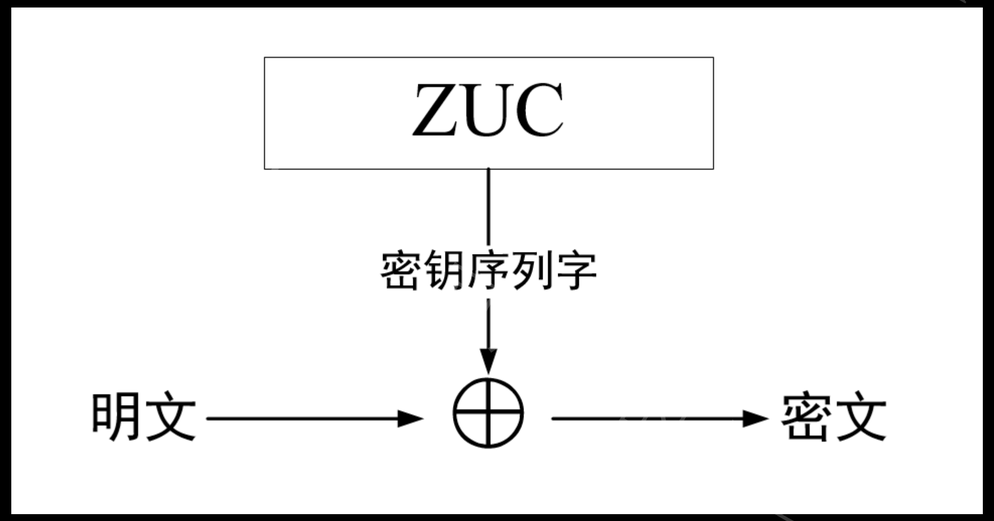
祖冲之序列密码算法

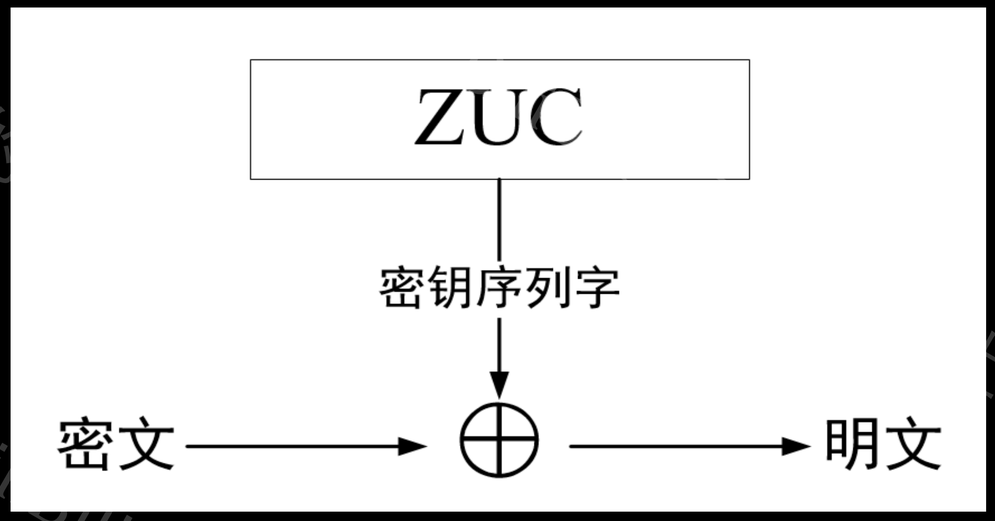
ZUC stream cipher algorithm

可厉害的土豆

简介

- ZUC为流密码算法





组成部分

- 线性反馈移位寄存器（LFSR)
- 比特重组（BR)
- 非线性函数（F）

线性反馈移位寄存器（LFSR）

- LFSR包括16个31比特寄存器单元变量$S_0, S_1, S_2 \cdots S_{15}$。
- LFSR分为两种运行模式：初始化模式 和 工作模式。

