

高效的超椭圆曲线前向安全签密方案

周宣武^{1,2}, 付 燕^{1,3}, 李 欣², 刘开华¹, 金志刚¹

(1 天津大学 电子信息工程学院, 天津 300072; 2 武警指挥学院, 天津 300250;
3 烟台保税港区综合服务中心, 山东 烟台 264001)

摘 要: 基于超椭圆曲线密码提出了一类高效的前向安全签密方案, 分析了计算性超椭圆曲线问题 CHCP 与判定性超椭圆曲线问题 DHCP, 证明了方案的机密性、不可伪造性、不可否认性及前向安全性, 最后对方案的实现效率进行了对比分析. 方案在保证基本安全性的同时, 高效地实现了签密的前向安全性, 适用于资源受限、效率敏感的环境, 有广阔应用前景.

关键词: 超椭圆曲线; 前向安全签密; 计算性超椭圆曲线问题; 安全模型; 可证明安全性

中图分类号: TP308.04

文献标识码: A

文章编号: 1000-7180(2014)12-0079-05

Forward Secure Signcryption Scheme Based on Hyper-elliptic Curve Cryptosystem

ZHOU Xuan-wu^{1, 2}, FU Yan^{1, 3}, LI Xin², LIU Kai-hua¹, JIN Zhi-gang¹

(1 School of Electronics and Information Engineering, Tianjin University, Tianjin 300072, China;
2 Command College of the Armed Police Forces, Tianjin 300250, China;
3 Administrative Center of Yantai Trade-free Port, Yantai 264001, China)

Abstract: In the paper, we presented an efficient signcryption scheme with forward security based on hyper-elliptic curve cryptosystem and analyzed computational hyper-elliptic curve problem CHCP and decisional hyper-elliptic curve problem DHCP. Then we proved the confidentiality, unforgeability, non-repudiation and forward security of the scheme and compared the efficiency of the scheme with other typical signcryption schemes. In addition to the basic security of signcryption, the scheme achieves forward security with much higher efficiency. The attackers cannot get symmetric key to recover the plaintext with the secret key of signcryption, and the signcryption text before the attack also remain secure and valid.

Key words: hyper-elliptic curve; forward secure signcryption; computational hyper-elliptic curve problem; security model; provable security

1 引言

文献[1]提出了签密(Signcryption)的密码原型, 签密能够在一个算法步骤内同时实现加密与签名的功能, 而计算与通信量却远小于两者之和. 自从签密出现以来, 它一直是密码学的研究热点, 前向安全的签密(Forward Secure Signcryption)满足签密的基本安全性质, 且签密私钥泄漏时, 攻击者通过公开信道获得签密文后, 仍然无法得到对称密钥恢复

明文信息. 同时, 攻击者也无法从之前生成的签密文中获得任何秘密信息, 保证了签密文的有效性与安全性. 前向安全的签密方案有效地降低了密钥泄漏给签密系统造成的危害, 提高了签密系统的适用性与可行性.

Zheng 提出的签密方案^[1]满足机密性与不可伪造性, 其效率也远高于传统的“Sign-then-Encrypt”算法结构. 但是该签密方案并不满足前向安全性. 针对 Zheng 方案的缺陷与不足, 文献[2-6]提出了不同

的前向安全签密方案.但是,这些改进的前向安全签密方案大多是基于身份或离散对数问题的签密,签密算法中存在复杂的对运算与指数运算;且方案的基本安全性及前向安全性缺乏严格的形式化定义与证明.

本文基于超椭圆曲线密码 HCC(Hyper-elliptic Curve Cryptosystem)提出了一类高效的前向安全签密方案,证明了方案的机密性、不可伪造性、不可否认性及附加性质,对比分析了方案的实现效率.

2 改进的前向安全签密方案

2.1 基本概念

超椭圆曲线(Hyper-elliptic Curve)是一类特殊的代数曲线,亏格为 1 的超椭圆曲线就是椭圆曲线(Elliptic Curve).因此超椭圆曲线密码体制 HCC 是椭圆曲线密码体制 ECC(Elliptic Curve Cryptosystem)的自然扩展与推广. HCC 的安全性基于有限域上超椭圆曲线的 Jacobian 上的离散对数问题的难解性.与其他典型的公钥密码体制相比, HCC 具有如下优点.

(1)HCC 具有可靠的安全性:首先基于相同阶的超椭圆曲线 Jacobian 群与椭圆曲线有理点群的密码体制,其安全强度是相同的.其次目前对低亏格的超椭圆曲线的攻击是指数时间的,且对于亏格小于 4 的非特殊超椭圆曲线没有发现亚指数时间攻击.

