



(12) 发明专利申请

(10) 申请公布号 CN 104683096 A

(43) 申请公布日 2015. 06. 03

(21) 申请号 201310631264. 2

(22) 申请日 2013. 11. 29

(71) 申请人 中国航天科工集团第三研究院第
八三五七研究所

地址 300308 天津市东丽区空港经济区保税
路 357 号

(72) 发明人 李宏耀

(74) 专利代理机构 北京卫平智业专利代理事务
所(普通合伙) 11392

代理人 符彦慈

(51) Int. Cl.

H04L 9/06(2006. 01)

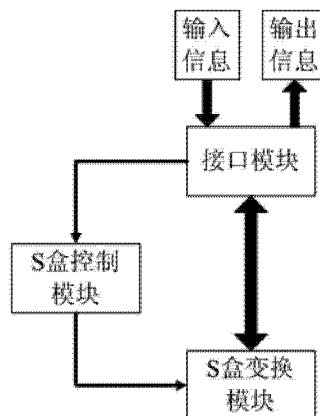
权利要求书3页 说明书7页 附图2页

(54) 发明名称

动态 S 盒变换方法及系统

(57) 摘要

本发明公开了一种动态 S 盒变换方法及系统,包括接口模块、S 盒控制模块和 S 盒变换模块,接口模块实现密钥、信息和控制信号的接收、存储与发送;S 盒控制模块实现整个 S 盒变换的动态控制;S 盒变换模块实现 S 盒变换的动态变换。本发明在 S 盒变换中增加了初始密钥奇偶性的依赖关系,同时增加了 S 盒变换的数目,让 S 盒变换动态化和多样化,克服了传统 S 盒变换固定单一且独立于密码算法的缺陷,提高了 S 盒变换输入和输出之间的复杂性,增强了密码算法的安全性能,且提高了运行速度,有效地节省了硬件资源。



1. 一种动态 S 盒变换系统,包括 :接口模块、S 盒控制模块和 S 盒变换模块 ;

所述接口模块包括密钥寄存器、输入信息存储器、输出信息存储器和控制信号寄存器,实现密钥、信息和控制信号的接收、存储与发送 ;

所述 S 盒控制模块包括奇偶判别器、加解密控制器和乘法累加运算单元控制器,实现整个 S 盒变换的动态控制 ;

所述 S 盒变换模块包括有限域 $GF(2^8)$ 乘法逆元变换器和 4 个乘法累加运算单元,实现 S 盒变换的动态变换。

2. 根据权利要求 1 所述的动态 S 盒变换系统,其特征在于,所述 S 盒变换依赖于初始密钥的奇偶性 ;初始密钥的奇偶性不同,则 S 盒变换的结果也不同。

3. 根据权利要求 1 所述的动态 S 盒变换系统,其特征在于,

所述的 S 盒变换包括 S 盒变换 1 和 S 盒变换 2,其中 S 盒变换 1 和 S 盒变换 2 分别与初始密钥的奇偶性相对应,并且 S 盒变换 1 和 S 盒变换 2 均包含了有限域 $GF(2^8)$ 的乘法逆元运算和仿射变换的线性运算。

4. 根据权利要求 3 所述的动态 S 盒变换系统,其特征在于,

所述有限域 $GF(2^8)$ 的乘法逆元运算中, S 盒变换 1 和 S 盒变换 2 均以 $m(x) = x^8 + x^4 + x^3 + x + 1$ 为不可约多项式,仿射变换的线性运算中, S 盒变换 1 的仿射变换为公式 1 和公式 3, S 盒变换 2 的仿射变换为公式 2 和公式 4 ;其中 :

公式 1 :

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

公式 2 :

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

公式 3:

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

公式 4:

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}。$$

5. 根据权利要求3所述的动态S盒变换系统,其特征在于:S盒变换1和S盒变换2共用同一个有限域GF(2⁸)乘法逆元变换器,实现有限域GF(2⁸)的乘法逆元运算。

6. 一种动态S盒变换方法,包括:

a. 密钥寄存器存储接收到的初始密钥信息;

