Network Working Group
Internet-Draft
Intended status: Informational
Expires: 19 February 2026

Y. Guo
L. Xia
Huawei
Y. Fu
China Unicom

18 August 2025

Using ShangMi in the Internet Key Exchange Protocol Version 2 (IKEv2)
draft-guo-ipsecme-ikev2-using-shangmi-03

Abstract

This document defines a set of cryptographic transforms for use in the Internet Key Exchange Protocol version 2 (IKEv2). The transforms are based on ISO and Chinese cryptographic standard algorithms (called "ShangMi" or “SM” algorithms).

The use of these algorithms with IKEv2 is not endorsed by the IETF. The SM algorithms is ISO standardization and are mandatory for some scenario in China, so this document provides a description of how to use the SM algorithms with IKEv2 and specifies a set of cryptographic transforms so that implementers can produce interworking implementations.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-guo-ipsecme-ikev2-using-shangmi/.

Discussion of this document takes place on the ipsec Working Group mailing list (mailto:ipsec@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ipsec/. Subscribe at https://www.ietf.org/mailman/listinfo/ipsec/.

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 https://datatracker.ietf.org/drafts/current/.

This Internet-Draft will expire on 19 February 2026.

Copyright Notice

Table of Contents

1. Introduction

This document describes a number of new transforms and a new authentication method using SM2 signature and SM3 hash function for IKEv2 ([RFC7296]), based on ISO and Chinese cryptographic standard algorithms ("SM" algorithms) for encryption, hash function, digital signature, and key exchange method. With the definition in this document, the SM algorithms can be used to implement IPSec protocols.

For a more detailed introduction to SM cryptographic algorithms, please see Section 1.1. These transforms follow the IKEv2 requirements. Specifically, all the encryption transforms use SM4 in different encryption mode (e.g. CBC mode, Galois/Counter (GCM) mode or Counter with CBC-MAC (CCM) mode) . The key exchange mechanism utilizes Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) over the SM2 elliptic curve, and the signature algorithm combines the SM3 hash function and the SM2 elliptic curve signature scheme.

1.1. The SM Algorithms

Several different SM cryptographic algorithms are used to integrate with IKEv2, including SM2 for key exchange and authentication, SM4 for encryption, and SM3 as the hash function.

SM2 is a set of cryptographic algorithms based on elliptic curve cryptography, including a digital signature, public key encryption and key exchange scheme. In this document, only the SM2 digital signature algorithm and basic key exchange scheme are involved, which have already been added to ISO/IEC 14888-3:2018 [ISO-SM2] (as well as to [GBT.32918.2-2016]). The parameter definition of SM2 is described in [GBT.32918.5-2017]. SM4 is a block cipher defined in [GBT.32907-2016] and now is being standardized by ISO to ISO/IEC 18033-3:2010 [ISO-SM4]. SM3 is a hash function that produces an output of 256 bits. SM3 has already been accepted by ISO in ISO/IEC 10118-3:2018 [ISO-SM3] and has also been described by [GBT.32905-2016].

Caution: This specification is not a standard and does not have IETF community consensus. It makes use of cryptographic algorithms that are national standards for China, as well as ISO/IEC standards (ISO/IEC 14888-3:2018 [ISO-SM2], ISO/IEC 18033-3:2010 [ISO-SM4] and ISO/IEC 10118-3:2018 [ISO-SM3]). Neither the IETF nor the IRTF has analyzed that algorithm for suitability for any given application, and it may contain either intended or unintended weaknesses.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Transforms Description

3.1. Encryption Transforms

The new encryption transforms introduced in this document add three encryption algorithms: ENCR_SM4_CBC, ENCR_SM4_GCM and ENCR_SM4_CCM.

ENCR_SM4_CBC is encryption transform based on SM4 for SM4[ISO-SM4] and [GBT.32907-2016]encryption algorithm using CBC mode.

ENCR_SM4_GCM (Transform ID XX) and ENCR_SM4_CCM (Transform ID XX) are AEAD transforms based on SM4 cipher in Galois/Counter mode and SM4 cipher in Counter with CBC-MAC mode, respectively. The hash function for both cipher suites is SM3 ([ISO-SM3]).

