(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105790926 A
(43)申请公布日 2016.07.20

(21)申请号 201410830365.7

(22)申请日 2014.12.26

(71)申请人 中国科学院沈阳自动化研究所
地址 110016 辽宁省沈阳市东陵区南塔街114号

(72)发明人 董策 段茂强 王剑 谢闯 杨志家

(74)专利代理机构 沈阳科苑专利商标代理有限公司 21002
代理人 许宗富 周秀梅

(51)Int.Cl.
H04L 9/06(2006.01)

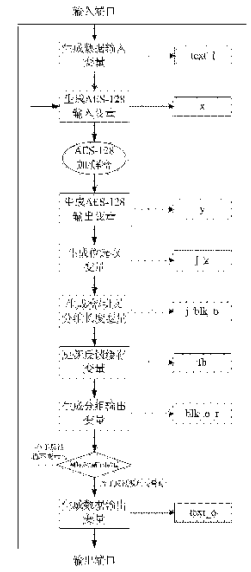
权利要求书1页 说明书5页 附图2页

(54)发明名称

用于WIA-PA安全的分组密码算法工作模式实现方法

(57)摘要

本发明涉及用于WIA-PA安全的分组密码算法工作模式实现方法，包括以下步骤：设置加密或解密操作类型；设置工作模式及分组输入的长度；加载密钥和初始化向量并设定反馈缓存变量；加载数据输入变量并生成AES-128加/解密的输入x；将待加/解密的输入x进行AES-128加/解密操作，生成输出y；更新反馈缓存变量值；根据操作类型和工作模式生成数据输出变量。本发明既能单独实现分组密法算法的多种工作模式，还能够支持IEEE 802.15.4协议中CCM*模式的加/解密功能和认证功能，能够满足WIA-PA网络的信息安全功能和需求。解决了传统上控制过程复杂、处理器工作负载繁重的弊端。



CN 105790926 A

1.用于WIA-PA安全的分组密码算法工作模式实现方法,其特征在于包括以下步骤:

1)设置加密或解密操作类型;

2)设置工作模式及分组输入的长度;

3)加载密钥和初始化向量并设定反馈缓存变量;

4)加载数据输入变量并生成AES-128加/解密的输入x;

5)将待加/解密的输入x进行AES-128加/解密操作,生成输出y;

6)更新反馈缓存变量值;当反馈循环计数值小于设定次数时,返回步骤4),否则执行下一步骤;

7)根据操作类型和工作模式生成数据输出变量text_o。

2.根据权利要求1所述的用于WIA-PA安全的分组密码算法工作模式实现方法,其特征在于所述生成输出y后,当工作模式为CFB、OFB和CTR时,生成位选取变量j_z和生成密/明文分组长度变量j_blk_o。

3.根据权利要求1所述的用于WIA-PA安全的分组密码算法工作模式实现方法,其特征在于所述生成输出y后,当工作模式为CBC时,生成密/明文分组变量blk_o。

4.根据权利要求1所述的用于WIA-PA安全的分组密码算法工作模式实现方法,其特征在于所述更新反馈缓存变量值后,当工作模式为CFB、OFB和CTR时,生成分组输出变量blk_o_r。

用于 WIA-PA 安全的分组密码算法工作模式实现方法

技术领域

[0001] 本发明属于加解密技术领域，具体说是一种应用于 WIA-PA 信息安全的分组密码算法工作模式控制模块的实现方法。

背景技术

[0002] WIA-PA（面向工业过程自动化的工业无线网络标准技术）标准是中国工业无线联盟针对过程自动化领域制定的，是基于 IEEE 802.15.4 标准的用于工业过程测量、监视与控制的无线网络系统。

[0003] WIA-PA 安全体系结构是建立在 IEEE 802.15.4 的安全服务基础上。WIA-PA 利用这些安全服务对传输的数据进行加密处理，并提供对接入网络的设备的身份认证、密钥管理等功能，WIA-PA 定义的网络层和应用层都包含该安全体系。