(2)HCC 实现效率高:HCC 操作数长度短,可以在一个很小的基域上构造具有较大素数因子的阶的 Jacobian 群.例如亏格为 3、有限域为 60 比特的 HCC,其安全性与 180 比特的 ECC 等同,远大于 1024 比特的 RSA.同时,在同样的定义域上,亏格越大可选项用于 HCC 的安全超椭圆曲线就越多^[7].

安全的超椭圆曲线及超椭圆曲线密码体制可以定义如下.

定义 1 超椭圆曲线 有限域 F_q 上的超椭圆曲线 $T(F_q)$ 是一个三元组: $T = (q, P, l)$. $J(F_q)$ 是它的 Jacobian, $\# J(F_q) = ht$, t 是 190 比特的大素数($t = 1$ 或是较小的余因子), q 约为 ht/g 比特. $P \in J(F_q)$ 是具有大素数阶的约化除子,它的阶为 l (满足 $l \geq 190$ bit. l, P 为公开参数.对于 $t \in Z_l^*$, $Q, G \in J(F_q)$, $Q = tG$ 表示超椭圆曲线上的乘法运算.

定义 2 超椭圆曲线离散对数 HCDLP (Hyper-elliptic Curve Discrete Logarithm Problem) HCDLP 是如下的计算: $x \leftarrow \text{HCDLP}(Q, P)$ (P 是约化除子,且 $Q \in J(F_q)$, $x \in Z_l^*$, $Q = xP$).

2.2 签密算法

超椭圆曲线前向安全签密方案 $\Sigma = (GC, GK, SC, USC)$.

公共参数生成算法 GC:

$GC(1^k) = \text{"On input } (1^k):$

$(T, H, K, (E, D)) \leftarrow GC(1^k).$ "

$T = (q, P, l, H: \{0, 1\}^* \rightarrow Z_l^*, K: J(F_q) \rightarrow \{0, 1\}^{l^k})$. ψ 表示一个从 $J(F_q)$ 到有限整数集 $Z_{q^{2g}} = \{0, 1, \dots, q^{2g} - 1\}$ 的单射函数,将其记为 $(P)_x$ 或 $(P)_q$. (E, D) 是安全的对称加密算法(密钥长度为 l^k). m 为明文消息, A 为签密发送人, B 签密接收人^[7].

密钥生成算法 GK:

$GK(A, 1^k) = \text{"On input } (A, 1^k):$

$sk_A \leftarrow_R Z_l^*, PK_A = sk_A P,$

$(sk_A, PK_A) \leftarrow \cdot.$ "

$GK(B, 1^k) = \text{"On input } (B, 1^k):$

$sk_B \leftarrow_R Z_l^*, PK_B = sk_B P,$

$(sk_B, PK_B) \leftarrow \cdot.$ "

签密生成算法 SC:

$SC(sk_A, PK_B, m) = \text{"On input } (sk_A, PK_B, m):$

If $sk_A \notin Z_l^*$ or $PK_B \notin J(F_q)$ return $\perp$,

$r \leftarrow_R Z_l^*, R' = rP, R'' = rPK_B,$

$k = K(R''), c \leftarrow E_k(m),$

$h \leftarrow H(m \parallel (R')_x), U = hP.$

$s = r(h - sk_A)^{-1} \bmod l,$

$C = (c, U, s).$ "

解签密算法 USC:

$USC(sk_B, PK_A, C) = \text{"On input } (sk_B, PK_A, C):$

If $sk_B \notin Z_l^*$ or $PK_A \notin E(F_q)$ return $\perp$,

Parse C into $(c, U, s),$

If $c \notin SP_E$ or $U \notin J(F_q)$ or $s \notin Z_l^*$ return $\perp$, else

$s(U - PK_A) = R', k = K(sk_B R'), m \leftarrow D_k(c),$

$U ? = H(m \parallel (R')_x)P,$

If the equation holds return m , else

return $\perp$.

3 方案证明与分析

3.1 方案的正确性

定义 3 超椭圆曲线签密的正确性

超椭圆曲线签密方案 $\Sigma = (GC, GK, SC, USC)$ 是正确的, 如果 $USC(sk_B, PK_A, C) = m$ 对于任何 $GK(ID, 1^k)$ 产生的公私钥对 (sk_A, PK_B) , 任何消息 $m \in SP_m(sk_A, PK_B)$, 任何 $SC(sk_A, PK_B, m)$ 输出的 $C \neq \perp$ 始终成立.

