软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(11):2898−2911 [doi: 10.13328/j.cnki.jos.004941]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

可证安全的抗泄露无证书混合签密机制*

周彦伟[1,3], 杨 波[1,3], 王青龙[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](长安大学 信息工程学院,陕西 西安 610064)

[3](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 传统的基于双线性映射的混合签密方案存在着计算效率较低的不足,同时,无法抵抗信息泄露对方案所造成的危害,针对上述不足,在不使用双线性映射的基础上,提出了安全、高效的抗泄露无证书混合签密机制,并在随机谕言机模型下,基于计算性 Diffie-Hellman 问题和离散对数问题对该机制的机密性和不可伪造性进行了证明.同时,分析了该方案的公开验证性、前/后向安全性和不可否认性等安全属性;与传统的无证书混合签密机制相比,该机制不仅具有更优的计算效率,而且在秘密信息存在一定泄露的前提下,依然保持其所声称的安全性,即该方案还具有抵抗秘密信息泄露的能力.

关键词: 无证书混合签密;抗泄露;随机谕言机;无双线性映射;离散对数;计算性 Diffie-Hellman

中图法分类号: TP309

中文引用格式: 周彦伟,杨波,王青龙.可证安全的抗泄露无证书混合签密机制.软件学报,2016,27(11):2898−2911. http://www.jos.org.cn/1000-9825/4941.htm

英文引用格式: Zhou YW, Yang B, Wang QL. Provably secure leakage-resilient certificateless hybrid signcryption scheme. Ruan Jian Xue Bao/Journal of Software, 2016,27(11):2898−2911 (in Chinese). http://www.jos.org.cn/1000-9825/4941.htm

Provably Secure Leakage-Resilient Certificateless Hybrid Signcryption Scheme

ZHOU Yan-Wei[1,3], YANG Bo[1,3], WANG Qing-Long[2]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](School of Information Engineering, Chang'an University, Xi'an 710062, China)

[3](State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

Abstract: A hybrid signcryption scheme should withstand various leakage attacks when applied in practical applications. This paper presents a new leakage-resilient certificateless hybrid signcryption (LR-CLHS) scheme without bilinear pairing. The security of this scheme is based on the computational Diffie-Hellman (CDH) assumption and discrete logarithm (DL) problem. Considering the computational costs, the proposal is more efficient than traditional certificateless hybrid signcryption schemes and has a short ciphertext length and high security. In the random oracle model, it is also indistinguishability against adaptive posteriori key-leakage chosen-ciphertext attacks (IND-KL-CCA2) according to the hardness of the CDH assumption, existentially unforgeable against key-leakage chosen-message attacks (EUF-KL-CMA) according to the hardness of the DL problem, and maintains the original security under the condition that the adversary learns a small amount of leakage about the secret key by the leakage attacks (e.g., side-channel attacks, etc).

* 基金项目: 国家自然科学基金(61572303, 61272436); 信息安全国家重点实验室(中国科学院信息工程研究所)开放课题(2015-MS-10); 陕西省重点科技创新团队项目(2014KTC-18)

Foundation item: National Natural Science Foundation of China (61572303, 61272436); Open Project of State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences) (2015-MS-10); Program of Key Science and Technology Innovation Team in Shaanxi Province (2014KTC-18)

收稿时间: 2015-06-27; 修改时间: 2015-09-10; 采用时间: 2015-11-18

Key words: certificateless hybrid signcryption; leakage-resilient; random oracle; without bilinear pairing; discrete logarithm; computational Diffie-Hellman

随着网络通信技术的发展,网络环境下的攻击方式层出不穷,因此,Internet 用户希望通信过程满足保密性和认证性.消息的保密性通常由加密来完成,而认证性则基于签名来实现.然而传统采用先签名后加密的方式,虽然能够保证消息的保密性和认证性,但其计算量较大、效率较低,并且传输代价大.文献[1]首先提出签密的概念,旨在让公钥加密和数字签名同时进行,使签密密文同时具有机密性和可靠性,并且相对于传统先签名后加密模式,具有更小的计算和传输代价.然而传统签密方案中要求传输消息取自某个特定的集合.Al-Riyami 等人提出了无证书公钥密码系统(certificateless public-key cryptography,简称 CL-PKC)[2].CL-PKC 减少了对可信第三方密钥生成中心(key generation center,简称 KGC)的依赖.在 CL-PKC 中,用户基于 KGC 为其计算的部分私钥和随机选取的秘密值生成用户的完整私钥;公钥由用户的秘密值、身份信息和系统参数计算得出,并对外安全公布.CL-PKC 解决了基于身份密码系统[3]中的用户密钥托管问题,也消除了传统公钥系统中公钥证书的复杂性管理问题,提高了密码系统的运行效率.文献[4,5]基于混合加密机制[6]提出了混合签密的概念,很好地解决了传统签密方案中传输消息受限的不足;混合签密由密钥封装机制(key encapsulation mechanism,简称 KEM)和数据封装机制(data encapsulation mechanism,简称 DEM)两部分组成.

