Network Working Group
Internet-Draft
Updates: 4880, 6637 (if approved)
Intended status: Standards Track
Expires: March 18, 2018

R. Tse
Ribose
W. Wong
Hang Seng Management College
J. Lloyd
D. Wyatt
E. Borsboom
Ribose

September 14, 2017

# OSCCA Extensions For OpenPGP
# draft-openpgp-oscca-02

## Abstract

This document enables OpenPGP (RFC4880) usage in an compliant manner with OSCCA regulations for use within China.

Specifically, it extends OpenPGP to support the usage of SM2, SM3 and SM4 algorithms, and provides the OSCCA-compliant OpenPGP profile "OSCCA-SM234".

## 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/.

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 March 18, 2018.

Table of Contents

## 1. Introduction

SM2 [GBT.32918.1-2016] [ISO.IEC.14888-3] [GMT-0003-2012] [SM2] [I-D.shen-sm2-ecdsa], SM3 [GBT.32905-2016] [ISO.IEC.10118-3] [GMT-0004-2012] [SM3] [I-D.shen-sm3-hash] and SM4 [GBT.32907-2016] [ISO.IEC.18033-3.AMD2] [GMT-0002-2012] [SM4] [I-D.ribose-cfrg-sm4] are cryptographic standards issued by the Organization of State Commercial Administration of China [OSCCA] as authorized cryptographic algorithms for use within China. These algorithms are published in public.

Adoption of this document enables exchange of OpenPGP-secured email [RFC4880] in a OSCCA-compliant manner through usage of the authorized combination of SM2, SM3 and SM4.

SM2 is a set of public key cryptographic algorithms based on elliptic curves that include:

- Digital Signature Algorithm [GBT.32918.2-2016] [ISO.IEC.14888-3] [SM2-2]
- Key Exchange Protocol [GBT.32918.3-2016] [SM2-3]
- Public Key Encryption Algorithm [GBT.32918.4-2016] [SM2-4]

SM3 [GBT.32905-2016] [ISO.IEC.10118-3] is a hash algorithm designed for electronic authentication purposes.

SM4 [GBT.32907-2016] [ISO.IEC.18033-3.AMD2] is a symmetric encryption algorithm designed for data encryption.

This document extends OpenPGP [RFC4880] and its ECC extension [RFC6637] to support SM2, SM3 and SM4:

- support the SM3 hash algorithm for data validation purposes
- support signatures utilizing the combination of SM3 with other digital signing algorithms, such as RSA, ECDSA and SM2
- support the SM2 asymmetric encryption algorithm for public key operations

- support usage of SM2 in combination with supported hash algorithms, such as SHA-256 and SM3
- support the SM4 symmetric encryption algorithm for data protection purposes
- defines the OpenPGP profile "OSCCA-SM234" to enable usage of OpenPGP in an OSCCA-compliant manner.

## 2. Conventions Used in This Document

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].

Compliant applications are a subset of the broader set of OpenPGP applications described in [RFC4880]. Any [RFC2119] keyword within this document applies to compliant applications only.

### 2.1. Definitions

OSCCA-compliant
: All cryptographic algorithms used are compliant with OSCCA [OSCCA] regulations.

SM2DSA
: The elliptic curve digital signature algorithm defined in [GBT.32918.2-2016]

SM2KEP
: The elliptic curve key exchange protocol defined in [GBT.32918.3-2016]

SM2PKE
: The public key encryption algorithm defined in [GBT.32918.4-2016]

### 2.2. Basic Operations

This document utilizes definitions of operations from [RFC7253] and are included here for reference.

c^i
: The integer c raised to the i-th power.

S || T
: String S concatenated with string T (e.g., 000 || 111 == 000111).

## 3. SM2 ECC Algorithms

SM2 is an elliptic curve based cryptosystem (ECC) [GBT.32918.1-2016] [GMT-0003-2012] [SM2] [I-D.shen-sm2-ecdsa] designed by Xiaoyun Wang et al. and published by [OSCCA].

It was first published by the OSCCA in public in 2010 [SM2], then standardized as [GMT-0003-2012] in 2012, included in [ISO.IEC.11889] in 2015, published as a Chinese National Standard as [GBT.32918.1-2016], and published in [ISO.IEC.14888-3] in 2017.

