



## 基于可调分组的认证加密实现方案

赵福祥

(西安外事学院 工学院, 西安 710077)

**摘 要:** 针对认证加密算法在实际应用中难以生成选择明文攻击的不可区分性问题, 结合硬件算法平台, 应用数据包标志序号、动态可调密钥计数器等提出一种改进的可调认证加密方案。通过增加小规模硬件部件换取可调因子与加密的并行计算, 支持受资源限制嵌入式设备应用, 可实现算法在网络中的平稳运行。实验结果表明, 该方案通过并行计算可缩短系统的运行时间, 提高系统的整体运行效率。

**关键词:** 可调加密模式; 硬件算法; 选择明文攻击; 嵌入式安全; 物联网

开放科学(资源服务)标志码(OSID):



中文引用格式: 赵福祥. 基于可调分组的认证加密实现方案[J]. 计算机工程, 2020, 46(6): 144-148.

英文引用格式: ZHAO Fuxiang. Authenticated encryption implementation scheme based on tweakable grouping[J]. Computer Engineering, 2020, 46(6): 144-148.

## Authenticated Encryption Implementation Scheme Based on Tweakable Grouping

ZHAO Fuxiang

(College of Engineering, Xi'an International University, Xi'an 710077, China)

**[Abstract]** The authentication encryption algorithm is difficult to generate the indistinguishability of Chosen Plaintext Attack (CPA) in practical application. Therefore, an improved encryption scheme of adjustable authentication is proposed by means of hardware algorithm platform, sign sequence number of application data packet and dynamic adjustable key counter. The algorithm can run smoothly on the network by adding small hardware components in exchange for the parallel computation of adjustable factor and encryption, which supports the application of resource-limited embedded devices. Experimental results show that this method can shorten the whole runtime of the system and improve the overall running efficiency.

**[Key words]** tweakable enciphering mode; hardware algorithm; Chosen Plaintext Attack (CPA); embedded security; Internet of Things (IoT)

DOI: 10.19678/j.issn.1000-3428.0054421

### 0 概述

网络技术的迅速发展使得更多信息化应用需借助优质平台得到普及。网络信息的传播具有广泛性和快速性, 而信息收集依靠网络下载才能完成。若要使网络技术得到更高水平的提升, 则需要扩大高速自动数据应用范围替代缓慢的人工数据, 使网络充分实现自动化。自物品条码化以后, 大量的物品信息被嵌入式功能设备自动注入网络, 构建自动识别的信息基础。这类嵌入式功能设备的组装成本确定了其应用的规模, 而规模的形成则需要有技术的潜力。为削减成本, 研究人员应采用低成本嵌入式

功能器件附加简化网络协议来实现, 如中继器网络、物联网等, 这样既保证了设备所属的功能实现, 又具有网络连接功能。由于嵌入式设备包含了功能实现与网络连接双重任务, 因此其作为网络节点的应用多为资源受限设备, 而资源受限造成网络协议的弱化, 它们只能执行用户数据报协议, 多数设备需支持移动而采用无线传输、电池供电等特点。

网络信息的安全不能缺少安全机制的保障, 无论是互联网还是物联网, 凡是涉及个人隐私信息、国家安全的机密信息、公务安全信息和法律保护的安全信息, 都应有相应的机密保护。而安全认证则是涉及个人身份与实体身份合法性的安全保护, 人物、