比特重组（BR）

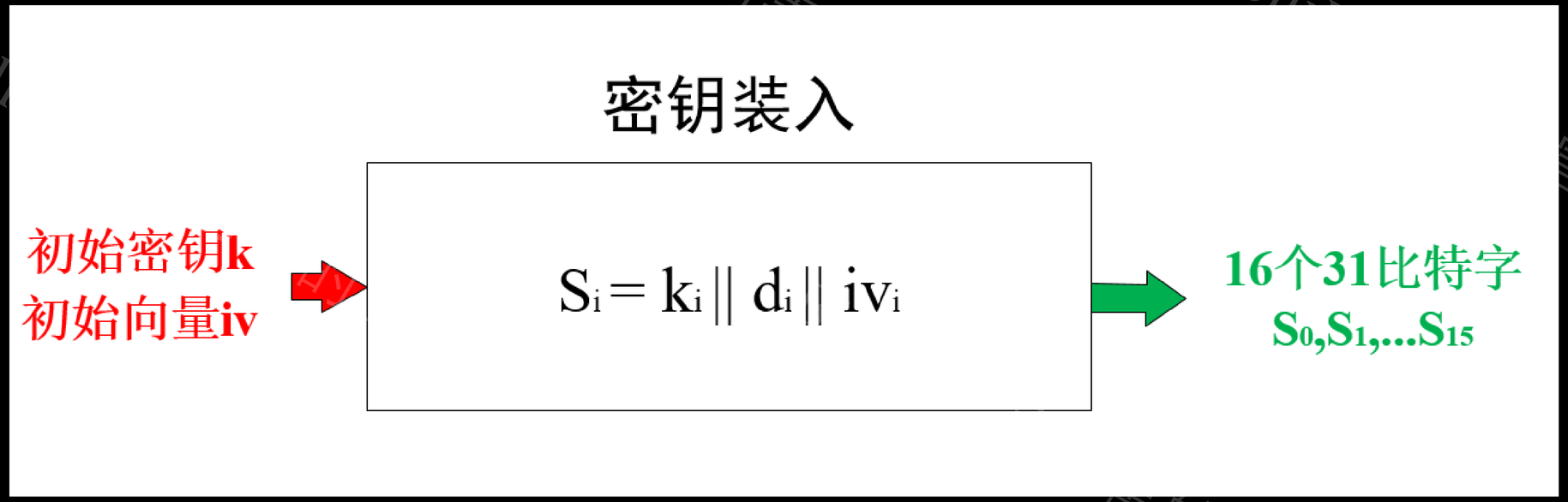
- 比特重组：从 LFSR的寄存器单元中抽取128比特组成4个32比特字：X_0, X_1, X_2, X_3。

非线性函数（F）

- 非线性函数有2个32比特长的存储单元R_1和R_2，其输入为来自上层BR的3个32比特字X_0,X_1,X_2，输出为一个32比特字W。
- 因此，非线性函数F是一个把96比特压缩为32比特的一个非线性压缩函数。

密钥装入

- 密钥载入过程将128比特的初始密钥k和128比特的初始向量iv扩展为16个31比特长的整数，作为LFSR寄存器单元$S_0, S_1, S_2 \cdots S_{15}$的初始状态。