正确性证明: 签密方案是正确的, 当且仅当 $USC(SC(sk_A, PK_B, m)) = m$.

根据解签密算法 USC 等式 $s(U - PK_A)$

由 $s = r(h - sk_A)^{-1} \bmod l, U = hP$

$\Rightarrow s(U + PK_A)$

$= r(h - sk_A)^{-1}(U - PK_A)$

$= r(h - sk_A)^{-1}(hP - sk_AP)$

$= r(h - sk_A)^{-1}(h - sk_A)P$

$= rP = R'$

$\Rightarrow sk_BR' = sk_B rP = rsk_BP = rPK_B = R''$

$K(sk_BR') = K(R'') = k$

$D_k(c) = m$

综合以上, 超椭圆曲线签密方案满足对于任何 $GK(ID, 1^k)$ 产生的公私钥对 (sk_A, PK_B) , 任何消息 $m \in SP_m(sk_A, PK_B)$, 任何 $SC(sk_A, PK_B, m)$ 输出的 $C \neq \perp$, $USC(sk_B, PK_A, C) = m$ 始终成立, 所以方案的正确性得证.

3.2 方案的机密性

定义 4 计算性超椭圆曲线问题 (Computational Hyper-elliptic Curve Problem, CHCP), $T = (q, P, D)$ 是一个超椭圆曲线, AC 是针对 CHCP 的攻击者, CHCP 定义如下:

Experiment $EXP_T^{CHCP}(AC)$

$d, e \leftarrow_R Z_l^*, D = dP, E = eP,$

$F \in J(F_q) \leftarrow AC^T(D, E),$

If $F = deP$ return 1 else return 0.

很明显, 可以证明:

$F = deP = dE = eD$ (1)

分析: 解决 CHCP 的明显方法是计算 D 或 E 的超椭圆曲线离散对数, 然后利用公式获得 HCDLP 密钥, 但是与椭圆曲线相同, 可能存在不计算超椭圆

曲线离散对数的方法. CHCP 目前仍然是计算上不可行的.

定义 5 判定性超椭圆曲线问题 (Decisional Hyper-elliptic Curve Problem, DHCP) 设 $T = (q, P, D)$ 是一个超椭圆曲线, AD 是针对 DHCP 的攻击者, DHCP 定义如下:

Experiment $EXP_T^{DHCP}(AD)$

$b \leftarrow_R \{0, 1\},$

If $b = 0, S_{ce_0}: d, e, f \leftarrow_R Z_l^*,$

If $b = 1, S_{ce_1}: d, e \leftarrow_R Z_l^*, f = de \pmod{l},$

$D = dP, E = eP, F = fP, b' \leftarrow AD^T(D, E, F),$

If $b' = b$ return 1 else return 0.

机密性证明: 攻击者首先可以攻击中间参数 R' 及对称密钥 k 破坏方案的机密性, 已知 $(R' = rP, PK_B = sk_BP)$ 求解 $R' = rsk_BP$ 是典型的计算性超椭圆曲线问题 CHCP, 因此攻击中间参数在计算上是不可行的. 由于方案中的对称加密算法 (E, D) 是安全的, 或者满足对称加密的被动不可区分性 (Passive Indistinguishability), 那么攻击者在不掌握对称密钥时就不能由 c 获得签密明文的信息. 其次, 明文消息 m 通过 $h \leftarrow H(m \| (R')_x)$ 进行了哈希运算, 由 h 攻击 m 等价于攻击哈希函数的单向性, 这在计算上也是不可行的. 在 IND-CCA2 安全模型下, 即使攻击者可以访问 Left-or-right 签密 oracle 和签密 oracle, 但是攻击者仍然无法将明文消息与签密文关联, 更无法获得明文消息, 所以超椭圆曲线前向安全签密方案满足适应性选择密文攻击下的不可区分性. 方案机密性得证.

3.3 方案的不可伪造性

(1) 假设 1 HCDLP 是困难的, 设 $T = (q, P, D)$ 是一个超椭圆曲线, AH 是一个攻击 HCDLP 且输出一个字符串的算法, 考虑如下试验:

Experiment $EXP_T^{HCDLP}(AH)$

$x \leftarrow_R Z_l^*, Q \leftarrow xP,$

$x' \leftarrow AH_T(Q).$

If $x' = x$ return 1 otherwise return 0.