基金项目: 陕西省教育厅专项科学研究计划(17JK1106); 陕西省自然科学基金研究计划(2014JM8323)。

作者简介: 赵福祥(1964—), 男, 副教授、博士, 主研方向为密码学、网络与信息安全。

收稿日期: 2019-03-28

修回日期: 2019-06-19

E-mail: zhaofuxiang@aliyun.com

网络节点和程序代码都可接受认证保护。网络常用的分组密码为 AES、认证公钥密码为 RSA,用于无线网络协议流密码为 RC4 等。这些常规密码算法都有大规模迭代计算步骤,用于网络安全协议,如 IPSEC、SSL 和 IEEE 802.11 等,然而却无法将已有安全协议或安全算法直接用于嵌入式功能器件构成的物联网,解决冲突的方法是根据嵌入式设备的安全工作需求做全新密码的算法设计,如轻重量密码算法<sup>[1]</sup>和认证加密算法<sup>[2]</sup>。轻重量密码算法的目标是为存储器系统配置安全算法,因而所构造的算法多为哈希或流密码的硬件算法<sup>[3]</sup>,以减少算法对设备的系统占用,实现轻重量配置。而认证加密算法的目标是合并认证与加密两个经典的安全步骤为一个步骤完成,缩短加密协议中的复杂过程。认证加密算法主体虽然为 AES,但不排除轻重量加密算法对认证加密算法的构成。现代加密技术强调算法采用多重叠加的综合模式来提高安全强度,以抵御选择明文攻击(CPA)或选择密文攻击(CCA)。如密码分组链(CBC)模式或可调加密模式<sup>[4]</sup>都是加密时叠加由密文本身产生的伪随机数而引起的不确定性扰动,以差别化相同明文在不同位置的密文值,从而增加攻击的难度。密码分组链的缺点是扰动的来源仅来自加密数据的反馈,相同明文的排列顺序会依然延续到密文中,若在公开的网络环境中输入经过巧妙设计的明文,所得密文强数字特征将可能增加被攻破的可能性。与密码分组链不同,可调加密模式的不确定性扰动来源于密文所在位置,通过采用顺序的分布,所产生不确定性扰动分布使得不同位置的相同密文特征均不相同<sup>[5]</sup>。

数据安全是信息安全应用的重要保证,资源受限的低成本嵌入式设备所使用的轻量级网络协议 DTLS 和压缩 IPSEC 在采用常规密码算法时,达不到实用效果。本文结合轻重量密码、认证加密技术和可调加密技术,使密码技术更适合资源受限制网络安全环境,并通过改进原有安全技术,提出基于可调分组的认证加密实现方案,以硬件支持的可调分组认证加密实现低成本嵌入式设备网络的安全支持。

## 1 模型结构

本文方案的目标是实现嵌入式自身安全与数据实时加密的需求、涉及嵌入式防护与抗密文结构分析等。各项实用关键性技术及组合都应围绕目标设置。

### 1.1 选择明文攻击的抵御

选择明文攻击来自于二战时期美日军事海战的历史<sup>[6-7]</sup>。基于现代密码技术在网络中应用密码算法公开的原则,这类攻击已成为不可避免的事实。抵御选择明文攻击成熟的方法是加密的同时加入确定的随机源数据,使相同的明文在加密后不再呈现密文相同的规律,从而阻断掉选择明文攻击的途径,如分组反馈密码链(CBC)模式,通过迭加反馈密码值产生随机效应,构建加密函数的扰乱数据平台,从

而使相同明文得到不同密文。然而,对于小量数据表现优异的模式,通过计算机运行后性能面临改变,如磁盘和网络加密要面对重复、海量数据,分组反馈密码链的随机作用出现缺陷,并产生可调加密的新模式。可调加密模式的形式化表示为  $E: K \times T \times P \rightarrow C$ ,即使明文空间  $D^P$  数据映射到对应的密文空间  $E_K^T(D^P)$ 。若给定  $K \in K$  和  $T \in T$ ,则  $E(K, T, \cdot) = E_K^T(\cdot)$  是保持长度的确定性置换,其中,  $K$  是密钥空间,  $T$  是可调因子集合。加密算法  $E$  的逆是解密算法  $D: T \times K \times S \rightarrow S$ ,即使密文空间  $D^C$  数据将映射到明文空间  $D_K^T(D^C)$ ,其中,  $X = D_K^T(Y)$  当且仅当  $E_K^T(X) = Y$ 。只要有相同可调参数则分组加密或解密功能将保持。若把加密函数看作二元函数,则可把可调参数作为计算变量,然后再映射到密钥函数,那么明文与密文都会增加相应的增量,即  $E_K(X + \Delta_T X) = Y + \Delta_T Y$ ,因此,在应用层面可调因子集合常按顺序取得连续密文分组区块的位置索引(号),从而对相同明文产生不同密文的差异效果,防止可调随机串的误用。但对于网络数据包来说,除考虑由数据包分组密码块的位置可调外,可通过扩展时间可调因子抵御相同数据重复性结构。

