匿名 CLPKC-TPKI 异构签密方案

张玉磊[1],张灵刚[1],张永洁[2],王 欢[1],王彩芬[1]
(1. 西北师范大学计算机科学与工程学院,甘肃兰州 730070; 2. 甘肃卫生职业学院,甘肃兰州 730000)

摘 要: 异构签密可以保证不同公钥密码系统之间数据传输的机密性和不可伪造性. 本文定义了从无证书公钥密码环境到传统公钥密码环境(CLPKC→TPKI)异构签密方案的形式化模型,并利用双线性对提出了一个 CLPKC→TPKI 异构签密方案. 在随机预言模型下,基于计算 Diffie-Hellman 和修改逆计算 Diffie-Hellman 困难假设,证明方案满足内部安全的机密性和不可伪造性. 同时,方案满足密文匿名性,可以有效地保护收发双方的身份隐私. 方案使用不同的密码系统参数,更接近于实际应用环境. 与已有异构签密方案相比,方案的效率较高,适合于收发双方身份保密和带宽受限的应用需求.

关键词: 异构签密; 无证书公钥密码; 密文匿名; 计算 Diffie-Hellman 困难问题; 修改逆计算 Diffie-Hellman 困难问题

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)10-2432-08

电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.10.022

CLPKC-to-TPKI Heterogeneous Signcryption Scheme with Anonymity

ZHANG Yu-lei[1], ZHANG Ling-gang[1], ZHANG Yong-jie[2], WANG Huan[1], Wang Cai-fen[1]
(1. *College of Computer Science and Engineering, Northwest Normal University, Lanzhou, Gansu* 730070, *China*;
2. *Gansu Health Vocational College, Lanzhou, Gansu* 730000, *China*)

Abstract: Heterogeneous signcryption, a cryptographic primitive, can simultaneously provide the confidentiality and unforgeability of data transmission between different public key cryptography. The paper gives the definition and security models of CLPKC-to-TPKI heterogeneous signcryption scheme between CLPKC (Certificateless Public Key Cryptography) and TPKI (Traditional Public Key Infrastructure), and presents a construction by using the bilinear pairing. In the random oracle model, based on the assumptions of Computational Diffie-Hellman and modifying Inverse Computational Diffie-Hellman, the scheme is proved to satisfy the confidentiality and unforgeability of the insider security. Moreover, it satisfies the properties of ciphertext anonymity which can efficiently protect the privacies of sender and receiver. Owing to the independence and difference of the system parameters in CLPKC and TPKI, the scheme is more suitable in the practical environments. Furthermore, the analysis of efficiency shows that, comparing to the existing heterogeneous signcryption schemes, the scheme is more efficient, so it is suitable for the requirements of identity hiding and constrained bandwidth.

Key words: heterogeneous signcryption; certificateless public key cryptography; ciphertext anonymity; computational Diffie-Hellman problem (CDH); modification inverse computational Diffie-Hellman problem(mICDH)

1 引言

签密[1]能够同时保证机密性和认证性,提高“单独实现加密和签名”的计算效率,在车联网等环境中有一定的应用[2,3]. 现有的大多数签密方案都是基于同一种公钥密码,即发送者和接收者的公钥密码环境相同. 随着大数据、云计算等应用的展开,跨平台应用及操作将越来越广泛. 为了保证异构(不同)密码环境中消息传输的机密性和认证性,有必要研究异构签密[4~7]问题.

2010 年,Sun 等[4]首次提出异构签密问题并构造了从传统公钥密码到身份公钥密码(Identity-based Public Key Cryptography, IDPKC)[8]的异构签密方案(TPKI→

收稿日期:2015-06-17;修回日期:2015-12-23;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61163038, No. 61262056, No. 61262057);甘肃省高等学校科研项目(No. 2015B-220, No. 2013A-014);西北师范大学青年教师科研能力提升计划项目(No. NWNU-LKQN-12-32)

IDPKC 型). 2011 年,Huang 等[5] 构造了 IDPKC→TPKI 型异构签密方案. 2013 年,Fu 等[6] 扩展 Sun 等人的研究工作,构造了一个 IDPKC→TPKI 多接收者异构签密方案. 同年,Li 等[7] 提出了新的 IDPKC→TPKI 型和 TPKI →IDPKC 型异构签密方案. 已有异构签密方案中,IDPKC 环境和 TPKI 环境使用了相同的系统参数,即不同的公钥密码环境未使用不同的系统参数.

为了隐藏发送方和接收方的身份信息,签密方案需要满足密文匿名性. 2004 年,Libert 等[9] 基于短签名[10]思想提出了满足密文匿名性的签密方案. 2005 年 Yang 等[11]指出 Libert 方案不满足机密性和密文匿名性,并提出了改进方案,但是该改进方案也不满足密文匿名性. 2010 年,Li 等[12]改进了 Yang 方案,提出了满足密文匿名性的签密方案.

本文定义了从无证书公钥密码(Certificateless Public Key Cryptography, CLPKC)[13] 到传统公钥密码 PKI (CLPKC→TPKI)异构签密方案的形式化定义和安全模型,并基于文献[12]提出了满足密文匿名性的 CLPKC →TPKI 异构签密方案. 方案具有以下几个特点:

(1)在随机预言模型下,基于计算 Diffie-Hellman (Computational Diffie-Hellman, CDH)困难问题和修改逆计算 Diffie-Hellman (modification Inverse Computational Diffie-Hellman, mICDH)困难问题,证明该方案满足签密内部安全模型[14]下的机密性和不可伪造性:即使发送者的私钥泄露,攻击者也不能从密文中恢复明文;接收者的私钥泄露,攻击者也不能伪造密文.

(2)满足密文匿名性. 攻击者无法从密文中获得发送方和接收方的身份信息,可以有效地保护收发双方的身份隐私.

(3)方案只需要 2 个双线性运算,减少了双线性对运算个数.

(4)方案设计了互不相同的密码系统参数,更接近于实际应用环境.

2　CLPKC→TPKI 异构签密方案定义

CLPKC→TPKI 异构签密需要同时考虑 CLPKC 和 TPKI 环境,因此,CLPKC→TPKI 异构签密方案必须考虑两种密码环境的建立、密钥生成、CLPKC 环境的签密和 TPKI 环境的解签密等过程. CLPKC→TPKI 异构签密方案一般包括以下算法.

