162f57a956666e17ae1f54a 95f566d54a66e16e4afd6a9f7ae1c5c5 5ae5d56afde916c5e94a6ec56695e14a fde1148416e94ad57ac5146ed59d1cc5 |

A.1.1. ARIA_128_CTR_HMAC_SHA1_80

| | |
|------------------------|--|
| Session Key: | 0c5ffd37a11edc42c325287fc0604f2e |
| Encrypted RTP Payload: | 1bf753f412e6f35058cc398dc851aae3 a6ccdc463fbed9cfb3de2fb76fdffa9 e481f5efb64c92487f59dabbc7cc72da 092485f3fbad87888820b86037311fa4 4330e18a59a1e1338ba2c21458493a57 463475c54691f91cec785429119e0dfc d9048f90e07fec50b528e8c62ee6e71 445de5d7f659405135aff3604c2ca4ff 4aaca40809cb9eee42cc4ad232307570 81ca289f2851d3315e9568b501fdce6d |

Authenticated portion || Rollover Counter:

```
8008315ebf2e6fe020e8f5eb1bf753f4
12e6f35058cc398dc851aae3a6ccdcb4
63fbed9cfb3de2fb76fdffa9e481f5ef
b64c92487f59dabbc7cc72da092485f3
fbad87888820b86037311fa44330e18a
59a1e1338ba2c21458493a57463475c5
4691f91cec785429119e0dfcd9048f90
e07fecd50b528e8c62ee6e71445de5d7
f659405135aff3604c2ca4ff4aaca408
09cb9eee42cc4ad23230757081ca289f
2851d3315e9568b501fdce6d00000000
```

Authentication Tag: f9de4e729054672b0e35

A.1.2. ARIA_192_CTR_HMAC_SHA1_80

Session Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe32

Encrypted RTP Payload: 86f4556486642caa67e9b40fef2acda0
6d442517d8d58c15e3e0b5c13a78b8b2
838b7b96961e11acb2af81348272888c
fd9d168ba091fe3e4f7f83c7871570a9
aa9f995036e44c35cb742b601e8d8d08
48320bad732929103f1bfbb1ae873178
0479c5df2d4d41f78f6b96d6832db3db
6af8b3612b27e18a0a29a8a1d280437e
b8dad58e78658ec3b069d7329431c356
c5e612b3dde5bd3f6c9f42f39cf35d3a

Authenticated portion || Rollover Counter:
8008315ebf2e6fe020e8f5eb86f45564
86642caa67e9b40fef2acda06d442517
d8d58c15e3e0b5c13a78b8b2838b7b96
961e11acb2af81348272888cfd9d168b
a091fe3e4f7f83c7871570a9aa9f9950
36e44c35cb742b601e8d8d0848320bad
732929103f1bfbb1ae8731780479c5df
2d4d41f78f6b96d6832db3db6af8b361
2b27e18a0a29a8a1d280437eb8dad58e
78658ec3b069d7329431c356c5e612b3
dde5bd3f6c9f42f39cf35d3a00000000

Authentication Tag: 3935fa37ee96dbc550d5

A.1.3. ARIA_256_CTR_HMAC_SHA1_80

Session Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe3216aa5eb105783b54

Encrypted RTP Payload: c424c59fd5696305e5b13d8e8ca76566
17ccd7471088af9debf07b55c750f804
a5ac2b737be48140958a9b420524112a
e72e4da5bca59d2b1019ddd7dbdc30b4
3d5f046152ced40947d62d2c93e7b8e5
0f02db2b6b61b010e4c1566884de1fa9
702cdf8157e8aedfe3dd77c76bb50c25
ae4d624615c15acfdeeb5f79482aaa01
d3e4c05eb601eca2bd10518e9d46b021
16359232e9eac0fabd05235dd09e6dea

Authenticated portion || Rollover Counter:
8008315ebf2e6fe020e8f5ebc424c59f
d5696305e5b13d8e8ca7656617ccd747
1088af9debf07b55c750f804a5ac2b73
7be48140958a9b420524112ae72e4da5
bca59d2b1019ddd7dbdc30b43d5f0461
52ced40947d62d2c93e7b8e50f02db2b
6b61b010e4c1566884de1fa9702cdf81
57e8aedfe3dd77c76bb50c25ae4d6246
15c15acfdeeb5f79482aaa01d3e4c05e
b601eca2bd10518e9d46b02116359232
e9eac0fabd05235dd09e6dea00000000