### 1.2 抗误用可调随机串的结构

兼顾效率与成本,网络数据传输采用分组数据的层次结构来管理数据,称为传输的数据包。按网络节点单次处理数据的最大限度,把一个传输的消息分成若干分组。每个分组都以数据包标志序号作为区分,在分组内可通过设置包内计数器标记每个字节。实现加密数据的无缝嵌入是经济而有效的方法,为简化数据包内数据单位与加密分组实际长度比值关系,方案简化各类传输单位为加密分组统一的数据块单位(简称块)。块既做数据操作单位,也可做加密单位,同时还兼做密钥更换单位。抗误用可调随机串的结构是由存储块号构成的函数,以保证密文在相同地址存储时的可调因子取值不同。当从数据包读出原来的数据值时则应按原始值读出。抗误用可调结构的计算公式如下:

$$T = F(\text{ID}_{\text{sec}}, \text{cont}_{\text{sec}})$$

其中,  $\text{ID}_{\text{sec}}$  是数据包标志号,  $\text{cont}_{\text{sec}}$  是数据包内加密块偏移地址计数器的值。

## 2 认证加密方案

基于置换的认证加密<sup>[8-10]</sup>是由海绵包和抗随机串误用的认证加密方案。海绵包生成一个密钥流用以加密用户数据,而用附加数据通过对密钥流的检验使加密数据得以认证。解密则使用反向的置换,整个算法紧凑,可用于在线方式处理数据,但加密算法安全信息熵值来源于用户密钥,仍需可调安全模式延展加密算法,通过所选数据块地址的加一操作取得新的随机串,充当可调密钥值,使不同加密数据块密钥不同。嵌入式加密的系统结构如图1所示。

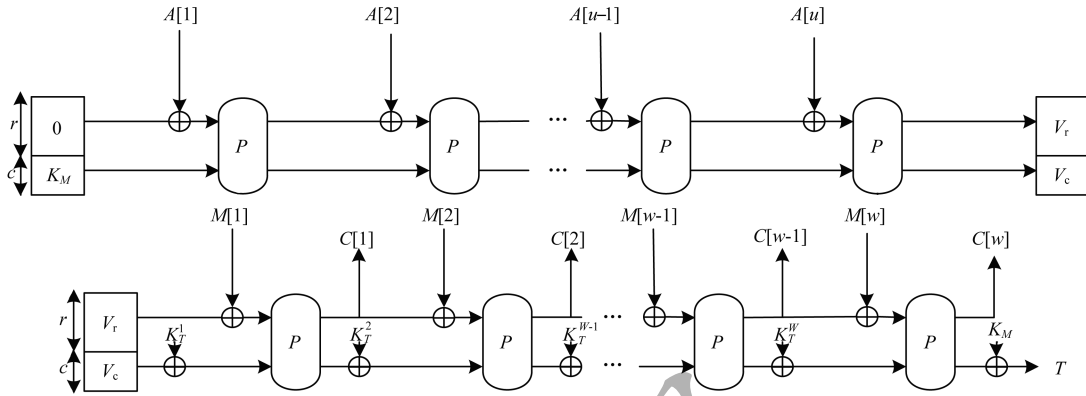


图 1 嵌入式加密的系统结构  
Fig. 1 System structure of embedded encryption

## 2.1 系统参数

设  $R = \{0, 1\}^r$  和  $C = \{0, 1\}^c$ , 假设两个字符串  $A$  和  $B$ , 其中,  $A \parallel B$  与  $AB$  可互换, 因此存在  $AB = A \parallel B \in R \times C \cong \{0, 1\}^{r+c}$ . 假设  $X \in R \times C$ ,  $X_r$  表示其在  $R$  方向的投影, 也称为比率分量,  $X_c$  表示其投影到  $C$ , 即容量分量。标记  $0 \in R$  为  $00 \cdots 00 \in R$  的简写表示, 而  $1 \in C$  为  $00 \cdots 01 \in C$  的简写表示, 符号  $\oplus$  表示两个 (或更多) 字符串的按位异或运算。