(1)CLPKC 系统建立算法. 该算法由 CLPKC 系统的 KGC 运行. 输入安全参数 l,输出系统主密钥 s(KGC 的私钥)、系统密钥 P_{pub}(KGC 的公钥)和系统参数 $Params_1$. KGC 公开 P_{pub}和 $Params_1$,保密 s.

(2)TPKI 系统建立及密钥生成算法. PKI 系统中的 CA 生成并发布系统参数 $Params_2$. 用户产生公/私钥对 pk_i/sk_i,CA 对用户的公钥进行签名并输出用户的证书.

(3)CLPKC 部分私钥生成算法. 该算法由 KGC 运行. 输入用户身份 ID_i、系统参数 $Params_1$ 和主密钥 s,输出用户的部分私钥 D_i.

(4)CLPKC 密钥生成算法. 用户选择秘密值 x_i,输入身份 ID_i 和系统参数 $Params_1$,输出用户的完整私钥 $S_i=(D_i,x_i)$和公钥 P_i.

(5)签密算法:输入接收者的公钥 pk_r,消息 m、发送者私钥 S_s、系统参数 $Params_1$ 及 $Params_2$,输出密文 σ.

(6)解签密算法:输入密文 σ、接收者私钥 sk_r、系统参数 $Params_1$ 及 $Params_2$,输出消息 m 或者符号"⊥". 其中,符号"⊥"表示密文不合法.

以上算法必须满足一致性约束条件:如果 $\sigma=\text{Signcrypt}(m,S_s,pk_r)$,则 $m=\text{Unsigncrypt}(\sigma,P_s,sk_r)$成立.

3　CLPKC→TPKI 异构签密方案安全模型

CLPKC→TPKI 异构签密方案必须满足不可伪造性和机密性,即适应性选择消息和身份攻击下的不可伪造性和适应性选择密文攻击下的密文不可区分性.

3.1　不可伪造性 CLPKC→TPKI

异构签密方案的不可伪造性主要考虑无证书密码环境中的两类攻击者 A_{I} 和 A_{II}[13,15]. A_{I} 表现为一般用户,它利用选定的公钥替换用户原有的公钥实现公钥替换攻击;A_{II}表现为密钥生成中心 KGC,它可以计算用户的部分私钥实现 KGC 攻击.

游戏 1　假定 F 为挑战者,CLPKC→TPKI 异构签密方案针对攻击者 A_{I} 的适应性选择消息和身份的攻击游戏由以下三个阶段组成.

初始阶段:F 运行"CLPKC 系统建立算法"产生系统参数 $Params_1$;F 运行"TPKI 系统建立及密钥生成算法"获得系统参数 $Params_2$ 和接收者公/私钥对(pk_r, sk_r),发送 $Params_1$、$Params_2$ 和(pk_r,sk_r)给 A_{I}.

攻击阶段:F 与 A_{I} 模拟过程中,能够对以下预言机进行多项式有界次适应性询问.

(1)部分私钥询问:A_{I} 提交用户身份 ID_i,F 运行"CLPKC 部分私钥生成算法",获得对应的部分私钥 D_i 并返回给 A_{I}.

(2)秘密值询问:A_{I} 提交用户身份 ID_i,F 运行"CLPKC 密钥生成算法"获得 ID_i 对应的秘密值 x_i 并返回给 A_{I}. 如果用户 ID_i 的公钥已经被替换,那么让 F 回答这样的询问是不合理的.

(3)公钥询问:A_{I} 输入身份 ID_i,F 运行"CLPKC 密钥生成算法",获得 ID_i 对应的公钥 P_i 并返回给 A_{I}.

(4)公钥替换询问:A_{I} 输入身份 ID_i 对应选择的公钥 P_i',F 用 P_i'替换 P_i,并将原秘密值 x_i 改为"⊥".

(5)签密询问:A_{I} 提交发送者身份 ID_i、公钥 P_i、接

收者公钥 pk_r 和消息 m_i,F 调用"CLPKC 密钥生成算法"获得 ID_i 的私钥 S_i,运行"签密算法"并返回密文 σ = Signcrypt(m_i,S_i,pk_r)给 A_{I}. 该询问中,本文采用的是弱无证书签密询问[15],即如果攻击者替换了用户的公钥,那么要求攻击者提供公钥对应的秘密值.

伪造阶段:A_{I} 提交消息 m^*、发送者身份 ID_A 及公钥 P_A、接收者公钥 pk_r 及密文 σ^*,如果以下三个条件成立,则 A_{I} 赢得该游戏:①σ^* 对于 P_A 和 pk_r 是一个合法的密文,"解签密算法"执行后不会输出符号"⊥". ②A_{I} 没有提交过对 ID_A 的"部分私钥询问". ③A_{I} 没有执行对(ID_A,m^*,pk_r)的"签密询问".

定义 1 如果没有任何多项式有界攻击者 A_{I} 在 t 时间内,经过以上询问以不可忽略的优势赢得游戏 1,那么称该 CLPKC→TPKI 异构签密方案在适应性选择消息和身份攻击下对于 A_{I} 攻击安全.

游戏 2 假定 F 为挑战者,CLPKC→TPKI 异构签密方案针对攻击者 A_{II}的适应性选择消息和身份的攻击游戏由以下三个阶段组成.

初始阶段:F 运行"CLPKC 系统建立算法"产生系统参数 Params_1 和主秘钥 s;运行"TPKI 系统建立及密钥生成算法"获得系统参数 Params_2 和接收者公/私钥对(pk_r,sk_r),发送 Params_1、Params_2、s 和(pk_r,sk_r)给 A_{II}.

攻击阶段:F 与 A_{II}模拟过程中,能够对以下预言机进行多项式有界次地适应性询问.

(1)秘密值询问和公钥询问与游戏 2 相同. 由于 A_{II} 持有系统主密钥,因此,不考虑部分私钥询问,同时不允许 A_{II}进行公钥替换询问.