输入信息寄存器存储接收到的待处理输入信息;

控制信号寄存器存储接收到的加解密控制信号;

b. 奇偶判别器用于判别初始密钥的奇偶性,并将判别结果传送给乘法累加运算单元控制器;

加解密控制器控制4个乘法累加运算单元,根据控制信号寄存器的值控制动态S盒工作于加密模式还是解密模式;

乘法累加运算单元控制器控制4个乘法累加运算单元,根据奇偶判别器的结果控制动态S盒工作于S盒变换1模式还是S盒变换2模式;

c. 有限域GF(2⁸)乘法逆元变换器存储有256个固定的逆元字节数据,该256个固定的逆元字节数据与有限域GF(2⁸)上的256个元素一一对应,将输入的数据用该存储器中的对应逆元替代;

4个乘法累加运算单元实现数据之间的乘积运算和加法运算。

d. 输出信息寄存器存储处理完毕的信息;等待外部设备读取。

动态 S 盒变换方法及系统

技术领域

[0001] 本发明涉及一种 S 盒变换方法及系统,具体涉及加解密过程中的动态 S 盒变换方法及系统。

背景技术

[0002] 随着计算机网络及通信技术的迅速发展,密码学的研究得到前所未有的重视,信息社会中的信息安全问题受到越来越多的关注,信息安全问题已经被我国政府提高到了国家发展战略的层次。

[0003] S 盒变换,也称字节替换变换,就是将一个字节数据用另一个不相关的字节数据替代。S 盒变换是许多密码算法中的唯一非线性变换,主要用于密码设计中的混淆功能,它的密码学性质往往决定了整个密码算法的安全性能。一般,在密码算法的整个算法过程中,S 盒变换是固定且唯一的,也即是一种静态的 S 盒变换,这样的 S 盒变换的输入和输出具有固定且单一的依赖关系,致使密码算法的抗破译性能不够高,有可能导致秘密信息的泄露、甚至重要情报被敌人获取,严重危害国家安全。

发明内容

[0004] 本发明旨在克服传统 S 盒变换固定单一且独立于密码算法的缺陷,让 S 盒变换动态化和多样化,加强 S 盒变换输入和输出之间的复杂性,增强密码算法的安全性能及提高运行速度,提供一种动态 S 盒变换方法及系统。

[0005] 本发明采用如下的技术方案实现的:

[0006] 一种动态 S 盒变换系统,包括接口模块、S 盒控制模块和 S 盒变换模块;

[0007] 接口模块包括密钥寄存器、输入信息存储器、输出信息存储器和控制信号寄存器,实现密钥、信息和控制信号的接收、存储与发送;

[0008] S 盒控制模块包括奇偶判别器、加解密控制器和乘法累加运算单元控制器,实现整个 S 盒变换的动态控制;

[0009] S 盒变换模块包括有限域 $GF(2^8)$ 乘法逆元变换器和 4 个乘法累加运算单元,实现 S 盒变换的动态变换。

[0010] 在上述系统基础,更进一步的小改进:

[0011] S 盒变换结果依赖于初始密钥的奇偶性;初始密钥的奇偶性不同,则 S 盒变换的结果也不同。

[0012] S 盒变换模块,还可包括两个子模块:S 盒变换 1 和 S 盒变换 2;其中 S 盒变换 1 和 S 盒变换 2 分别与初始密钥的奇偶性相对应,并且 S 盒变换 1 和 S 盒变换 2 均包含了有限域 $GF(2^8)$ 的乘法逆元运算和仿射变换的线性运算;

[0013] 有限域 $GF(2^8)$ 的乘法逆元运算中,S 盒变换 1 和 S 盒变换 2 均以 $m(x)=x^8+x^4+x^3+x+1$ 为不可约多项式,仿射变换的线性运算中,S 盒变换 1 的仿射变换为公式 1 和公式 3,S 盒变换 2 的仿射变换为公式 2 和公式 4;