算法运行

- 祖冲之算法的输入参数为 初始密钥k、初始向量iv和正整数L，输出参数为L个密钥字Z。

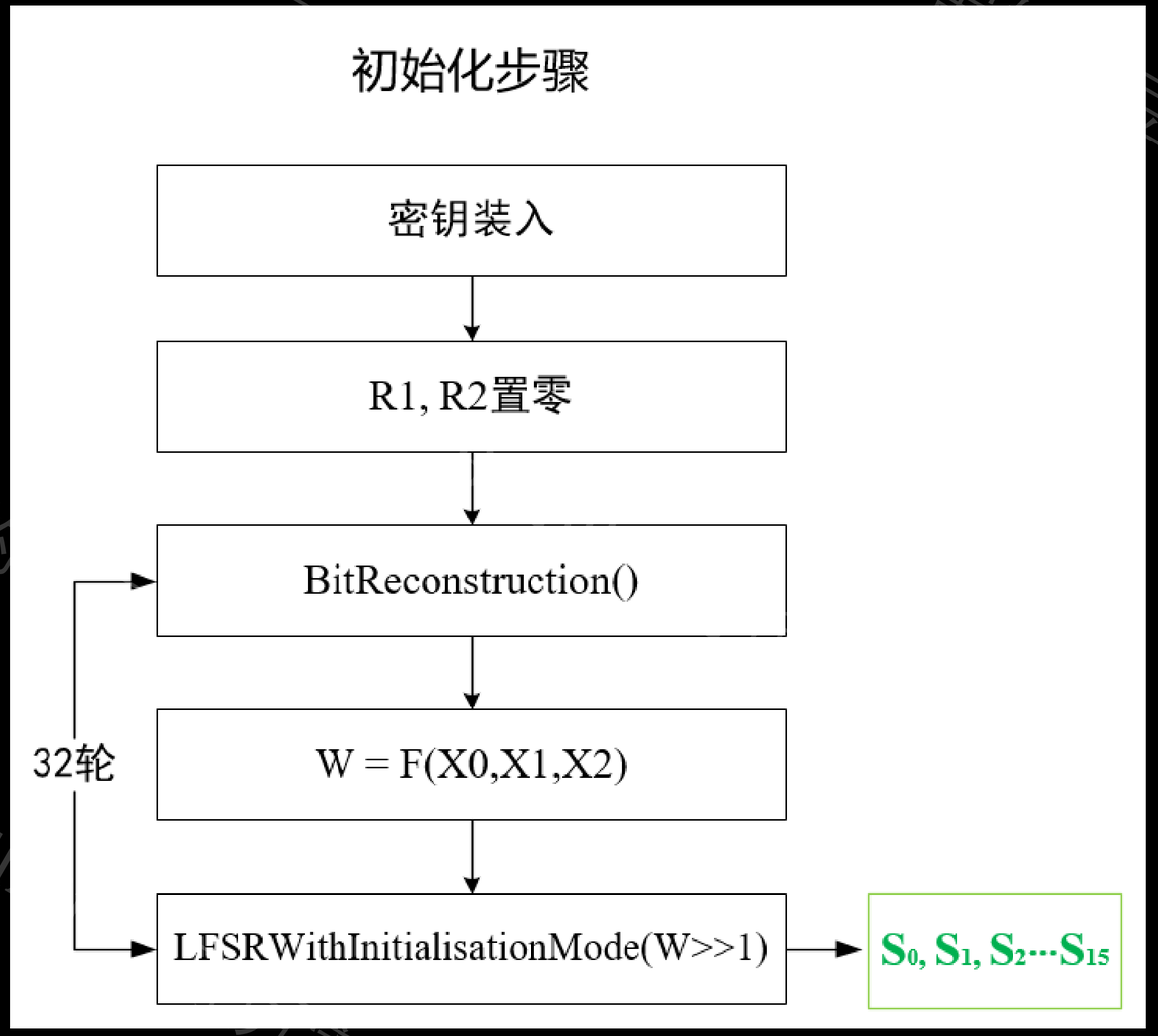