The SM2 cryptosystem is composed of three distinct algorithms:

- an elliptical curve digital signature algorithm ("SM2DSA") [GBT.32918.2-2016], [ISO.IEC.14888-3], [SM2-2], also described in [I-D.shen-sm2-ecdsa];
- a key exchange protocol ("SM2KEP") [GBT.32918.3-2016] [SM2-3]; and
- a public key encryption algorithm ("SM2PKE") [GBT.32918.4-2016] [SM2-4].

This document will refer to all three algorithms for the usage of OpenPGP [RFC4880].

### 3.1. SM2 Digital Signature Algorithm

The SM2 Digital Signature Algorithm is intended for digital signature and verifications in commercial cryptographic applications, including, but not limited to:

- identity authentication
- protection of data integrity
- verification of data authenticity

The process of digital signature signing and verification along with their examples are found in [GBT.32918.2-2016], [ISO.IEC.14888-3], [SM2-2], and also described in [I-D.shen-sm2-ecdsa].

The SM2DSA process requires usage of a hash function within. For OSCCA-compliant usage, a OSCCA-compliant hash function such as SM3 [GBT.32905-2016] MUST also be used.

Formal security proofs for SM2 are provided in [SM2-SigSecurity] indicating that it satisfies both EUF-CMA security and security against generalized strong key substitution attacks.

The SM2DSA algorithm has been cryptanalyzed by multiple parties with the current strongest attack being nonce [SM2-DSA-Nonces] [SM2-DSA-Nonces2] and lattice attacks [SM2-DSA-Lattice].

In terms of OpenPGP usage, SM2DSA is an alternative to the ECDSA algorithm specified in [RFC6637].

For OpenPGP compatibility, these additional requirements MUST be adhered to:

- SM2DSA allows use of an optional "user identity" string which is hashed into "ZA" (Section 3.5 of [SM2-2] and Section 5.1.4.4 of [I-D.shen-sm2-ecdsa]). In OpenPGP, the user identifier "IDA" MUST be the empty string.

- While SM2DSA usually signs "H(ZA || msg)" (Section 4.1 [SM2-2]), but in OpenPGP, following the convention of [RFC6637], we do not directly sign the raw message "msg", but its hash "H(msg)". Therefore when a message is signed by SM2DSA in OpenPGP, the algorithm MUST sign the content of "H(ZA || H(msg))" instead of "H(ZA || msg)". Both hash algorithms used here MUST be identical.

## 3.2. SM2 Key Exchange Protocol

The SM2 Key Exchange Protocol is used for cryptographic key exchange, allowing the negotiation and exchange of a session key within two to three message transfers.

The process of key exchange and verification along with their examples are found in [GBT.32918.3-2016] [SM2-3], and also described in [I-D.shen-sm2-ecdsa].

SM2KEP is not used with OpenPGP as it is a two- to three- pass key exchange mechanism, while in OpenPGP, public keys of recipients are available initially.

The SM2KEP is now considered insecure due to [SM2-KEP-Comments], similar in status to the Unified Model and MQV schemes described in [NIST.SP.800-56Ar2].

## 3.3. SM2 Public Key Encryption

The SM2 Public Key Encryption algorithm is an elliptic curve (ECC) based asymmetric encryption algorithm. It is used for cryptographic encryption and decryption, allowing the message sender to utilize the public key of the message receiver to encrypt the message, with the recipient decrypting the messaging using his private key.

The full description of SM2PKE is provided in [GBT.32918.4-2016].

It utilizes a public key size of 512 bits and private key size of 256 bits [GBT.32918.4-2016] [GMT-0003-2012].

The process of encryption and decryption, along with their examples are found in [GBT.32918.4-2016] and [SM2-4].

The SM2PKE process requires usage of a hash function within. For OSCCA-compliant usage, a OSCCA-compliant hash function such as SM3 [GBT.32905-2016] MUST also be used.

In OpenPGP, SM2PKE is an alternative to RSA specified in [RFC4880].

### 3.4. Recommended SM2 Curve

The recommended curve is specified in [GBT.32918.5-2017] [SM2-5] and provided here for reference. SM2 uses a 256-bit elliptic curve.