Authentication Tag: 192f515fab04bbb4e62c

A.2. ARIA-GCM Test Vectors

Common values are organized as follows:

Rollover Counter: 00000000
Sequence Number: 315e
SSRC: 20e8f5eb
Encryption Salt: 000000000000000000000000

Initialization Vector: 000020e8f5eb00000000315e
Payload: f57af5fd4ae19562976ec57a5a7ad55a
5af5c5e5c5fd5c55ad57a4a7272d572
62e9729566ed66e97ac54a4a5a7ad5e1
5ae5fdd5fd5ac5d56ae56ad5c572d54a
e54ac55a956afd6aed5a4ac562957a95
16991691d572fd14e97ae962ed7a9f4a

955af572e162f57a956666e17ae1f54a
95f566d54a66e16e4afd6a9f7ae1c5c5
5ae5d56afde916c5e94a6ec56695e14a
fde1148416e94ad57ac5146ed59d1cc5
AAD: 8008315ebf2e6fe020e8f5eb

A.2.1. ARIA_128_GCM

Key: e91e5e75da65554a48181f3846349562

Encrypted RTP Payload: 4d8a9a0675550c704b17d8c9ddc81a5c
d6f7da34f2fe1b3db7cb3dfb9697102e
a0f3c1fc2dbc873d44bceae8e444297
4ba21ff6789d3272613fb9631a7cf3f1
4bacbeb421633a90ffbe58c2fa6bdca5
34f10d0de0502ce1d531b6336e588782
78531e5c22bc6c85bbd784d78d9e680a
a19031aaf89101d669d7a3965c1f7e16
229d7463e0535f4e253f5d18187d40b8
ae0f564bd970b5e7e2adfb211e89a953

Authentication Tag: 5abace3f37f5a736f4be984bbffbedc1

A.2.2. ARIA_256_GCM

Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe3216aa5eb105783b54

Encrypted RTP Payload: 6f9e4bc8c85fc0128fb1e4a0a20cb9
932ff74581f54fc013dd054b19f99371
425b352d97d3f337b90b63d1b082adee
ea9d2d7391897d591b985e55fb50cb53
50cf7d38dc27dda127c078a149c8eb98
083d66363a46e3726af217d3a00275ad
5bf772c7610ea4c23006878f0ee69a83
97703169a419303f40b72e4573714d19
e2697df61e7c7252e5abc6bade876ac4
961bfac4d5e867afca351a48aed52822

Authentication Tag: e210d6ced2cf430ff841472915e7ef48

A.3. ARIA-CCM Test Vectors

Common values are organized as follows:

Rollover Counter: 00000000
Sequence Number: 315e
SSRC: 20e8f5eb
Encryption Salt: 000000000000000000000000

Initialization Vector: 000020e8f5eb00000000315e
Payload: f57af5fd4ae19562976ec57a5a7ad55a
5af5c5e5c5fdf5c55ad57a4a7272d572
62e9729566ed66e97ac54a4a5a7ad5e1
5ae5fdd5fd5ac5d56ae56ad5c572d54a
e54ac55a956afd6aed5a4ac562957a95
16991691d572fd14e97ae962ed7a9f4a
955af572e162f57a956666e17ae1f54a
95f566d54a66e16e4afd6a9f7ae1c5c5
5ae5d56afde916c5e94a6ec56695e14a
fde1148416e94ad57ac5146ed59d1cc5

AAD: 8008315ebf2e6fe020e8f5eb

A.3.1. ARIA_128_CCM

Key: 974bee725d44fc3992267b284c3c6750

Encrypted RTP Payload: 621e408a2e455505b39f704dcbac4307
daabbd6d670abc4e42f2fd2fca263f09
4f4683e6fb0b10c5093d42b69dce0ba5
46520e7c4400975713f3bde93ef13116
0b9cbcd6df78a1502be7c6ea8d395b9e
d0078819c3105c0ab92cb67b16ba51bb
1f53508738bf7a37c9a905439b88b7af
9d51a407916fdfea8d43bf253721846d
c1671391225fc58d9d0693c8ade6a4ff
b034ee6543dd4e651b7a084eae60f855

