The SM4 Block Cipher Algorithm And Its Modes Of Operations
draft-crypto-sm4-00

Abstract

This document describes the SM4 symmetric blockcipher algorithm published as GB/T 32907-2016 by the Organization of State Commercial Administration of China (OSCCA).

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 March 13, 2018.

Copyright Notice

Copyright (c) 2017 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 ........................................... 3
   1.1. History ........................................... 3
   1.2. Applications ....................................... 4
   1.3. Cryptanalysis ...................................... 4
2. Terms and Definitions .................................... 5
3. Symbols And Abbreviations ................................ 5
4. Compute Structure ...................................... 6
5. Key And Key Parameters .................................. 6
6. Round Function F ....................................... 6
   6.1. Round Parameter Structure ........................... 6
   6.2. Mixer Substitution T ................................ 7
       6.2.1. Non-linear Transformation tau ................... 7
   6.3. Linear Substitution L ............................... 8
7. Calculation ............................................ 8
   7.1. SM4 Encryption ..................................... 8
   7.2. SM4 Decryption ..................................... 9
   7.3. SM4 Key Expansion ................................... 9
       7.3.1. Transformation Function T' ...................... 10
       7.3.2. System Parameter FK ............................ 10
       7.3.3. Constant Parameter CK ......................... 10
8. Modes of Operation .................................... 11
   8.1. Variables And Primitives ........................... 11
   8.2. Initialization Vector ............................... 12
   8.3. SM4-ECB ............................................ 12
       8.3.1. SM4-ECB Encryption .............................. 13
       8.3.2. SM4-ECB Decryption .............................. 13
   8.4. SM4-CBC ............................................ 14
       8.4.1. SM4-CBC Encryption .............................. 14
       8.4.2. SM4-CBC Decryption .............................. 15
   8.5. SM4-CFB ............................................ 15
       8.5.1. SM4-CFB Variants ............................... 16
       8.5.2. SM4-CFB Encryption .............................. 16
       8.5.3. SM4-CFB Decryption .............................. 17
   8.6. SM4-OFB ............................................ 17
       8.6.1. SM4-OFB Encryption .............................. 18
       8.6.2. SM4-OFB Decryption .............................. 18
   8.7. SM4-CTR ............................................ 19
       8.7.1. SM4-CTR Encryption .............................. 19
       8.7.2. SM4-CTR Decryption .............................. 20
9. Object Identifier ..................................... 21
10. Security Considerations ............................... 21
11. IANA Considerations .................................. 22
12. Appendix A: Example Calculations ....................... 22
   12.1. Example 1 ......................................... 22
   12.2. Example 2 ......................................... 23
13. References ........................................... 24
1. Introduction

SM4 [GBT.32907-2016] is a cryptographic standard issued by the Organization of State Commercial Administration of China [OSCCA] as authorized cryptographic algorithms for the use within China. The algorithm is applicable published in public.

SM4 is a symmetric encryption algorithm, specifically a blockcipher, designed for data encryption.

This document does not aim to introduce a new algorithm, but to provide a clear and open description of the SM4 algorithm in English, and also to serve as a stable reference for IETF documents that utilize this algorithm.

While this document is similar to [SM4-En] in nature, [SM4-En] is a textual translation of "SMS4" [SM4] published in 2006, and this document follows the updated text and structure of [GBT.32907-2016]. The sections 1 to 7 of this document are intentionally mapped to the corresponding sections 1 to 7 of the [GBT.32907-2016] standard for convenience of the reader.

1.1. History

The "SMS4" algorithm (the former name of SM4) was invented by Shu-Wang Lu [LSW-Bio], first published in 2003 as part of [GB.15629.11-2003], then published independently in 2006 [SM4] by OSCCA, officially renamed to "SM4" in 2012 in [GMT-0002-2012] published by OSCCA, and finally standardized in 2016 as a Chinese National Standard (GB Standard) [GBT.32907-2016].