$R$  的一个元素称为分组, 设  $R^*$  表示长度为  $r$  倍数的字符串的集合, 最多  $2^{c/2}$  个分组。确定边界  $2^{c/2}$  是为了定义一个随机函数作为在有限的函数集上的采样, 应注意证明  $2^{c/2}$  分组长度的查询边界变得较小<sup>[11]</sup>。同样, 设  $R^+$  表示长度为  $r$  正倍数的字符串集合, 最多  $2^{c/2}$  个分组。给定  $M \in R^+$ , 将它划分为分组, 即  $M[1]M[2] \cdots M[w] \leftarrow M$ , 其中, 每个  $M[i]$  是一个分组,  $w$  是字符串  $M$  的分组长度。

## 2.2 算法描述

加密算法  $E$  接受输入密钥  $K \in K = C$ , 相关的数据  $A \in R^*$ , 消息  $M \in R^+$ , 并返回密文  $C \in R^+$  和标签  $T \in C$ , 即  $(C, T) \rightarrow E_K(A, M)$ 。另一方面,  $D$  接收输入密钥  $K \in C$ , 相关的数据  $A \in R^*$ , 密文  $C \in R^+$  和标签  $T \in C$ , 并返回消息  $M \in R^+$  或拒绝符号  $\perp$ , 即  $M/\perp \leftarrow D_K(A, C, T)$ , 如算法 1、算法 2 所示。这两个函数是合理的, 每当加密消息  $(C, T) \leftarrow E_K(A, M)$ , 返回总是得到消息密文  $C$  与标签  $T$ ; 如果解密的过程没通过验证, 获得拒绝  $\perp$ , 否则可获得  $M \leftarrow D_K(A, C, T)$ 。

### 算法 1 认证加密算法 $E_{K_H}^{K_T}(A, M)$

输入  $K_H, K_T \in C, A \in R^*, M \in R^+$

输出  $C \in R^+, T \in C$

1.  $V \leftarrow (0, K_H) \in R \times C$
2. if  $A \neq \Phi$  then
3.  $A[1]A[2] \cdots A[u] \leftarrow A$
4. for  $i = 1$  to  $u$  do
5.  $V \leftarrow p(A[i] \oplus V_r, V_c)$
6. end
7. end
8.  $M[1]M[2] \cdots M[w] \leftarrow M$
9. for  $i = 1$  to  $w$  do

10.  $V \leftarrow V \oplus K_T^i$
11.  $V \leftarrow p(M[i] \oplus V_r, V_c)$
12.  $C[i] \leftarrow V_r$
13. end
14.  $C \leftarrow C[1]C[2] \cdots C[w]$
15.  $T \leftarrow V_c \oplus K_H$
16. return  $(C, T)$

### 算法 2 验证解密算法 $D_{K_H}^{K_T}(A, C, T)$

输入  $K_H, K_T \in C, A \in R^*, C \in R^+, T \in C$

输出  $M \in R^+$  or  $\perp$

1.  $V \leftarrow (0, K_H) \in R \times C$
2. if  $A \neq \Phi$  then
3.  $A[1]A[2] \cdots A[u] \leftarrow A$
4. for  $i = 1$  to  $u$  do
5.  $V \leftarrow p(A[i] \oplus V_r, V_c)$
6. end
7. end
8.  $C[1]C[2] \cdots C[w] \leftarrow C$
9.  $C[0] \leftarrow V_r, V_0 \leftarrow V_c$
10.  $V \leftarrow (C[w], K_H \oplus T)$
11. for  $i = w$  to  $1$  do
12.  $V \leftarrow p^{-1}(V)$
13.  $M[i] \leftarrow C[i-1] \oplus V_r$
14.  $V_c \leftarrow V_c \oplus K_T^i$
15.  $V \leftarrow C[i-1] \parallel V_c$
16. end
17.  $M \leftarrow M[1]M[2] \cdots M[w]$
18. if  $V_0 = V_c$  then
19. return  $M$
20. else
21. return  $\perp$
22. end

在基于置换的认证加密<sup>[12]</sup>中, 随机串的包是可选的。如果随机串需要, 它可以被包含作为相关数据的一部分。当允许随机串为任意长度时, 作为随机串和相关的数据应清晰可辨<sup>[13]</sup>。