Authentication Tag: 40f04b6467e300f6b336aedf9df4185b

A.3.2. ARIA_256_CCM

Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe3216aa5eb105783b54

Encrypted RTP Payload: ff78128ee18ee3cb9fb0d20726a017ff
67fbd09d3a4c38aa32f6d306d3fdda37
8e459b83ed005507449d6cd981a4c1e3
ff4193870c276ef09b6317a01a228320
6ae4b4be0d0b235422c8abb001224106
56b75e1ffc7fb49c0d0c5d6169aa7623

```
610579968037aee8e83fc26264ea8665
90fd620aa3c0a5f323d953aa7f8defb0
d0d60ab5a9de44dbaf8eae74ea3ab5f3
0594154f405fd630aa4c4d5603efdfa1
```

Authentication Tag: 87b6bd222c55365a9c7d0b215b77ea41

A.3.3. ARIA_128_CCM_8

Key: 974bee725d44fc3992267b284c3c6750

Encrypted RTP Payload: 621e408a2e455505b39f704dcbac4307
daabbd6d670abc4e42f2fd2fca263f09
4f4683e6fb0b10c5093d42b69dce0ba5
46520e7c4400975713f3bde93ef13116
0b9cbcd6df78a1502be7c6ea8d395b9e
d0078819c3105c0ab92cb67b16ba51bb
1f53508738bf7a37c9a905439b88b7af
9d51a407916fdfea8d43bf253721846d
c1671391225fc58d9d0693c8ade6a4ff
b034ee6543dd4e651b7a084eae60f855

Authentication Tag: dd2282c93a67fe4b

A.3.4. ARIA_256_CCM_8

Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe3216aa5eb105783b54

Encrypted RTP Payload: ff78128ee18ee3cb9fb0d20726a017ff
67fbd09d3a4c38aa32f6d306d3fdda37
8e459b83ed005507449d6cd981a4c1e3
ff4193870c276ef09b6317a01a228320
6ae4b4be0d0b235422c8abb001224106
56b75e1ffc7fb49c0d0c5d6169aa7623
610579968037aee8e83fc26264ea8665
90fd620aa3c0a5f323d953aa7f8defb0
d0d60ab5a9de44dbaf8eae74ea3ab5f3
0594154f405fd630aa4c4d5603efdfa1

Authentication Tag: 828dc0088f99a7ef

A.3.5. ARIA_128_CCM_12

Key: 974bee725d44fc3992267b284c3c6750

Encrypted RTP Payload: 621e408a2e455505b39f704dcbac4307
daabbd6d670abc4e42f2fd2fca263f09
4f4683e6fb0b10c5093d42b69dce0ba5
46520e7c4400975713f3bde93ef13116
0b9cbcd6df78a1502be7c6ea8d395b9e
d0078819c3105c0ab92cb67b16ba51bb
1f53508738bf7a37c9a905439b88b7af
9d51a407916fdfea8d43bf253721846d
c1671391225fc58d9d0693c8ade6a4ff
b034ee6543dd4e651b7a084eae60f855

Authentication Tag: 01f3dedd15238da5ebfb1590

A.3.6. ARIA_256_CCM_12

Key: 0c5ffd37a11edc42c325287fc0604f2e
3e8cd5671a00fe3216aa5eb105783b54

Encrypted RTP Payload: ff78128ee18ee3cb9fb0d20726a017ff
67fbd09d3a4c38aa32f6d306d3fdda37
8e459b83ed005507449d6cd981a4c1e3
ff4193870c276ef09b6317a01a228320
6ae4b4be0d0b235422c8abb001224106
56b75e1ffc7fb49c0d0c5d6169aa7623
610579968037aee8e83fc26264ea8665
90fd620aa3c0a5f323d953aa7f8defb0
d0d60ab5a9de44dbaf8eae74ea3ab5f3
0594154f405fd630aa4c4d5603efdfa1

Authentication Tag: 3615b7f90a651de15da20fb6

A.4. Key Derivation Test Vector

This section provides test vectors for the default key derivation function, which uses ARIA in Counter Mode. In the following, we walk through the initial key derivation for the ARIA Counter Mode cipher, which requires a 16/24/32 octet session encryption key according to the session encryption key length and a 14 octet session salt, and an authentication function which requires a 94 octet session authentication key. These values are called the cipher key, the cipher salt, and the auth key in the following. The test vectors are generated in the same way with the test vectors of key derivation functions in [RFC3711] and [RFC6188] but with each invocation of AES replaced with an invocation of ARIA.