AH 的 HCDLP advantage 定义如下:

$Adv_T^{HCDLP}(AH) = \zeta(1^k, T) =$

$Pr(EXP_T^{HCDLP}(AH) = 1) - Pr[1^k,$

$x \leftarrow_R Z_l^*, Q \leftarrow xP; EXP_T^{HCDLP}(AH) = 1]$ (2)

给定超椭圆曲线 T 及安全参数 $1^k, \zeta(1^k, T)$ 满足, 对于任意 c 存在 k_c , 使得 $\zeta(1^k, T) \leq k^{-c}$ 对于任何 $k \geq k_c$ 都成立.

(2) 不可伪造性证明

伪造攻击意在构造 $C' = (c', U', s')$ 满足解签密算法及验证式, 攻击者可以随机选择 r 计算得到 $(R' = rP, R'' = rPK_B)$, 以及伪造的私钥 k , 对伪造签密消息 m' 进行对称加密得到密文 c' , 同样可以计算得到 $U = H(m' \parallel (R')_x)P$, 伪造签密参数 (c', U') 成功. 但是对于参数 s' 的伪造在计算上却是不可行的. 首先, 攻击者无法通过公式 $s = r(h - sk_A)^{-1} \bmod l$ 得到 s' , 因为他不掌握签密私钥 sk_A . 其次, 也无法通过公式 $s(U - PK_A) = R'$ 得到 s' , 因为在已知 $(U - PK_A, R')$ 时求解 s 是典型的超椭圆曲线离散对数问题, 这在计算上也是不可行的.

从可证明安全性的角度分析, 在 UF-CMA 安全模型下, 伪造攻击者 A 能够访问签密 oracle 和解签密 oracle, 并且可以任意选取明文 $m \in SP_m(sk_A, PK_B)$ 伪造签密文. 通过以上分析可知, 即使任意选取明文 m , 伪造签密仍然等价于攻击超椭圆曲线离散对数问题或者计算性超椭圆曲线问题 CHCP. 因此, 在合理的资源限制下 (时间复杂度, 询问的次数与长度), 伪造攻击者能够输出一个字符串 (m, C') , 满足 $m \leftarrow USC(sk_B, PK_A, C')$ 且 m 不是他向签密 oracle 的询问, 其概率也是完全可以忽略的. 即方案满足适应性选择消息攻击下抗存在性伪造攻击, 签密方案的不可伪造性得证.

3.4 方案的不可否认性

由于超椭圆曲线前向安全签密方案满足不可伪造性, 且方案中签密文 C 是不可复制的, 不存在签密文的副本, 所以签密发送者不能否认合法的签密及签密行为.

3.5 方案的前向安全性

前向安全性是一种更强的机密性, 在签密私钥泄露时, 签密方案仍然要满足机密性要求. 签密方案中, 公开信道传输的签密文 $C = (c, U, s)$ 是公开参数. 在超椭圆曲线前向安全签密方案中, 对于前向安全性攻击者 $(c, U, s, sk_A, PK_A, PK_B)$ 皆为公开参数, 攻击者可以计算出 $s(U - PK_A) = R', s^{-1}P = r^{-1}(hP - sk_AP)$ 即:

$$s^{-1}P = r^{-1}(hP - sk_AP) = r^{-1}(U - PK_A)$$

参数 $(U, PK_A, s^{-1}P)$ 已知, 由 $(U - PK_A), s^{-1}P$ 求解 r^{-1} , 这是典型的 HCDLP 问题, 攻击无法获得随机数 r 计算 $k = K(rPK_B)$ 攻击中间参数及对称密钥. 同时, 已知 $R' = rP, PK_B = sk_BP$, 求解 $R'' = rPK_B$. 这是典型的计算性超椭圆曲线问题 CHCP, 此攻击在计算上是不可行的. 所以攻击者也无法通过 R' 和 PK_B 计算中间参数恢复对称密钥, 也就无法解密恢复明文信息 m .

若攻击者在掌握参数 (s, sk_A) 时, 根据公式 $s = r(h - sk_A)^{-1} \bmod l$ 攻击 r . 针对哈希运算 $h \leftarrow H(m \parallel (R')_x)$, 攻击者可以计算 $s(U - PK_A)$ 得到 R' , 但由于哈希运算中引入了明文消息 m , 攻击者仍然无法计算 $H(m \parallel (R')_x)$ 得到 h . 因此, 通过 $s = r(h - sk_A)^{-1} \bmod l$ 的关系攻击参数 r 也是不可行的.

综合以上, 签密密钥 sk_A 泄露并不会影响到之前生成签密文的安全性与有效性, 方案的前向安全性得证.

