基于椭圆曲线的签密方案

崔文军[1] 贾志娟[1] 胡明生[1*] 公 备[2] 王利朋[1]

[1](郑州师范学院信息科学与技术学院 河南 郑州 450044)

[2](北京工业大学计算机学院 北京 100124)

摘 要 签密方案既能够满足数字签名又可以满足公钥加密,且成本远低于“先签名后加密”。针对求解椭圆曲线离散对数问题的困难性,提出基于椭圆曲线的签密方案,并证明了其前向安全性和可公开验证性。相比现有的方案,该方案主要用到了模乘运算,且模指数与模逆运算均为 0 次。与文献[8]方案相比较,该方案模乘运算少了一次,签密长度少 $|n|$,计算量明显较少,在理论上达到了复杂度的最小值。

关键词 签密 离散对数问题 前向安全 公开验证 模乘

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.03.051

SIGNCRYPTION SCHEME BASED ON ELLIPTIC CURVES

Cui Wenjun[1] Jia Zhijuan[1] Hu Mingsheng[1*] Gong Bei[2] Wang Lipeng[1]

[1](*College of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, Henan, China*)

[2](*College of Computer Science, Beijing University of Technology, Beijing 100124, China*)

Abstract Signcryption can satisfy both the functions of the digital signature and public key encryption, and its cost is much lower than “signature followed by encryption”. To solve the elliptic curve(ECC) discrete logarithm problem, this paper proposes a signcryption scheme based on ECC, and its forward security and public verifiability are proved. Compared with the existing schemes, the proposed scheme mainly used the model multiplication, and both the numbers of model index and model inverse were reached zero time. Compared with literature [8], our scheme has less modular multiplication once, less signcryption length $|n|$, less computation, and the minimum complexity in theory.

Keywords Signcryption Discrete logarithm problem Forward security Public verification Model multiplication

0 引 言

随着计算机等网络通信设施的高速发展与应用,信息安全已然成为当今社会重要的研究热点之一,其中应用于数据传输、存储和身份认证的安全加解密算法,对构建安全平稳的网络环境有着至关重要的作用。

自公钥密码学出现以来,是否可以以安全和认证的方式传递任意长度的消息,且所耗代价低于传统的“先签名后加密”,这个疑问到 20 世纪 90 年代似乎从未得到过解决。幸运的是,Zheng[1] 找到了一种名为“签密”的新加密方案,它既能够满足数字签名又可以公钥加密,且成本远低于“先签名后加密”。随后,大量科研工作人员对各类相关方案进行了学习和研究。文献[2]改进了 Zheng 的方案,使得接受者不再需要私钥进行签名验证,并且任何人仅仅使用发送者的公钥便可验证方案,也就是说方案具有了公开验证的性质,但其不具备前向安全性。文献[3]借助离散对数问题思考了一个具有前向安全性的签密方案,但不具备公开验证的性质。文献[4]借助双线性对给出了一个基于身份的签密方案,而后证明了该方案在 BDH 问题难以解决的前提下是安全的。文献[5]展现了一个既可

收稿日期:2019 - 02 - 28。国家自然科学基金项目(U1304614,U1204703);河南省科技攻关项目(162102310238);河南省教育科学“十三五”规划一般课题((2018)-JKGHYB-0279);郑州市创新型科技人才队伍建设工程基金项目(131PCXTD597)。**崔文军**,助教,主研领域:密码学,信息安全。**贾志娟**,教授。**胡明生**,教授。**公备**,教授。**王利朋**,助教。