随着研究工作的逐渐深入,国内外众多学者分别基于双线性映射提出了新的混合签密方案[7−11].文献[7]将混合签密的概念推广到无证书体制下,提出了无证书混合签密的概念,指出无证书混合签密可以由无证书签密密钥封装机制(certificateless signcryption key encapsulation mechanism,简称 CLSC-KEM)和数据封装机制构成,并且给出了无证书混合签密机制的基本组成算法.文献[8]提出了基于身份的混合签密机制.文献[9]指出文献[10]提出的对文献[7]的攻击算法是不成立的,同时,构造的无证书混合签密机制具有密文长度短、计算速度快的优点,但该方案不具有不可否认性.文献[11]构建了一个随机谕言机模型下可证明安全的无证书混合签密机制.

现代密码学安全性的前提条件是,假定密钥对可能的攻击者来说是完全隐藏的,即秘密信息是完全保密的.然而随着各种各样的边信道攻击[12−15]的出现,例如时间攻击、电源损耗、冷启动攻击、音频分析等攻击,均能从保密密钥或者加密系统的内部状态提取出所要获得的部分关于保密密钥的信息,从而泄露系统或者密钥的安全性.因此,许多现有的可证安全的密码学协议[7−11]在实际应用中不再保持其所声称的安全性.

近年来,对抗泄露密码学的研究[16−19]已引起密码学研究者的广泛关注,即在秘密信息存在部分泄露的前提下,设计仍然保持安全的密码机制.因此,设计更接近于现实环境的密码学机制,已成为当前密码学研究领域的热点问题.针对传统基于双线性映射的混合签密方案[7−11]存在计算效率低的不足,同时无法抵抗信息泄露对方案所造成的危害,本文在不使用双线性映射的前提下,提出了安全、高效抗泄露的无证书混合签密机制.

1 基础知识

1.1 困难性问题

离散对数(discrete logarithm,简称 DL)问题:令群 G 的阶为大素数 q,设 P 为群 G 的任意一个生成元,给定 $P,bP\in G$,对任意未知的 $b\in Z_q^*$, DL 问题的目标是计算 b.任意的概率多项式时间(probabilistic polynomial time,简称 PPT)算法 $\mathcal{A}$ 成功地解决 DL 问题的概率 $Adv^{DL}(\mathcal{A})=\Pr[\mathcal{A}(P,bP)=b]$ 是可忽略的,其中,概率来源于 b 在 Z_q^* 上的随机选取和算法 $\mathcal{A}$ 的随机选择.

计算性 Diffie-Hellman(computational Diffie-Hellman,简称 CDH)问题:令群 G 的阶为大素数 q,设 P 为群 G 的任意一个生成元,给定 $P,aP,bP\in G$,对于任意未知的 $a,b\in Z_q^*$,CDH 问题的目标是计算 $abP\in G$.任意的 PPT 算法 $\mathcal{A}$ 成功地解决 CDH 困难问题的概率 $Adv^{CDH}(\mathcal{A})=\Pr[\mathcal{A}(P,aP,bP)=abP]$ 是可忽略的,其中概率来源于 a,b 在 Z_q^* 上的随机选取和算法 $\mathcal{A}$ 的随机选择.

1.2 统计距离和最小熵

定义 1. 有限域Ω上随机变量 X 与 Y 间的统计距离为 $SD(X,Y)=\frac{1}{2}\sum_{w\in\Omega}|\Pr[X=w]-\Pr[Y=w]|$.

定义 2. 设 X 是随机变量,则 X 的最小熵 $H_\infty(X)$定义为 $H_\infty(X)=-\log(\mathrm{Max}_x\Pr[X=x])$,最小熵表示在没有附加信息的前提下,猜测随机变量 X 的最大概率.