[0004] IEEE 802.15.4 安全服务是基于 CCM* 安全模式生成一系列的安全机制。IEEE802.15.4 规定 CCM* 安全模式中使用的加密函数为 128 位数据分组长度和 128 位密钥长度的 AES 加密算法，即 AES-128 加密算法。CCM* 模式是 CCM 加密模式的扩展。CCM 模式结合了 CTR 和 CBC-MAC 而衍生出来的安全模式，既包含了加 / 解密功能，又包含了认证功能。

[0005] 分组密码又称块密码算法，是一种对称密码算法，将明文划分成固定长度的分组进行加密。分组密码算法工作模式是分组密码算法的使用方式，主要包括电码本模式 (ECB)、密码分组链接模式 (CBC)、密码反馈模式 (CFB)、输出反馈模式 (OFB)、计数器模式 (CTR) 等。

[0006] AES（高级加密标准），是由 NIST（美国国家标准与技术研究院）于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。AES 加密算法，又称为 Rijndael 加密算法，该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位 (16 字节) 分组加密和解密数据。IEEE 802.15.4 采用固定的 128 位密钥，记为 AES-128。不论对于 AES 加密算法还是解密算法，都是使用轮变换的操作。轮变换操作次数与密钥的位数有关，AES-128 轮数为 10 轮。IEEE 802.15.4 协议中只用到了 AES-128 加密算法，明文首先进行一个密钥加的操作，然后进行 10 次轮变换操作。轮变换包括 4 个操作：字节置换、行换位、列混合和密钥加。

[0007] 传统无线网络节点所采用的安全机制存在一个弊端，大多由软件实现或只实现了 AES 加解密功能。即在一次加解密或身份认证流程中，处理器必须进行多次干预，既使控制过程复杂化，也增加了处理器的工作负载。

发明内容

[0008] 本发明提出了一种适用于 WIA-PA 信息安全的分组密码算法工作模式控制模块的实现方法，以克服上述技术不足。

[0009] 本发明为实现上述目的所采用的技术方案是：用于 WIA-PA 安全的分组密码算法工作模式实现方法，包括以下步骤：

[0010] 1) 设置加密或解密操作类型；

[0011] 2) 设置工作模式及分组输入的长度；

[0012] 3) 加载密钥和初始化向量并设定反馈缓存变量；

[0013] 4) 加载数据输入变量并生成 AES-128 加 / 解密的输入 x；

[0014] 5) 将待加 / 解密的输入 x 进行 AES-128 加 / 解密操作，生成输出 y；

[0015] 6) 更新反馈缓存变量值；当反馈循环计数值小于设定次数时，返回步骤 4)，否则执行下一步骤；

[0016] 7) 根据操作类型和工作模式生成数据输出变量 text_o。

[0017] 所述生成输出 y 后，当工作模式为 CFB、OFB 和 CTR 时，生成位选取变量 j_z 和生成密 / 明文分组长度变量 j_blk_o。

[0018] 所述生成输出 y 后，当工作模式为 CBC 时，生成密 / 明文分组变量 blk_o。

[0019] 所述更新反馈缓存变量值后，当工作模式为 CFB、OFB 和 CTR 时，生成分组输出变量 blk_o_r。

[0020] 本发明具有以下有益效果及优点：

[0021] 1. 本发明以 AES-128 加解密为基础，通过控制信号的控制，既能单独实现分组密法算法的多种工作模式，还能够支持 IEEE 802.15.4 协议中 CCM* 模式的加 / 解密功能和认证功能，能够满足 WIA-PA 网络的信息安全功能和需求。

[0022] 2. 本发明解决了传统上控制过程复杂、处理器工作负载繁重的弊端。

附图说明

[0023] 图 1 为本发明的分组密码算法工作模式控制模块示意图；

[0024] 图 2 为 AES-128 加密操作的结构示意图；

[0025] 图 3 为 AES-128 解密操作的结构示意图。

具体实施方式

[0026] 下面结合附图对本发明做进一步的详细说明。

[0027] 见图 1 所示，本发明中分组密码算法工作模式 (block cipher operation mode) 控制模块，由以下几部分组成：

[0028] ●输入端口：输入端口接收上一级通信链路到达的数据信号、控制信号、密钥和初始化向量，通过该端口实现设置工作模式、设置分组大小、加载密钥、加载初始化向量和加载数据信号等操作步骤；