以满足前向安全性又满足公开验证性的签密方案,并基于求解离散对数的困难性问题和 CDH 问题困难性证明了方案具备安全性。文献[6]基于求解离散对数问题的困难性和 Hash 函数的单向性提出了一个新的签密方案,通过将参数 r 隐藏在指数位置(即 $R=g^r$),使得攻击者即便获取了发送者的私密钥也不可能获得此次以及之前的秘密信息,即证明了方案具有前向安全性。当发送方与接收方发生纠纷时,接受方便可交由第三方进行验证,仅需公开签名和明文消息的哈希函数,这样就保护了明文消息,达到了公开验证的目的。文献[7]对 Zheng 的方案进行了研究和改善,改进后的方案主要包括两次加解密运算和五次模指数运算,而后给出了一个基于 ECC 的签密方案。文献[8]详细分析了文献[7]的方案,指出其数字签密方案并没有前向安全性且提出的椭圆曲线数字签密方案复杂度过高,并针对这两个问题做出了改进,使得椭圆曲线数字签密方案摒弃模指数与模逆计算,依靠模乘运算,计算量有了较大幅度减少。基于 DL 和 CDH 问题的困难性,文献[9]利用双线性对设计了一个无证书的签密方案,并进行了有效性、不可伪造性和效率分析。由于签密长度较短,该方案能较好适应计算能力受限的环境。在 BDH 和 CDH 问题困难性的假设下,由于公钥签密不能处理任意长度的消息,文献[10]在随机预言模型下,设计了一个无证书混合签密方案,并证明了相关的安全性。文献[11]对最近提出的六个签密方案分别设计了密码学方面的改进,指出六个方案均不能满足方案的保密性,详细分析了文献[9]方案,对其保密性和不可伪造性给出了相关方面的攻击,并证明了改进的措施安全性。文献[12]提出了一种无双线性映射的高效无证书签密方案,基于 CDH 假设和 DL 困难性问题,验证了该方案具有不可伪造性、机密性、不可否认性和公开验证性等优良的安全性质。文献[13]结合了混合签密和环签密的优势,采取 KEM-DEM 机制生成了对称密钥,并基于离散对数问题和计算性 DH 问题,证明了方案具有不可伪造性和机密性。文献[14]给出了一个无 Hash 函数的签密方案,并证明了该方案具有抗伪造性、前向安全性和公开验证性等性质。文献[15]设计了一种基于椭圆曲线的前向安全的签名方案,该方案不仅可以抗随机数攻击,而且具有前向安全性。该方案比 ECDSA 方案少了 1 次倍点运算、2 次模乘运算和 2 次模逆运算,运算量较小。文献[16]对一种基于椭圆曲线前向安全数字签名方案进行了分析,指出了其安全性漏洞并给出具体攻击方法。

1　预备知识

1.1　有限域上的椭圆曲线[17-18]

一般来说,称形如 $E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 的方程为椭圆曲线的曲线方程,其中 $a_1,a_2,a_3,a_4,a_6\in$ 域 K。其中,基于有限域 Z_p 上的椭圆曲线方程为:

$$y^2=x^3+ax+b \tag{1}$$

基于有限域 $GF(2^m)$ 的椭圆曲线方程为:

$$y^2+xy=x^3+ax+b \tag{2}$$

ECC 的域参数为 (q,a,b,G,n,h)。其中 q 为素数 p 或 $q=2^m$。常用的椭圆曲线是非奇异的,即 $4a^3+27b^2\neq 0$。G 是椭圆曲线上的基点,n 是点 G 的大素数阶,即 n 是满足 $nG=0$ 的最小正整数。h 是一个有椭圆曲线的阶除以 n 产生的余因子,且 $h\leqslant 4$。

1.2　椭圆曲线离散对数问题

对于椭圆曲线 E,P 是其上一点,且阶为大素数 n。取任一数 $k\in Z_n^*$,则易得出 $Q=kP$,但由 P 和 Q 求解 k 却是异常困难的。其中,kP 表示点 P 与自身相加 k 次,即 $kP=P+P+\cdots+P$,共 k 个 P 相加,称 k 为 Q 的椭圆曲线离散对数。

1.3　汉明距离[19]

用 $d(x,y)$ 代表汉明距离,它表示相同长度的字符串 x 和 y 对应位置上不同字符的个数。

1.4　Hash(哈希)函数[17,20]

Hash 函数可以说是一种压缩映射。不论消息串的长度大小,均可被映射成较短定长的消息串。具体性质如下:

(1) 正向计算简单性:对于 Hash 函数 h 和消息 x,计算 $h(x)$ 是极为简单的;

(2) 逆向计算困难性(也称单向性):对给定的任意值 y,求解 $h(x)=y$ 中的 x 是困难的。

2　文献[6]方案

2.1　初始化

参数:p 是一个大素数,q 是 $p-1$ 的一个大素因子,$g\in Z_p^*$ 是 q 阶元素,$x_a\in Z_p^*$ 是发送者 A 的私密钥,$y_a=g^{x_a}\bmod p$ 是 A 的公密钥。类似可得,x_B 和 y_B 分别是接受者 B 的私密钥和公密钥。(E,D) 是安全的加解密方案。

2.2 签 密

A 任取 $k \in Z_q^*$，计算：

$$K = h(y_b^k \bmod p)$$

加密：

$$c = E_K(m)$$

$$r = h(h(m), y_b, g^k \bmod p)$$

$$R = g^r \bmod p$$

$$s = k(r + x_a)^{-1} \bmod q$$

A 将消息 m 签名为 (c, R, s)，并将其发送给 B。

2.3 解 密

B 收到 A 的签名后，进行如下解密计算：

$$K = h((y_a R)^{sx_b} \bmod p)$$

解密：

$$m = D_K(c)$$

签名验证：

$$R = g^{h(h(m), y_b, (y_a R)^s \bmod p)} \bmod p$$

若签名验证通过证明签名有效，则 B 接受明文消息和来自 A 的签名。

2.4 方案分析

文献[6]方案主要依赖于求解离散对数问题的困难性和 Hash 函数的单向性。通过将参数 r 隐藏在指数位置（即 $R = g^r$），使得攻击者即便获取了发送者的私密钥也不可能获得此次以及之前的秘密信息，即证明了方案具有前向安全性。当发送者与接收者发生纠纷时，接受者便可交由第三方进行验证，仅需公开签名和 $h(m)$，这样就保护了明文消息，达到了公开验证的目的。或者在签解密的过程及公开验证阶段，用密文 c 代替 $h(m)$，避免一次哈希运算，提高计算效率和速度。在方案设计过程中，用到了大量模指数运算，和一次模逆运算，导致运算代价高昂，费时费力。如果能在摒弃模指数和模逆这样高代价运算的前提下实现方案的可公开验证性和前向安全性，这样的方案更值得推广和应用。

3 文献[8]方案

3.1 初始化

设 $GF(p)$ 为有限域，E' 是有限域 $GF(p)$ 上的椭圆曲线，取 E' 上一点 G，要求 G 的阶为满足安全要求的素数 n。发送者 A 选取 $x_A \in Z_n^*$ 作为私密钥，同时得到公开钥 $y_A = x_A G$。相似地，接受者 B 选取私密钥 $x_B \in Z_n^*$ 并得到公开钥 $y_B = x_B G$。(E, D) 是安全的加解密方案。