SM4 was originally created for use in protecting wireless networks [SM4], and is mandated in the Chinese National Standard for Wireless LAN WAPI (Wired Authentication and Privacy Infrastructure) [GB.15629.11-2003]. A proposal was made to adopt SMS4 into the IEEE 802.11i standard, but the algorithm was eventually not included due to concerns of introducing inoperability with existing ciphers.

The latest SM4 standard [GBT.32907-2016] was proposed by OSCCA, standardized through TC 260 of the Standardization Administration of the People’s Republic of China (SAC), and was drafted by the following individuals at the Data Assurance and Communication Security Research Center (DAS Center) of the Chinese Academy of
Sciences, the China Commercial Cryptography Testing Center and the Beijing Academy of Information Science & Technology (BAIST):

- Shu-Wang Lu
- Dai-Wai Li
- Kai-Yong Deng
- Chao Zhang
- Peng Luo
- Zhong Zhang
- Fang Dong
- Ying-Ying Mao
- Zhen-Hua Liu

### 1.2. Applications

SM4 (and SMS4) has prevalent hardware implementations [SM4-FPGA] [SM4-VLSI], due to its being the only OSCCA-approved symmetric encryption algorithm allowed for use in China.

SM4 can be used with multiple modes (See Section 8).

### 1.3. Cryptanalysis

A number of attacks have been attempted on SM4, such as [SM4-Analysis] [SM4-Linear], but there are no known feasible attacks against the SM4 algorithm by the time of publishing this document.

There are, however, security concerns with regards to side-channel attacks [SideChannel] 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.

There have been improvements to the hardware embodiment of SM4 such as [SM4-VLSI] that may resist such attacks.
In order to improve security of the SM4 cryptographic process, secure white-box implementations such as [SM4-WhiteBox] have been proposed. Speed enhancements, such as [SM4-HiSpeed], have also been proposed.

2. Terms and Definitions

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].

The following terms and definitions apply to this document.

block length
   Bit-length of a message block.

key length
   Bit-length of a key.

key expansion algorithm
   An operation that converts a key into a round key.

rounds
   The number of iterations that the round function is run.

round key
   A key used in each round on the blockcipher, derived from the input key, also called a subkey.

word
   a 32-bit quantity

S-box
   The S (substitution) box function produces 8-bit output from 8-bit input, represented as Sbox(.)

3. Symbols And Abbreviations

S xor T
   bitwise exclusive-or of two 32-bit vectors S and T. S and T will always have the same length.

a <<< i
   32-bit bitwise cyclic shift on a with i bits shifted left.
4. Compute Structure

The SM4 algorithm is a blockcipher, with block size of 128 bits and a key length of 128 bits.

Both encryption and key expansion uses 32 rounds of a nonlinear key schedule per block. Each round processes one of the four 32-bit words that constitute the block.

The structure of encryption and decryption are identical, except that the round key schedule has its order reversed during decryption.

Using a 8-bit S-box, it only uses exclusive-or, cyclic bit shifts and S-box lookups to execute.

5. Key And Key Parameters

Encryption key length is 128-bits, and represented below, where each MK_i, (i = 0, 1, 2, 3) is a word.

MK = (MK_0, MK_1, MK_2, MK_3)

The round key schedule is derived from the encryption key, represented as below where each rk_i (i = 0, ..., 31) is a word:

(rk_0, rk_1, ..., rk_31)

System parameters used for key expansion is represented as FK, where each FK_i (i = 0, ..., 3) is a word:

FK = (FK_0, FK_1, FK_2, FK_3)

Constant parameters used for key expansion is represented as CK, where each CK_i (i = 0, ..., 31) is a word:

CK = (CK_0, CK_1, ..., CK_31)

6. Round Function F

6.1. Round Parameter Structure

Given the 128-bit input below, where each $X_i$ is a 32-bit word:

(X_0, X_1, X_2, X_3)

And the round key rk is a 32-bit word:

The round function F is defined as:
F(X₀, X₁, X₂, X₃, rk) = X₀ xor T(X₁ xor X₂ xor X₃ xor rk)

6.2. Mixer Substitution T

T is a reversible substitution function that outputs 32 bits from an input of 32 bits.