3.1.1. ENCR_SM4_CBC

The specification of ENCR_SM4_CBC is as follows: The CBC (Cipher Block Chaining) mode is defined in [NIST.SP.800-38A] and utilized with the SM4 algorithm in the following sections. The input plaintext of SM4-CBC MUST be a multiple of the block size, which is 128-bits in SM4. SM4-CBC requires an additional input, the IV, that is unpredictable for a particular execution of the encryption process. The IV does not have to be secret. The IV itself, or criteria enough to determine it, MAY be transmitted with ciphertext.

A simple test vector of ENCR _SM4_CBC is given in Appendix A of this document.

3.1.2. ENCR_SM4_GCM

The ENCR_SM4_GCM authenticated encryption algorithm is defined in [GCM], using SM4 as the block cipher, by providing the key, nonce, plaintext, and additional associated data to that mode of operation. An authentication tag conforming to the requirements of IKEv2 as specified in [RFC5282] MUST be constructed using the partial contents of the IKEv2 message, starting from the first octet of the Fixed IKE Header through the last octet of the Payload Header of the Encrypted Payload (i.e., the fourth octet of the Encrypted Payload). This includes any payloads that are between the Fixed IKE Header and the

Encrypted Payload. The additional data input that forms the authentication tag MUST be the partial contents of the IKEv2 message, starting from the first octet of the Fixed IKE Header through the last octet of the Payload Header of the Encrypted Payload (i.e., the fourth octet of the Encrypted Payload). This includes any payloads that are between the Fixed IKE Header and the Encrypted Payload. The ENCR_SM4_GCM has four inputs: an SM4 key, an initialization vector (IV), a plaintext content, and optional additional authenticated data (AAD). ENCR_SM4_GCM generates two outputs: a ciphertext and message authentication code.

The input and output lengths are as follows:

The SM4 key length is 16 octets.

The max plaintext length is $2^{36} - 31$ octets.

The max AAD length is $2^{61} - 1$ octets.

The nonce length is 12 octets.

The authentication tag length is 16 octets.

The max ciphertext length is $2^{36} - 15$ octets.

The nonce is generated by the party performing the authenticated encryption operation. Within the scope of any authenticated encryption key, the nonce value MUST be unique. That is, the set of nonce values used with any given key MUST NOT contain any duplicates. Using the same nonce for two different messages encrypted with the same key destroys the security properties of GCM mode.

3.1.3. ENCR_SM4_CCM

The ENCR_SM4_CCM authenticated encryption algorithm is defined in [CCM] using SM4 as the block cipher. The generation of the authentication tag MUST conform to IKEv2 (See [RFC5282]) as described in the above paragraph. ENCR_SM4_CCM has four inputs: an SM4 key, a nonce, a plaintext, and optional additional authenticated data (AAD). ENCR_SM4_CCM generates two outputs: a ciphertext and a message authentication code.

The input and output lengths are as follows:

The SM4 key length is 16 octets.

The max plaintext length is $2^{24} - 1$ octets.

The max AAD length is $2^{64} - 1$ octets.

The max ciphertext length is $2^{24} + 15$ octets

To have a common set of terms for ENCR _SM4_GCM and ENCR _SM4_CCM, the ENCR _SM4_GCM IV is referred to as a nonce in the remainder of this document.

A simple test vector of ENCR _SM4_GCM and ENCR _SM4_CCM is given in Appendix A of this document.

3.2. Pseudorandom Function Transform

This specification defines a new transform of Type 2 (Pseudorandom Function Transform IDs):

PRF_HMAC_SM3 (Transform ID XX). The PRF uses the SM3 hash function with a 256-bit output defined in [ISO-SM3] and [GBT.32905-2016] and with HMAC construction. The PRF has a 256-bit block size and a 256-bit output length.

PRF_ HMAC_SM3 is hash-based message authentication code (or HMAC), which is defined in [RFC2104], using SM3 as the hash function. The PRF_ HMAC_SM3 has two inputs: HMAC key and the plaintext. The output of PRF_ HMAC_SM3 is 256 bits.

3.3. Integrity Algorithm Transform

This specification defines a new transform of Type 3 (Integrity Algorithm Transform IDs):

AUTH_HMAC_SM3 (Transform ID XX). The MAC uses the SM3 hash function with a 256-bit output defined in [ISO-SM3] and [GBT.32905-2016] and with HMAC construction. AUTH_HMAC_SM3 is specified as described in 2.2.

While no fixed key length is specified in [RFC2104], this specification requires that when used as an integrity/authentication algorithm, a fixed key length equal to the output length of the hash functions MUST be supported, and key lengths other than the output length of the associated hash function MUST NOT be supported. These key length restrictions are the same with HMAC-SHA-256 (see [RFC4868] Sec2.1.1).