[0029] ●输出端口：通过该端口实现读出数据信号操作，使经过加解密处理的数据流入通信链路的下一处理单元；

[0030] ● AES-128 加解密模块：实现数据的加密和解密操作；

[0031] ●生成数据输入变量等控制逻辑：基于 AES-128 加解密模块，实现分组密码算法工作模式的控制。

[0032] 本实施例采用硬件描述语言 Verilog 编写 RTL 代码，使用逻辑综合工具

designCompiler 生成 Verilog 网表，形成分组密码算法工作模式控制模块电路。控制模块电路包括顺序连接的生成数据输入变量模块、生成 AES-128 输入变量模块、AES-128 加 / 解密模块、生成 AES-128 输出变量模块、生成位选取变量模块、生成密 / 明文分组长度变量模块、更新反馈缓存变量模块、生成分组输出变量模块、判断反馈循环计数值模块、生成数据输出变量模块；所述判断反馈循环计数值模块与生成 AES-128 输入变量模块连接。

[0033] 本发明的分组密码算法工作模式控制模块实现方法如下：

[0034] 步骤 1：根据需求设置分组密码算法工作模式控制模块的操作类型。操作类型可分为加密和解密两种。

[0035] 步骤 2：根据需求设置分组密码算法工作模式。本发明中设置了五种常用的分组密码算法工作模式：ECB、CBC、CFB、OFB 和 CTR。

[0036] ECB（电码本工作模式）是分组密码算法的一种工作模式，明文分组直接作为加密算法的输入，对应的输出作为密文分组。

[0037] CBC（密码分组链接工作模式）是分组密码算法的一种工作模式，当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

[0038] CFB（密码反馈工作模式）是分组密码算法用于构造序列密码的一种工作模式，用密文依次更新存储该密码算法启动变量的反馈缓冲器。

[0039] OFB（输出反馈工作模式）是分组密码算法用于构造序列密码的一种工作模式，用该算法当前时刻的输出作为下一时刻的输入。

[0040] CTR（计数器工作模式）是分组密码算法用于构造序列密码的一种工作模式，通过加密不断变化的计数器来产生密钥序列。

[0041] 步骤 3：根据需求设置工作模式为 CFB、OFB 和 CTR 时分组输入的长度（单位：bit）。分组输入的长度可以设置为 8-bit、16-bit、32-bit、64-bit 和 128-bit。