(2)签密询问:A_{II}提交发送者身份 ID_i 及公钥 P_i、接收者公钥 pk_r 和消息 m_i,F 调用"CLPKC 密钥生成算法"获得 ID_i 的私钥 S_i,运行"签密算法"并返回密文 σ 给 A_{II}.

伪造阶段:A_{II}提交消息 m^*、发送者身份 ID_A 及公钥 P_A、接收者公钥 pk_r 及对应的密文 σ^*,如果以下三个条件成立,则 A_{II}赢得上述游戏:①σ^* 对于 P_A 和 pk_B 是一个合法的密文,即"解签密算法"执行后不会输出符号"⊥". ②A_{II}没有提交过对 ID_A 的"秘密值询问". ③A_{II}没有执行对(ID_A,m^*,pk_r)的"签密询问".

定义 2 如果没有任何多项式有界攻击者 A_{II} 在 t 时间内,经过以上询问以不可忽略的优势赢得游戏 2,那么称该 CLPKC→TPKI 异构签密方案在适应性选择消息和身份攻击下对于 A_{II}攻击安全.

注意:游戏 1 和游戏 2 允许攻击者可以获得接收者的私钥,这样可以确保方案满足不可伪造性的内部安全性,即使接收者的私钥泄漏,攻击者也不能伪造一个有效的密文.

定义 3 如果存在敌手 A_{I} 和 A_{II}以不可忽略的概率在游戏 1 和游戏 2 中获胜,则该方案在适应性选择消息和身份攻击下具有存在不可伪造性.

3.2 机密性 CLPKC→TPKI

异构签密方案的机密性主要考虑普通攻击者,包括 CLPKC 和 TPKI 环境中的任意攻击者.

游戏 3 CLPKC→TPKI 异构签密方案的适应性选择密文攻击游戏由以下五个阶段组成,该游戏在攻击者 A 和挑战者 F 之间进行.

初始阶段:F 运行"CLPKC 系统建立算法",产生系统参数 Params_1 和主密钥 s;F 运行"TPKI 建立及密钥生成算法"产生系统参数 Params_2 和接收者的公/私钥对 pk_r/sk_r. F 发送参数 Params_1、Params_2、主密钥 s 和接收者的公钥 pk_r 给 A.

阶段 1:F 与 A 模拟过程中,A 能够对签密预言机和解签密预言机进行多项式有界次适应性询问.

签密询问:A 提交消息 m、发送者私钥 S_i 及接收者公钥 pk_r,调用"签密算法"生成并返回密文 σ = (C,V)给 A.

解签密询问:A 提交发送者公钥 P_i 和密文 σ 给 F,F 输入接收者私钥 sk_r,运行"解签密算法"并将结果返回给 A.

挑战阶段:A 决定何时结束"阶段 1"并进入"挑战阶段". A 选择两个长度相同的消息 m_0 和 m_1、发送者身份 ID_i、接收者公钥 pk_r 作为挑战信息并发送给 F. F 首先调用"CLPKC 密钥生成算法"获得发送者的私钥 S_s,然后随机选择 $b \in \{0,1\}$,对 m_b 执行"签密算法"获得密文 σ^* = Signcrypt(m_b,S_s,pk_r),最后发送 σ^* 给 A 作为挑战密文.

阶段 2:A 可以像"阶段 1"对以上预言机进行多项式有界次适应性询问,F 同样按照"阶段 1"那样给出反馈. 但是,A 不能提交关于 σ^* 的解签密询问.

猜测阶段:A 选择了一个比特 $b' \in \{0,1\}$,如果 $b'=b$,则 A 赢得游戏. 定义 A 赢得游戏的优势为:$\mathrm{Adv}(A) = \left|\Pr[b'=b]-\frac{1}{2}\right|$,$\Pr[b'=b]$表示 $b'=b$ 的概率.

注意:游戏 3 允许攻击者能够获得 CLPKC 环境中用户的完整私钥,这样,可以确保方案满足机密性的内部安全性,即使发送者私钥泄漏,攻击者也不能从密文中恢复出原始消息.

定义 4 如果没有任何多项式有界攻击者在 t 时间内,经过以上询问以不可忽略的优势赢得游戏 3,那么称这个 CLPKC→TPKI 异构签密方案在适应性选择密文攻击下具有密文不可区分性.

3.3 密文匿名性

游戏 4 CLPKC→TPKI 异构签密方案的密文匿名

性游戏由以下五个阶段组成,攻击者 A 和挑战者 F 之间进行以下游戏.

初始阶段: F 运行"TPKI 系统建立及密钥生成算法"生成两个公/私钥对$(pk_{r,0},sk_{r,0})$和$(pk_{r,1},sk_{r,1})$作为密文接收者,并将公钥 $pk_{r,0}$ 和 $pk_{r,1}$ 发送给 A. F 运行"CLPKC 部分私钥生成算法"和"CLPKC 密钥生成算法"生成两个公/私钥对$(P_{s,0},S_{s,0})$和$(P_{s,1},S_{s,1})$作为密文发送者,并将私钥 $S_{s,0}$和 $S_{s,1}$发送给 A. 注意:A 可以是任意攻击者.

阶段 1: F 与 A 模拟过程中,A 能够执行多项式有界次的签密和解签密询问. 签密询问时,A 提交一个接收者的公钥 pk_w 和消息 m 给 F. 如果 $pk_w \neq pk_{r,c}$,则 F 运行"签密算法"返回密文 $\sigma=\text{Signcrypt}(m,S_{s,c'},pk_w)$,其中 $c\in\{0,1\}$,$c'\in\{0,1\}$;如果 $pk_w=pk_{r,c}$,返回错误符号"$\perp$". 解签密询问时,攻击者 A 提交一个密文 σ 给挑战者 F 获得 $\text{Unsigncrypt}(\sigma,P_{s,c'},sk_{r,c})$的结果.

挑战阶段: A 决定何时结束"阶段 1"并进入"挑战阶段". A 选择消息 m 及发送者的私钥 $S_{s,0}$和 $S_{s,1}$. F 选择 $c,c'\in\{0,1\}$并计算 $\sigma^*=\text{Signcrypt}(m,S_{s,c'},pk_{r,c})$,发送 σ^*给 A 作为挑战密文.

阶段 2: A 可以像"阶段 1"一样进行多项式有界次适应性询问. 但是,不能提交对 σ^*的解签密询问.