It consists of a non-linear transform tau and linear transform L.

T(.) = L(tau(.))

6.2.1. Non-linear Transformation tau

tau is composed of four parallel S-boxes.

Given a 32-bit input of A, where each aᵢ is a 8-bit string:

A = (a₀, a₁, a₂, a₃)

The output is a 32-bit B, where each bᵢ is a 8-bit string:

B = (b₀, b₁, b₂, b₃)

B is calculated as follows:

(b₀, b₁, b₂, b₃) = tau(A)

tau(A) = (Sbox(a₀), Sbox(a₁), Sbox(a₂), Sbox(a₃))

The Sbox lookup table is shown here:
For example, input "EF" will produce an output read from the S-box table row E and column F, giving the result $Sbox(EF) = 84$.

6.3. Linear Substitution L

The output of non-linear transformation function $\tau$ is used as input to linear transformation function $L$.

Given $B$, a 32-bit input:

$L$ produces a 32-bit output $C$:

$$C = L(B)$$

$$L(B) = B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24)$$

7. Calculation

7.1. SM4 Encryption

The encryption algorithm consists of 32 rounds and 1 reverse transform $R$.

Given a 128-bit plaintext input, where each $X_i$ is a 32-bit word:

$$(X_0, X_1, X_2, X_3)$$

The output is a 128-bit ciphertext, where each $Y_i$ is a 32-bit word:
(Y_0, Y_1, Y_2, Y_3)

Each round key is designated as rk_i, where each rk_i is a 32-bit word and i = 0, 1, 2, ..., 31.

a. 32 rounds of calculation

i = 0, 1, ..., 31

X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)

b. reverse transformation

(Y_0, Y_1, Y_2, Y_3) = R(X_32, X_33, X_34, X_35)

R(X_32, X_33, X_34, X_35) = (X_35, X_34, X_33, X_32)

Please refer to Section 12 for a sample calculation.

7.2. SM4 Decryption

Decryption takes an identical process as encryption, with the only difference the order of the round key sequence.

During decryption, the round key sequence is:

(rk_31, rk_30, ..., rk_0)

7.3. SM4 Key Expansion

Round keys used during encryption are derived from the encryption key.

Specifically, given the encryption key MK, where each MK_i is a 32-bit word:

MK = (MK_0, MK_1, MK_2, MK_3)

Each round key rk_i is created as follows, where i = 0, 1, ..., 31.

(K_0, K_1, K_2, K_3) = (MK_0 xor FK_0, MK_1 xor FK_1, MK_2 xor FK_2, MK_3 xor FK_3)

rk_i = K_{i + 4}

K_{i + 4} = K_i xor T' (K_{i + 1} xor K_{i + 2} xor K_{i + 3} xor CK_i)
Since the decryption key is identical to the encryption key, the round keys used in the decryption process are derived from the decryption key through the identical process to that of during encryption.

7.3.1. Transformation Function T’

The transformation function T’ is created from T by replacing the linear transform function L with L’.

\[ L'(B) = B \text{ xor } (B << 13) \text{ xor } (B << 23) \]

7.3.2. System Parameter FK

System parameter FK given in hexadecimal notation, is:

FK_0 = A3B1BAC6 FK_1 = 56AA3350 FK_2 = 677D9197 FK_3 = B27022DC

7.3.3. Constant Parameter CK

The method to retrieve values from the constant parameter CK is as follows.

Let \( \text{ck}_{i, j} \) be the j-th byte \((i = 0, 1, ..., 31; j = 0, 1, 2, 3)\) of \( \text{CK}_i \).