## 3 硬件算法的选择

基于可调的认证加密的实现带来了明显的安全增益, 实现认证与加密业务合并和抵御选择明文/密文攻击设置。轻量密码算法的改进改善了资源的占

用与能源的耗费,但作为经典算法,仍然固守了大数据量迭代算法方式。因此,本质特性决定了系统需做合理的设计选择。因为受限资源设备的环境因素与可调加密认证加密算法的操作需求存在较大差异,所以在系统的任务目标和任务实现上应采取不同的配置,有效地发挥可调加密算法在系统中的安全效能<sup>[14]</sup>。

系统实现的目标确定出系统实现的原则与方法。体现其最关键的任务是确定可调认证加密的基础算法。尽管轻量级算法中 Keccak 和 Quark 都属于基于置换的密码算法,且算法 Keccak 被选为 sha3 标准,但独立设置的硬件算法更有利于受限设备程序的运行与能量控制,相比较而言,Quark 参数更适合资源受限环境的应用,算法的相关参数如表 1 所示。实时系统应该利于短程序的执行,而长处理程序与系统命令共同运行则需要设置更低的级别,使认证加密时间延长,系统处理效能降低。

表 1 嵌入式加密算法的相关参数

Table 1 Related parameter of embedded encryption algorithm

算法	结构参数			性能参数		
	$n$	$c$	$r$	门等效	能耗/J	延迟/ms
u-Quark 算法	136	128	8	1 379	2.44	544
d-Quark 算法	176	160	16	1 702	3.10	704
s-Quark 算法	256	224	32	2 296	4.35	1 024
Keccak [72,128] 算法	200	128	72	2 520	5.60	900
Keccak [40,160] 算法	200	160	40	2 520	5.60	900

#### 4 电路仿真验证

采用密码的硬件算法是封闭大数据处理峰值点有效提高并行度的方法<sup>[15]</sup>。Quark 硬件算法可保留原有置换结构与相关参数作为新系统设置,增加可调密钥设置达到独立、安全与并行的目标,选择出新算法的核心结构基调,根据实际数据宽度需求确定 u-Quark 作为系统算法的基础,表 1 列出了 Quark 多种规格数据参数。从表 1 数据可以看出,数据签名宽度为 17 字符,位宽为 136 位,输入宽度为 1 字符,位宽为 8 位,选择参数均以最小数据为标准,以适用资源受限系统的应用。

作为系统中可调硬件的并行数据处理器,具有独立的算法控制信号系统十分必要。控制信号组织数据的输入与输出,并控制数据处理过程的步骤与迭代<sup>[16]</sup>。完全自主的控制信号使可调分组认证加密算法在系统中独立完成整个加密处理,与系统中的其他部分构成并行处理过程。图 2 给出算法控制信号波形的起始与结束过程,其中起始过程包括状态初始化控制信号和数据输入控制信号,结束过程包括签名输出的控制信号。图 3 给出无数据输入时的签名仿真波形,波形包括空数据输入、迭代处理与签名数据输出。迭代过程有 544 个时钟步骤,累计输出 17 个迭代过程,即位宽为 136 位。若选择时钟周期为 100 ns,则完成签名后用时为 925  $\mu$ s。