3.4. Key Exchange Method Transform

This specification defines one new transform of Type 4 (Key Exchange Method Transform IDs): curveSM2. This transform uses a fixed elliptic curve parameter set defined in [GBT.32918.5-2017]. The specification of curveSM2 is defined in clause 3.2 of RFC 8998 [RFC8998] as ” curveSM2” , which is used to define new cipher suites for TLS 1.3 protocol.

Implementations of the key exchange mechanism defined in this document MUST conform to what [GBT.32918.5-2017] requires; that is to say, the only valid elliptic curve parameter set for the ” curveSM2” key exchange is defined as follows:

curveSM2: A prime field of 256 bits.

$y^2 = x^3+ ax + b$

p = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

a = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

b = 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

n = FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

Gx = 32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

Gy = BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

4. Authentication Method

This section specifies the use of the SM2 signature algorithm as the authentication method for IKEv2 protocol.

The SM2 signature algorithm is defined in [ISO-SM2]. The SM2 signature algorithm is based on elliptic curves. The SM2 signature algorithm uses a fixed elliptic curve parameter set defined in [GBT.32918.5-2017]. This curve is named "curveSM2" as defined in section 2.4.

Implementations of the signature scheme mechanism defined in this document MUST conform to what [GBT.32918.5-2017] requires.

5. Hash Algorithms

The SM2 digital signature algorithm uses the SM3 hash functions defined in [ISO-SM3] and [GBT.32905-2016]. This specification defines one new value for the "IKEv2 Hash Algorithms" registry: SM3 (value XX) for the SM3 hash function with a 256-bit output length.

The specification of SM3 is defined as follows:

The SM3 algorithm is intended to address multiple use cases for commercial cryptography, including, but not limited to: - the use of digital signatures and their verification; - the generation and verification of message authenticity codes; as well as - the generation of random numbers.

SM3 has a Merkle-Damgard construction and is similar to SHA-2 [NIST.FIPS.180-4]of the MD4 [RFC6150] family, with the addition of several strengthening features including a more complex step function and stronger message dependency than SHA-256 [RFC6234]. SM3 produces an output hash value of 256 bits long, based on 512-bit input message blocks, on input lengths up to 2^(m) [GBT.32905-2016]. This details the SM3 algorithm and its internal steps can be find in [GBT.32905-2016].

6. IANA Considerations

IANA maintains a registry called "Internet Key Exchange Version 2 (IKEv2) Parameters" with subregistries like "Transform Type Values", “IKEv2 Authentication Method” and “IKEv2 Hash Algorithms”.

This document describes 3 new encryption transforms, 1 pseudorandom function transform, 1 integrity algorithm transform, 1 key exchange method transform and a new authentication method using SM2 signature and SM3 hash function for IKEv2 ([RFC7296]).

IANA is requested to assign 3 new Transform IDs to the "Transform Type 1 - Encryption Algorithm Transform IDs" subregistry,

Number	Name	ESP Reference	IKEv2 Reference
TBD	ENCR_SM4_CBC	TBD	TBD
TBD	ENCR_SM4_GCM	TBD	TBD
TBD	ENCR_SM4_CCM	TBD	TBD

Table 1

1 Transform ID to the “Transform Type 2 - Pseudorandom Function Transform IDs” subregistry,

Number	Name	ESP Reference	IKEv2 Reference
TBD	PRF_HMAC_SM3	TBD	TBD

Table 2

1 Transform ID to the “Transform Type 3 - Integrity Algorithm Transform IDs” subregistry,

Number	Name	ESP Reference	IKEv2 Reference
TBD	AUTH_HMAC_SM3	TBD	TBD

Table 3

1 Transform ID to the “Transform Type 4 - Key Exchange Method Transform IDs” subregistry,

Number	Name	ESP Reference	IKEv2 Reference
TBD	curveSM2	TBD	TBD

Table 4

1 new Authentication Method to the “IKEv2 Authentication Method” subregistry,

Value	Authentication Method	Reference
TBD	curveSM2	TBD

Table 5

and 1 new Hash function to the “IKEv2 Hash Algorithms” subregistry.

Value	Hash Algorithm	Reference
TBD	SM3	TBD

Table 6

7. Security Considerations

At the time of writing, there are no known weak keys for SM cryptographic algorithms SM2, SM3 and SM4, and no security issues have been found for these algorithms.