需要强调的是, 尽管由于哈希运算中引入了明文消息 m , 本文方案实现了签密的前向安全性. 但是, 在解签密及验证算法中同样需要明文消息, 所以方案无法向第三方公开参数进行验证, 即方案不满足公开验证性.

3.6 方案的效率分析

超椭圆曲线密码体制可以在相对 ECC 更小的域上, 实现更高的安全性. 本文超椭圆曲线签密方案在有限域 $GF(2^{95})$ 的安全性与 $GF(2^{190})$ 上的 ECC 签密方案相当. 若超椭圆曲线的亏格为 3, 方案的优势更突出. 虽然, HCC 签密方案的实现速度仍低于 ECC 签密方案, 但这种差距已经显著减小. 特别是采用一些优化算法或超椭圆曲线选取恰当时两类签密方案的差距完全可以忽略.

但是, 由于在相同的安全强度下 HCC 可以使用长度更短的操作数, 而且可用于密码系统的安全超椭圆曲线的选取余地较大. 所以, 基于超椭圆曲线的签密方案的整体系统开销会小于基于椭圆曲线、离散对数等其他公钥密码系统的签密方案.

4 结束语

本文基于超椭圆曲线公钥密码提出了一类前向安全的签密方案, 并对方案的机密性、不可伪造性、不可否认性及附加性质及实现效率进行了证明分

析. 方案充分利用了超椭圆曲线安全参数小、实现效率高的优势,在保证签密系统安全性的基础上高效地实现了前向安全的附加性质.

参考文献:

- [1] Zheng Y L. Digital signcryption or how to achieve cost (Signature&Encryption) << Cost (Signature) + Cost (Encryption)[C]// Advances in Cryptology- Crypto'97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179.
- [2] 周宣武. 具有附加性质的签密方案及其应用研究[D]. 天津: 天津大学, 2013.
- [3] Elsayed Mohamed, Hassan Elkamchouchi. Elliptic curve signcryption with encrypted message authentication and forward secrecy[J]. International Journal of Computer Science and Network Security, 2009, 9(1): 395-398.
- [4] Lei F Y, Chen W, Chen K F. Efficient identity based signcryption scheme with public verifiability and forward security[J]. Wuhan University Journal of Natural Sciences-English Edition, 2005, 10(1): 248-250.
- [5] Hwang Renjunn, Lai Chihhua, Su Fengfu. An efficient signcryption scheme with forward secrecy based on elliptic curve [J]. Applied Mathematics and Computation, 2006, 167(2): 870-881.
- [6] 张明武, 杨波, 张文政. 密文匿名的高效前向安全短签密方案 [J]. 北京邮电大学学报, 2010, 33(4): 131-134.
- [7] Zhou Xuanwu. Improved signcryption schemes based on hyper-elliptic curves cryptosystem [J]. Applied Mechanics and Materials, 2010, (20-23): 546-552.

作者简介:

周宣武 男, (1980—), 博士后. 研究方向为密码学与信息安全. E-mail: schwoodchow@163.com.

付燕 女, (1985—), 博士研究生. 研究方向为可信计算.

李欣 男, (1965—), 副教授. 研究方向为网络安全.

刘开华 男, (1956—), 教授, 博士生导师. 研究方向为计算机网络, 软件无线电技术.

金志刚 男, (1973—), 教授, 博士生导师. 研究方向为计算机网络与信息安全.

(上接第 78 页)

- [2] 李鹏程. 瞬态电场测量系统的研制与试验[J]. 电网与清洁能源, 2010(8): 41-44.
- [3] National Instrument. NI FlexRIO FPGA module installation guide and specifications[S]. USA, 2011.
- [4] National Instruments Corporation. 高速数据流盘处理: 编程与标定[EB/OL]. [2008-01-24]. <http://zone.ni.com/devzone/cda/tut/p/id/6458>.
- [5] 龙华伟. LabVIEW 8.2.1 与 DAQ 数据采集[M]. 北京: 清华大学出版社. 2008.
- [6] 彭小平. LabVIEW FPGA 模块在测量控制系统中的开发流程及特点[J]. 工业控制计算机, 2007, 20(5): 22-23.
- [7] 张宇. 基于 LabVIEW 的多功能数据采集系统的设计与实现[J]. 自动化仪表, 2013, 34(8): 24-26.

作者简介:

赵海增 女, (1988-), 硕士研究生. 研究方向为计算机控制与数据采集. E-mail: haizeng@ipp.ac.cn.

季振山 男, (1963-), 研究员, 硕士生导师. 研究方向为计算机控制和数据采集系统.