猜测阶段: A 随机选择 $d,d'\in\{0,1\}$,如果$(d,d')=(c,c')$,则 A 赢得以上游戏. 定义攻击者 A 赢得游戏 4 的优势为:$\text{Adv}(A)=\left|\Pr[(d,d')=(c,c')]-\frac{1}{4}\right|$.

定义 5　如果没有任何多项式有界攻击者以不可忽略的优势赢得游戏 4,则该 CLPKC→TPKI 异构签密方案在适应性选择密文攻击下具有密文匿名性.

限于篇幅,本文略去方案中用到的数学基础知识内容,例如 CDH 困难问题和 mICDH 困难问题等.

4　具体 CLPKC→TPKI 异构签密方案

CLPKC→TPKI 异构签密方案的算法如下.

(1)TPKI 系统建立及密钥生成算法. 设 k_2 为 TPKI 系统安全参数,q_2 为 k_2 比特的大素数,定义阶均为 q_2 的群 G_{T1}和乘法群 G_{T2},生成元 $P_2\in G_{T1}$,l_2 表示 G_{T1}元素长度,定义双线性映射 $e':G_{T1}\times G_{T1}\to G_{T2}$. 发布系统参数 $\text{Params}_2=\{G_{T1},G_{T2},q_2,P_2,e'\}$. 用户产生公/私钥对 pk_i/sk_i,其中,$pk_i=x_iP_2$. CA 生成并发布用户公钥证书.

(2)CLPKC 系统建立算法. 设 k_1 为 CLPKC 系统安全参数,q_1 为 k_1 比特的大素数,定义阶均为 q_1 的加法群 G_1 和乘法群 G_2,生成元 $P_1\in G_1$,l_1 表示 G_1 元素长度,双线性映射 $e:G_1\times G_1\to G_2$. KGC 定义哈希函数

$$H_1:\{0,1\}^{l_{id}}\to G_1,\ H_2:G_1\to Z_{q_1}^*,$$

$$H_3:\{0,1\}^*\to Z_{q_1}^*,\ H_4:\{0,1\}^*\to\{0,1\}^{l_m+l_{id}+3l_1},$$

其中,l_{id}为身份长度,l_m 为消息长度,l_1 为 G_1 元素长度. KGC 选取 $s\in Z_{q_1}^*$为主密钥,计算 $P_{\text{pub}}=sP_1$,发布系统参数 $\text{Params}_1=\{G_1,G_2,e,q_1,P_1,P_{\text{pub}},H_1,H_2,H_3,H_4\}$并保存 s.

(3)CLPKC 部分私钥生成算法. 用户提交身份 ID_i,KGC 计算 $Q_i=H_1(ID_i)$和 $D_i=sQ_i$,发送 D_i 给用户.

(4)CLPKC 用户密钥生成算法. 用户选择秘密值 $x_i\in Z_{q_1}^*$,计算公钥 $P_i=x_iP_1$. 然后计算 $y_i=H_2(P_i)$,生成用户的私钥 $S_i=\frac{1}{x_i+y_i}D_i$.

(5)签密算法. 发送者获得接收者的公钥证书(包含公钥 $pk_B=x_BP_z$)后,执行以下过程.

①随机选择 $r_1\in Z_{q_1}^*$,$r_2\in Z_{q_2}^*$,计算 $Q_A=H_1(ID_A)$,$U=r_1Q_A$ 和 $V=r_2P_2$.

②计算 $T=r_2pk_B$,$h=H_3(m,U,P_A,V,pk_B,T)$和 $W=(r_1+h)S_A$.

③计算 $C=(m\parallel ID_A\parallel P_A\parallel W\parallel U)\oplus H_4(V,pk_B,T)$,得到消息 m 的密文 $\sigma=(C,V)$.

(6)解签密算法:接收者收到密文 $\sigma=(C,V)$后,执行以下过程.

①计算 $T'=x_BV$,恢复包含消息 m 的比特串 $(m\parallel ID_A\parallel P_A\parallel W\parallel U)=C\oplus H_4(V,pk_B,T')$.

②计算 $y_A=H_2(P_A)$,$h=H_3(m,U,P_A,V,pk_B,T')$和 $Q_A=H_1(ID_A)$.

③检查等式 $e(W,P_A+y_AP_1)\overset{?}{=}e(U+hQ_A,P_{\text{pub}})$是否成立. 若成立,则返回消息 m,否则返回错误符号"$\perp$".

5　安全性分析及效率对比

5.1　不可伪造性

定理 1　随机预言模型下,假设 CDH 问题和 mICDH 问题困难,则 CLPKC→TPKI 异构签密方案在适应性选择消息和身份攻击下存在性不可伪造,即适应性选择消息和身份攻击对于 A_{I} 和 A_{II}安全.

引理 1　随机预言模型下,如果存在一个攻击者 A_{I} 能够以 ε 优势攻破 CLPKC→TPKI 异构签密方案的 A_{I} 类安全性,那么存在一个算法 F 能够以

$$\left(1-\frac{1}{q_{H_1}}\right)^{q_{pr}}\left(1-\frac{q_s}{2^{\text{poly}(k_1)}}\right)^{q_{H_1}}\frac{1}{q_{H_1}}\left(1-\frac{1}{q_{H_3}}\right)\varepsilon$$

的优势解决 CDH 困难问题,其中 q_{pr}、q_s、q_{H_1}和 q_{H_3}分别表示部分私钥询问、签密询问、H_1 询问和 H_3 询问的最大次数.

证明　A_{I} 是攻击者,F 是 CDH 问题挑战者. F 给定一个 CDH 问题实例(P_1,aP_1,bP_1),F 的目标是使用 A_{I} 解决 CDH 问题,即计算 abP_1.

初始阶段: F 运行"CLPKC 系统建立"算法,产生系

统参数 Params_1，设 $P_{\text{pub}}=aP_1$. F 运行“TPKI 系统建立及密钥生成算法”获得系统参数 Params_2 和接收者公钥/私钥对 (pk_r,sk_r). F 发送 Params_1、Params_2、挑战身份 ID^* 和接收者公钥/私钥对 (pk_r,sk_r) 给 A_1.