#### 3.4.1. Definitions

p
: an integer larger than 3

a, b
: elements of F_q, defines an elliptic curve E on F_q

n
: Order of base point G (n is a prime factor of E(F_q))

x_G
: x-coordinate of generator G

y_G
: y-coordinate of generator G

#### 3.4.2. Elliptic Curve Formula

y^2 = x^3 + ax + b

#### 3.4.3. Curve Parameters

```
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
x_G = 32C4AE2C 1F198119 5F990446 6A39C994
      8FE30BBF F2660BE1 715A4589 334C74C7
y_G = BC3736A2 F4F6779C 59BDCEE3 6B692153
      D0A9877C C62A4740 02DF32E5 2139F0A0
```

## 4. SM3 Hash Algorithm

The SM3 Cryptographic Hash Algorithm [GBT.32905-2016] is an iterative hash function designed by Xiaoyun Wang et al., published by [OSCCA] as an alternative to SHA-2 [NIST.FIPS.180-4].

It was first published by the OSCCA in public in 2010 [SM3], then published in the OSCCA standard [GMT-0004-2012] in 2012, published as a Chinese National Standard as [GBT.32905-2016] in 2016, and included in the [ISO.IEC.10118-3] standard in 2017.

The algorithm is designed to be used for commercial cryptographic applications including, but not limited to:

- digital signatures and their verification
- message authentication code generation and their verification
- 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 [SM3-Boomerang].

SM3 produces an output hash value of 256 bits long, based on 512-bit input message blocks [SM3-Boomerang], on input lengths up to 2^(m).

The specification of SM3 is described in [GBT.32905-2016], [SM3] and [I-D.shen-sm3-hash].

## 5. SM4 Symmetric Encryption Algorithm

SM4 [GBT.32907-2016] [I-D.ribose-cfrg-sm4] [ISO.IEC.18033-3.AMD2] [GMT-0002-2012] [SM4] is a symmetric encryption algorithm designed by Shuwang Lu et al. originally intended for the usage of wireless local area network (Wireless LAN) products.

SM4 is a 128-bit blockcipher, uses a key size of 128 bits and internally uses an 8-bit S-box. It performs 32 rounds per block. Decryption is achieved by reversing the order of encryption.

SMS4 was first published in public as part of WAPI (Wired Authentication and Privacy Infrastructure), the Chinese National Standard for Wireless LAN [GB.15629.11-2003]. It was then published independently by the OSCCA in 2006 [SM4], formally renamed to SM4 in 2012 [GMT-0002-2012], published as a Chinese National Standard in 2016 [GBT.32907-2016], and included in [ISO.IEC.18033-3.AMD2] in 2017.

It is a required encryption algorithm specified in WAPI [GB.15629.11-2003].

## 6. Supported Algorithms

### 6.1. Public Key Algorithms

The SM2 algorithm is supported with the following extension.

The following public key algorithm IDs are added to expand Section 9.1 of [RFC4880], "Public-Key Algorithms":

| ID | Description of Algorithm |
|---|---|
| TBD | SM2 |

Compliant applications MUST support both usages of SM2 Section 3:

- SM2 Digital Signature Algorithm (SM2DSA) [GBT.32918.2-2016]

- SM2 Public Key Encryption (SM2PKE) [GBT.32918.4-2016]

### 6.2. Symmetric Key Algorithms

The SM4 algorithm is supported with the following extension.

The following symmetric encryption algorithm ID is added to expand Section 9.2 of [RFC4880], "Symmetric-Key Algorithms":

| ID | Description of Algorithm |
|---|---|
| TBD | SM4 |

Compliant applications MUST support SM4 Section 5.

### 6.3. Hash Algorithms

The SM3 algorithm is supported with the following extension.

The following symmetric encryption algorithm IDs are added to expand Section 9.3 of [RFC4880], "Hash Algorithms":

| ID | Description of Algorithm |
|---|---|
| TBD | SM3 |

Compliant applications MUST support SM3 Section 4.

## 7. Conversion Primitives

The encoding method of [RFC6637] Section 6 MUST be used, and is compatible with the definition given in [SEC1].

For clarity, according to the EC curve MPI encoding method of [RFC6637], the exact size of the MPI payload for the "SM2 Recommended" 256-bit curve [GBT.32918.5-2017], is 515 bits.