- 算法运行过程包括 初始化步骤 和 工作步骤。

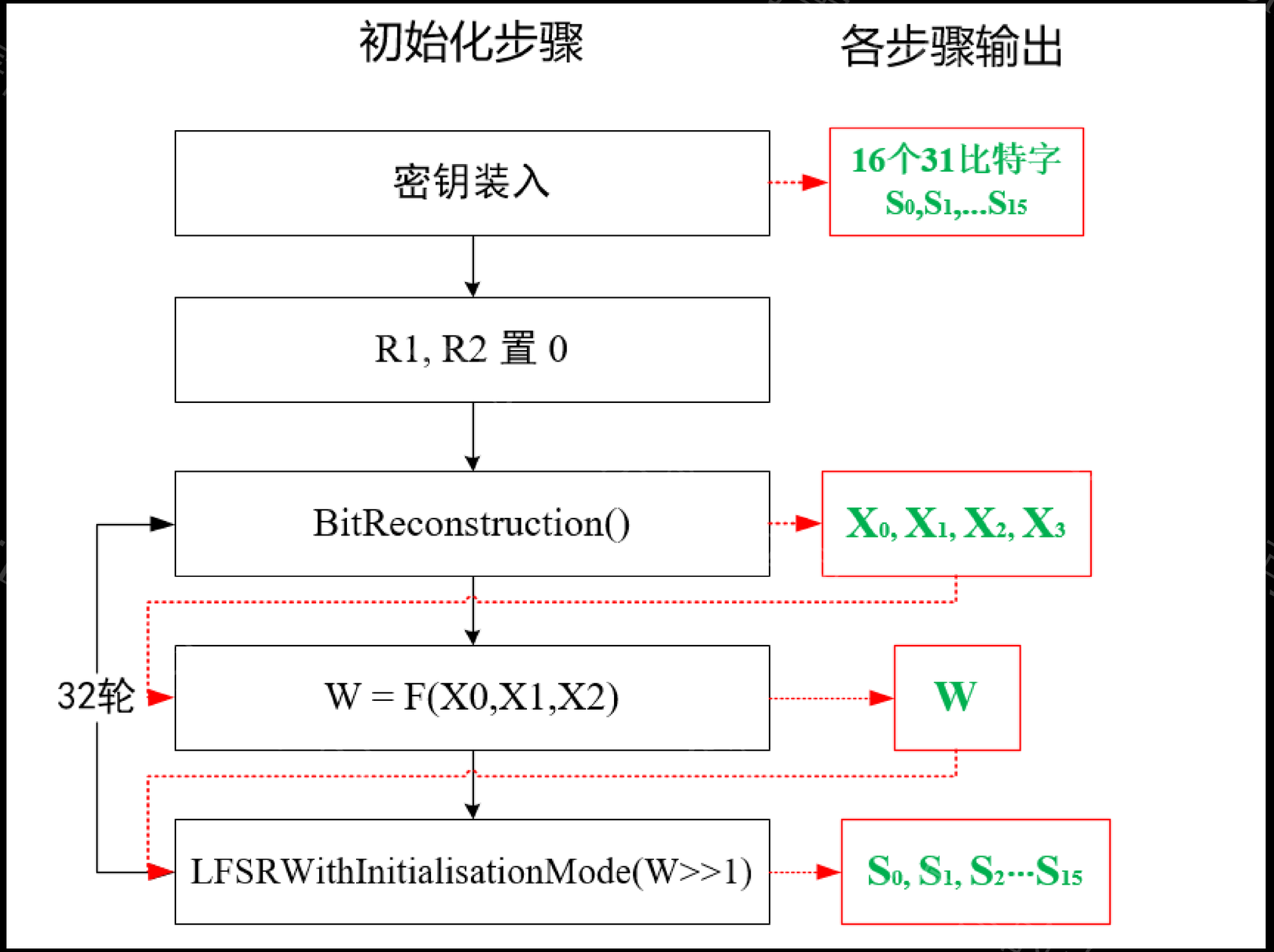
L = [LENGTH /32]

