(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108123792 B
(45)授权公告日 2021.05.18

(21)申请号 201711372105.X

(22)申请日 2017.12.19

(65)同一申请的已公布的文献号
申请公布号 CN 108123792 A

(43)申请公布日 2018.06.05

(73)专利权人 武汉瑞纳捷电子技术有限公司
地址 430073 湖北省武汉市东湖新技术开发区金融港一路7号光谷智慧园15栋01号楼

(72)发明人 陈毅成 龚明杨 张明宇

(74)专利代理机构 深圳市科进知识产权代理事务所(普通合伙) 44316
代理人 赵勍毅

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/00(2006.01)
H04L 9/14(2006.01)

(56)对比文件
CN 104734845 A,2015.06.24
CN 107154843 A,2017.09.12
CN 107223320 A,2017.09.29
US 2017214398 A1,2017.07.27

审查员 安佳

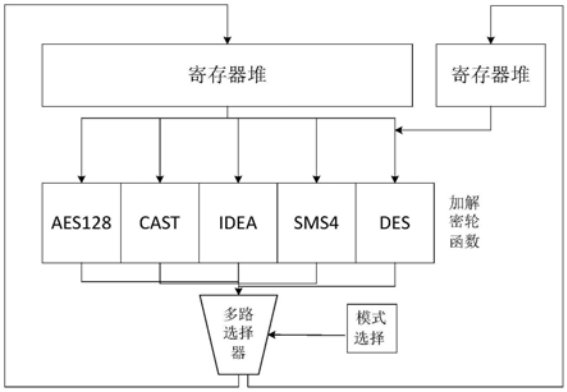
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种SM4算法电路的功耗加扰方法

(57)摘要

本发明公开了一种SM4算法电路的功耗加扰方法,其包括:根据分组加密算法构建功耗加扰电路;在多种算法协处理器的数据迭代寄存器堆中,增设用于存储中间明文数据的明文寄存器;在多种算法协处理器的密钥迭代寄存器堆中,增设用于存储中间密钥数据的密钥寄存器;需要保护的SM4算法电路进行运算的同时启动功耗加扰电路;所述SM4算法电路和功耗加扰电路从数据迭代寄存器堆中获得初始明文,从密钥迭代寄存器堆中获得初始密钥后,同时开始运算;所述SM4算法电路输出运算结果,所述功耗加扰电路的运算结果对应存储于明文寄存器和密钥寄存器。本发明能够在SM4硬件电路中实现抗功耗攻击,同时无需改变原电路架构、易于实现、防护效果好。



CN 108123792 B

1.一种SM4算法电路的功耗加扰方法,其特征在于,包括有如下步骤:

步骤S1,根据分组加密算法构建功耗加扰电路;

步骤S2,在多种算法协处理器的数据迭代寄存器堆中,增设用于存储中间明文数据的明文寄存器,以令被保护的SM4算法和功耗加扰算法并行执行明文运算;

步骤S3,在多种算法协处理器的密钥迭代寄存器堆中,增设用于存储中间密钥数据的密钥寄存器,以令被保护的SM4算法和功耗加扰算法并行执行密钥运算;

步骤S4,需要保护的SM4算法电路进行运算的同时启动功耗加扰电路;

步骤S5,所述SM4算法电路和功耗加扰电路从数据迭代寄存器堆中获得初始明文,从密钥迭代寄存器堆中获得初始密钥后,同时开始运算;

步骤S6,所述SM4算法电路输出运算结果,所述功耗加扰电路的运算结果对应存储于明文寄存器和密钥寄存器;

步骤S7:再次启动功耗加扰电路时,将明文寄存器和密钥寄存器清零;

所述分组加密算法包括AES算法、DES算法、CAST算法和IDEA算法;

所述功耗加扰电路采用AES算法、DES算法、CAST算法和IDEA算法中的一种执行加扰运算;

所述功耗加扰电路以轮询或者随机排序的方式利用AES算法、DES算法、CAST算法和IDEA算法执行加扰运算。

2.如权利要求1所述的SM4算法电路的功耗加扰方法,其特征在于,所述多种算法协处理器包括有数据和控制接口、加解密控制电路、轮控制电路、AES/DES/SM4/CAST/IDEA轮操作电路和AES/DES/SM4/CAST/IDEA密钥扩展电路。

3.如权利要求2所述的SM4算法电路的功耗加扰方法,其特征在于,所述数据和控制接口用于实现:

控制消息输入输出;

明文、密钥以及初始密钥的初始化;

产生中断信号并通知位于上行的CPU提取处理完毕的数据;

选择加密模式。

4.如权利要求3所述的SM4算法电路的功耗加扰方法,其特征在于,所述AES算法、DES算法、SM4算法、CAST算法和IDEA算法的明文和密钥宽度均为128位,当有数据需要加解密时,CPU通过总线将需要加解密的数据写入寄存器堆,再将需要加解密的数据输出到数据迭代寄存器堆。

5.如权利要求2所述的SM4算法电路的功耗加扰方法,其特征在于,所述轮控制电路用于控制轮密钥扩展迭代的次数以及轮操作迭代的次数。

6.如权利要求5所述的SM4算法电路的功耗加扰方法,其特征在于,解密数据时使用密钥的顺序是:所述轮控制电路从最后一轮密钥开始使用,当自减到0时解密过程结束,产生解密完成信号。

一种SM4算法电路的功耗加扰方法

技术领域

[0001] 本发明涉及集成电路硬件实现和信息安全技术领域，尤其涉及一种SM4算法电路的功耗加扰方法。

背景技术

[0002] SMS4是中国国家密码局公布的商用分组密码标准，作为行业标准广泛应用于无线局域网中；其安全性已经经过工程应用的实际检验。在智能卡、物联网领域也有SMS4的应用。SM4算法在POS机、智能卡、计算机网络、存储系统中被广泛应用，以此来实现关键数据的保密。SM4算法设计时考虑了抵御数学上的攻击，但是新出现的旁路攻击(Side Channel Attack)成为必须考虑的因素。

[0003] 当一个器件执行加密操作时，通过测量加解密时的操作时间、功耗或者电磁辐射，就有可能获得与密钥相关的信息，攻击者通过观测这些旁路信息，然后经过相关性分析、统计处理等分析处理，即可成功获取加密密钥等机密信息。其中最具威胁的攻击方法是功耗分析。常用的功耗分析的方法有简单功耗分析(SPA，Simple Power Analysis)、差分功耗分析(DPA，Differential Power Analysis)、相关功耗分析(CPA，correlation power analysis)。由于数理统计的运用，于时间分析攻击相比，功耗分析攻击具有更高的强度，且更难防范。电磁辐射攻击与功耗攻击的基本原理类似，相应的抗功耗攻击的防护也具有一定的抗电磁辐射攻击的能力。因此，从某种意义上来说，功耗攻击成为旁路攻击中对加密电路最具威胁的旁路攻击手段。

[0004] 当前，集成电路大都采用静态单轨标准单元实现，其功耗与输入输出翻转状态密切相关。以最简单的反向器为例，反向器在不同的工作模式下功耗存在明显差别，输出端存在0－1和1－0翻转时，存在充放电过程，消耗较多能量；而输出端不发生翻转时，反向器仅存在漏电流。其它更复杂标准单元工作时，功耗同样与输入和输出翻转存在相关性，因此由大量标准单元组成的电路所消耗的功耗同样与在处理的数据存在统计意义上的相关性。针对加密电路的旁路攻击原理如图1所示，攻击者在拥有设备操纵权限后，进行各种旁路信息的测量，能够得到大量的泄漏信息输出，再利用统计知识进行处理就可以得到密钥。

[0005] 将图1中针对加密电路的旁路攻击原理进一步分析，可描述为对每个明文L和密钥K来说，一个密码运算可以被看作一个包含n个中间结果的序列D:D1(L,K,t1),D2(L,K,t2),…,Dn(L,K,tn)，其中密文等于Dn(L,K,tn)。如果知道加密算法，攻击者能够根据明文和猜测的密钥，预先计算出中间结果D，但是很难确定的指出在这个中间结果对应的某个时间点t时刻的中间结果，因为电路的实现细节几乎不可能知道。另一方面，对应操作的一组旁路测量量，如功耗等L:L1,L2,…,Ln以及采样时间T1,T2,…,Tn能够被容易的获得。进行了一些统计处理之后，可以判断中间结果D和功耗L是否具有相关性，攻击者从而可以判断假定的密钥是否正确。

[0006] 抗功耗攻击的SM4设计有两种基本的方法：一种是采用特殊的电路结构和逻辑形式实现SM4，如使用差分级联开关逻辑(DCVSL，Differential Cascade Voltage Switch