攻击阶段：F 与 A_1 模拟过程中，F 维护列表 $L_1\sim L_4$、$L=(ID_i,x_i,P_i,c)$ 和 $L'=(ID_i,D_i)$ 保存 $H_1\sim H_4$ 预言机询问、公钥询问、秘密值询问和部分私钥询问过程中产生的数据，所有列表初始为空. A_1 能够对以下预言机进行多项式有界次地适应性询问.

H_1 询问：F 保持列表 $L_1=(ID_i,Q_i,t_i)$，A_1 询问 H_1 预言机：①若 $ID_i=ID^*$，则 F 返回 $Q_i=bP_1$，并将 $(ID_i,Q_i,\perp)$ 增加到表 L_1 中. “$\perp$”表示不能确定 bP_1 的系数. ②若 $ID_i\neq ID^*$，则 F 选择 $t_i\in Z_{q_1}^*$，计算 t_iP_1，返回 t_iP_1 并将 (ID_i,Q_i,t_i) 增加到表 L_1 中.

H_2 询问：F 保持列表 $L_2=(P_i,y_i)$，A_1 询问 H_2 预言机，若 L_2 中存在询问项则直接返回，否则，F 选择 $y_i\in Z_{q_1}^*$，返回 y_i 并将 (P_i,y_i) 增加到表 L_2 中.

H_3 询问：F 保持列表 $L_3=(m,U_i,P_i,V_i,pk_r,T_i,h_i)$，$A_1$ 询问 H_3 预言机，F 首先检查 L_3 中是否存在元组 $(m,U_i,P_i,V_i,pk_r,T_i,h_i)$. 若存在相应项，则直接返回结果 h_i；否则随机选择 $h_i\in Z_{q_1}^*$，返回 h_i 给攻击者 A_1，并且将 $(m,U_i,P_i,V_i,pk_r,T_i,h_i)$ 增加到表 L_3.

H_4 询问：F 保持列表 $L_4=(V_i,pk_r,T_i,\omega_i)$，$A_1$ 询问 H_4 预言机，首先检查 L_4 中是否存在元组 (V_i,pk_r,x_rV_i). 若存在相应项，则直接返回结果 ω_i；否则随机选择 $\omega_i\in\{0,1\}^{l_m+l_{id}+3l_1}$，返回 ω_i 给 A_1，并且将 $(V_i,pk_r,x_rV_i,\omega_i)$ 增加到表 L_4.

公钥询问：F 保持列表 $L=(ID_i,x_i,P_i,c)$，A_1 输入身份 ID_i，若列表 L 中存在 (ID_i,x_i,P_i,c)，则直接返回 P_i；否则，F 随机选择 $x_i\in Z_{q_1}^*$，计算 $P_i=x_iP_1$，返回 P_i 给 A_1 并将 $(ID_i,x_i,P_i,1)$ 增加到表 L.

秘密值询问：F 保持列表 $L=(ID_i,x_i,P_i,c)$，A_1 输入身份 ID_i，若列表 L 中存在元组 (ID_i,x_i,P_i,c) 并且 $c=1$，则直接返回 x_i；若列表 L 中存在元组但 $c=0$，则用户的公钥已被替换，终止该询问并返回. 若列表 L 中不存在元组，F 执行“公钥询问”获得并返回 x_i.

公钥替换询问：A_1 提交身份 ID_i 和 P_i'，F 查找列表 L，若存在对应 ID_i，则令 $P_i=P_i'$，$c=0$；否则先对 ID_i 进行公钥询问，然后令 $P_i=P_i'$，并令 $x_i=\perp$ 和 $c=0$，修改表 L 中相应元组.

部分私钥询问：F 保持列表 $L'=(ID_i,D_i)$，A_1 输入身份 ID_i，然后执行以下过程：①若 $ID_i=ID^*$，则 F 失败并终止. ②若 $ID_i\neq ID^*$，并且若列表 L' 中存在对应部分私钥信息，则直接返回；否则，F 检查表 L_1 获得 t_i 值，计算 $D_i=t_iaP_1$，返回 D_i 给 A_1 并将 (ID_i,D_i) 增加到表 L'.

签密询问：A_1 提交发送者身份 ID_s、接收者公钥 pk_r 和消息 m，执行以下过程：

(I)若 $ID_s\neq ID^*$，则 F 能够计算 ID_s 的完整私钥 $S_s=\dfrac{1}{x_s+y_s}t_iaP_1$，然后正常执行签密算法并返回相应的密文 $\sigma=\text{Signcrypt}(m,S_s,pk_r)$.

(II)若 $ID_s=ID^*$，F 调用“TPKI 系统建立及密钥生成”算法获得接收者的公/私钥对 $(pk_r=x_rP_2,x_r)$. F 从 L_1 和 L_2 中获得 (ID_i,Q_i,t_i) 和 (ID_i,x_i,P_i,c)，然后执行以下过程：

①若 $c=1$，F 随机选择 θ_1、$h\in Z_{q_1}^*$，$\theta_2\in Z_{q_2}^*$，查表 L_2 获得 (P_i,y_i). 若 (P_i,y_i) 不存在，则 F 选择 $y_i\in Z_{q_1}^*$，并将 (P_i,y_i) 增加到表 L_2. F 计算 $W=\theta_1aP_1$，$V=\theta_2P_2$，$U=\theta_1(P_i+y_iP)-hQ_i$. 对于 H_4 预言机，询问 (V,pk_r,x_rV)，选择 $\omega_i\in\{0,1\}^{l_m+l_{id}+3l_1}$，增加 (V,pk_r,x_rV,ω) 到 L_4. 令 $H_3(m,U,P_i,V,pk_r,x_rV)=h$，增加 (m,U,P_i,V,pk_r,x_rV,h) 到 L_3. 如果 $H_3(m,U,P_i,V,pk_r,x_rV,h)$ 的值已经存在，那么 F 将终止，这样的概率最多为 $q_s/2^{\text{poly}(k_1)}$. 计算 $C=(m\parallel ID_i\parallel P_i\parallel W\parallel U)\oplus\omega$ 返回 $\sigma=(C,V)$ 给 A_1.

