祖冲之序列密码算法

合订本

第 1 部分：算法描述；

第 2 部分：基于祖冲之算法的机密性算法；

第 3 部分：基于祖冲之算法的完整性算法。

ICS 35.040
L 80
备案号：36822—2012

GM

中华人民共和国密码行业标准

GM/T 0001.1—2012

祖冲之序列密码算法
第1部分：算法描述

ZUC stream cipher algorithm—
Part 1: Description of the algorithm

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发布

目　　次

祖冲之序列密码算法
第1部分:算法描述

1 范围

GM/T 0001的本部分描述了祖冲之序列密码算法,可用于指导祖冲之算法相关产品的研制、检测和使用。

2 术语和约定

以下术语和约定适用于本文件。

2.1

比特 bit

二进制字符0和1称之为比特。

2.2

字节 byte

由8个比特组成的比特串称之为字节。

2.3

字 word

由2个以上(包含2个)比特组成的比特串称之为字。

本部分主要使用31比特字和32比特字。

2.4

字表示 word representation

本部分字默认采用十进制表示。当字采用其他进制表示时,总是在字的表示之前或之后添加指示符。例如,前缀0x指示该字采用十六进制表示,后缀下角标2指示该字采用二进制表示。

2.5

高低位顺序 bit ordering

本部分规定字的最高位总是位于字表示中的最左边,最低位总是位于字表示中的最右边。

3 符号和缩略语

3.1 运算符

$+$	算术加法运算
mod	整数取余运算
$\oplus$	按比特位逐位异或运算
$\boxplus$	模2^{32}加法运算
$\|\|$	字符串连接符
$\cdot_H$	取字的最高16比特
$\cdot_L$	取字的最低16比特
$<<<k$	32比特字左循环移k位
$>>k$	32比特字右移k位

$\underline{a} \rightarrow \underline{b}$　向量 $\underline{a}$ 赋值给向量 $\underline{b}$，即按分量逐分量赋值

3.2 符号

下列符号适用于本部分：

$s_0, s_1, s_2, \cdots, s_{15}$	线性反馈移位寄存器的 16 个 31 比特寄存器单元变量
X_0, X_1, X_2, X_3	比特重组输出的 4 个 32 比特字
R_1, R_2	非线性函数 F 的 2 个 32 比特记忆单元变量
W	非线性函数 F 输出的 32 比特字
Z	算法每拍输出的 32 比特密钥字
k	初始种子密钥
iv	初始向量
D	用于算法初始化的字符串常量

3.3 缩略语

下列缩略语适用于本部分：

ZUC	祖冲之序列密码算法或祖冲之算法
LFSR	线性反馈移位寄存器
BR	比特重组
F	非线性函数

4 算法描述

4.1 算法整体结构

祖冲之算法逻辑上分为上中下三层，见图 1。上层是 16 级线性反馈移位寄存器(LFSR)；中层是比特重组(BR)；下层是非线性函数 F。

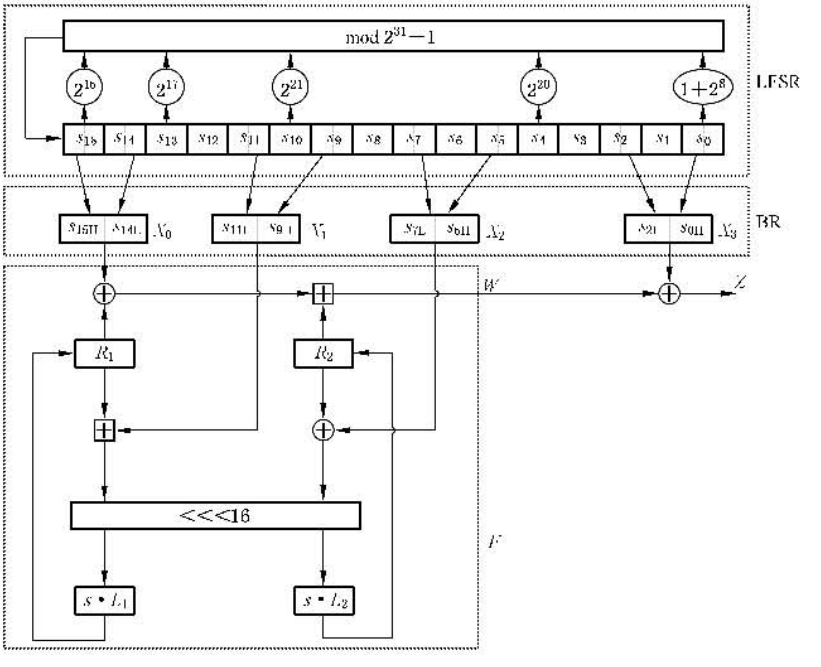

图 1　祖冲之算法结构图

4.2 线性反馈移位寄存器 LFSR

4.2.1 概述

LFSR 包括 16 个 31 比特寄存器单元变量 $s_0, s_1, \cdots, s_{15}$。

LFSR 的运行模式有 2 种：初始化模式和工作模式。

4.2.2 初始化模式

在初始化模式下，LFSR 接收一个 31 比特字 u。u 是由非线性函数 F 的 32 比特输出 W 通过舍弃最低位比特得到，即 $u-W>>1$。在初始化模式下，LFSR 计算过程如下：

LFSRWithInitialisationMode(u)

{

(1) $v-2^{15}s_{15}+2^{17}s_{13}+2^{21}s_{10}+2^{20}s_4+(1+2^8)s_0 \bmod (2^{31}-1)$；

(2) $s_{16}-(v+u) \bmod (2^{31}-1)$；

(3) 如果 $s_{16}-0$，则置 $s_{16}-2^{31}-1$；

(4) $(s_1, s_2, \cdots, s_{15}, s_{16}) \rightarrow (s_0, s_1, \cdots, s_{14}, s_{15})$。

}

4.2.3 工作模式

在工作模式下，LFSR 不接收任何输入。其计算过程如下：

LFSRWithWorkMode()

{

(1) $s_{16}-2^{15}s_{15}+2^{17}s_{13}+2^{21}s_{10}+2^{20}s_4+(1+2^8)s_0 \bmod (2^{31}-1)$；

(2) 如果 $s_{16}-0$，则置 $s_{16}-2^{31}-1$；

(3) $(s_1, s_2, \cdots, s_{15}, s_{16}) \rightarrow (s_0, s_1, \cdots, s_{14}, s_{15})$。

}

4.3 比特重组 BR

比特重组从 LFSR 的寄存器单元中抽取 128 比特组成 4 个 32 比特字 X_0、X_1、X_2、X_3。BR 的具体计算过程如下：

BitReconstruction()

{

(1) $X_0-s_{15H} \| s_{14L}$；

(2) $X_1-s_{11L} \| s_{9H}$；

(3) $X_2-s_{7L} \| s_{5H}$；

(4) $X_3-s_{2L} \| s_{0H}$。

}

4.4 非线性函数 F

F 包含 2 个 32 比特记忆单元变量 R_1 和 R_2。

F 的输入为 3 个 32 比特字 X_0、X_1、X_2，输出为一个 32 比特字 W。F 的计算过程如下：

$F(X_0, X_1, X_2)$

{