3.2 签 密

（1）A 任取 $r \in Z_n^*$，计算：

$$R = rG = (r_1, r_2)$$

$$K_{AB} = ry_B = (k, l)$$

加密：

$$c = E_k(m)$$

Hash 函数值 $e = h(m, r_1)$，汉明重 $w = ham(e)$。

（2）随机取整数 $\alpha, \beta (0 < \alpha, \beta < n)$，计算：

$$u = (r - \alpha r_1 - \beta m) \bmod n$$

$$s = (w + \alpha r_1 + x_A) \bmod n$$

签密为 (c, R, s, β, u)，将签名发送给 B。

3.3 解 密

收到 A 的签名后，B 进行如下解密计算：

$$K_{AB} = x_B R = (k, l)$$

解密：

$$m = D_k(c)$$

Hash 函数值 $e = h(m, r_1)$，汉明重 $w = ham(e)$。

接着再计算：

$$\gamma = (s - w + \beta m + u) \bmod n$$

验证等式：

$$\gamma G - y_A = R$$

若正确，则接受签密。

3.4 方案分析

由于椭圆曲线的签解密算法具有密钥长度和签名长度短的优势，使得椭圆曲线有着较广的应用。相较于文献[6]方案，文献[8]方案是基于求解椭圆曲线离散对数问题的困难性进行签解密设计的。其在满足公开验证性和前向安全性的基础上，模指数与模逆运算 0 次，且主要用到了模乘运算。方案计算速度和效率有了大范围提高，计算量达到了较小范围。若对该方案进行改进，降低模乘运算的次数是主要的研究方向之一。

4 方案设计

文献[6]方案在签解密过程中用到了模指数和模逆运算，导致运算成本高、复杂度大、代价高昂。文献[8]方案模指数与模逆运算 0 次，主要用到了模乘运算。本文在文献[8]方案的基础上进行改进，降低模乘运算的次数是主要的研究方向。本方案借助于求解椭圆曲线离散对数问题的困难性、Hash 函数单向性和汉明距离等密码学知识进行签密，待收到签名后进行解密，并验证等式 $\beta G - w_A = R$ 的成立性。整个方案保

证了正确性和安全性,同时具备一些优良性质。签解密过程中主要用到了模乘运算,通过效率分析可知,本文方案在签密过程中比文献[8]方案少了一次模乘运算,签密长度少$|n|$。故本文方案在理论上达到了复杂度最小化。

4.1　初始化

设E'为有限域$GF(p)$上的椭圆曲线,取E'上一点G,要求G的阶为满足安全要求的素数n。发送者 A 选取$x_A \in Z_n^*$作为私密钥,同时得到公开钥$w_A = x_A G$。相似地,接受者 B 选取私密钥$x_B \in Z_n^*$并得到公开钥w_B。(E,D)是安全的加解密方案。

4.2　签　密

(1) 发送者 A 任取$r \in Z_n^*$,计算:

$$R = rG$$

$$K = rw_B = (k_1, k_2)$$

加密:

$$c = E_{k_1}(m)$$

Hash 函数值$e_1 = h(c, k_2)$。

此时任选与e_1等长的e_2,计算:

$$d = d(e_1, e_2)$$

(2) 随机取正整数$t(t < n)$,得到:

$$\alpha = r + d + x_A - tc \bmod n$$

签密为(c, R, e_2, t, α),并将其发送给 B。

4.3　解　密

(1) 接受者 B 收到(c, R, e_2, t, α)后,计算:

$$K = x_B R = (k_1, k_2)$$

解密:

$$m = D_{k_1}(c)$$

Hash 函数值$e_1 = h(c, k_2)$,汉明距离$d = d(e_1, e_2)$。

(3) 计算:

$$\beta = (\alpha - d + tc) \bmod n$$

验证等式:

$$\beta G - w_A = R$$

若验证等式正确说明签名有效,则 B 接受明文消息和来自 A 的签名。

5　方案分析

5.1　正确性证明

$$\beta G - w_A = (\alpha - d + tc)G - x_A G =$$

$$(r + d + x_A - tc - d + tc - x_A)G =$$

$$rG = R$$

上述说明此方案的验证过程正确。

5.2　安全性分析

5.2.1　抗私密钥攻击

攻击者获取签名(c, R, e_2, t, α)后,想要恢复明文消息m首先需获知k_1(由于$m = D_{k_1}(c)$)。而获取k_1的途径有两种。第一种途径是获知接受者 B 的私密钥x_B,通过$K = x_B R = (k_1, k_2)$得知。但由$w_B = x_B G$求解私密钥x_B等同于求解椭圆曲线离散对数问题,显然这是不现实的。这样便可实现抗私密钥攻击。第二种途径可详看前向安全性的证明。