## 8. SM2 Key Derivation Function

A key derivation function (KDF) is necessary to implement EC encryption.

The SM2PKE KDF is defined in Section 3.4.3 of [GBT.32918.4-2016] (and Section 5.4.3 of [I-D.shen-sm2-ecdsa], Section 3.4.3 of [SM2-4]).

For OSCCA-compliance, it SHOULD be used in conjunction with an OSCCA-approved hash algorithm, such as SM3 [GBT.32905-2016].

The SM2PKE KDF is equivalent to the KDF2 function defined in Section 13.2 of [IEEE.1363a.2004] given the following assignments:

- Parameter
  - v as hBits, the output length of the selected hash function Hash
- Input
  - KEYLEN as oBits
  - Z as the plaintext string; and
  - PB is set to the empty bit string.

Pseudocode of the SM2KDF function is provided here for convenience. This function contains edited variable names for clarity.

## 8.1. Prerequisites

- Hash(S) is a hash function that outputs a v-bit long hash value based on input S.
- MSB(b, S) is a function that outputs the b most significant bits of the bitstream S.
- Floor(r) and Ceil(r) are the floor and ceiling functions respectively for the input of real number r. Both functions outputs an integer.

## 8.2. Inputs

KEYLEN
: Desired key length. A positive integer less than (2^32 - 1) x v.

Z
: Plaintext. String of any length.

## 8.3. Outputs

K
: Generated key. String of length KEYLEN.

K is defined as follows.

```
Counter = 1                  // a 32-bit counter
n = KEYLEN / v

for each 1 <= i <= Ceil(n)
  Ha_i = Hash( Z || Counter )
  Counter = Counter + 1
end for

if n is a whole number then
  Ha! = Ha_{Ceil(n)}
else
  Ha! = MSB(KEYLEN - (v x Floor(n)), Ha_{Ceil(n)})
end if

K = Ha_1 || Ha_2 || ... || Ha_{Ceil(n)-1} || Ha!
```

## 9. Encoding of Public and Private Keys

### 9.1. Public-Key Packet Formats

The following algorithm-specific packets are added to Section 5.5.2 of [RFC4880], "Public-Key Packet Formats", to support SM2DSA and SM2PKE.

This document extends the algorithm-specific portion with the following fields.

Algorithm-Specific Fields for SM2DSA keys:

- a variable-length field containing a curve OID, formatted as follows:
  - a one-octet size of the following field; values 0 and 0xFF are reserved for future extensions
  - octets representing a curve OID, described in Section 11
- MPI of an EC point representing a public key

Algorithm-Specific Fields for SM2PKE keys:

- a variable-length field containing a curve OID, formatted as follows:
  - a one-octet size of the following field; values 0 and 0xFF are reserved for future extensions
  - octets representing a curve OID, described in Section 11

- MPI of an EC point representing a public key

Note that both SM2DSA and SM2PKE public keys are composed of the same sequence of fields, and use the same codepoint to identify them. They are distinguished by the key usage flags.

## 9.2. Secret-Key Packet Formats

The following algorithm-specific packets are added to Section 5.5.3. of [RFC4880], "Secret-Key Packet Formats", to support SM2DSA and SM2PKE.

This document extends the algorithm-specific portion with the following fields.

Algorithm-Specific Fields for SM2DSA or SM2PKE secret keys:

- an MPI of an integer representing the secret key, which is a scalar of the public EC point

# 10. Message Encoding with Public Keys

## 10.1. Public-Key Encrypted Session Key Packets (Tag 1)

Section 5.1 of [RFC4880], "Public-Key Encrypted Session Key Packets (Tag 1)" is extended to support SM2PKE using the following algorithm specific fields for SM2PKE, through applying the KDF described in Section 8.

Algorithm Specific Fields for SM2 encryption:

- The SM2 ciphertext is formatted in the OpenPGP bitstream as a single MPI. This consists of:
  - "C = (C1 || C3 || C2)" (step A8 of Section 4.1 [SM2-4]), followed by
  - a single octet giving the code for the hash algorithm used within the calculation of the KDF mask "t" (step A5 of Section 4.1 [SM2-4]) and the calculation of "C3" (step A7 of Section 4.1 [SM2-4]). For OSCCA compliance, this MUST be an OSCCA-approved hash function, and in any case, it SHOULD be a hash which is listed in the receiving keys "Preferred Hash Algorithms" list (Section 5.2.3.8 of [RFC4880]).