Logic),或者波动动态数字逻辑(WDDL,Wave Dynamic Digital Logic),并且在版图设计中采用差分布线技巧,以及随机开关逻辑(RSL,Random Switching Logic)等,上述方法所需电路面积和额外的功耗都比较大。另一种方法的是采用掩蔽技术,将SM4中加密解密的中间结果随机化,这种方法可以在智能卡上采用软件实现,也可以在电路上实现。在加密算法运算时,每一个中间值都与某个作为掩码的随机数进行变换,使得功耗信息不仅与密钥有关,而且与引入的随机数相关。这种方法实现起来简便易行,不依赖工艺。针对线性运算的部分掩蔽和恢复都比较容易,对非线性运算的S盒,这种掩蔽则非常困难。

发明内容

[0007] 本发明要解决的技术问题在于,针对现有技术的不足,提供一种在SM4硬件电路中实现抗功耗攻击,同时无需改变原电路架构、易于实现、防护效果好的SM4算法电路的功耗加扰方法。

[0008] 为解决上述技术问题,本发明采用如下技术方案。

[0009] 一种SM4算法电路的功耗加扰方法,其包括有如下步骤:步骤S1,根据分组加密算法构建功耗加扰电路;步骤S2,在多种算法协处理器的数据迭代寄存器堆中,增设用于存储中间明文数据的明文寄存器,以令被保护的SM4算法和功耗加扰算法并行执行明文运算;步骤S3,在多种算法协处理器的密钥迭代寄存器堆中,增设用于存储中间密钥数据的密钥寄存器,以令被保护的SM4算法和功耗加扰算法并行执行密钥运算;步骤S4,需要保护的SM4算法电路进行运算的同时启动功耗加扰电路;步骤S5,所述SM4算法电路和功耗加扰电路从数据迭代寄存器堆中获得初始明文,从密钥迭代寄存器堆中获得初始密钥后,同时开始运算;步骤S6,所述SM4算法电路输出运算结果,所述功耗加扰电路的运算结果对应存储于明文寄存器和密钥寄存器。

[0010] 优选地,还包括有步骤S7:再次启动功耗加扰电路时,将明文寄存器和密钥寄存器清零。

[0011] 优选地,所述分组加密算法包括AES算法、DES算法、CAST算法和IDEA算法。

[0012] 优选地,所述功耗加扰电路采用AES算法、DES算法、CAST算法和IDEA算法中的一种执行加扰运算。

[0013] 优选地,所述功耗加扰电路以轮询或者随机排序的方式利用AES算法、DES算法、CAST算法和IDEA算法执行加扰运算。

[0014] 优选地,所述多种算法协处理器包括有数据和控制接口、加解密控制电路、轮控制电路、AES/DES/SM4/CAST/IDEA轮操作电路和AES/DES/SM4/CAST/IDEA密钥扩展电路。

[0015] 优选地,所述数据和控制接口用于实现:控制消息输入输出;明文、密钥以及初始密钥的初始化;产生中断信号并通知位于上行的CPU提取处理完毕的数据;选择加密模式。

[0016] 优选地,所述AES算法、DES算法、SM4算法、CAST算法和IDEA算法的明文和密钥宽度均为128位,当有数据需要加解密时,CPU通过总线将需要加解密的数据写入寄存器堆,再将需要加解密的数据输出到数据迭代寄存器堆。

[0017] 优选地,所述轮控制电路用于控制轮密钥扩展迭代的次数以及轮操作迭代的次数。

[0018] 优选地,解密数据时使用密钥的顺序是:所述轮控制电路从最后一轮密钥开始使

用,当自减到0时解密过程结束,产生解密完成信号。

[0019] 本发明公开的SM4算法电路的功耗加扰方法,在支持多种加密算法的协处理器中,针对需要防护的SM4电路的轮运算单元,利用有相似结构的其他算法电路,构造具有同样运算时间的加密轮电路。需要保护的电路进行运算的时候,同时启动由AES或者DES等分组加密算法构成的功耗加扰电路,并且将需要保护的SM4电路的输入明文和密钥同样输入到扰动电路,功耗加扰电路和SM4电路同时进行加密运算。基于上述方法,使得整个电路密钥运算和功能的相关性被噪声掩蔽,功耗分析攻击的难度将极大增加,进而在SM4硬件电路中实现抗功耗攻击,同时本发明无需改变原电路架构,不仅易于实现,而且防护效果更好。