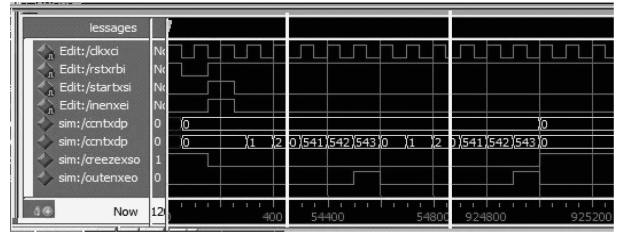


图 2 算法控制信号波形的起始与结束

Fig. 2 Start and end of algorithm control signal waveform

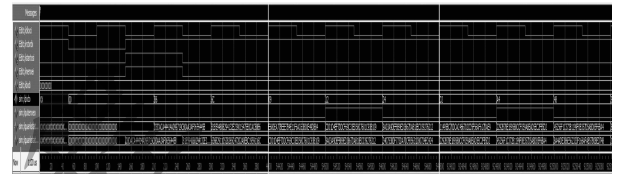


图 3 签名的仿真波形

Fig. 3 Simulation waveform of signature

#### 5 方案评估

对可调分组的认证加密方案所做评估应该完成两个方面的工作,即证明所构建的系统能够完成认证加密的所有工作任务,以及证明所构建系统足够高效,可以在实际应用中接受。因为方案的置换与结构来自于 Quark 算法,各项工作可从相关文献中获得,剩下只需证明方案可以完成认证加密的所有工作任务。认证加密算法属大规模迭代算法,合理组织数据测试就变得较为方便<sup>[17-18]</sup>。在本文方案中,可把算法签名的初始值看作密钥,所得到的摘要值是对空附加数据的签名,签名后得  $C[0] = 8a4ade386e562b33f, T = 166afab57b0bed748$ ,可看作是空加密数据的认证加密值。然后,把可调密钥的值与被加密数据值进行异或,导入算法后析出各分组加密值,从而完成认证加密基本任务的所有步骤。

现有方案中的算法只是一个基本的认证加密算法,除硬件算法的实现适合资源受限的嵌入式应用外,没有实施任何加密模式的保护,不能抵御选择明文方式的攻击。与现有方案相比,本文方案增加了可调加密模式,使之可抵御选择明文的攻击,因而可适用于网络的开放环境中,另外,现有方案算法为应用于资源受限的嵌入式硬件算法,在改进过程中只增加了包内加密计数器这类简单硬件,并没有增加系统资源的占用,因而仍适用于资源受限的嵌入式环境<sup>[19-20]</sup>。结合本文算法这两项优点,可将本文方案算法应用于物联网对互联网跨网络的安全连接。

本文贡献主要有以下 3 点:

1) 提出采用可调模式支持的基于置换的认证加密算法,使应用于受限嵌入环境中认证加密算法可成功抵御选择明文攻击,满足网络开放条件下的安全需求。

2) 给出适合于网络数据包的可调模式的加密的实现方法,使可调模式能够顺利实现,提高了网络安全级别,且代价较小,从而最大限度地满足了受限嵌入环境中的安全需求。

3) 提供了硬件算法的实现, 支持资源受限环境下物联网设备的安全需求, 以硬件配制简化了此类设备的结构设计。

在网络异构环境下, 各种设备运行条件并不相同, 资源受限的嵌入式网络设备选择硬件算法处理可调认证加密的任务, 而常规设备并无资源限制, 则可采用软件或硬件算法处理相应的任务。虽然软硬件算法所使用的方法不同, 但执行的数字标准应相同。若物联网设备与互联网设备通信, 当数据跨过物联网特殊的路由器后, 物联网设备运用硬件算法处理认证加密数据, 而互联网设备则使用软件算法来处理相同认证加密数据。

## 6 结束语

本文提出一个基于可调加密认证的加密方案, 以支持资源受限的物联网设备的安全应用。在已有的认证加密方法基础上实现可调模式操作, 增加算法抵御选择明文攻击的能力, 以数据包标志号与偏移地址计数器的值为可调参数, 使加密密文成为抗误用可调随机串的结构。本文改进方案使原认证加密算法不仅支持资源受限设备的应用, 而且可支持物联网对互联网跨网络开放的安全应用。由于嵌入式安全是一项综合技术, 对认证加密算法可调模式的处理虽然有效, 但仍然存在未知风险, 下一步将对贴合实际的固有安全数字特性进行研究, 以更好地抵御选择明文的攻击。

