

ICS 35.040

CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 17964-2008

**Information technology -- Security techniques -- Modes of
operation for a block cipher
(English Translation)**

Issued on: June 26, 2008

Implemented on: November 1, 2008

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine**

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	6
2 Normative references...	6
3 Terms and definitions...	6
3.1 Terms...	6
3.2 Definitions...	8
4 Abbreviations and symbols...	10
5 Electronic codebook (ECB) operation mode...	10
5.1 Definition of variable...	10
5.2 Description of ECB encryption...	10
5.3 Description of ECB decryption...	10
6 Cipher block chaining (CBC) operation mode...	11
6.1 Definition of variable...	11
6.2 Description of CBC encryption...	11
6.3 Description of CBC decryption...	12
7 Cipher feedback (CFB) operation mode...	13
7.1 Definition of parameter...	13
7.2 Definition of variable...	13
7.3 Description of CFB encryption...	13
7.4 Description of CFB decryption...	15
7.5 Suggestion...	16
8 Output feedback (OFB) operation mode...	16
8.1 Definition of parameter...	16
8.2 Definition of variable...	17
8.3 Description of OFB encryption...	17
8.4 Description of OFB decryption...	18
9 Counter (CTR) operation mode...	19
9.1 Definition of variable...	19
9.2 Description of CTR encryption...	20
9.3 Description of CTR decryption...	21
10 Block chaining (BC) operation mode...	21

10.1 Definition of variable...	21
10.2 Description of BC encryption...	22
10.3 Description of BC decryption...	23
11 Output feedback with a nonlinear function (OFBNLF) operation mode...	23
11.1 Definition of variable...	23
11.2 Description of OFBNLF encryption...	24
11.3 Description of OFBNLF decryption...	24
Annex A (normative) Nature of operation mode...	26
A.1 Nature of electronic codebook (ECB) operation mode...	26
A.2 Nature of cipher block chaining (CBC) operation mode...	27
A.3 Nature of cipher feedback (CFB) operation mode...	29
A.4 Nature of output feedback (OFB) operation mode...	30
A.5 Nature of counter (CTR) operation mode...	31
A.6 Block chaining (BC) operation mode...	32
A.7 Nature of output feedback with a nonlinear function (OFBNLF) operation mode...	33
Annex B (informative) Example of operation mode...	35
B.1 Overview...	35
B.2 ECB mode...	35
B.3 CBC mode...	35
B.4 CFB mode...	36
B.5 OFB mode...	36
B.6 CTR mode...	37
Bibliography...	39

1 Scope

This Standard specifies seven operation modes of block cipher algorithm, so as to standardize the use of block cipher.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Standard, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable.

For undated references, the latest edition of the referenced document applies.

GB/T 1988-1998, Information technology - 7-bit Coded character set for information interchange (eqv ISO/IEC 646.1991)

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Terms

3.1.1

block chaining (BC) operation mode an operation mode of block cipher algorithm; the current plaintext block is different from the exclusive OR values of all previous ciphertext blocks or operated then encrypted to obtain the current ciphertext block

3.1.2

block cipher also known as block cipher algorithm; it is a symmetric cryptographic algorithm;

it divides plaintext into fixed-length blocks for encryption

3.1.3

block cipher operation mode a use mode of block cipher algorithm, mainly including electronic codebook (ECB) operation mode, cipher block chaining (CBC) operation mode, cipher starting data that is brought for data transformation so as to increase security or synchronize cipher devices during cryptographic transformation

3.1.14

key key information or parameter that controls cryptographic transformation

3.1.15

output feedback with a nonlinear function (OFBNLF) operation mode an operation mode of block cipher algorithm; it is a variant of OFB and ECB; its key varies with each block

3.1.16

output feedback (OFB) operation mode an operation mode that block cipher algorithm is used to construct sequence cipher; use the output of the current time of this algorithm as the input of the next moment

3.1.17

plain text/clear text data to be encrypted

3.2.1 Encryption expression

In this Standard, the functional relationship specified by block cipher is recorded as.

Where,

P is plaintext block;

C is ciphertext block;

K is key;

EK is encryption operation that uses key K.

3.2.2 Decryption expression

The corresponding decryption function is recorded as.

A special case of this function starts with the m-bit variable I(m) of all "1"s and moves the k-bit variable F into it. The result is.

Where, the left-most m-k bit is "1".

4 Abbreviations and symbols

AES advanced encryption standard

BC block chaining

CBC cipher block chaining

CFB cipher feedback

CTR counter

DEA data encryption algorithm

ECB electronic codebook

IV initialization value

OFB output feedback

OFBNLF output feedback with a nonlinear function

5.1 Definition of variable

- a) Sequence consisting of q plaintext blocks P1, P2,..., Pq. Each block is n bits.
- b) Key K.
- c) Result sequence consisting of q ciphertext blocks C1, C2,..., Cq. Each block is n bits.