A.4.1. ARIA_128

The inputs to the key derivation function are the 16 octet master key and the 14 octet master salt:

```

master key:  elf97a0d3e018be0d64fa32c06de4139
master salt:  0ec675ad498afeebb6960b3aabe6

index DIV kdr:          000000000000
label:                  00
master salt:            0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afeebb6960b3aabe6      (x, PRF input)

x*2^16:                0ec675ad498afeebb6960b3aabe60000  (ARIA-CTR input)

cipher key:            dbd85a3c4d9219b3e81f7d942e299de4  (ARIA-CTR output)

```

ARIA-CTR crypto suite requires 14 octet cipher salt while ARIA-CCM and ARIA-GCM crypto suites require 12 octet cipher salt.

```

index DIV kdr:          000000000000
label:                  02
master salt:            0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afee9b6960b3aabe6      (x, PRF input)

x*2^16:                0ec675ad498afee9b6960b3aabe60000  (ARIA-CTR input)

                       9700657f5f34161830d7d85f5dc8be7f  (ARIA-CTR output)

cipher salt:           9700657f5f34161830d7d85f5dc8      (ARIA-CTR cipher
suite)

                       9700657f5f34161830d7d85f          (ARIA-CCM or
ARIA-GCM cipher suite)

index DIV kdr:          000000000000
label:                  01
master salt:            0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afeeab6960b3aabe6      (x, PRF input)

x*2^16:                0ec675ad498afeeab6960b3aabe60000  (ARIA-CTR input)

```

Below, the auth key is shown on the left, while the corresponding ARIA input blocks are shown on the right.

| auth key | ARIA input blocks |
|----------------------------------|----------------------------------|
| d021877bd3eaf92d581ed70ddc050e03 | 0ec675ad498afeeab6960b3aabe60000 |
| f11257032676f2a29f57b21abd3a1423 | 0ec675ad498afeeab6960b3aabe60001 |
| 769749bdc5dd9ca5b43ca6b6c1f3a7de | 0ec675ad498afeeab6960b3aabe60002 |
| 4047904bcf811f601cc03eaa5d7af6db | 0ec675ad498afeeab6960b3aabe60003 |
| 9f88efa2e51ca832fc2a15b126fa7be2 | 0ec675ad498afeeab6960b3aabe60004 |
| 469af896acb1852c31d822c45799 | 0ec675ad498afeeab6960b3aabe60005 |

A.4.2. ARIA_192

The inputs to the key derivation function are the 24 octet master key and the 14 octet master salt:

```

master key: 0c5ffd37a11edc42c325287fc0604f2e3e8cd5671a00fe32
master salt: 0ec675ad498afeebb6960b3aabe6

index DIV kdr:          000000000000
label:                  00
master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afeebb6960b3aabe6      (x, PRF input)

x*2^16:                0ec675ad498afeebb6960b3aabe60000 (ARIA-CTR input)

cipher key: f320af2386a1cde64c3aa5f55d68002e (ARIA-CTR 1st output)
            d13cbe548b627649                (ARIA-CTR 2nd Output)

```

ARIA-CTR cipher suite requires 14 octet cipher salt while ARIA-CCM and ARIA-GCM cipher suites require 12 octet cipher salt.

```

index DIV kdr:          000000000000
label:                  02
master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afee9b6960b3aabe6      (x, PRF input)

x*2^16:                0ec675ad498afee9b6960b3aabe60000 (ARIA-CTR input)

                    55c7e3555baf0fdc91c589cfb871b098 (ARIA-CTR output)

cipher salt: 55c7e3555baf0fdc91c589cfb871      (ARIA-CTR cipher
suite)
            55c7e3555baf0fdc91c589cf          (ARIA-CCM or
ARIA-GCM cipher suite)