[0042] 同时根据分组输入的长度，设置反馈循环变量。同时根据分组输入的长度，设置反馈循环计数值等于 0。

[0043] 步骤 4：加载 key（密钥），密钥长度为 128-bit。

[0044] 步骤 5：加载 iv（初始化向量），初始化向量长度为 128-bit。

[0045] 当工作模式为 CBC、CFB、OFB 和 CTR 时，同时设定 fb（反馈缓存变量）的初值。

[0046] 步骤 6：加载 text_i（数据输入变量），数据输入变量长度为 128-bit。

[0047] 步骤 7：生成 AES-128 加 / 解密模块的输入 x(AES-128 输入变量)，AES-128 输入变量长度为 128-bit。

[0048] 当模块操作类型是加密且工作模式为 ECB 时，x = text_i；

[0049] 当模块操作类型是加密且工作模式为 CBC 时，x = text_i^fb；

[0050] 当模块操作类型是加密且工作模式为 CFB、OFB 和 CTR 时，x = fb；

[0051] 当模块操作类型是解密且工作模式为 ECB 和 CBC 时，x = text_i；

[0052] 当模块操作类型是解密且工作模式为 CFB、OFB 和 CTR 时，x = fb；

[0053] 步骤 8：将待加 / 解密的 x(AES-128 输入变量）进行加 / 解密操作，生成 y(AES-128 输出变量）。

[0054] 本发明方法中加密或解密的操作基于现有 AES-128 算法，每一轮的密钥加等操作采用现有 AES-128 算法中的方法。

[0055] 图 2 可以视为一个 AES-128 加密操作的循环结构示意图（以 2 次轮变换为例）。

[0056] 首先，加载明文数据，以每 128 位进行分组。

[0057] 然后是密钥扩展操作，生成用于 10 次轮变换操作的轮密钥 k(0) ～ k(9)。

[0058] 接着，待加密的明文数据首先经过一个初始密钥加操作，然后进行 10 次轮变换，最后生成密文数据。

[0059] 轮变换由字节置换、行换位、列混合和密钥加共 4 个操作构成。最后一次轮变换只有字节置换、行换位和密钥加共 3 个操作。

[0060] 轮变换及其每一步操作都作用在中间结果上，将该中间结果成为状态。状态可以表示为一个矩形的字节数组，该数组共有 4 行 4 列。

[0061] 字节置换是作用在字节上的砖匠置换。

[0062] 行换位是一个字节换位，它将 4 字节行按照不同的偏移量进行循环移位。

[0063] 列混合是作用在 4 字节列上的砖匠置换。

[0064] 密钥加是指中奖结果（状态）与一个轮密钥逐位异或。

[0065] 图 3 可以视为一个 AES-128 解密操作的循环结构示意图（以 2 次轮变换为例）。

[0066] 首先，加载密文数据，以每 128 位进行分组。

[0067] 然后是密钥扩展操作，生成用于 10 次轮变换求逆操作的轮密钥 k(0) ～ k(9)。

[0068] 接着，待解密的密文数据首先进行 10 次轮变换，最后再使用一个密钥加操作，生成明文数据。

[0069] 轮变换由密钥加、列混合求逆、行换位求逆和字节置换求逆共 4 个操作构成。第一次轮变换只有密钥加、行换位求逆和字节置换求逆共 3 个操作。

[0070] 步骤 9 :当工作模式为 CFB、OFB 和 CTR 时，生成 j_z（位选取变量）。位选取变量的长度由分组输入的长度决定。可参考 GB-T17964。

[0071] 步骤 10 :当工作模式为 CBC 时，生成 blk_o（密 / 明文分组变量）。密 / 明文分组变量的长度为 128-bit。

[0072] 步骤 11 :当工作模式为 CFB、OFB 和 CTR 时，生成 j_blk_o（密 / 明文分组长度变量）。密 / 明文分组长度变量的长度由分组输入的长度决定。可参考 GB-T17964。

[0073] 步骤 12 :更新反馈缓存变量 fb 的值。同时反馈循环计数值加 1。

[0074] 步骤 13 :当工作模式为 CFB、OFB 和 CTR 时，生成 blk_o_r（分组输出变量）。分组输出变量的长度为 128-bit。

[0075] 步骤 14 :比较反馈循环计数值与反馈循环变量的大小。当反馈循环计数值小于反馈循环次数时，返回值步骤 7 ;当反馈循环计数值等于反馈循环次数时，进入下一步骤。

[0076] 步骤 15 :生成 text_o（数据输出变量）。

[0077] 数据输出变量的长度为 128-bit，并通过输出端口被链路下一单元读取。

[0078] 当工作模式为 ECB 和 CBC 时，text_o ＝ y ;

[0079] 当模块操作类型是加密且工作模式为 ECB 和 CBC 时，text_o ＝ y ;

[0080] 当模块操作类型是加密且工作模式为 CFB、OFB 和 CTR 时，text_o ＝ blk_o_r ;

[0081] 当模块操作类型是解密且工作模式为 ECB 时，text_o ＝ y ;

[0082] 当模块操作类型是解密且工作模式为 CBC 时，text_o ＝ blk_o ;

[0083] 当模块操作类型是解密且工作模式为 CFB、OFB 和 CTR 时，text_o ＝ blk_o_r ;

[0084] 以上给出了本发明的一个具体实现方式，目的在于提供一种应用于 WIA-PA 协议信息安全的分组密码算法工作模式控制模块的实现方法，以克服上述技术不足。该方法以 AES-128 加解密操作为基础，通过控制信号的控制，既能单独实现分组密法算法的多种工作模式，还能够支持协议中 CCM* 模式的加密 / 认证码产生的并行处理功能，以及 CCM* 模式的解密 / 认证码确认的并行处理功能。