Therefore, each \( \text{ck}_{i, j} \) is a 8-bit string, and each \( \text{CK}_i \) a 32-bit word.

\[ \text{CK}_i = (\text{ck}_{i, 0}, \text{ck}_{i, 1}, \text{ck}_{i, 2}, \text{ck}_{i, 3}) \]

\[ \text{ck}_{i, j} = (4i + j) \times 7 \pmod{256} \]

The constant parameter \( \text{CK}_i \), \((i = 0, 1, ..., 31)\) values, in hexadecimal, are:
8. Modes of Operation

This document defines multiple modes of operation for the SM4 blockcipher algorithm.

The CBC (Cipher Block Chaining), ECB (Electronic CodeBook), CFB (Cipher Feedback), OFB (Output FeedBack) and CTR (Counter) modes are defined in [NIST.SP.800-38A] and utilized with the SM4 algorithm in the following sections.

8.1. Variables And Primitives

Hereinafter we define:

SM4Encrypt(P, K)
The SM4 algorithm that encrypts plaintext $P$ with key $K$, described in Section 7.1

\textbf{SM4Decrypt}($C$, $K$)

The SM4 algorithm that decrypts ciphertext $C$ with key $K$, described in Section 7.2

$b$

block size in bits, defined as 128 for SM4

$P_j$

block $j$ of ciphertext bitstring $P$

$C_j$

block $j$ of ciphertext bitstring $C$

\textbf{NBlocks}($B$, $b$)

Number of blocks of size $b$-bits in bitstring $B$

$IV$

Initialization vector

$LSB(b, S)$

Least significant $b$ bits of the bitstring $S$

$MSB(b, S)$

Most significant $b$ bits of the bitstring $S$

8.2. Initialization Vector

The CBC, CFB and OFB modes require an additional input to the encryption process, called the initialization vector (IV). The identical IV is used in the input of encryption as well as the decryption of the corresponding ciphertext.

The IV MUST fulfill the following requirements for security:

- CBC, CFB modes. The IV for a particular execution must be unpredictable.
- OFB mode. Each execution must be given a unique IV.

8.3. SM4-ECB

In SM4-ECB, the same key is utilized to create a fixed assignment for a plaintext block with a ciphertext block, meaning that a given plaintext block always gets encrypted to the same ciphertext block.
As described in [NIST.SP.800-38A], this mode should be avoided if this property is undesirable.

This mode requires input plaintext to be a multiple of the block size, which in this case of SM4 it is 128-bits. It also allows multiple blocks to be computed in parallel.

8.3.1. SM4-ECB Encryption

Inputs:
- P, plaintext, length MUST be multiple of b
- K, SM4 128-bit encryption key

Output:
- C, ciphertext, length is a multiple of b

C is defined as follows.

\[ n = \text{NBlocks}(P, b) \]

\[ \text{for } i = 1 \text{ to } n \]
\[ C_i = \text{SM4Encrypt}(P_i, K) \]
\[ \text{end for} \]

\[ C = C_1 || ... || C_n \]

8.3.2. SM4-ECB Decryption

Inputs:
- C, ciphertext, length MUST be multiple of b
- K, SM4 128-bit encryption key

Output:
- P, plaintext, length is a multiple of b

P is defined as follows.
n = NBlocks(C, b)  
for i = 1 to n  
P_i = SM4Decrypt(C_i, K)  
end for  
P = P_1 || ... || P_n  

8.4. SM4-CBC  

SM4-CBC is similar to SM4-ECB that the input plaintext 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. 

Since CBC encryption relies on a forward cipher operation that depend on results of the previous operation, it cannot be parallelized. However, for decryption, since ciphertext blocks are already available, CBC parallel decryption is possible.  