### 10.2. Signature Packet (Tag 2)

#### 10.2.1. Version 3 Signature Packet Format

Section 5.2.2 of [RFC4880] defines the signature format for "Version 3 Signature Packet Format". Similar to ECDSA [RFC6637], no change in the format is necessary for SM2DSA.

#### 10.2.2. Version 4 Signature Packet Format

Section 5.2.3 of [RFC4880] defines the signature format for "Version 4 Signature Packet Format". Similar to ECDSA [RFC6637], no change in the format is necessary for SM2DSA.

## 11. SM2 ECC Curve OID

This section provides the curve OID of the "SM2 Recommended Curve" [GBT.32918.5-2017] described in Section 3, according to the method of [RFC6637].

We specify the curve OID of the "SM2 Recommended Curve" to be the registered OID entry of "SM2 Elliptic Curve Cryptography" according to [GMT-0006-2012], which is "1.2.156.10197.1.301".

The table below specifies the exact sequence of bytes of the mentioned curve:

| ASN.1 Object Identifier | OID len | Curve OID bytes in hexadecimal representation | Curve name |
|---|---|---|---|
| 1.2.156.10197.1.301 | 8 | 2A 81 1C CF 55 01 82 2D | SM2 Recommended |

The complete ASN.1 DER encoding for the SM2 Recommended curve OID is "06 08 2A 81 1C CF 55 01 82 2D", from which the first entry in the table above is constructed by omitting the first two octets. Only the truncated sequence of octets is the valid representation of a curve OID.

## 12. Compatibility Profiles

### 12.1. OSCCA SM234 Profile

The "OSCCA SM234" profile is designed to be compliant to OSCCA regulations. A compliant OpenPGP implementation MUST implement the following items as described by this document:

- SM2 Recommended Curve (Section 11)
- SM2 (SM2DSA and SM2PKE) (Section 3)
  - The hash function selected in SM2DSA and SM2PKE MUST also be OSCCA-compliant, such as SM3 [SM3]
- SM3 (Section 4)
- SM4 (Section 5)

## 13. Security Considerations

- Products and services that utilize cryptography are regulated by the OSCCA [OSCCA]; they must be explicitly approved or certified by the OSCCA before being allowed to be sold or used in China.
- SM2 [GBT.32918.1-2016] is an elliptic curve cryptosystem (ECC) published by the OSCCA [OSCCA]. Its security relies on the assumption that the elliptic curve discrete logarithm problem (ECLP) is computationally infeasible. With advances in cryptanalysis, new attack algorithms may reduce the complexity of ECLP, making it easier to attack the SM2 cryptosystem that is considered secure at the time this document is published. You SHOULD check current literature to determine if the algorithms in SM2 have been found vulnerable.
- SM3 [GBT.32905-2016] is a cryptographic hash algorithm published by the OSCCA [OSCCA]. No formal proof of security is provided. As claimed in [I-D.shen-sm3-hash], the security properties of SM3 are under public study. There are no known feasible attacks against the SM3 algorithm at the time this document is published.
- SM4 [GBT.32907-2016] is a blockcipher certified by the OSCCA [OSCCA]. No formal proof of security is provided. There are no known feasible attacks against the SM4 algorithm by the time of publishing this document. On the other hand, there are security concerns with regards to side-channel attacks, when the SM4 algorithm is implemented in a device [SM4-Power]. For instance, [SM4-Power] illustrated an attack by measuring the power consumption of the device. A chosen ciphertext attack, assuming a fixed correlation between the sub-keys and data mask, is able to

recover the round key successfully. When the SM4 algorithm is implemented in hardware, the parameters/keys SHOULD be randomly generated without fixed correlation.

- SM2 has a key length of 512 bits for the public key and 256 bits for the private key. It is considered an alternative to ECDSA P-256 [RFC6637]. Its security strength is comparable to a 128-bit symmetric key strength [I-D.ietf-msec-mikey-ecc], e.g., AES-128 [NIST.FIPS.197].

- SM3 is a hash function that generates a 256-bit hash value. It is considered as an alternative to SHA-256 [RFC6234].