5.2.2　不可伪造性

若对签名进行伪造,主要有两类人,一是除 B 之外的攻击者,二是 B 本人。

(1) 攻击者想伪造 A 进行签名$(c', R', e_2', t', \alpha')$使 B 验证等式$\beta G - w_A = R$成立。该过程需要由最初签密中的方程解出后续所要用到的一些参数,而求解这些参数一定会遇到求解椭圆曲线离散对数问题和 Hash 函数求逆问题,这是不现实的。

(2) 由解密过程可知,接受者 B 伪造签名,此时接受者 B 知道的信息有m、c、R、d、t、α。对于签密方程$\alpha = r + d + x_A - tc$,若通过$R = rG$解出$r$等同于求解椭圆曲线离散对数问题,显然是不可能的。一个方程含有两个未知量r和x_A(A 的私密钥),故无法求解签密方程。

综上,任何攻击者均无法对签名进行伪造。

5.2.3　前向安全性

若发送者 A 的私密钥x_A被攻击者获取,本方案保证了除接受者 B 可以得知消息明文m外,其余攻击者均无法恢复m。这主要体现在获取解密密钥k_1上(由于$m = D_{k_1}(c)$)。而获取k_1的途径有两种:

(1) 由$K = rw_B = (k_1, k_2)$可知需要知道r(w_B是接受者 B 的公开钥)。而$R = rG$,想要解出r等同于求解椭圆曲线离散对数问题。

(2) 由$K = x_B R = (k_1, k_2)$可知需要知道接受者 B 的私密钥x_B。

综上,不论是获得r还是x_B,对于攻击者来说都是不可能的。

故本方案具有前向安全性。

5.2.4　不可否认性

即本方案满足公开验证性。当矛盾出现时,即发送者 A 否认签密,接受者 B 可将签名(c, R, e_2, t, α)提供给第三方可信中心进行解签密证实。第三方在安全可信的基础上证实 A 确定发送过该消息,这样便达到了不可否认的目的。验证过程中只是对密文c进行公

开验证,保护了明文消息 m。因此,本文方案具有一定的保密性。

5.3 效率分析

最新能够同时保持前向安全性和可公开验证性两种性质的签密方案即为文献[6]和文献[8]方案。由表1可知,文献[6]方案是基于求解 Z_p 上离散对数问题的困难性进行设计的,虽保障了安全性,但在签密的过程中主要依靠模指数和模逆运算,导致方案运算成本大,不太适用于广泛应用。本文方案与文献[8]方案是基于求解椭圆曲线离散对数问题的困难性进行签密的,主要用到了模乘运算。但本文方案在签密过程中比文献[8]方案少了一次模乘运算,签密长度少了 $|n|$。因而,本文方案运算量有了大幅度减少,加快了计算效率和速度,在理论上达到了复杂度的最小值。

表1 三种方案效率比较

运算	文献[6]方案		文献[8]方案		本文方案	
	签密	解密	签密	解密	签密	解密
模指数	有	有	无	无	无	无
模逆	有	无	无	无	无	无
模乘			2	1	1	1
Hash 函数			1	1	1	1
签密长度			$5\|n\|$		$4\|n\|$	