②若 $c=0$，根据无证书弱签密攻击[15]的定义，F 从攻击者获得替换公钥对应的秘密值 x_i'，然后使用 x_i' 模拟 $c=1$ 类似的过程.

伪造阶段：A_1 输出消息 m、发送者身份 ID_s 及公钥 P_s、接收者公钥/私钥 $(pk_r,sk_r=x_r)$ 和密文 $\sigma^*=(C^*,V^*)$：

①若 $ID_s\neq ID^*$ 则 F 失败终止，F 不能解决 CDH 困难问题. ②若 $ID_s=ID^*$，根据分叉引理[16]，F 选择不同的哈希函数 H_3 获得 h'，并再次利用 A_1 获得另一个有效的密文 $\sigma'=(C',V')$，其中 $h'\neq h$，则有以下等式成立：

$$(m\parallel ID_s\parallel P_s\parallel W\parallel U)=C^*\oplus H_3(V^*,pk_r,x_rV^*)$$

和

$$e(W,P_s+y_sP_1)=e(U+hQ_s,P_{\text{pub}})$$

及

$$(m\parallel ID_s\parallel P_s\parallel W'\parallel U)=C'\oplus H_3(V',pk_r,x_rV')$$

和

$$e(W',P_s+y_sP_1)=e(U+h'Q_s,P_{\text{pub}})$$

并且，

$$h=H_3(m,U,P_s,V^*,pk_r,x_rV^*),$$
$$h'=H_3(m,U,P_s,V',pk_r,x_rV').$$

则有以下等式成立：

$$e(W-W',P_s+y_sP_1)=e(hQ_s-h'Q_s,P_{\text{pub}}),$$
$$e((x_s+y_s)(W-W'),P_1)=e((h-h')abP_1,P_1).$$

获得 CDH 问题的一个解：

$$abP_1=\frac{(x_s+y_s)}{(h-h')}(W-W')$$

以下分析 F 成功解决 CDH 问题的优势. F 失败终

止的情况有两种:第一种是 A_{I} 已经对 ID_s^* 进行过"部分私钥询问",再继续询问部分私钥时 F 失败终止. 第二种是签密询问时,如果 $H_3(m,U,P_i,V,pk_r,x_rV,h)$ 的值在 L_3 中已经存在,那么 F 将终止. 因此,当部分私钥询问和签密询问都未终止的情况下 F 模拟也不终止.

定义 E_1 为"部分私钥询问过程未终止"事件,E_2 为"签密询问过程未终止"事件,E_3 为"成功伪造一个合法密文"事件,E_4 为"E_3 发生的条件下,存在 $ID_s=ID^*$,分叉引理使用成功,得到 CDH 困难问题的一个解"事件. 如果以上事件都发生,则 F 成功解决 CDH 问题,其优势可定义为:

$$\Pr[E_1\wedge E_2\wedge E_3\wedge E_4]=\Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_2\wedge E_1]$$

对于部分私钥询问,若 $ID_i=ID^*$ 则终止,容易计算部分私钥询问未终止的概率为 $(1-1/q_{H_1})$,则 $\Pr[E_1]\geqslant(1-1/q_{H_1})^{q_{pr}}$.

对于签密询问,若 $H_3(m,U,P_i,V,pk_r,x_rV,h)$ 的值已经存在,那么 F 将终止,则 H_3 值不存在的概率为 $(1-q_s/2^{\mathrm{poly}(k_1)})$,则 $\Pr[E_2|E_1]\geqslant(1-q_s/2^{\mathrm{poly}(k_1)})^{q_{H_3}}$.

又因为 $\Pr[E_3|E_2\wedge E_1]=\varepsilon$,则

$$\Pr[E_1\wedge E_2\wedge E_3\wedge E_4]\geqslant\left(1-\frac{1}{q_{H_1}}\right)^{q_{pr}}\left(1-\frac{q_s}{2^{\mathrm{poly}(k_2)}}\right)^{q_{H_3}}\frac{1}{q_{H_1}}\left(1-\frac{1}{q_{H_3}}\right)\varepsilon$$

其中 q_{pr}、q_s、q_{H_1} 和 q_{H_3} 分别表示部分私钥询问、签密询问、H_1 哈希询问和 H_3 哈希询问的最大次数.

引理 2　随机预言模型下,如果存在一个攻击者 A_{II} 能够以 ε 的优势攻破 CLPKC→TPKI 异构签密方案的 A_{II} 类安全性,那么存在一个算法 F 能够以

$$\left(1-\frac{1}{q_{sv}}\right)^{q_{sv}}\left(1-\frac{q_s}{2^{\mathrm{poly}(k_1)}}\right)^{q_{H_3}}\frac{1}{q_{sv}}\left(1-\frac{1}{q_{H_3}}\right)\varepsilon$$

的优势解决 mICDH 困难问题,其中 q_{sv}、q_s 和 q_{H_3} 分别表示秘密值询问、签密询问和 H_3 询问的最大次数.

证明　A_{II} 是攻击者,F 是 mICDH 问题挑战者. F 给定一个 mICDH 问题实例 (P_1,aP_1,b),F 的目标是使用 A_{II} 解决 mICDH 问题,即计算 $(a+b)^{-1}P_1$.

初始阶段:F 运行"CLPKC 系统建立"算法,产生系统参数 Params_1,选择 $s\in Z_{q_1}^*$ 为系统主密钥,计算系统密钥 $P_{\mathrm{pub}}=sP_1$. F 运行"TPKI 系统建立及密钥生成算法"获得系统参数 Params_2 和接收者公钥/私钥对 (pk_r,sk_r). F 发送 Params_1、Params_2、s、挑战身份 ID^* 和接收者公钥/私钥对 (pk_r,sk_r) 给 A_{II}.

攻击阶段:F 与 A_{II} 模拟过程中,F 维护列表 $L_1\sim L_4$、$L=(ID_i,x_i,P_i)$ 和 $L'=(ID_i,D_i)$,保存 $H_1\sim H_4$ 询问、公钥询问、秘密值询问过程中产生的数据,所有列表初始为空. A_{II} 能够对以下预言机进行多项式有界次地适应性询问.