附图说明

[0020] 图1为现有技术中针对加密电路的旁路攻击原理图。

[0021] 图2为本发明方法中多种算法协处理器的结构框图。

[0022] 图3为未进行加扰的轮运算电路框图。

[0023] 图4为已加扰轮运算电路框图。

具体实施方式

[0024] 下面结合附图和实施例对本发明作更加详细的描述。

[0025] 本发明公开了一种SM4算法电路的功耗加扰方法,结合图2至图4所示,其包括有如下步骤:

[0026] 步骤S1,根据分组加密算法构建功耗加扰电路;

[0027] 步骤S2,在多种算法协处理器的数据迭代寄存器堆中,增设用于存储中间明文数据的明文寄存器,以令被保护的SM4算法和功耗加扰算法并行执行明文运算;

[0028] 步骤S3,在多种算法协处理器的密钥迭代寄存器堆中,增设用于存储中间密钥数据的密钥寄存器,以令被保护的SM4算法和功耗加扰算法并行执行密钥运算;

[0029] 步骤S4,需要保护的SM4算法电路进行运算的同时启动功耗加扰电路;

[0030] 步骤S5,所述SM4算法电路和功耗加扰电路从数据迭代寄存器堆中获得初始明文,从密钥迭代寄存器堆中获得初始密钥后,同时开始运算;

[0031] 步骤S6,所述SM4算法电路输出运算结果,所述功耗加扰电路的运算结果对应存储于明文寄存器和密钥寄存器。

[0032] 进一步地,还包括有步骤S7:再次启动功耗加扰电路时,将明文寄存器和密钥寄存器清零。

[0033] 上述SM4算法电路的功耗加扰方法,在支持多种加密算法的协处理器中,针对需要防护的SM4电路的轮运算单元,利用有相似结构的其他算法电路,构造具有同样运算时间的加密轮电路。需要保护的电路进行运算的时候,同时启动由AES或者DES等分组加密算法构成的功耗加扰电路,并且将需要保护的SM4电路的输入明文和密钥同样输入到扰动电路,功耗加扰电路和SM4电路同时进行加密运算。基于上述方法,使得整个电路密钥运算和功能的相关性被噪声掩蔽,功耗分析攻击的难度将极大增加,进而在SM4硬件电路中实现抗功耗攻击,同时本发明无需改变原电路架构,不仅易于实现,而且防护效果更好。

[0034] 作为一种优选方式,所述分组加密算法包括AES算法、DES算法、CAST算法和IDEA算

法。

[0035] 本实施例中，所述功耗加扰电路采用AES算法、DES算法、CAST算法和IDEA算法中的一种执行加扰运算。例如选择AES-128对所有分组明文进行加扰。

[0036] 在本发明的另一实施例中，所述功耗加扰电路以轮询或者随机排序的方式利用AES算法、DES算法、CAST算法和IDEA算法执行加扰运算。例如第一个128比特明文启动AES128，第二个128比特明文启动DES，第三个128比特明文启动CAST，第四个128比特明文启动IDEA，如此循环。

[0037] 所述步骤S5中，每一个分组加密启动时，作为加扰运算启动时，从数据迭代寄存器堆中获得初始明文，从密钥迭代寄存器堆中获得初始密钥，上述明文寄存器与SM4明文为同一个寄存器，上述密钥寄存器与SM4的密钥寄存器为同一个寄存器，基于这种设计，使得明文和密钥获得了更大的噪声和混乱度，加大了CPA和DPA攻击的对功耗曲线的区分难度。

[0038] 关于多种算法协处理器的组成结构，请参照图2，所述多种算法协处理器包括有数据和控制接口、加解密控制电路、轮控制电路、AES/DES/SM4/CAST/IDEA轮操作电路和AES/DES/SM4/CAST/IDEA密钥扩展电路。其中：

[0039] 所述数据和控制接口用于实现：控制消息输入输出；明文、密钥以及初始密钥的初始化；产生中断信号并通知位于上行的CPU提取处理完毕的数据；以及选择加密模式。

[0040] 作为一种优选方式，所述AES算法、DES算法、SM4算法、CAST算法和IDEA算法的明文和密钥宽度均为128位，当有数据需要加解密时，CPU通过总线将需要加解密的数据写入寄存器堆，再将需要加解密的数据输出到数据迭代寄存器堆。