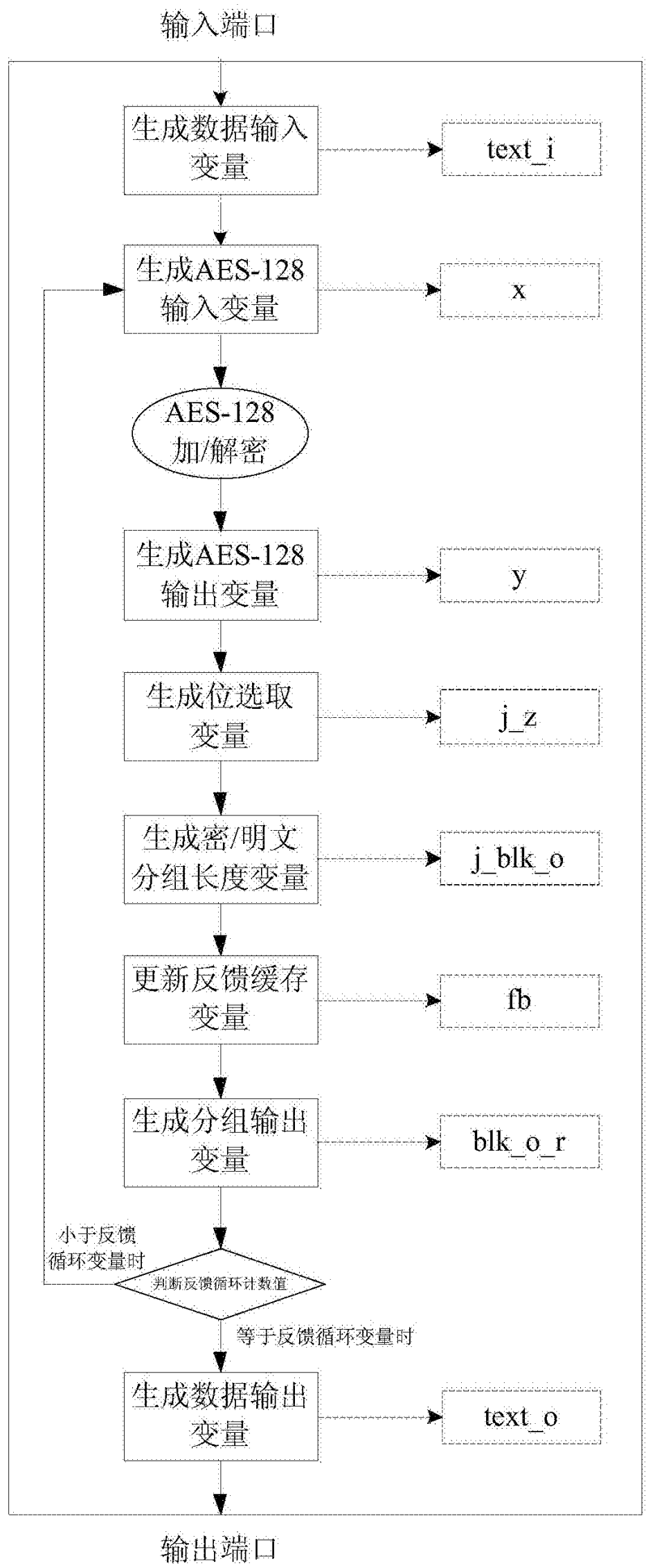

输入端口
生成数据输入变量
text_i
生成AES-128输入变量
x
AES-128加/解密
生成AES-128输出变量
y
生成位选取变量
j_z
生成密/明文分组长度变量
j_blk_o
更新反馈缓存变量
fb
生成分组输出变量
blk_o_r
小于反馈循环变量时
判断反馈循环计数值
等于反馈循环变量时
生成数据输出变量
text_o
输出端口