***H*₁ 询问:**F 保持列表 $L_1=(ID_i,Q_i,t_i)$,A_{II} 询问 H_1 预言机,若 L_1 中存在询问项则直接返回,否则,F 选择 $t_i\in Z_{q_1}^*$,计算 t_iP_1,返回 t_iP_1 并增加 (ID_i,Q_i,t_i) 到表 L_1.

公钥询问:F 保持列表 $L=(ID_i,x_i,P_i,\beta)$,A_{II} 输入身份 ID_i,F 检查表 L 中是否存在身份 ID_i. 若存在则 F 直接返回 P_i. 若不存在,则执行以下过程:①若 $ID_i=ID^*$,则 F 返回 $P_i=\beta aP_1$,并将元组 $(ID_i,\perp,P_i,\beta)$ 增加到表 L. 其中,"$\perp$"表示不能确定 βaP_1 的系数. ②若 $ID_i\neq ID^*$,则 F 选择 $x_i\in Z_{q_1}^*$,计算 $P_i=x_iP_1$,返回 x_iP_1 并将元组 $(ID_i,x_i,P_i,\perp')$ 增加到表 L. 其中,"$\perp'$"表示不关心对应位置的值.

***H*₂ 询问:**F 保持列表 $L_2=(P_i,y_i)$,A_{II} 询问 H_2 预言机. F 首先检查表 $L=(ID_i,x_i,P_i,\beta)$ 中是否存在询问项 P_i. 若不存在,则 F 选择 $y_i\in Z_{q_1}^*$,返回 y_i 并将 (P_i,y_i) 增加到表 L_2. 若存在,则执行以下过程:① 若 $\beta=\perp'$,则 F 选择 $y_i\in Z_{q_1}^*$,返回 y_i 并将 (P_i,y_i) 增加到表 L_2. ② 若 $\beta\neq\perp'$,则返回 β 值并计算 βb,返回 βb 并将 (P_i,y_i) 增加到表 L_2.

***H*₃ 询问、*H*₄ 询问:**与引理 1 证明过程中 H_3 询问和 H_4 询问过程相同.

秘密值询问:A_{II} 输入身份 ID_i,F 检查表 L 是否存在身份 ID_i. 若存在则 F 返回 x_i,否则执行过程:①若 $ID_i=ID^*$,则 $\beta\neq\perp'$ 且 $x_i=\perp$,F 失败并终止. ②若 $ID_i\neq ID^*$,则 $\beta=\perp'$ 且 $x_i\neq\perp$,F 返回 x_i.

签密询问:A_{II} 提交发送者的身份 ID_s、接收者公钥 pk_r 和消息 m,执行以下过程:

①若 $ID_s\neq ID^*$,则 F 能够计算 ID_s 的完整私钥 $S_i=\dfrac{1}{x_i+y_i}st_iP_1$,然后正常执行签密算法并返回相应的签密 $\sigma=\mathrm{Signcrypt}(m,S_s,pk_r)$.

②若 $ID_s=ID^*$,则 F 调用"TPKI 系统建立及密钥生成算法"获得接收者的公/私钥对 $(pk_r=x_rP_2,x_r)$,F 从 L_1、L_2 和 L 中获得 $Q_i=t_iP_1$、$H_2(P_i)=\beta b$ 和 $P_i=\beta aP_1$,然后执行以下过程:F 随机选择 $\theta_1,h\in Z_{q_1}^*$,$\theta_2\in Z_{q2}^*$,计算 $U=\theta_1(P_i+y_iP_1)-hQ_i$,$W=\theta sP_1$,$V=\theta_2P_2$. 对于 H_3 预言机,询问 (V,pk_r,x_rV) 的值,随机选择 $\omega_i\in\{0,1\}^{l_m+l_{id}+3l_1}$ 并增加 (V,pk_r,x_rV,ω) 到 L_4. 增加 (m,U,P_i,V,pk_r,x_rV,h) 到 L_3,如果 $H_3(m,U,P_i,V,pk_r,x_rV,h)$ 的值已经存在,那么 F 将终止. 计算 $C=(m\|ID_i\|P_i\|W\|U)\oplus\omega$ 并返回 $\sigma=(C,V)$ 给 A_{II}.

伪造阶段:A_{II} 输出消息 m、发送者的身份 ID_s、发送者公钥 P_s、接收者公钥/私钥对 (pk_r,sk_r) 和密文 $\sigma^*=(C^*,V^*)$:①若 $ID_s\neq ID^*$ 则 F 失败终止,不能解决 mICDH 困难问题. ②若 $ID_s=ID^*$,根据分叉引理[16],F 选择不同的哈希函数 H_3 获得 h',并再次利用 A_{II} 的能力,获

得另一个有效的密文 $\sigma' = (C', V')$,其中,$h' \neq h$. 与引理 1 相似,有以下等式成立:

$$e(W - W', P_s + y_s P_1) = e(hQ_s - h'Q_s, P_{\text{pub}})$$

$$e(W - W', \beta a P_1 + \beta b P_1) = e((h - h')st_s P_1, P_1)$$

因此,可以获得 mICDH 问题的一个解:

$$\frac{1}{a+b}P_1 = \beta \frac{W - W'}{(h - h')st_s}.$$

以下分析 F 成功解决 mICDH 问题的优势. F 失败终止的情况有两种:A_{II} 对 ID_s^* 已经进行过"秘密值询问";签密询问时 $H_3(m, U, P_i, V, pk_r, x_r V, h)$ 的值在 L_3 中已经存在. 当秘密值询问和签密询问都未终止的情况下 F 模拟不终止.

与引理 1 相似,F 成功解决 mICDH 问题的优势为

$$\varepsilon' \geqslant \left(1 - \frac{1}{q_{sw}}\right)^{q_{sw}} \left(1 - \frac{q_s}{2^{\text{poly}(k_1)}}\right)^{q_{H_1}} \frac{1}{q_{sw}} \left(1 - \frac{1}{q_{H_3}}\right) \varepsilon$$

其中 q_{sw}、q_s 和 q_{H_3} 分别表示秘密值询问、签密询问和 H_3 询问的最大询问次数.

5.2 机密性

定理 2 随机预言模型下,如果存在一个攻击者 A 能够以 ε 的优势攻破 CLPKC→TPKI 异构签密方案,那么存在算法 F 能够以 $2\varepsilon(1 - q_u/2^{\text{poly}(k_2)})$ 的优势解决 CDH 困难问题,其中 q_u 表示解签密最大询问次数,k_2 为 TPKI 系统安全参数.