[0014] 公式 1 :

$$\begin{array}{c}
 y_7 \\
 y_6 \\
 y_5 \\
 y_4 \\
 y_3 \\
 y_2 \\
 y_1 \\
 y_0
 \end{array}
 =
 \begin{bmatrix}
 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0
 \end{bmatrix}
 \begin{array}{c}
 x_7 \\
 x_6 \\
 x_5 \\
 x_4 \\
 x_3 \\
 x_2 \\
 x_1 \\
 x_0
 \end{array}
 +
 \begin{array}{c}
 0 \\
 0 \\
 0 \\
 0 \\
 0 \\
 1 \\
 0 \\
 1
 \end{array}$$

[0015]

[0016] 公式 2 :

$$\begin{array}{c}
 y_7 \\
 y_6 \\
 y_5 \\
 y_4 \\
 y_3 \\
 y_2 \\
 y_1 \\
 y_0
 \end{array}
 =
 \begin{bmatrix}
 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \begin{array}{c}
 x_7 \\
 x_6 \\
 x_5 \\
 x_4 \\
 x_3 \\
 x_2 \\
 x_1 \\
 x_0
 \end{array}
 +
 \begin{array}{c}
 1 \\
 1 \\
 0 \\
 0 \\
 1 \\
 1 \\
 0 \\
 0
 \end{array}$$

[0017]

[0018] 公式 3 :

$$\begin{array}{c} [0019] \end{array}
 \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix}
 =
 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}
 \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix}
 +
 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

[0020] 公式 4 :

$$\begin{array}{c} [0021] \end{array}
 \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix}
 =
 \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}
 \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix}
 +
 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

[0022] S 盒变换 1 和 S 盒变换 2 共用同一个有限域 $GF(2^8)$ 乘法逆元变换器, 实现有限域 $GF(2^8)$ 的乘法逆元运算。

[0023] 一种动态 S 盒变换方法, 包括 :

- [0024] a. 密钥寄存器存储接收到的初始密钥信息；
- [0025] 输入信息寄存器存储接收到的待处理输入信息；
- [0026] 控制信号寄存器存储接收到的加解密控制信号；
- [0027] b. 奇偶判别器判别初始密钥的奇偶性，并将判别结果传送给乘法累加运算单元控制器；
- [0028] 加解密控制器控制 4 个乘法累加运算单元，根据控制信号寄存器的值控制动态 S 盒工作于加密模式或解密模式；根据模式选择的结果对待处理信息进行 S 盒变换；
- [0029] 乘法累加运算单元控制器控制 4 个乘法累加运算单元，根据奇偶判别器的结果控制动态 S 盒工作于 S 盒变换 1 模式或 S 盒变换 2 模式；
- [0030] c. 有限域 $GF(2^8)$ 乘法逆元变换器存储有 256 个固定的逆元字节数据，该 256 个固定的逆元字节数据与有限域 $GF(2^8)$ 上的 256 个元素一一对应，将输入的数据用该存储器中的对应逆元替代；
- [0031] 4 个乘法累加运算单元实现数据之间的乘积运算和加法运算；
- [0032] d. 输出信息寄存器存储处理完毕的信息；等待外部设备读取。
- [0033] 本发明的优点是，将初始密钥的奇偶性和 S 盒变换联系到一起，同时增加了 S 盒变换的数目，让 S 盒变换动态化和多样化，增强了 S 盒变换的输入和输出之间的依赖关系，使得密文和明文之间的依赖关系更加复杂，增强了密码算法的安全性能；同时将两种 S 盒变换及其逆变换集成在一个系统中，共用同一个有限域乘法逆元变换器，实现加密的动态 S 盒变换和解密的动态 S 盒变换，提高了运行速度，且有效地节省了硬件资源。

附图说明

- [0034] 图 1 是本发明提供的一种动态 S 盒变换系统的结构框图；
- [0035] 图 2 是本发明提供的一种动态 S 盒变换方法的示意图；
- [0036] 图 3 是有限域 $GF(2^8)$ 上的 256 个字节数据及其逆元数据表。