- SM4 is a blockcipher symmetric algorithm with a key length of 128 bits. It is considered as an alternative to AES-128 [NIST.FIPS.197].

- Security considerations offered in [RFC6637] and [RFC4880] also apply.

## 14. IANA Considerations

The IANA "Pretty Good Privacy (PGP)" registry [RFC8126] has made the following assignments for algorithms described in this document, namely:

- ID XXX of the "Public Key Algorithms" namespace for SM2 Section 3

- ID XXX of the "Hash Algorithms" namespace for SM3 Section 4

- ID XXX of the "Symmetric Key Algorithms" namespace for SM4 Section 5

## 15. Examples

### 15.1. Public Key Example

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xlIEWbGKWmMIKoEcz1UBgi0CAwQx5lUJNwGp01AB7YfAye0oMmyIPYe/cQPVwh8/7RCu
ywZLMDDAM7qn6TNqTtdKW+7tLFhtOC4yzDVK8UjN/ccazSBTTTIgMjU2LWJpdCBrZXkg
PGphY2tAbG9jYWxob3N0PsJ0BBNjaQAmBQJZsYpfAhsDBQsJCAcCBhUICQoLAgUWAgMB
AAkQC/UcNw0bAZcAAJt5AP4oXvi3xl2RUwAvVjlzXtLL87g6x9cIBS7EB/cvAsw78AEA
/Wt6qWlBVZ6TYiqNPt9An/4cjKyNpAv7S9u3neGXWUU=
=RJ3C
-----END PGP PUBLIC KEY BLOCK-----
```

### 15.2. Signature Example

Detached signature of the string "SM2 example" using the above key:

```
-----BEGIN PGP SIGNATURE-----
wmQEAGMIABYFAlmxj+cFAwAAAAAJEAv1HDcNGwGXAAB+SQEAy5AHKgiRxgOogB/2sfge
JaVoLgpxvDp9yIcaLfP++xkBAPGuZ1f9FjxVd5jlCGd1jFzAPpt8N2Lc3FQDqVjgJvV9
=Xbbj
-----END PGP SIGNATURE-----
```

## 16. References

### 16.1. Normative References

[GBT.32905-2016]
Standardization Administration of the People's Republic of China, "GB/T 32905-2016 Information Security Techniques -- SM3 Cryptographic Hash Algorithm", August 2016, <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=45B1A67F20F3BF339211C391E9278F5E>.

[GBT.32907-2016]
Standardization Administration of the People's Republic of China, "GB/T 32907-2016 Information Security Technology -- SM4 Block Cipher Algorithm", August 2016, <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=7803DE42D3BC5E80B0C3E5D8E873D56A>.

[GBT.32918.1-2016]
Standardization Administration of the People's Republic of China, "GB/T 32918.1-2016 Information Security Technology -- Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves -- Part 1: General", August 2016, <http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2032918.1-2016%27>.

[GBT.32918.2-2016]
Standardization Administration of the People's Republic of China, "GB/T 32918.2-2016 Information Security Technology -- Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves -- Part 2: Digital Signature Algorithm", August 2016, <http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2032918.2-2016%27>.

[GBT.32918.3-2016]
Standardization Administration of the People's Republic of China, "GB/T 32918.3-2016 Information Security Technology -- Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves -- Part 3: Key Exchange", August 2016, <http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2032918.3-2016%27>.

[GBT.32918.4-2016]
Standardization Administration of the People's Republic of China, "GB/T 32918.4-2016 Information Security Technology -- Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves -- Part 4: Public Key Encryption Algorithm", August 2016, <http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2032918.4-2016%27>.

[GBT.32918.5-2017]
Standardization Administration of the People's Republic of China, "GB/T 32918.5-2017 Information Security Technology -- Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves -- Part 5: Parameter Definition", May 2017, <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=728DEA8B8BB32ACFB6EF4BF449BC3077>.

[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/info/rfc2119>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[RFC6637] Jivsov, A., "Elliptic Curve Cryptography (ECC) in OpenPGP", RFC 6637, DOI 10.17487/RFC6637, June 2012, <https://www.rfc-editor.org/info/rfc6637>.

## 16.2. Informative References

[GB.15629.11-2003]
Standardization Administration of the People's Republic of China, "Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", May 2003, <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=74B9DD11287E72408C19C4D3A360D1BD>.

[GMT-0002-2012]
Organization of State Commercial Administration of China, "GM/T 0002-2012: SM4 Block Cipher Algorithm", March 2012, <http://www.oscca.gov.cn/Column/Column_32.htm>.

[GMT-0003-2012]
Organization of State Commercial Administration of China, "GM/T 0003-2012: Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves", March 2012, <http://www.oscca.gov.cn/Column/Column_32.htm>.

[GMT-0004-2012]
Organization of State Commercial Administration of China, "GM/T 0004-2012: SM3 Hash Algorithm", March 2012, <http://www.oscca.gov.cn/Column/Column_32.htm>.

[GMT-0006-2012]
Organization of State Commercial Administration of China, "GM/T 0006-2012: Cryptographic Application Identifier Criterion Specification", March 2012, <http://www.oscca.gov.cn/Column/Column_32.htm>.

[I-D.ietf-msec-mikey-ecc]
Milne, A., "ECC Algorithms for MIKEY", draft-ietf-msec-mikey-ecc-03 (work in progress), June 2007.

[I-D.ribose-cfrg-sm4]
Tse, R. and W. Wong, "The SM4 Block Cipher Algorithm And Its Modes Of Operations", draft-ribose-cfrg-sm4-00 (work in progress), September 2017.

[I-D.shen-sm2-ecdsa]
Shen, S., Shen, S., and X. Lee, "SM2 Digital Signature Algorithm", draft-shen-sm2-ecdsa-02 (work in progress), February 2014.

[I-D.shen-sm3-hash]
Shen, S. and S. Shen, "SM3 Hash function", draft-shen-sm3-hash-01 (work in progress), February 2014.

[IEEE.1363a.2004]
Institute of Electrical and Electronics Engineers, "IEEE Std 1363a-2004: IEEE Standard Specifications for Public-Key Cryptography -- Amendment 1: Additional Techniques", September 2004, <http://grouper.ieee.org/groups/1363/>.

[ISO.IEC.10118-3]
International Organization for Standardization, "ISO/IEC FDIS 10118-3 -- Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions", June 2017, <https://www.iso.org/standard/67116.html>.

[ISO.IEC.11889]
International Organization for Standardization, "ISO/IEC 11889-1:2015 -- Information technology -- Trusted platform module library", August 2015, <https://www.iso.org/standard/66510.html>.

[ISO.IEC.14888-3]
International Organization for Standardization, "ISO/IEC 14888-3:2016-03 -- Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms", September 2017, <https://www.iso.org/standard/70631.html>.

[ISO.IEC.18033-3.AMD2]