6 结 语

本文借助于求解椭圆曲线离散对数问题的困难性设计了一个签密方案。已有的多数方案不能同时提供前向安全性和可公开验证性两种性质。文献[6]方案和文献[8]方案具备了这两种性质。本文先对文献[6]方案进行分析,发现文献[6]方案中用到了模指数和模逆运算,这样导致计算成本高、复杂度大、代价高昂,故而进行广泛推广不太适用。由于椭圆曲线的签解密算法具有密钥长度和签名长度短的优势,使得椭圆曲线有着广泛应用。文献[6]方案是基于求解椭圆曲线离散对数问题的难度而设计的。该方案运用模乘运算进行方案的设计,使得方案具备了公开验证性和前向安全性,且模指数与模逆运算0次。对该方案进行改进,降低模乘运算次数是主要的研究方向之一。针对此问题,设计了本文方案。本文方案将签密过程与求解椭圆曲线离散对数的困难性和哈希函数的单向性相结合,能够同时满足前向安全性和可公开验证性,安全性高,且签密过程中仅用到了模乘运算,运算速度快。正确性证明部分说明了本方案的验证过程是正确的。通过验证等式 $\beta G - w_A = R$ 的正确性,说明接受者收到了来自发送者的签名。针对方案的不可伪造性,本文主要分两部分进行分析,一是除接受者之外的攻击者进行伪造签名,二是接受者伪造签名。通过分析得知任何攻击者(包括B)均不能对签密进行伪造。对于前向安全性,本文假设了发送者的私密钥被攻击者获取,但最终除接受者外其他任何人都得不到消息明文。这主要体现在获取解密密钥 k_1 上,本文进行了两种情况的分析,分别是签密和解密阶段对于解密密钥的获取。由于方案的验证过程需要的是密文消息,这样就可以保证了明文消息的机密性,进而体现出方案可公开验证性的性质。最后,本文方案进行了效率分析。分析表明,本文方案模指数与模逆运算0次,在签密过程中比文献[8]方案少一次模乘,且签密长度少了 $|n|$。因而,本文方案运算量有了大幅度减少,加快了计算效率和速度,在理论上达到了复杂度的最小值,有着较广的应用性,为签密技术在网络通信等安全领域提供了一定的理论基础。

同时,签密技术在各个领域已经得到了广泛的应用,如防火墙[21]和电子现金支付[22]等。安全的签密技术可以实现信息的保密传输和生成签名的身份认证,保障交易过程安全进行。在物联网、云计算等相关领域,如在无线传感器网络中,利用签密技术进行密钥分发和节点的可信认证,具有广泛的应用前景。随着计算机技术的发展,利用求解椭圆曲线离散对数的困难性,设计更加优化安全的算法,减少密钥长度,仍有很多的工作要做。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption)[C]//CRYPTO'97 LNCS 1294. Berlin Springer-verlag, 1997: 165 - 179.

[2] Bao F, Deng R H. A signcryption scheme with signature directly verifiable by public key[C]//International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 1998: 55 - 59.

[3] Jung H Y, Lee D H, Lim J I, et al. Signcryption schemes with forward secrecy[J]. Proceedings of WISA2001, Springer-Verlag, 2001: 403 - 475.

[4] 李发根,胡予濮,李刚. 一个高效的基于身份的签密方案[J]. 计算机学报,2006,29(9):1641 - 1647.

[5] 李艳平,谭示崇,王育民. 一个公开可验证和前向安全的签密方案[J]. 计算机应用研究,2006,23(9):98 - 106.