8.4.1. SM4-CBC Encryption  

Inputs:  
o P, plaintext, length MUST be multiple of b  
o K, SM4 128-bit encryption key  
o IV, 128-bit, unpredictable, initialization vector  

Output:  
o C, ciphertext, length is a multiple of b  

C is defined as follows.  

n = NBlocks(P, b)  
C_1 = SM4Encrypt(P_1 xor IV, K)  
for i = 2 to n  
C_i = SM4Encrypt(P_i xor C_{i - 1}, K)  
end for  
C = C_1 || ... || C_n
8.4.2. SM4-CBC Decryption

Inputs:
- C, ciphertext, length MUST be a multiple of b
- K, SM4 128-bit encryption key
- IV, 128-bit, unpredictable, initialization vector

Output:
- P, plaintext, length is multiple of b

P is defined as follows.

\[ n = N\text{Blocks}(C, b) \]
\[ P_1 = \text{SM4Decrypt}(C_1, K) \oplus IV \]
\[ \text{for } i = 2 \text{ to } n \]
\[ P_i = \text{SM4Decrypt}(C_i, K) \oplus C_{i-1} \]
\[ \text{end for} \]
\[ P = P_1 \mid \ldots \mid P_n \]

8.5. SM4-CFB

SM4-CFB relies on feedback provided by successive ciphertext segments to generate output blocks. The plaintext given must be a multiple of the block size.

Similar to SM4-CBC, SM4-CFB requires an IV that is unpredictable for a particular execution of the encryption process.

SM4-CFB further allows setting a positive integer parameter s, that is less than or equal to the block size, to specify the size of each data segment. The same segment size must be used in encryption and decryption.

In SM4-CFB, since the input block to each forward cipher function depends on the output of the previous block (except the first that depends on the IV), encryption is not parallelizable. Decryption, however, can be parallelized.
8.5.1. SM4-CFB Variants

SM4-CFB takes an integer s to determine segment size in its encryption and decryption routines. We define the following variants of SM4-CFB for various s:

- SM4-CFB-1, the 1-bit SM4-CFB mode, where s is set to 1.
- SM4-CFB-8, the 8-bit SM4-CFB mode, where s is set to 8.
- SM4-CFB-64, the 64-bit SM4-CFB mode, where s is set to 64.
- SM4-CFB-128, the 128-bit SM4-CFB mode, where s is set to 128.

8.5.2. SM4-CFB Encryption

Inputs:

- P#, plaintext, length MUST be multiple of s
- K, SM4 128-bit encryption key
- IV, 128-bit, unpredictable, initialization vector
- s, an integer 1 <= s <= b that defines segment size

Output:

- C#, ciphertext, length is a multiple of s

C# is defined as follows.

\[ n = \text{NBlocks}(P\#, s) \]

\[ I_1 = IV \]

\[ \text{for } i = 2 \text{ to } n \]

\[ I_i = \text{LSB}(b - s, I_{i-1}) \| I_{i-1} \]

\[ \text{end for} \]

\[ \text{for } i = 1 \text{ to } n \]

\[ O_j = \text{SM4Encrypt}(I_i, K) \]

\[ \text{end for} \]

\[ \text{for } i = 1 \text{ to } n \]

\[ C_{i-1} = P_{i-1} \text{ xor } \text{MSB}(s, O_j) \]

\[ \text{end for} \]

\[ C# = C_{i-1} \| \ldots \| C_n \]
8.5.3. SM4-CFB Decryption

Inputs:
- C#, ciphertext, length MUST be a multiple of s
- K, SM4 128-bit encryption key
- IV, 128-bit, unpredictable, initialization vector
- s, an integer 1 <= s <= b that defines segment size

Output:
- P#, plaintext, length is multiple of s

P is defined as follows.

\[ n = N\text{Blocks}(P\#, s) \]
\[ I_1 = \text{IV} \]
\[ \text{for } i = 2 \text{ to } n \]
\[ \quad I_i = \text{LSB}(b - s, I_{i-1}) \mid \mid C\#_{j-1} \]
\[ \text{end for} \]
\[ \text{for } i = 1 \text{ to } n \]
\[ \quad O_j = \text{SM4Encrypt}(I_i, K) \]
\[ \text{end for} \]
\[ \text{for } i = 1 \text{ to } n \]
\[ \quad P\#_i = C\#_1 \xoplus \text{MSB}(s, O_j) \]
\[ \text{end for} \]
\[ P\# = P\#_1 \mid \mid ... \mid \mid P\#_n \]

8.6. SM4-OFB

SM4-OFB is the application of SM4 through the Output Feedback mode. This mode requires that the IV is a nonce, meaning that the IV MUST be unique for each execution for an input key. OFB does not require the input plaintext to be a multiple of the block size.