具体实施方式

- [0037] 下面，结合附图和具体实施例，对发明的 X 种实施方式作进一步的说明。
- [0038] 实施例 1
- [0039] 如附图 1、2 所示，一种动态 S 盒变换方法及系统，接口模块包括密钥寄存器、输入信息存储器、输出信息存储器和控制信号寄存器，实现密钥、信息和控制信号的接收、存储与发送；S 盒控制模块包括奇偶判别器、加解密控制器和乘法累加运算单元控制器，实现整个 S 盒变换的动态控制；S 盒变换模块包括有限域 $GF(2^8)$ 乘法逆元变换器和 4 个乘法累加运算单元，实现 S 盒变换的动态变换。
- [0040] 如附图 2 所示，有限域 $GF(2^8)$ 乘法逆元变换器中存储有 256 个有限域 $GF(2^8)$ 的逆元字节数据，该字节数据是将有限域 $GF(2^8)$ 上的 256 个数据以 $m(x)=x^8+x^4+x^3+x+1$ 为不可约多项式求逆得到的 256 个逆元数据，结果如表 1 所示。有限域 $GF(2^8)$ 乘法逆元变换器根据接收到的字节信息，输出相对应的字节逆元信息。
- [0041] 如附图 2 所示，4 个乘法累加运算单元包括乘法累加运算单元 1、乘法累加运算单元 2、乘法累加运算单元 3 和乘法累加运算单元 4。其中乘法累加运算单元 1 完成公式 1 的

矩阵运算；乘法累加运算单元 2 完成公式 2 的矩阵运算；乘法累加运算单元 3 完成公式 3 的矩阵运算；乘法累加运算单元 4 完成公式 4 的矩阵运算。

[0042] 公式 1：

$$[0043] \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

[0044] 公式 2：

$$[0045] \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

[0046] 公式 3：

$$[0047] \quad \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

[0048] 公式 4 :

$$[0049] \quad \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

[0050] 如附图 2 所示,本发明工作过程如下:

[0051] (1) 接收信息及处理命令

[0052] 控制信号寄存器接收加解密的处理命令并存储;信息存储器接收待处理信息并存储;密钥寄存器接收加解密的初始密钥并存储。

[0053] (2) 数据处理

[0054] (a)、奇偶判别

[0055] 奇偶判别器将密钥寄存器的初始密钥做逐位异或运算,判断初始密钥的奇偶性,并将结果送入乘法累加运算单元控制器。

[0056] (b)、模式选择

[0057] 加解密控制器根据控制信号寄存器的值决定变换工作于加密模式还是解密模式：如果加解密控制器的信号值为 1，则乘法累加运算单元 1 和乘法累加运算单元 2 失效，乘法累加运算单元 3 和乘法累加运算单元 4 有效；如果加解密控制器的信号值为 0，则乘法累加运算单元 1 和乘法累加运算单元 2 有效，乘法累加运算单元 3 和乘法累加运算单元 4 失效。

[0058] 乘法累加运算单元控制器根据接收到的奇偶判别器的结果选择相应的乘法累加运算单元：如果奇偶判别器的结果为 1，则乘法累加运算单元 1 和乘法累加运算单元 3 有效，乘法累加运算单元 2 和乘法累加运算单元 4 失效；如果奇偶判别器的结果为 0，则乘法累加运算单元 1 和乘法累加运算单元 3 失效，乘法累加运算单元 2 和乘法累加运算单元 4 有效。

[0059] (c)、S 盒变换

[0060] 根据模式选择的结果对待处理信息进行 S 盒变换：如果加解密控制器的信号值为 1，同时奇偶判别器的值为 1，则将待处理信息送入有限域 $GF(2^8)$ 乘法逆元变换器，再将得到的逆元值送入乘法累加运算单元 3，完成整个 S 盒变换；如果加解密控制器的信号值为 0，同时奇偶判别器的值为 0，则将待处理信息送入乘法累加运算单元 2，再将得到的结果送入有限域 $GF(2^8)$ 乘法逆元变换器，完成整个 S 盒逆变换。