LENGTH 为明文消息的比特长度

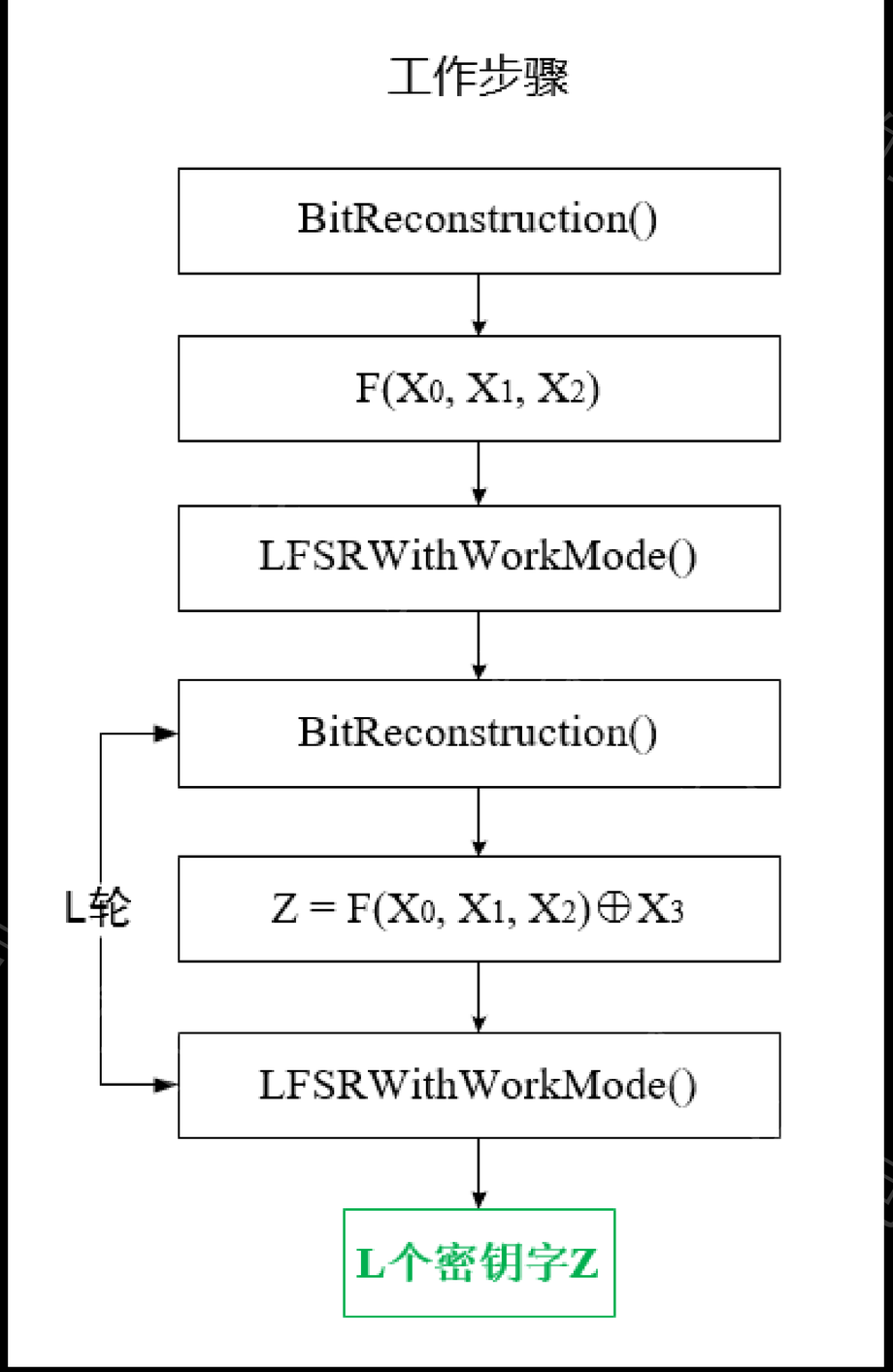
- 初始化步骤：

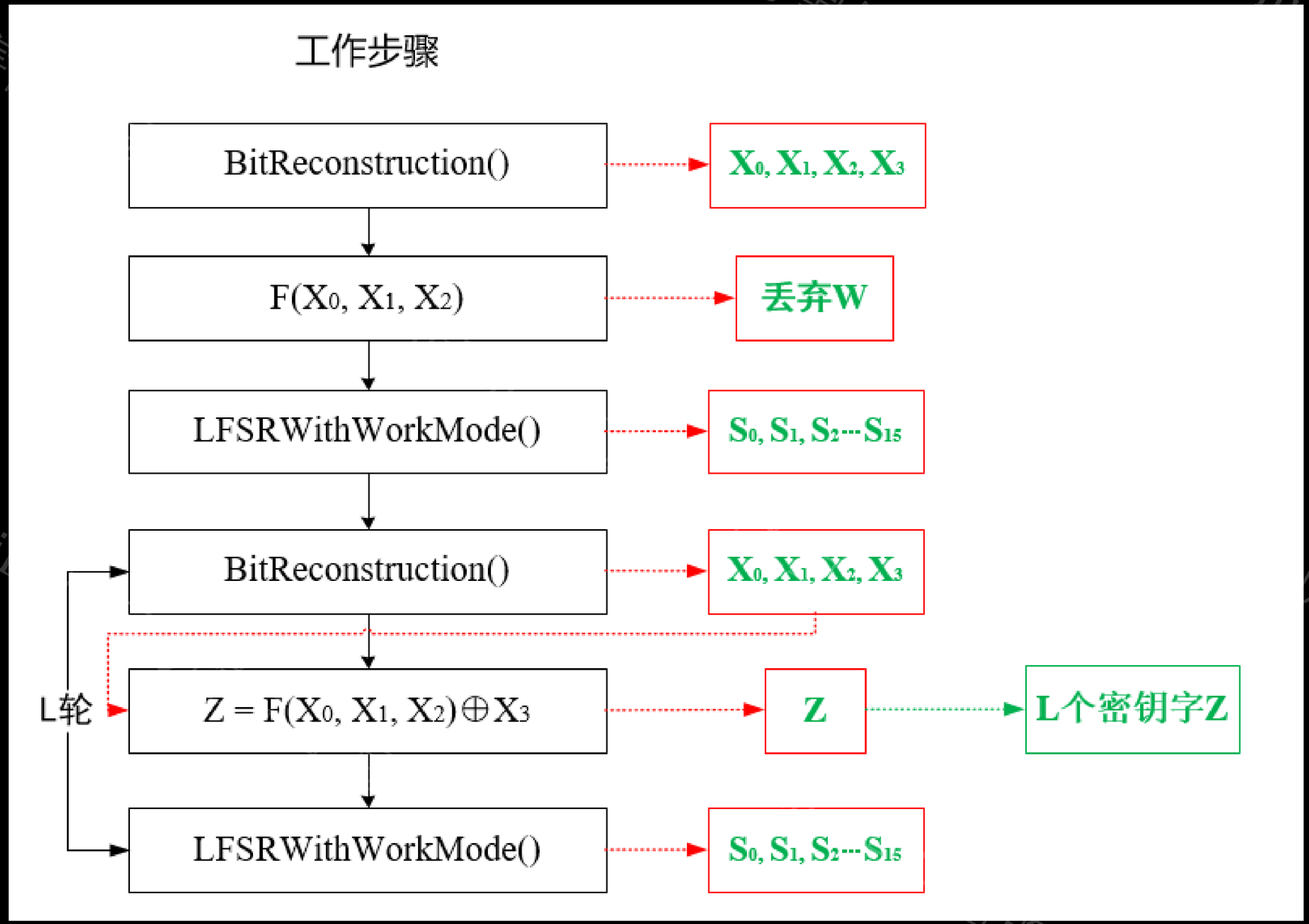
- 调用密钥装载过程，将128比特的初始密钥 k 和128比特的初始向量 iv 装入到LFSR的寄存器单元变量$S_0, S_1, S_2 \cdots S_{15}$ 中，作为LFSR的初态；并置非线性函数 F 中的32比特存储单元 R1 和 R2 全为0。然后重复循环过程32次。