[0041] 本实施例中，所述轮控制电路用于控制轮密钥扩展迭代的次数以及轮操作迭代的次数。进一步地，解密数据时使用密钥的顺序是：所述轮控制电路从最后一轮密钥开始使用，当自减到0时解密过程结束，产生解密完成信号。

[0042] 结合图3和图4所示，加扰电路增加了一个寄存器堆，存储加扰的中间结果，相比传统电路而言，加扰的轮电路的多路选择器有两个输出，包括正常运算和加扰运算的中间结果。

[0043] 本发明公开的SM4算法电路的功耗加扰方法中，整个电路密钥运算和功能的相关性被噪声掩蔽，功耗分析攻击的难度将极大增加，同时本发明无需改变SM4的电路结构，能够以部分功耗增加的代价大幅度提高SM4电路抵御功耗分析攻击的能力。基于上述特性，使得本发明实现了在SM4硬件电路中的抗功耗攻击处理，特别适用于可能受到旁路攻击的手机SIM卡、智能卡、加密芯片、安全芯片等硬件产品。

[0044] 以上所述只是本发明较佳的实施例，并不用于限制本发明，凡在本发明的技术范围内所做的修改、等同替换或者改进等，均应包含在本发明所保护的范围内。

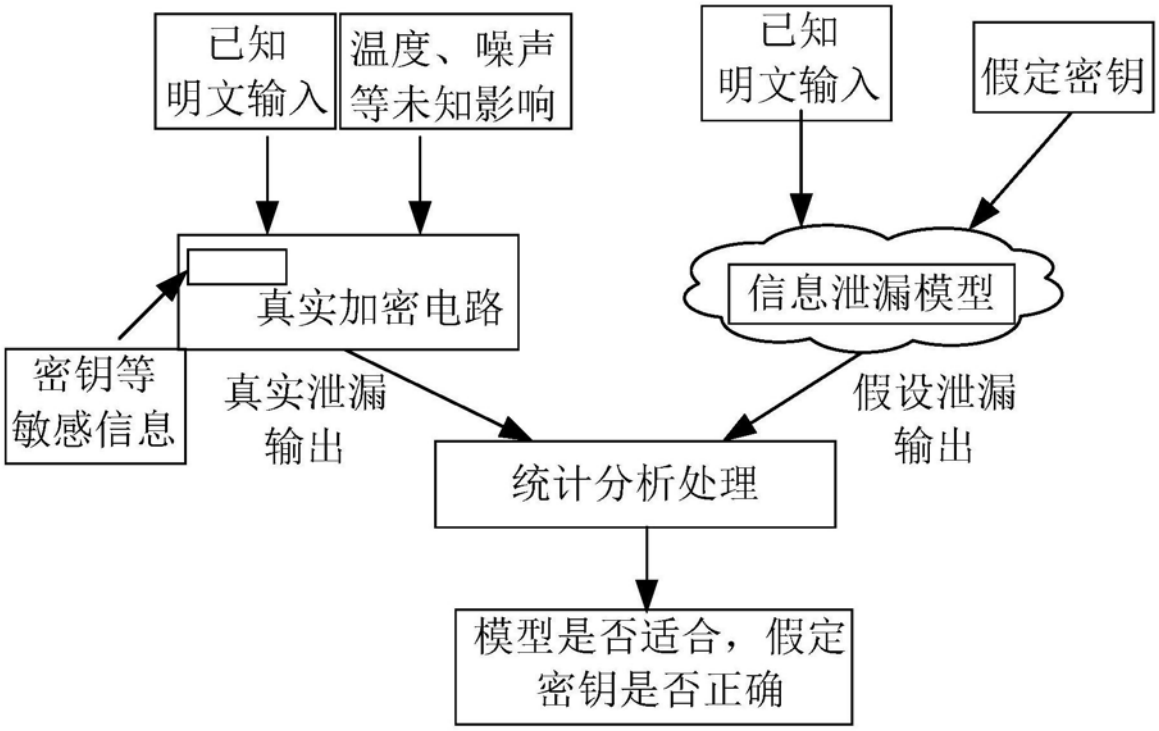

已知
明文输入
温度、噪声
等未知影响
已知
明文输入
假定密钥
真实加密电路
信息泄漏模型
密钥等
敏感信息
真实泄漏
输出
假设泄漏
输出
统计分析处理
模型是否适合，假定
密钥是否正确