定义 3. 在变量 Y 已知时,变量 X 的平均最小熵为 $\tilde{H}_\infty(X|Y)=-\log(E_{y\leftarrow Y}[2^{-H_\infty(X|Y=y)}])$,平均最小熵 $\tilde{H}_\infty(X|Y)$表示在变量 Y 已知时,变量 X 的不可预测性.

引理 1[16]. 对于随机变量 X,Y 和 Z,若 Y 的取值最多有 2^λ个,则有 $\tilde{H}_\infty(X|(Y,Z))\geqslant\tilde{H}_\infty(X|Z)-\lambda$ 成立.

1.3 随机提取

定义 4. 若对于满足 $X\in\{0,1\}^n$ 和 $\tilde{H}_\infty(X|I)\geqslant k$ 的任意随机变量(X,I)有 $SD((Ext(X,S),S,I),(U_m,S,I))\leqslant\varepsilon$(其中,$S\in\{0,1\}^t$ 和 $U_m\in\{0,1\}^m$)成立,则称函数 $Ext:\{0,1\}^n\times\{0,1\}^t\to\{0,1\}^m$ 是平均情况的(k,ε)-强提取器.

1.4 非交互式零知识论证

设$\mathcal{R}$是关于(x,y)的 NP 关系,其对应的语言为 $L_{\mathcal{R}}=\{y|\exists x,\text{s.t.}(x,y)\in\mathcal{R}\}$, 则$\mathcal{R}$上的非交互式零知识(non-interactive zero-knowledge,简称 NIZK)论证包含下述 3 种算法:

(1) $(CRS,TK)\leftarrow Setup(1^k)$:生成公共参考串 CRS 和陷门密钥 TK.

(2) $\pi\leftarrow Prove_{CRS}(x,y)$:生成论据$\pi$,其中,$\mathcal{R}(x,y)=1$.

(3) $0/1\leftarrow Verify_{CRS}(x,y)$:验证论据$\pi$的正确性.

为了方便 NIZK 论证的使用,在具体使用过程中,可将算法 Prove 和 Verify 的下标 CRS 省略,可根据上下文推导.文献[16]详细介绍了 NIZK 论证的完整性、可靠性和可组合的零知识性等安全属性.

若存在一个 PPT 提取器 Ext 可从恶意证明者 P'产生的任意证据π中提取出相应的证据 x',其中,P'能够接触其他状态的模拟证明,但 P'仅能看到关于真实状态的模拟证明,则满足上述条件的 NIZK 论证称为真实模拟提取的 NIZK(tSE-NIZK).

1.5 抗泄露的困难关系

设 $\mathcal{O}_{SK}^{k,\lambda}()$ 是泄露谕言机(其中,k 是安全参数,λ是泄露参数),其输入为任意高效可计算的函数 $f_i:\mathcal{SK}\to\{0,1\}^\lambda$ $(i\geqslant1)$(其中,$\mathcal{SK}$是私钥空间),输出为 $f_i(SK)$.敌手可适应性询问 $\mathcal{O}_{SK}^{k,\lambda}()$ 以 $f_i()(i\geqslant1)$获知相应私钥 SK 的泄露信息,条件是对同一 SK 泄露信息的总量不能超过λ;不失一般性,可假设敌手对谕言机 $\mathcal{O}_{SK}^{k,\lambda}()$ 询问一次, $\mathcal{O}_{SK}^{k,\lambda}()$ 返回相应的泄露信息 $f(SK)$,但 $f(SK)$的长度不能超过λ.

定义 5. 若 PPT 抽样算法 $KeyGen()$生成的关系$\mathcal{R}$满足下述条件,则$\mathcal{R}$是抗泄露的困难关系:

① 对于所有的$(x,y)\leftarrow KeyGen(1^k)$,都有$(x,y)\in\mathcal{R}$.

② 对于任意(x,y),存在多项式时间算法判断$(x,y)\in\mathcal{R}$是否成立.

③ 对于任意的 PPT 敌手 $\mathcal{A}^{\mathcal{O}_{SK}^{k,\lambda}()}$,有 $\Pr\left[\mathcal{R}(x',y)=1\middle|\begin{matrix}(x,y)\leftarrow KeyGen(1^k)\\ x'\leftarrow\mathcal{A}^{\mathcal{O}_{SK}^{k,\lambda}()}(x,y)\end{matrix}\right]\leqslant negl(k)$ 成立.