In OFB, the routines for encryption and decryption are identical. As each forward cipher function (except the first) depends on previous results, both routines cannot be parallelized. However, given a known IV, output blocks could be generated prior to the input of plaintext (encryption) or ciphertext (decryption).
8.6.1. SM4-OFB Encryption

Inputs:

- P, plaintext, composed of \((n - 1)\) blocks of size \(b\), with the last block \(P_n\) of size \(1 \leq u \leq b\)
- K, SM4 128-bit encryption key
- IV, a nonce (a unique value for each execution per given key)

Output:

- C, ciphertext, composed of \((n - 1)\) blocks of size \(b\), with the last block \(C_n\) of size \(1 \leq u \leq b\)

\(C\) is defined as follows.

\[
\begin{align*}
    n &= \text{NBlocks}(P, b) \\
    I_1 &= \text{IV} \\
    \text{for } i = 1 \text{ to } (n - 1) \\
    O_i &= \text{SM4Encrypt}(I_i) \\
    I_{i + 1} &= O_i \\
    \text{end for} \\
    \text{for } i = 1 \text{ to } (n - 1) \\
    C_i &= P_i \oplus O_i \\
    \text{end for} \\
    C_n &= P_n \oplus \text{MSB}(u, O_n) \\
    C &= C_1 \mid \ldots \mid C_n
\end{align*}
\]

8.6.2. SM4-OFB Decryption

Inputs:

- C, ciphertext, composed of \((n - 1)\) blocks of size \(b\), with the last block \(C_n\) of size \(1 \leq u \leq b\)
- K, SM4 128-bit encryption key
- IV, the nonce used during encryption

Output:
Internet-Draft                                            September 2017

8.7. SM4-CTR

SM4-CTR is an implementation of a stream cipher through a block
cipher primitive. It generates a "keystream" of keys that are used
to encrypt successive blocks, with the keystream created from the
input key, a nonce (the IV) and an incremental counter. The counter
could be any sequence that does not repeat within the block size.

Both SM4-CTR encryption and decryption routines could be
parallelized, and random access is also possible.

8.7.1. SM4-CTR Encryption

Inputs:

- P, plaintext, composed of \((n - 1)\) blocks of size \(b\), with the last
  block \(P_n\) of size \(1 \leq u \leq b\)

- K, SM4 128-bit encryption key

- IV, a nonce (a unique value for each execution per given key)

- T, a sequence of counters from \(T_1\) to \(T_n\)

Output:
C is defined as follows.

\[
\begin{align*}
n &= \text{NBlocks}(P, b) \\
\text{for } i = 1 \text{ to } n \\
\quad &O_i = \text{SM4Encrypt}(T_i) \\
\text{end for} \\
\text{for } i = 1 \text{ to } (n - 1) \\
\quad &C_i = P_i \text{ xor } O_i \\
\text{end for} \\
C_n &= P_n \text{ xor } \text{MSB}(u, O_n) \\
C &= C_1 || ... || C_n
\end{align*}
\]

### 8.7.2. SM4-CTR Encryption

Inputs:

- C, ciphertext, composed of \((n - 1)\) blocks of size \(b\), with the last block \(C_n\) of size \(1 \leq u \leq b\)
- \(K\), SM4 128-bit encryption key
- IV, a nonce (a unique value for each execution per given key)
- \(T\), a sequence of counters from \(T_1\) to \(T_n\)

Output:

- \(P\), plaintext, composed of \((n - 1)\) blocks of size \(b\), with the last block \(P_n\) of size \(1 \leq u \leq b\)

\(P\) is defined as follows.
n = NBlocks(C, b)

for i = 1 to n
    O_i = SM4Encrypt(T_i)
end for

for i = 1 to (n - 1)
    P_i = C_i xor O_i
end for

P_n = C_n xor MSB(u, O_n)

C = C_1 || ... || C_n

9. Object Identifier

The Object Identifier for SM4 is the value "1.2.156.10197.1.104", specified in [GMT-0006-2012].