International Organization for Standardization, "ISO/IEC WD1 18033-3/AMD2 -- Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers -- Amendment 2", June 2017, <https://www.iso.org/standard/54531.html>.

[NIST.FIPS.180-4]
National Institute of Standards and Technology, "FIPS 180-4 Secure Hash Standard (SHS)", August 2015, <http://dx.doi.org/10.6028/NIST.FIPS.180-4>.

[NIST.FIPS.197]
National Institute of Standards and Technology, "FIPS 197 Advanced Encryption Standard (AES)", November 2001, <https://doi.org/10.6028/NIST.FIPS.197>.

[NIST.SP.800-56Ar2]
Barker, B., Chen, L., Roginsky, A., and M. Smid, "SP 800-56Ar2 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography", May 2013, <http://dx.doi.org/10.6028/NIST.SP.800-56Ar2>.

[OSCCA] Organization of State Commercial Administration of China, "Organization of State Commercial Administration of China", May 2017, <http://www.oscca.gov.cn>.

[RFC6150] Turner, S. and L. Chen, "MD4 to Historic Status", RFC 6150, DOI 10.17487/RFC6150, March 2011, <https://www.rfc-editor.org/info/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/info/rfc6234>.

[RFC7253] Krovetz, T. and P. Rogaway, "The OCB Authenticated-Encryption Algorithm", RFC 7253, DOI 10.17487/RFC7253, May 2014, <https://www.rfc-editor.org/info/rfc7253>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[SEC1] Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography", September 2010, <http://www.secg.org/SEC1-Ver-1.0.pdf>.

[SM2] Organization of State Commercial Administration of China, "Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves", December 2010, <http://www.oscca.gov.cn/UpFile/2010122214822692.pdf>.

[SM2-2] Organization of State Commercial Administration of China, "Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves -- Part 2: Digital Signature Algorithm", December 2010, <http://www.oscca.gov.cn/UpFile/2010122214822692.pdf>.

[SM2-3] Organization of State Commercial Administration of China, "Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves -- Part 3: Key Exchange Protocol", December 2010, <http://www.oscca.gov.cn/UpFile/2010122214822692.pdf>.

[SM2-4] Organization of State Commercial Administration of China, "Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves -- Part 4: Public Key Encryption Algorithm", December 2010, <http://www.oscca.gov.cn/UpFile/2010122214822692.pdf>.

[SM2-5] Organization of State Commercial Administration of China, "Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves -- Part 5: Parameter definitions", December 2010, <http://www.oscca.gov.cn/UpFile/2010122214836668.pdf>.

[SM2-DSA-Lattice] Cao, W., Feng, J., Zhu, S., Chen, H., Wu, W., Han, X., and X. Zheng, "Practical Lattice-Based Fault Attack and Countermeasure on SM2 Signature Algorithm", November 2016, <https://doi.org/10.1007/978-3-319-29814-6_6>.

[SM2-DSA-Nonces] Liu, M., Chen, J., and H. Li, "Partially Known Nonces and Fault Injection Attacks on SM2 Signature Algorithm", November 2013, <https://dx.doi.org/10.1007/978-3-319-12087-4_22>.

[SM2-DSA-Nonces2] Chen, J., Liu, M., Shi, H., and H. Li, "Mind Your Nonces Moving: Template-Based Partially-Sharing Nonces Attack on SM2 Digital Signature Algorithm", November 2015, <https://doi.acm.org/10.1145/2714576.2714587>.

[SM2-KEP-Comments] Xu, X. and D. Feng, "Comments on the SM2 Key Exchange Protocol", December 2011, <https://dx.doi.org/10.1007/978-3-642-25513-7_12>.

[SM2-SigSecurity] Zhang, Z., Yang, K., Zhang, J., and C. Chen, "Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks", December 2015, <https://link.springer.com/chapter/10.1007/978-3-319-27152-1_7>.

[SM3] Organization of State Commercial Administration of China, "SM3 Cryptographic Hash Algorithm", December 2010, <http://www.oscca.gov.cn/UpFile/20101222141857786.pdf>.

[SM3-Boomerang]
Bai, D., Yu, H., Wang, G., and X. Wang, "Improved Boomerang Attacks on Round-Reduced SM3 and Keyed Permutation of BLAKE-256", April 2015, <https://doi.org/10.1049/iet-ifs.2013.0380>.

[SM4] Organization of State Commercial Administration of China, "SM4 block cipher algorithm", December 2010, <http://www.oscca.gov.cn/UpFile/200621016423197990.pdf>.

[SM4-Power]
Du, Z., Wu, Z., Wang, M., and J. Rao, "Improved chosen-plaintext power analysis attack against SM4 at the round-output", October 2015, <http://dx.doi.org/10.6028/NIST.FIPS.180-4>.

## Appendix A. Acknowledgements

The authors would like to thank the following persons for their valuable advice and input.

- The Ribose RNP team for their input and implementation

## Authors' Addresses

Ronald Henry Tse
Ribose
Suite 1111, 1 Pedder Street
Central, Hong Kong
Hong Kong

Email: ronald.tse@ribose.com
URI: https://www.ribose.com

Dr. Wai Kit Wong
Hang Seng Management College
Hang Shin Link, Siu Lek Yuen
Shatin, New Territories
Hong Kong

Email: wongwk@hsmc.edu.hk
URI: https://www.hsmc.edu.hk

Jack E. Lloyd
Ribose
United States of America

Email: jack@randombit.net
URI: https://www.ribose.com

Daniel Elliot Wyatt
Ribose
608 W Cork St, Apt 2
Winchester, VA
United States of America

Email: daniel.wyatt@ribose.com
URI: https://www.ribose.com

Erick Borsboom
Ribose
Suite 1111, 1 Pedder Street
Central, Hong Kong
Hong Kong

Email: erick.borsboom@ribose.com
URI: https://www.ribose.com