图1

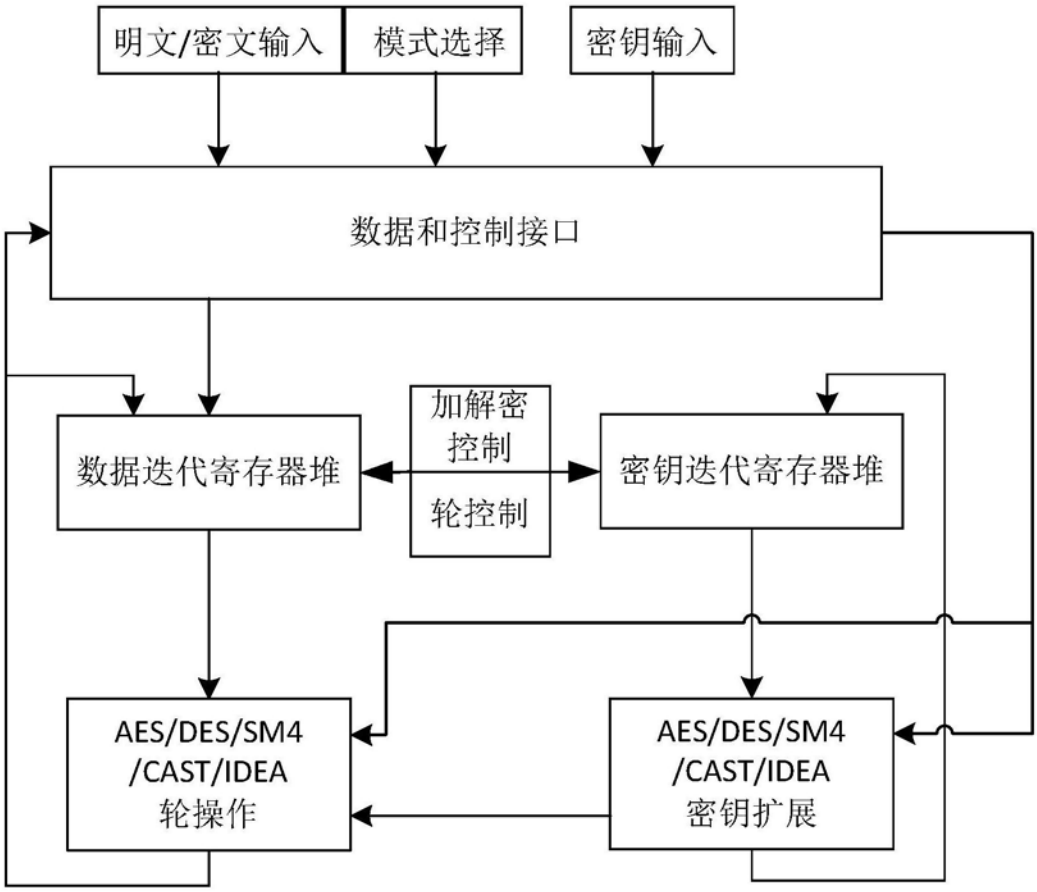

明文/密文输入
模式选择
密钥输入
数据和控制接口
数据迭代寄存器堆
加解密控制
轮控制
密钥迭代寄存器堆
AES/DES/SM4/CAST/IDEA轮操作
AES/DES/SM4/CAST/IDEA密钥扩展