A related work [CQCY21] analyzed the security of SM2 algorithm , and the cryptanalysis results shows that SM2 is existentially unforgeable against adaptively chosen-message attacks in the generic group model if the underlying hash function is uniform and collision-resistant and the underlying conversion function is almost-invertible. Besides, SM2 is secure against the generalized key substitution attacks if the underlying hash functions H and h are modeled as non-programmable random oracles (NPROs) [ZYZC15].

As a result of the increasing prevalence and exploitation of side-channel attacks ([JYW20], [WDW18], [LZHZ18]), the SM4 algorithm is now confronted with significant threats when utilized in smart cards and other cryptographic devices. However, these attacks can be mitigated through the implementation of side-channel protection ([ZCC24], [SZ24], [SCZ24], [JUP23]). On the other hand, the classic cryptanalysis techniques are not applicable to the entire cipher and are impractical, do not compromise the overall security of SM4.

8. References

8.1. Normative References

[CCM] NIST Special Publication 800-38C, "Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality", DOI 10.6028/NIST.SP.800-38C , May 2004, <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>.

[GCM] NIST Special Publication 800-38D, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", DOI 10.6028/NIST.SP.800-38D , November 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>.

[ISO-SM2] International Organization for Standardization, "IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms", ISO/IEC 14888-3:2018 , November 2018.

[ISO-SM3] International Organization for Standardization, "IT Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions", ISO/IEC 10118-3:2018 , October 2018.

[ISO-SM4] International Organization for Standardization, "Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers", ISO/IEC 18033-3:2010 , December 2010.

[NIST.FIPS.180-4] NIST FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, "Secure Hash Standard (SHS)", NIST.FIPS.180-4 , August 2015, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.

[NIST.SP.800-38A] NIST Special Publication 800-38A, "NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation --Methods and Techniques", INIST.SP.800-38A , December 2001, <<http://dx.doi.org/10.6028/NIST.SP.800-38A>>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/rfc/rfc2104>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/rfc/rfc4868>.

[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, DOI 10.17487/RFC5282, August 2008, <https://www.rfc-editor.org/rfc/rfc5282>.

[RFC6150] Turner, S. and L. Chen, "MD4 to Historic Status", RFC 6150, DOI 10.17487/RFC6150, March 2011, <https://www.rfc-editor.org/rfc/rfc6150>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/rfc/rfc6234>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/rfc/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8998] Yang, P., "ShangMi (SM) Cipher Suites for TLS 1.3", RFC 8998, DOI 10.17487/RFC8998, March 2021, <https://www.rfc-editor.org/rfc/rfc8998>.

8.2. Informative References

[CQCY21] Cui, X Qin, C Cai, T Yuen, H., "Security on SM2 and GOST signatures against related key attacks", 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 155-163) , October 2021.

[GBT.32905-2016]
Standardization Administration of China, "Information security technology --- SM3 cryptographic hash algorithm", GB/T 32905-2016 , March 2017, <<http://www.gmbz.org.cn/upload/2018-07-24/1532401392982079739.pdf>>.

[GBT.32907-2016]
Standardization Administration of the People’s Republic of China, "Information security technology -- SM4 block cipher algorithm", GB/T 32907-2016 , March 2017, <<http://www.gmbz.org.cn/upload/2018-04-04/1522788048733065051.pdf>>.

[GBT.32918.2-2016]
Standardization Administration of the People’s Republic of China, "Information security technology --- Public key cryptographic algorithm SM2 based on elliptic curves --- Part 2: Digital signature algorithm", GB/T 32918.2-2016 , March 2017, <http://www.gmbz.org.cn/upload/2018-07-24/1532401673138056311.pdf>.

[GBT.32918.5-2017]
Standardization Administration of the People’s Republic of China, "Information security technology --- Public key cryptographic algorithm SM2 based on elliptic curves --- Part 5: Parameter definition", GB/T 32918.5-2017 , December 2017, <<http://www.gmbz.org.cn/upload/2018-07-24/1532401863206085511.pdf>>.

[JUP23] Proceedings of the 26th Asia and South Pacific Design Automation Conference, "FPGA based countermeasures against side channel attacks on block ciphers", Proceedings of the 28th Asia and South Pacific Design Automation Conference. 2023 365-371, 2023.