初始化步骤
各步骤输出
密钥装入
16个31比特字
S0,S1,...S15
R1, R2 置 0
BitReconstruction()
X0, X1, X2, X3
32轮
W = F(X0,X1,X2)
W
LFSRWithInitialisationMode(W>>1)
S0, S1, S2…S15

- 工作步骤：

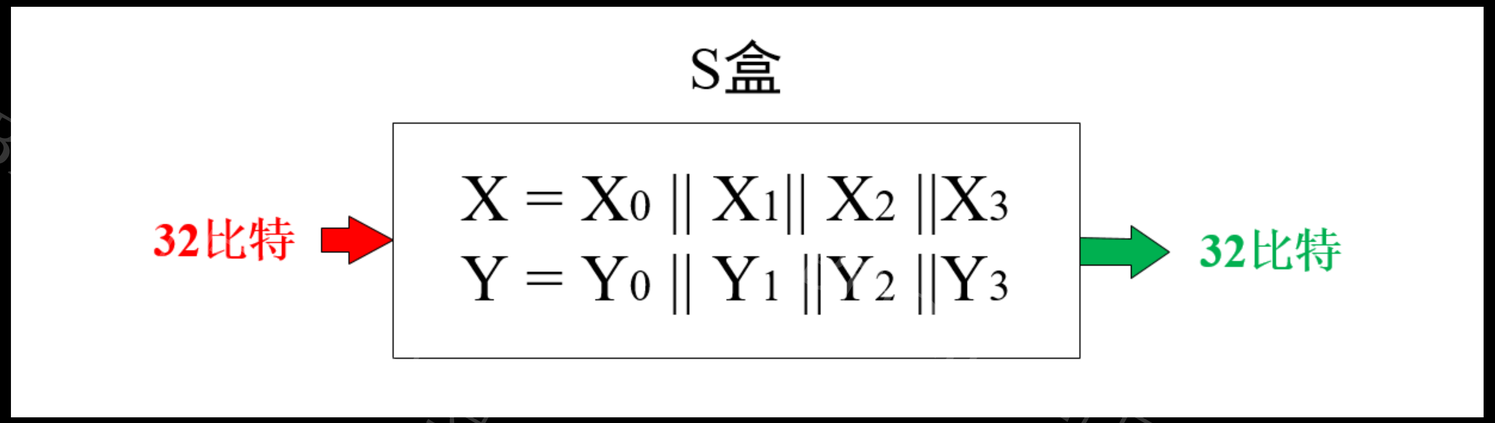

工作步骤
BitReconstruction()
F(X0, X1, X2)
LFSRWithWorkMode()
BitReconstruction()
Z = F(X0, X1, X2)⊕X3
L轮
LFSRWithWorkMode()
L个密钥字Z


工作步骤
BitReconstruction()
X0, X1, X2, X3
F(X0, X1, X2)
丢弃W
LFSRWithWorkMode()
S0, S1, S2…S15
BitReconstruction()
X0, X1, X2, X3
L轮
Z = F(X0, X1, X2)⊕X3
Z
L个密钥字Z
LFSRWithWorkMode()
S0, S1, S2…S15

S 盒

32 = 8 || 8 || 8 || 8

即以8比特为单位进行转换



- 输入：00111010　　即 3A
- 输出：FD　　即 11111101

参考资料

[1]

[2]

[1] https://openstd.samr.gov.cn/bzgk/gb/
[2] https://zhuanlan.zhihu.com/p/531692793

“

感谢观看

祝你每顿吃饱

每晚睡好

身体健康

学业有成

工作顺利

”

—可厉害的土豆