图2

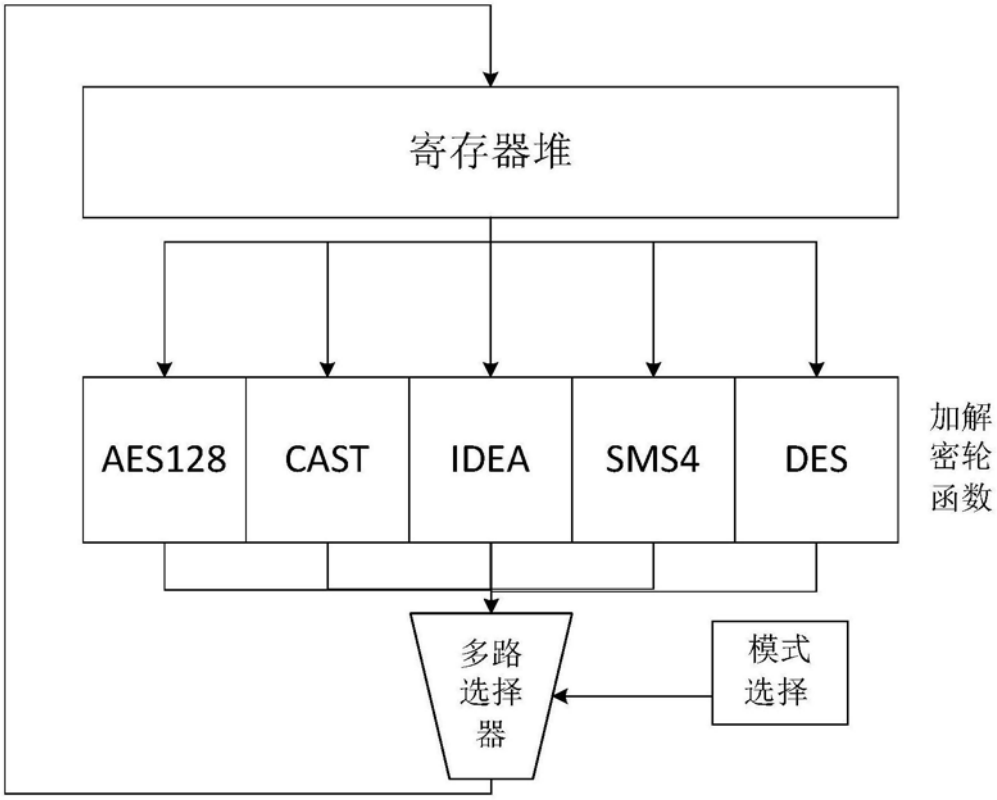

寄存器堆
AES128
CAST
IDEA
SMS4
DES
加解
密轮
函数
多路
选择
器
模式
选择

图3

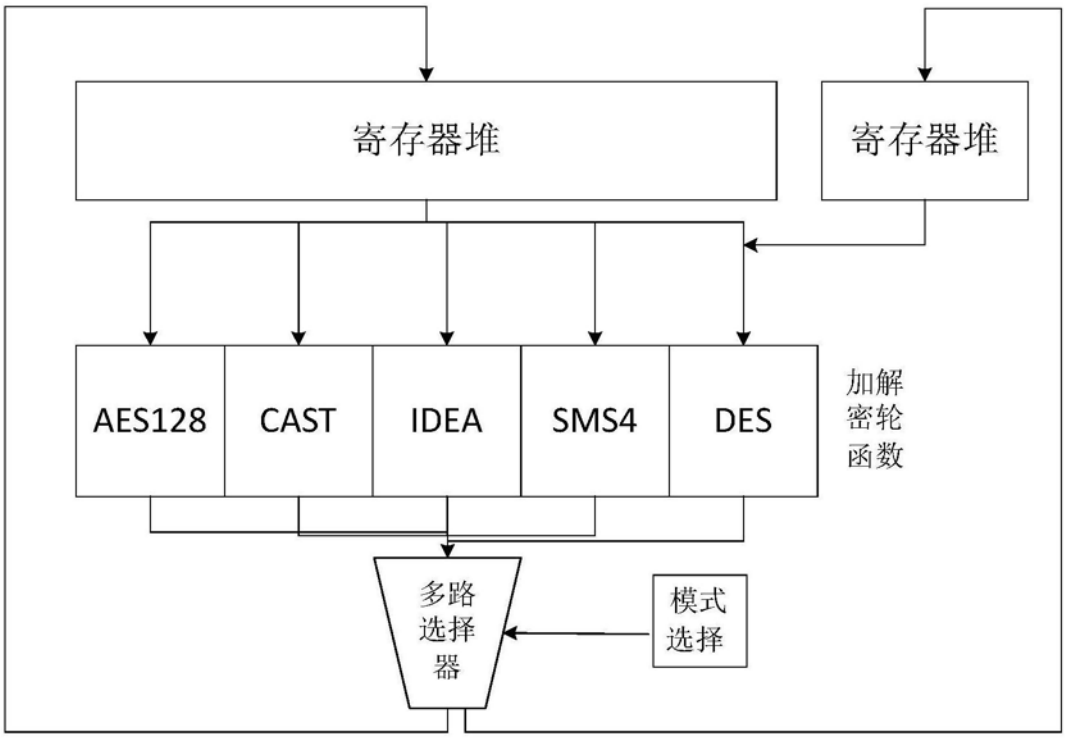

寄存器堆
寄存器堆
AES128
CAST
IDEA
SMS4
DES
加解
密轮
函数
多路
选择
器
模式
选择

图4