[0061] (3) 信息输出

[0062] 输出信息存储器接收 S 盒变换完成的数据并存储，等待外部设备读取。

[0063] 以上所述仅为本发明的较佳可行实施例，并非因此局限本发明的专利范围，故凡是运用本发明说明书及附图内容所作的等效结构变化，均包含于本发明的保护范围。

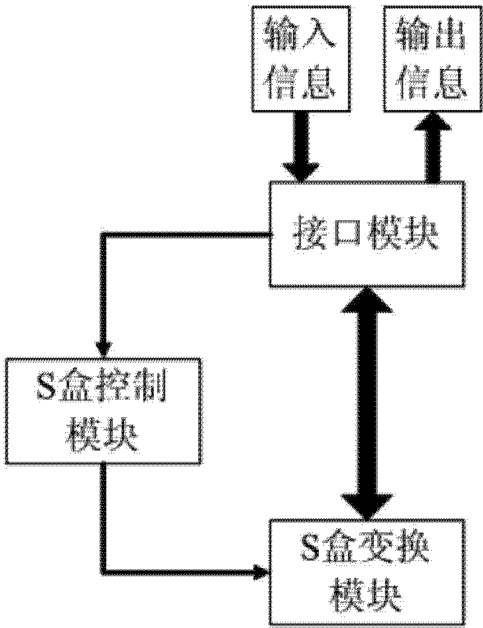


图 1

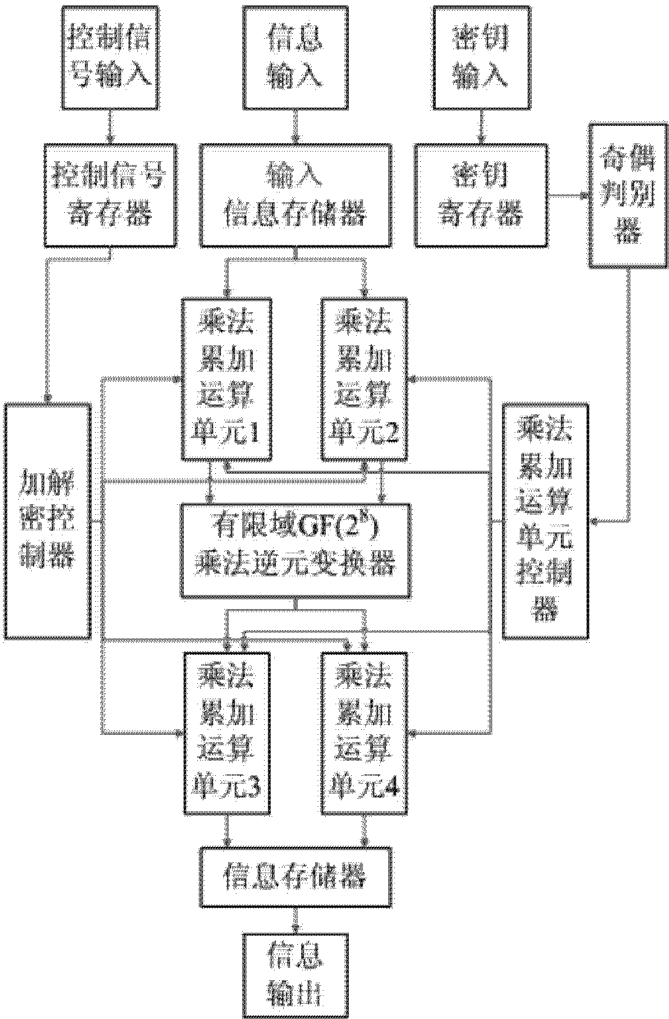


图 2

原值	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
逆元	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
原值	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
逆元	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
原值	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F
逆元	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
原值	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
逆元	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
原值	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
逆元	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
原值	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F
逆元	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
原值	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F
逆元	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
原值	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F
逆元	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
原值	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F
逆元	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
原值	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F
逆元	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
原值	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	AF
逆元	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
原值	B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	BA	BB	BC	BD	BE	BF
逆元	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
原值	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF
逆元	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
原值	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	DE	DF
逆元	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
原值	E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	EE	EF
逆元	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
原值	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF
逆元	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

图 3