### 参考文献

- [1] MANIIFAVAS C, HATZIVASILIS G, RANTOS K. Lightweight cryptography for embedded systems—a comparative analysis [C]//Proceedings of International Workshop on Data Privacy Management and Autonomous Spontaneous Security. Berlin, Germany: Springer, 2013: 333-349.
- [2] RALPY A, ROBIN A. Software benchmarking of the 2nd round CAESAR candidates [EB/OL]. [2019-02-21]. <http://eprint.iacr.org/2016/740>.
- [3] HOMSIRIKAMOL E, DIEHL D, FEROPURI A, et al. CAESAR hardware API [EB/OL]. [2019-02-21]. <http://eprint.iacr.org/2016/626>.
- [4] GRANGER R, JOVANOVIĆ P. Improved masking for tweakable blockciphers with applications to authenticated encryption [C]//Proceedings of Advances in Cryptology-EUROCRYPT'16. Berlin, Germany: Springer, 2016: 263-293.
- [5] ZHAO Fuxiang. Tweakable enciphering implementation scheme based on hardware support [J]. Computer Engineering, 2015, 41(10): 144-147, 154. (in Chinese)  
赵福祥. 基于硬件支持的可调加密实现方案[J]. 计算机工程, 2015, 41(10): 144-147, 154.
- [6] KATZ J, LINDELL Y. Modern cryptography: principle and protocols [M]. REN Wei, Translation. Beijing: National Defense Industry Press, 2011: 50-51. (in Chinese)  
KATZ J, LINDELL Y. 现代密码学——原理与协议[M]. 任伟, 译. 北京: 国防工业出版社, 2011: 50-51.
- [7] MAO Wenbo. Modern cryptography: theory and practice [M]. WANG Jilin, WU Qianhong, Translation. Beijing: Electronic Industry Press, 2004: 118-121. (in Chinese)  
毛文波. 现代密码学——理论与实践[M]. 王继林, 伍前红, 译. 北京: 电子工业出版社, 2004: 118-121.
- [8] AUAMSSON J P, HENZEN L, MEIER W, et al. Quark: a lightweight hash [J]. Journal of Cryptology, 2013, 26(2): 313-339.
- [9] BERTONI G, DAEMEN J, PEETERS M, et al. Keccak implementation overview, V3.2 [EB/OL]. [2019-03-21]. <http://keccak.noekeon.org>.
- [10] ANDREEVA E, BILGIN B, BOGDANOV A, et al. APE: authenticated permutation-based encryption for lightweight cryptography [C]//Proceedings of FSE'14. Berlin, Germany: Springer, 2014: 168-186.
- [11] MENNINK B. XPX: generalized tweakable even-mansour with improved security guarantees [C]//Proceedings of Advances in Cryptology-EUROCRYPT'16. Berlin, Germany: Springer, 2016: 64-94.
- [12] BERTONI G, DAEMEN J, PEETERS M, et al. Permutation-based encryption, authentication and authenticated encryption [EB/OL]. [2019-03-21]. <http://www.hyperelliptic.org/djb/diac/record.pdf>.
- [13] PEYRIN T, SEURIN Y. Counter-in-tweak: authenticated encryption modes for tweakable block cipher [C]//Proceedings of Advances in Cryptology-EUROCRYPT'16. Berlin, Germany: Springer, 2016: 33-63.
- [14] ANDREEVA E, BOGDANOV A, LUYKX A, et al. Parallelizable and authenticated online ciphers [C]//Proceedings of Advances in Cryptology-EUROCRYPT'13. Berlin, Germany: Springer, 2013: 424-443.
- [15] AOKI K, YASUDA K. The security of the OCB mode of operation without the SPRP assumption [C]//Proceedings of Advances in Cryptology-EUROCRYPT'13. Berlin, Germany: Springer, 2013: 202-220.
- [16] DATTA N, NANDI M. ELmE: a misuse resistant parallel authenticated encryption [C]//Proceedings of ACISP'14. Berlin, Germany: Springer, 2014: 306-321.
- [17] ZHANG Pei, ZHANG Wenying. Related-key impossible differential attack of QARMA algorithm [J]. Computer Engineering, 2019, 45(1): 91-95. (in Chinese)  
张佩, 张文英. QARMA 算法的相关密钥不可能差分攻击[J]. 计算机工程, 2019, 45(1): 91-95.
- [18] YANG Xiaodong, GAO Guojuan, ZHOU Qixu, et al. E-government data security exchange scheme based on proxy re-signature [J]. Computer Engineering, 2017, 43(2): 183-188. (in Chinese)  
杨小东, 高国娟, 周其旭, 等. 基于代理重签名的电子政务数据安全交换方案[J]. 计算机工程, 2017, 43(2): 183-188.
- [19] RODR L, FLORES G, MORALES-SANDOVAL M, et al. Compact FPGA hardware architecture for public key encryption in embedded devices [J]. PLoS ONE, 2018, 13(1): 190-193.
- [20] NASROLLAHOPOUR M, GHOLAMREZANEZHAD M, KAMARZARRIN M, et al. A compact and efficient implementation of modified MMF2 encryption on FPGA [J]. Canadian Journal of Electrical and Computer Engineering, 2018, 41(1): 3-7.