图 1

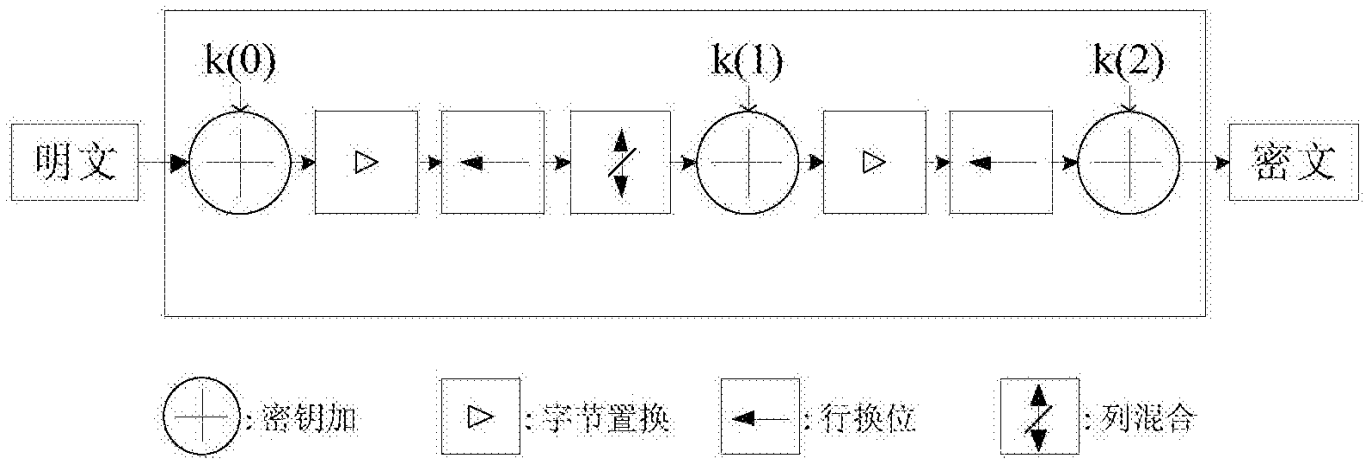

k(0)
k(1)
k(2)
明文
密文
:密钥加
:字节置换
:行换位
:列混合

图 2

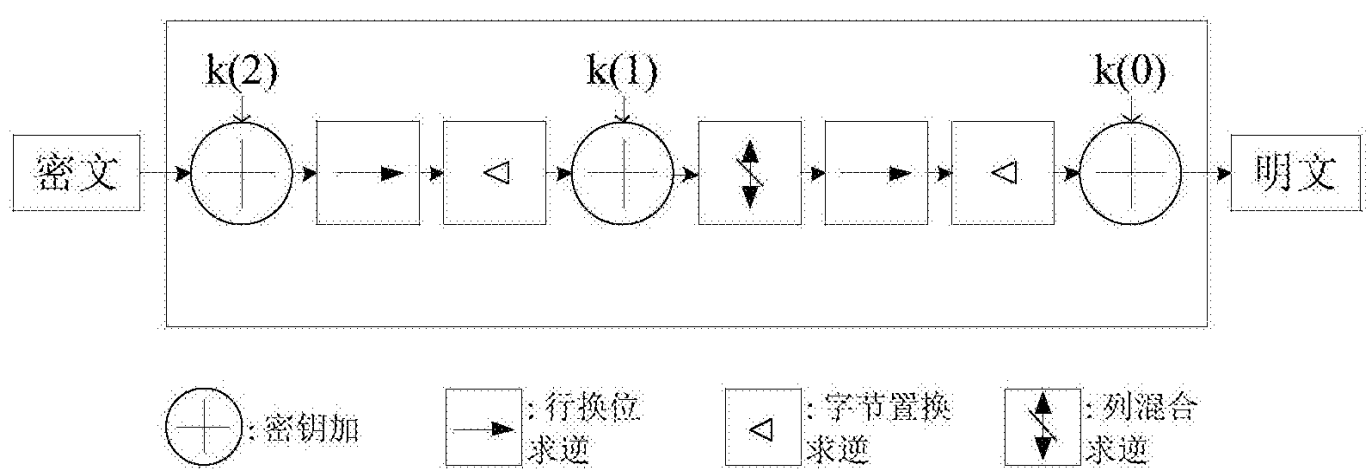

k(2)
k(1)
k(0)
密文
明文
:密钥加
:行换位
求逆
:字节置换
求逆
:列混合
求逆

图 3