定义 6. 若 PPT 抽样算法 $KeyGen()$生成的关系$\mathcal{R}$满足下述条件,则称关系$\mathcal{R}$是 SPR(second-preimage resistant)关系:

① 对于所有的$(x,y)\leftarrow KeyGen(1^k)$,都有$(x,y)\in\mathcal{R}$.

② 对于任意(x,y),存在多项式时间算法判断$(x,y)\in\mathcal{R}$是否成立.

③ 对于任意的 PPT 敌手$\mathcal{A}$,有 $\Pr\left[\mathcal{R}(x',y)=1\wedge x'\neq x\middle|\begin{matrix}(x,y)\leftarrow KeyGen(1^k)\\ x'\leftarrow\mathcal{A}(x,y)\end{matrix}\right]\leqslant negl(k)$ 成立.

引理 2[16]. 若关系$\mathcal{R}(x,y)$是 SRP 关系,则关系$\mathcal{R}(x,y)$也是一个抗λ-泄露的困难关系,且可容忍的泄露量为

$\tilde{H}_\infty(x\,|\,y)-\omega(\log k)$, 其中,$k$ 为安全参数.

实例:关系 $\mathcal{R}'(x',y')=\{aP=A\wedge bP=B+P_{Pub}H(ID,A,B)|x'=(a,b),y'=(P,P_{Pub},H,ID,A,B)\}$ 由 PPT 抽样算法 $KeyGen_{\mathcal{R}'}()$ 和判定算法 $Check_{\mathcal{R}'}()$ 组成,相关算法的具体定义如下:

(1) 算法 $(x',y')\leftarrow KeyGen_{\mathcal{R}'}(1^k)$

① G 为阶是大素数 q 的循环群,P 为 G 的一个生成元,定义抗碰撞哈希函数 $H:\{0,1\}^l\times G\times G\rightarrow Z_q^*$.

② 均匀随机选取 $a,r,s\in Z_q^*$ 和 $ID\in\{0,1\}^l$,计算 $P_{Pub}=sP,A=aP,B=rP$ 和 $b=r+sH(ID,A,B)$.

③ 设 $x'=(a,b)$和 $y'=(P,P_{Pub},H,ID,A,B)$,输出(x',y').

(2) 算法 $0/1\leftarrow Check_{\mathcal{R}'}(x',y')$

若 $x'=(a,b)$和 $y'=(P,P_{Pub},H,ID,A,B)$同时满足等式 $aP=A$ 和 $bP=B+P_{Pub}(ID,A,B)$,则返回 1,表示$(x',y')\in\mathcal{R}'$;否则,返回 0,表示$(x',y')\notin\mathcal{R}'$.

引理 3. 关系$\mathcal{R}'(x',y')$是 SRP 关系.

证明:

① 由关系$\mathcal{R}'(x',y')$的具体定义可知,对于任意的$(x',y')\leftarrow KeyGen(1^k)$,有$(x',y')\in\mathcal{R}'$成立.

② 由 $Check_{\mathcal{R}'}()$ 的定义可知,对于任意的(x',y'),算法 $Check_{\mathcal{R}'}()$ 能够判断$(x',y')\in\mathcal{R}'$是否成立.

③ 假设存在 PPT 敌手$\mathcal{A}$能够以不可忽略的概率攻破关系$\mathcal{R}'(x',y')$的安全性,则有对于$(x',y')\in\mathcal{R}'$,存在$(x'',y')\in\mathcal{R}'\wedge x''\neq x'$,其中,$x'=(a,b),y'=(P,P_{Pub},H,ID,A,B)$和 $x''=(a'',b'')$.

根据$\mathcal{R}'$的定义可知,$\begin{cases}aP=A\\ bP=B+P_{Pub}H(ID,A,B)\end{cases}$ 和 $\begin{cases}a''P=A\\ b''P=B+P_{Pub}H(ID,A,B)\end{cases}$ 成立,则 $a''=a\wedge b''=b$,即 $x''=x'$.这与前提假设 $x''\neq x'$相矛盾,因此,对于任意的 PPT 敌手$\mathcal{A}$有 $\Pr\left[\mathcal{R}'(x',y')=1\wedge(x''\neq x')\,\middle|\,\begin{matrix}(x',y')\leftarrow KeyGen(1^k)\\ x''\leftarrow\mathcal{A}(x',y')\end{matrix}\right]\leqslant negl(k)$ 成立.综上所述,关系$\mathcal{R}'(x',y')$是 SRP 关系. □

推论. 关系$\mathcal{R}'(x',y')$是一个抗λ-泄露的困难关系,其中,$\lambda\leqslant\tilde{H}_\infty(x'\,|\,y')-\omega(\log k)$,k 为安全参数.