[JYW20] JIN, H YANG, X WANG, Q YUAN, Y., "Improved differential fault attack for SM4 cipher", Journal of Cryptologic Research, 2020, 7(4) 453464, July 2020, <[{"DOI"=>"10.13868/j.cnki.jcr.000380"}]>.

[LZHZ18] LOU, F ZHANG, J HUANG, X ZHAO, H LIU, X., "Research on trace driven Cache analysis on SM4", Journal of Cryptologic Research, 2018, 5(4) 430441, 2018.

[SCZ24] Proceedings of the 26th Asia and South Pacific Design Automation Conference, "Micro-architectural cache side-channel attacks and countermeasures", Proceedings of the 26th Asia and South Pacific Design Automation Conference. 2021 441-448, 2024.

[SZ24] Security and Communication Networks, "Survey of CPU Cache-Based Side-Channel Attacks: Systematic Analysis, Security Models, and Countermeasures", Security and Communication Networks, 2021, 2021(1) 5559552, 2024.

[WDW18] WU, Z DU, M WANG, Y WANG, K WANG, T YU, Z., "Chosen-plaintext algorithm for chosen-plaintext power analysis against SM4", Journal of Cryptologic Research, 2018, 5(4) 421429, 2018.

[ZCC24] Zhang J, Chen C, Cui J, et al, "Timing side-channel attacks and countermeasures in CPU microarchitectures", ACM Computing Surveys, 2024, 56(7) 1-40, 2024.

[ZYZC15] Zhang, K Yang, J Zhang, C Chen, Z., "Security of the SM2 signature scheme against generalized key substitution attacks", International Conference on Research in Security Standardisation (pp. 140-153) , December 2015.

Appendix A. Appendix A. Test Vectors

All values are in hexadecimal and are in network byte order (big endian).

A.1. SM4_CBC Test Vectors

key:0123456789ABCDEFFEDCBA9876543210

iv : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

in : 0123456789ABCDEFFEDCBA9876543210

out : F0A2B07E64DD2C2590F93E4EDD90FBB4

A.2. SM4_GCM Test Vectors

Initialization Vector : 00001234567800000000ABCD
Key : 0123456789ABCDEFFEDCBA9876543210

Plaintext : AAAAAAAAAAAAAAAABBBBBBBBBBBBBBBB
CCCCCCCCCCCCCCCCDDDDDDDDDDDDDDDD EEEEEEEEEEEEEEEEFFFFFFFFFFFFFFFF
EEEEEEEEEEEEEEEEAAAAAAAAAAAAAAAA

Associated Data : FEEDFACEDEADBEEFFEEDFACEDEADBEEFABADDAD2

CipherText : 17F399F08C67D5EE19D0DC9969C4BB7D
5FD46FD3756489069157B282BB200735 D82710CA5C22F0CCFA7CBF93D496AC15
A56834CBCF98C397B4024A2691233B8D

Authentication Tag : 83DE3541E4C2B58177E065A9BF7B62EC

A.3. SM4_CCM Test Vectors

Initialization Vector : 000012345678000000000ABCD

Key : 0123456789ABCDEFFEDCBA9876543210

Plaintext : AAAAAAAAAAAAAAAABBBBBBBBBBBBBBBB
CCCCCCCCCCCCCCCCDDDDDDDDDDDDDDDD EEEEEEEEEEEEEEEEFFFFFFFFFFFFFFFF
EEEEEEEEEEEEEEEEAAAAAAAAAAAAAAAA

Associated Data : FEEDFACEDEADBEEFFEEDFACEDEADBEEFABADDAD2

CipherText : 48AF93501FA62ADBCD414CCE6034D895
DDA1BF8F132F042098661572E7483094 FD12E518CE062C98ACEE28D95DF4416B
ED31A2F04476C18BB40C84A74B97DC5B

Authentication Tag : 16842D4FA186F56AB33256971FA110F4

A.4. SM3 Test Vectors

in: 616263

out: 66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0

A.5. AUTH_HMAC_SM3 Test Vectors

Key: 00112233445566778899AABBCCDDEEFF

in: abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq

out: DC813339153491AD81477754EB3DF00DBB3CC3E6A69F9CACCE737DB7E61342FF

Appendix B. Acknowledgments

TBD

Authors’ Addresses

Yanfei Guo
Huawei Technologies
China
Email: guoyanfei3@huawei.com

Liang Xia
Huawei Technologies
China
Email: frank.xialiang@huawei.com

Yu Fu
China Unicom
China
Email: fuy186@chinaunicom.cn