10. Security Considerations

- Products and services that utilize cryptography are regulated by OSCCA [OSCCA]; they must be explicitly approved or certified by OSCCA before being allowed to be sold or used in China.

- SM4 [GBT.32907-2016] is a blockcipher certified by OSCCA [OSCCA]. No formal proof of security is provided. There are no known feasible attacks against 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.

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

- SM4-CFB: The OFB mode requires a unique IV for every message that is ever encrypted under the given key. If, contrary to this requirement, the same IV is used for the encryption of more than one message, then the confidentiality of those messages may be compromised. In particular, if a plaintext block of any of these messages is known, say, the jth plaintext block, then the jth
output of the forward cipher function can be determined easily
from the jth ciphertext block of the message. This information
allows the jth plaintext block of any other message that is
encrypted using the same IV to be easily recovered from the jth
ciphertext block of that message. Confidentiality may similarly
be compromised if any of the input blocks to the forward cipher
function for the encryption of a message is designated as the IV
for the encryption of another message under the given key.

11. IANA Considerations

This document does not require any action by IANA.

12. Appendix A: Example Calculations

12.1. Example 1.

This example demonstrates encryption of a plaintext.

Plaintext: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Encryption key: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Status of the round key (rk_i) and round output (X_i) per round:
12.2. Example 2

This example demonstrates encryption of a plaintext 1,000,000 times repeatedly using a fixed encryption key.

Plaintext: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Encryption Key: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Ciphertext: 59 52 98 C7 C6 FD 27 1F 04 02 F8 04 C3 3D 3F 66
13. References

13.1. Normative References


13.2. Informative References


[LSW-Bio] Sun, M., "Lv Shu Wang -- A life in cryptography", November 2010, <http://press.ustc.edu.cn/sites/default/files/fujian/field_fujian_multi/20120113/%E5%90%95%E8%BF%B0%E6%9C%9B%20%E5%AF%86%E7%A0%81%E4%B8%80%E6%A0%B7%E7%9A%84%E4%BA%BA%E7%94%9F.pdf>.
[NIST.FIPS.197]
National Institute of Standards and Technology, "NIST FIPS 197: Advanced Encryption Standard (AES)", November 2001,
<https://doi.org/10.6028/NIST.FIPS.197>.

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


[SideChannel]
Lei, Q., Wu, L., Zhang, S., Zhang, X., Li, X., Pan, L., and Z. Dong, "Software Hardware Co-design for Side-Channel Analysis Platform on Security Chips", December 2015,
<https://doi.org/10.1109/CIS.2015.102>.

[SM4]
Organization of State Commercial Administration of China, "SMS4 Cryptographic Algorithm For Wireless LAN Products", January 2006,

[SM4-Analysis]
Kim, T., Kim, J., Kim, S., and J. Sung, "Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher", June 2008,


[SM4-FPGA] Cheng, H., Zhai, S., Fang, L., Ding, Q., and C. Huang, "Improvements of SM4 Algorithm and Application in Ethernet Encryption System Based on FPGA", July 2014,

[SM4-HiSpeed] Lv, Q., Li, L., and Y. Cao, "High-speed Encryption & Decryption System Based on SM4", July 2016,
<http://dx.doi.org/10.14257/ijsia.2016.10.9.01>.
[SM4-Linear]
Liu, M. and J. Chen, "Improved Linear Attacks on the Chinese Block Cipher Standard", November 2014,

[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,

[SM4-VLSI]

[SM4-WhiteBox]
Bai, K. and C. Wu, "A secure white-box SM4 implementation", May 2008,
<http://dx.doi.org/10.1002/sec.1394>.

Appendix A.  Acknowledgements

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

o Jack Lloyd and Daniel Wyatt of 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