由引理 2 和引理 3 可知,该推论成立.

1.6 抗泄露的签名

文献[16]基于抗泄露困难关系和 tSE-NIZK 论证构造抗泄露的签名机制.令关系$\mathcal{R}(x,y)$是由 PPT 抽样算法 $KeyGen_{\mathcal{R}}(1^k)$ 生成的λ-抗泄露困难关系;$\Pi=(Setup,Prove,Verify)$是关系$\mathcal{R}(x,y)$上支持标签的 tSE-NIZK 论证.

签名机制$\Gamma=(KeyGen,Sign,SigVer)$的具体描述如下:

① $KeyGen(1^k)$:输出 $SK=x$ 和 $PK=(CRS,y)$,其中,$(x,y)\leftarrow KeyGen_{\mathcal{R}}(1^k)$ 和$(CRS,*)\leftarrow Setup(1^k)$.

② $Sign(SK,K)$:输出$\pi\leftarrow Prove^M(x,y)$,其中,消息 M 作为算法 $Prove$ 的标签.

③ $SigVer(PK,\pi,M)$:输出 $Verify^M(\pi,y)$.

引理 4[16]. 关系$\mathcal{R}(x,y)$是抗λ-泄露的困难关系;令$\Pi=(Setup,Prove,Verify)$是关系$\mathcal{R}(x,y)$上支持标签的 tSE-NIZK 论证,则$\Gamma=(KeyGen,Sign,SigVer)$是抗$\lambda$-泄露的签名机制.

1.7 安全模型

无证书混合签密方案将面临$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类敌手的攻击,其中,$\mathcal{A}_{\mathrm{I}}$类敌手无法掌握系统的主密钥,但其具有替换合法用户公钥的能力,则$\mathcal{A}_{\mathrm{I}}$ 类敌手为恶意的用户.本文中,$\mathcal{A}_{\mathrm{I}}^i(i=1,2)$ 为$\mathcal{A}_{\mathrm{I}}$ 类敌手,其中,$\mathcal{A}_{\mathrm{I}}^1$ 是攻击方案机密性的敌手,$\mathcal{A}_{\mathrm{I}}^2$ 是攻击方案不可伪造性的敌手.$\mathcal{A}_{\mathrm{II}}$类敌手可掌握系统的主密钥,但其不具有替换合法用户公钥的能力,则$\mathcal{A}_{\mathrm{II}}$ 类敌手为恶意的 KGC.本文中,$\mathcal{A}_{\mathrm{II}}^i(i=1,2)$ 为$\mathcal{A}_{\mathrm{II}}$ 类敌手,其中,$\mathcal{A}_{\mathrm{II}}^1$ 是攻击方案机密性的敌手,$\mathcal{A}_{\mathrm{II}}^2$ 是攻击方案不可伪造性的敌手.

1.7.1 机密性

机密性要求在适应性选择密文的密钥泄露攻击(indistinguishability against adaptive key-leakage chosen-ciphertext attacks,简称 IND-KL-CCA2)下加密是不可区分的,即对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 和 $\mathcal{A}_{\mathrm{II}}^{1}$,在下述游戏 1 和游戏 2 中获胜的优势是可忽略的.

游戏 1:该游戏的参与者有敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 和挑战者 $\mathcal{C}$,其中,$\mathcal{C}$ 作为 $\mathcal{A}_{\mathrm{I}}^{1}$ 的谕言机.设安全参数为 k 和泄露参数为 λ,具体执行过程如下:

初始化:$\mathcal{C}$ 运行 $(Params,S_{MSK})\leftarrow Setup(1^k)$ 算法,生成系统公开参数 $Params$ 和主密钥 S_{MSK};发送 $Params$ 给 $\mathcal{A}_{\mathrm{I}}^{1}$,秘密保存 S_{MSK}.

阶段 1:该阶段 $\mathcal{A}_{\mathrm{I}}^{1}$ 可进行多项式有界次的下述询问,并且询问是适应性进行的;$\mathcal{C}$ 基于谕言机 $\mathcal{O}_{SK}^{k,\lambda}()$ 回答任意用户的泄露询问,条件是,对同一私钥 SK 泄露询问,输出 $\sum_{k=1}^{i} f_k(SK)$ 的总长度不超过泄露参数 λ.