```

```

index DIV kdr:          000000000000
label:                  01
master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afeeab6960b3aabe6      (x, PRF input)

x*2^16:                 0ec675ad498afeeab6960b3aabe60000 (ARIA-CTR input)

```

Below, the auth key is shown on the left, while the corresponding ARIA input blocks are shown on the right.

| auth key | ARIA input blocks |
|----------------------------------|----------------------------------|
| 116902524517f7e767a979ad7678d53a | 0ec675ad498afeeab6960b3aabe60000 |
| 8cae05a5c9a315d1304f634c81a06617 | 0ec675ad498afeeab6960b3aabe60001 |
| 31fe099d4dcd2202421fe01fc12c65ad | 0ec675ad498afeeab6960b3aabe60002 |
| 009e920031654855af5d9e820a7831e0 | 0ec675ad498afeeab6960b3aabe60003 |
| bc2b4744d2a33053eb685138252f2d82 | 0ec675ad498afeeab6960b3aabe60004 |
| 9a89f4a9aa4f97fde0cce9bad3d5 | 0ec675ad498afeeab6960b3aabe60005 |

A.4.3. ARIA_256

The inputs to the key derivation function are the 32 octet master key and the 14 octet master salt:

```

master key: 0c5ffd37a11edc42c325287fc0604f2e
             3e8cd5671a00fe3216aa5eb105783b54
master salt: 0ec675ad498afeebb6960b3aabe6

index DIV kdr:          000000000000
label:                  00
master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:                    0ec675ad498afeebb6960b3aabe6      (x, PRF input)

x*2^16:                 0ec675ad498afeebb6960b3aabe60000 (ARIA-CTR input)

cipher key: 0649a09d93755fe9c2b2efbalcce930a (ARIA-CTR 1st output)
             f2e76ce8b77e4b175950321aa94b0cf4 (ARIA-CTR 2nd output)

```

ARIA-CTR cipher suite requires 14 octet cipher salt while ARIA-CCM and ARIA-GCM cipher suites require 12 octet cipher salt.

```

index DIV kdr:          000000000000
label:                  02

```

```

master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:         0ec675ad498afee9b6960b3aabe6      (x, PRF input)

x*2^16:     0ec675ad498afee9b6960b3aabe60000 (ARIA-CTR input)
           194abaa8553a8eba8a413a340fc80a3d (ARIA-CTR output)

cipher salt: 194abaa8553a8eba8a413a340fc8      (ARIA-CTR cipher
suite)
           194abaa8553a8eba8a413a34          (ARIA-CCM or
ARIA-GCM cipher suite)

index DIV kdr:          000000000000
label:                  01
master salt: 0ec675ad498afeebb6960b3aabe6
-----
xor:         0ec675ad498afeeab6960b3aabe6      (x, PRF input)

x*2^16:     0ec675ad498afeeab6960b3aabe60000 (ARIA-CTR input)

```

Below, the auth key is shown on the left, while the corresponding ARIA input blocks are shown on the right.

| auth key | ARIA input blocks |
|----------------------------------|----------------------------------|
| e58d42915873b71899234807334658f2 | 0ec675ad498afeeab6960b3aabe60000 |
| 0bc460181d06e02b7a9e60f02ff10bfc | 0ec675ad498afeeab6960b3aabe60001 |
| 9ade3795cf78f3e0f2556d9d913470c4 | 0ec675ad498afeeab6960b3aabe60002 |
| e82e45d254bfb8e2933851a3930ffe7d | 0ec675ad498afeeab6960b3aabe60003 |
| fca751c03ec1e77e35e28dac4f17d1a5 | 0ec675ad498afeeab6960b3aabe60004 |
| 80bdac028766d3b1e8f5a41faa3c | 0ec675ad498afeeab6960b3aabe60005 |

Authors' Addresses

Woo-Hwan Kim
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: whkim5@ensec.re.kr

Jungkeun Lee
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: jklee@ensec.re.kr

Dong-Chan Kim
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: dongchan@ensec.re.kr

Je-Hong Park
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: jhpark@ensec.re.kr

Daesung Kwon
National Security Research Institute
P.O.Box 1, Yuseong
Daejeon 305-350
Korea

EMail: ds_kwon@ensec.re.kr