[6] 戚明平,陈建华,何德彪. 具有前向安全性的可公开验证的签密方案[J]. 计算机应用研究,2014,31(10):3093

-3094.
[7] 张建航,胡予璞,齐新社. 具有前向安全性和公开可验证性的签密方案[J]. 计算机应用研究,2011,28(2):733-737.
[8] 周克元. 公开验证和前向安全数字签密方案的分析和改进[J]. 西北师范大学学报(自然科学版),2015,51(6):50-53.
[9] 刘志远. 一个安全的无证书签密方案[J]. 计算机应用研究,2013,30(5):1533-1535.
[10] 俞惠芳,杨波. 可证安全的无证书混合签密[J]. 计算机学报,2016,38(4):804-813.
[11] 周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学,2016,38(11),2246-2253.
[12] 周彦伟,杨波,王青龙. 安全的无双线性映射的无证书签密机制[J]. 软件学报,2017,28(10):2757-2768.
[13] 祁正华,王翔. 高效的无证书混合环签密[J]. 南京邮电大学学报(自然科学版),2018,38(1):98-105.
[14] 周克元. 基于双难题的数字签密方案研究[J]. 计算机应用与软件,2017,34(10):316-319.
[15] 张平,栗亚敏. 前向安全的椭圆曲线数字签名方案[J/OL]. 计算机工程与应用:1-8[2019-02-28]. http://kns.cnki.net/kcms/detail/11.2127.TP.20190119.1157.004.html.
[16] 李靳元,缪祥华. 对前向安全数字签名方案的分析与改进[J]. 吉林大学学报(信息科学版),2017,35(6):608-611.
[17] 杨波. 现代密码学[M]. 2 版. 北京:清华大学出版社,2007.
[18] Al-Somani T F, Ibrahim M K, Gutub A. High performance elliptic curve GF(2m) crypto-processor[J]. Information Technology Journal, 2006, 5(4):742-748.
[19] Wan S S, Chen H W, Cao R J. An analogic selection sorting algorithm for synthesis of reversible logic circuits[J]. Chinese Journal of Computers, 2010, 33(12):2343-2352.
[20] 孙奕,陈性元,杜学绘,等. 一种用于流交换的代理重签名方案[J]. 软件学报,2015,26(1):129-144.
[21] 黎忠文,黎仁峰,钟迪,等. 一个高效的多方混合签密方案[J]. 科学技术与工程,2014,14(17):83-86.
[22] 梁艳,张筱,郑志明. 基于无证书群签名方案的电子现金系统[J]. 通信学报,2016,37(5):184-190.

(上接第 265 页)

[9] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001, 22(8):22-28.
[10] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication[C]//International workshop on open problems in network security, 2015:112-125.
[11] Yu S, Lv K, Shao Z, et al. A high performance blockchain platform for intelligent devices[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018:260-261.
[12] Jin H, Dai X, Xiao J. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]//2018 IEEE 38th International Conference on Distributed Computing Systems(ICDCS). IEEE Computer Society,2018:1203-1211.

(上接第 298 页)

算法不可能差分分析的复杂度,使得其时间复杂度低于穷举搜索的攻击复杂度。

参 考 文 献

[1] Daesung K, Jaesung K, Sangwoo P, et al. New block cipher: ARIA[C]//International Conference on Information Security and Cryptology, 2003:432-445.
[2] Stinson D. 密码学原理与实践[M]. 冯登国,译. 3 版. 北京:电子工业出版社,2009.
[3] 李超,孙兵,李瑞林. 分组密码的攻击方法与实例分析[M]. 北京:科学出版社,2010.
[4] Liu Y, Gu D, Liu Z, et al. New improved impossible differential attack on reduced-round AES-128[C]//Computer Science and Convergence. Berlin:Springer, 2012:453-461.
[5] Dunkelman O. Techniques for cryptanalysis of block ciphers[D]. Haifa, Israel Institute of Technology, Faculty of Computer Science,2006.
[6] Biryukov A, Wagner D. Slide attacks[C]//Proceedings of the 6th International Workshop on Fast Software Encryption. Springer-Verlag, 1999:245-259.
[7] 杜承航. 分组密码算法 ARIA 的不可能差分分析和中间相遇攻击[D]. 济南:山东大学,2011.
[8] Wu W L, Zhang W T, Feng D G. Impossible differential cryptanalysis of reduced-round ARIA and Camellia[J]. Journal of Computer Science and Technology,2007,22(3):449-456.
[9] Li S, Song C. Improved impossible differential cryptanalysis of ARIA[C]//2008 International Conference on Information Security and Assurance(isa 2008). IEEE Computer Society, 2008:129-132.
[10] Du C, Chen J. Impossible differential cryptanalysis of ARIA reduced to 7 rounds[C]//Cryptology and Network Security - 9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14, 2010. Proceedings. DBLP, 2010.
[11] Su C M. New impossible differential attack on 7-round reduced ARIA[J]. Journal od Computer Applications,2012,32(1):45-48.
[12] 谢高淇,卫宏儒. ARIA 分组密码算法的不可能差分攻击[J]. 计算机研究与发展,2018,55(6):1201-1210.