5.3 密文匿名性

定理 3 随机预言模型下,若存在一个攻击者 A 能够以 ε 的优势攻破 CLPKC→TPKI 异构签密方案的密文匿名安全性,则存在一个算法 F 能够以 $\frac{4}{3}(1 - q_u/2^{\text{poly}(k_2)})\varepsilon$ 的优势解决 CDH 困难问题. 其中,q_u 表示解签密询问的最大询问次数,k_2 为 TPKI 系统安全参数.

由于定理 2 和定理 3 的证明过程与文献[12]相似,限于文献篇幅,略去它们的证明过程.

5.4 效率分析

公开文献显示当前没有 CLPKC-TPKI 异构签密方案,因此,无法与同类 CLPKC→TPKI 异构签密方案进行效率比较. 文献[7]的 IDPKC→TPKI 异构签密方案是当前效率最高的异构签密方案,本节对比两个方案的效率. 用 e 表示幂运算个数,P 表示双线性对运算个数. 由表 1 可知,本文方案的计算效率优于文献[7]方案.

表 1 效率对比

方案	预运算	签密	解签密	密文匿名	系统参数
文献[7]	$1P$	$1e + 0P$	$2P + 1e$	不满足	相同
本文	$0P$	$0e + 0P$	$2P$	满足	不同

6 小结

一般而言,签密方案默认发送方和接收方具有相同的密码环境. 但是,在许多应用中,发送方和接收方可能处于不同的密码环境,即异构密码环境. 本文定义了 CLPKC→TPKI 异构签密的形式化定义和安全模型,设计了一个 CLPKC→TPKI 异构签密方案. 在随机预言模型下,证明方案能够满足签密的内部安全性. 方案中 CLPKC 和 TPKI 密码环境具有互不相同的参数. 同时,方案满足匿名性,任何人都不能获得密文收发双方的身份信息,该特性可以满足无线移动匿名接入的要求.

参考文献

[1] Zheng Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption) [A]. Advances in the Cryptology-CRYPTO [C]. California: Springer, 1997. 165 – 179.

[2] Ma Z, Li F H, Ma J F, et al. CL-TAP: An efficient certificateless based trusted access protocol for WLAN[J]. Chinese Journal of Electronics, 2014, 23(1): 142 – 146.

[3] 张宇,陈晶,杜瑞颖,等. 适于车载网安全通信的高效签密方案[J]. 电子学报,2015,43(3):512 – 517.
Zhang Yu, Chen Jing, Du Rui-ying, et al. An efficient signcryption scheme for secure communication of VANET[J]. Acta Electronica Sinica, 2015, 43(3): 512 – 517. (in Chinese)

[4] Sun Y X, Li H. Efficient signcryption between TPKI and IDPKC and its multi-receiver construction[J]. Science China Information Sciences, 2010, 53(3): 557 – 566.

[5] Huang Q, Wong D S, Yang G M. Heterogeneous signcryption with key privacy[J]. The Computer Journal, 2011, 54(4): 525 – 536.

[6] Fu X T, Li X W, Liu W. IDPKC-to-TPKI construction of multi-receiver signcryption[A]. Proceedings of the INCoS (5)[C]. Xian: IEEE, 2013. 335 – 339.

[7] Li F G, Zhang H, Takagi T. Efficient signcryption for heterogeneous systems[J]. IEEE Systems Journal, 2013, 7(3): 420 – 429.

[8] Shamir A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology[C]. Heidelberg: Springer, 1985. 47 – 53.

[9] Libert B, Quisquater J. Efficient signcryption with key privacy from gap Diffie-Hellman groups[A]. Advances in Public Key Cryptography-PKC[C]. Berlin, Springer, 2004. 187 – 200.

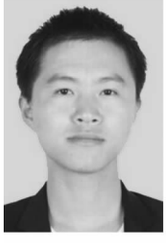
[10] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[A]. Advances in Cryptology-Asiacrypt[C]. Berlin: Springer, 2001. 514 – 532.

[11] Yang G M, Wong D S, Deng X T. Analysis and improvement of a signcryption scheme with key privacy[A]. Advances in Public Key Cryptography-PKC [C]. Berlin,

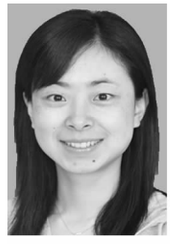
Springer,2005. 218 – 232.
[12] Li C K, Yang G M, Wong D S, et al. An efficient signcryption scheme with key privacy and its extension to ring signcryption[J]. Journal of Computer Security, 2010, 18(3):451 – 473.
[13] Al-Riyami S, Paterson K. Certificateless public key cryptography[A]. Advances in the Cryptology-Asiacrypt[C]. Berlin:Springer,2003. 452 – 474.
[14] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption[A]. Advance in Cryptography-EUROCRYPT[C]. Berlin, Springer, 2002. 83 – 107.
[15] Barbosa M, Farshim P. Certificateless signcryption[A] Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)[C]. Tokyo:ACM,2008. 69 – 372.
[16] Pointcheval D, Jacques S. Security proofs for signature schemes[A]. Advances in Cryptology-Eurocrypt[C]. Berlin:Springer,1996. 387 – 398.

作者简介

张玉磊　男,1979 年出生于甘肃靖远,博士,西北师范大学计算机科学与工程学院副教授,硕士生导师. 研究方向为网络与信息安全、密码学、安全协议分析与设计.
E-mail:zhangyl@nwnu.edu.cn



张灵刚　男,1990 年出生于甘肃省灵台县,西北师范大学计算机科学与工程学院硕士生. 研究方向为网络与信息安全.
E-mail:linggang01@126.com



张永洁(通信作者)　女,1978 年出生于甘肃武都,硕士,甘肃卫生职业学院副教授. 研究方向为网络与信息安全.
E-mail:zyjie78@163.com

王　欢　女,1991 年出生于河北省枣强县,西北师范大学计算机科学与工程学院硕士生研究生. 研究方向为网络与信息安全.
E-mail:1530749678@qq.com