- 公钥生成询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于 ID 的公钥生成询问时,发送相应的公钥 PK_{ID} 给 $\mathcal{A}_{\mathrm{I}}^{1}$.
- 部分密钥生成询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于 ID 的部分密钥生成询问时,发送相应的部分密钥 (y_{ID},Y_{ID}) 给 $\mathcal{A}_{\mathrm{I}}^{1}$.
- 公钥替换询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于 ID 的公钥替换询问时,用 PK_{ID}^{*} 替换 ID 原始的公钥 PK_{ID}.
- 私钥生成询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于 ID 的私钥生成询问时,发送相应的私钥 SK_{ID} 给 $\mathcal{A}_{\mathrm{I}}^{1}$.
- 混合签密询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于身份-消息对 $\langle ID_S,ID_R,M\rangle$ 的混合签密询问时,运行混合签密算法 $\sigma=Sign_{hybrid}(SK_{ID_S},PK_{ID_R},M)$,并发送密文 σ 给 $\mathcal{A}_{\mathrm{I}}^{1}$.
- 解混合签密询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_{\mathrm{I}}^{1}$ 关于身份-密文对 $\langle ID_S,ID_R,\sigma\rangle$ 的解签密询问时,运行解混合签密算法 $M=UnSign_{hybrid}(PK_{ID_S},SK_{ID_R},\sigma)$,并发送明文 M 给 $\mathcal{A}_{\mathrm{I}}^{1}$.
- 泄露询问:$\mathcal{A}_{\mathrm{I}}^{1}$ 输入身份 ID 和多项式可计算函数 $f_i:\mathcal{SK}\rightarrow\{0,1\}^{\lambda_i}(i\geqslant 1)$,$\mathcal{C}$ 返回私钥 SK_{ID} 的泄露信息 $f_i(SK_{ID})$,但关于 SK_{ID} 的泄露总长度不能超过 λ,否则忽略 $\mathcal{A}_{\mathrm{I}}^{1}$ 的本次询问.

挑战:阶段 1 结束后,$\mathcal{A}_{\mathrm{I}}^{1}$ 选择两个等长的明文消息 (M_0,M_1) 和两个不同的身份 (ID_S,ID_R).$\mathcal{C}$ 随机选择 $b\leftarrow\{0,1\}$,生成 $\sigma_b=Sign_{hybrid}(SK_{ID_S},PK_{ID_R},M_b)$,将挑战密文 σ_b 发送给 $\mathcal{A}_{\mathrm{I}}^{1}$.

阶段 2:该阶段类似于阶段 1,$\mathcal{A}_{\mathrm{I}}^{1}$ 可对除挑战密文 σ_b 之外的任意密文 σ 进行适应性解混合签密询问;但该阶段不允许进行适应性泄露询问.

输出:$\mathcal{A}_{\mathrm{I}}^{1}$ 输出对随机数 b 的猜测 b',则当 $b=b'$ 且下述条件都成立时,称敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 赢得上述游戏:

① 任意阶段,$\mathcal{A}_{\mathrm{I}}^{1}$ 对身份 ID_R 不能进行私钥和部分密钥生成询问.

② 对被替换公钥的任何身份,$\mathcal{A}_{\mathrm{I}}^{1}$ 不能进行私钥生成询问.

③ 阶段 2 中 $\mathcal{A}_{\mathrm{I}}^{1}$ 对挑战密文 σ_b 不进行解混合签密询问,同时不能对任何身份进行泄露询问.

于是,对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^{1}$,在该游戏中获胜的优势为 $Adv_{LR\text{-}CLHS,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1}}^{IND\text{-}KL\text{-}CCA2}(k,\lambda)=\left|\Pr[\mathcal{A}_{\mathrm{I}}^{1}\text{ wins}]-\frac{1}{2}\right|$.

特别地,现有抗泄露密码机制的研究中[16−19],虽然安全模型中允许敌手对泄露谕言机可进行适应性的询问,但是为避免在游戏的第 2 个阶段中敌手通过编码挑战密文从而形成特殊的泄露函数以达到区分密文对应明文目的,限制阶段 2 中敌手不允许对泄露谕言机进行询问.下述游戏具有相同的限制,本文不再赘述.

游戏 2:该游戏的参与者有敌手 $\mathcal{A}_{\mathrm{II}}^{1}$ 和挑战者 $\mathcal{C}$,其中,$\mathcal{C}$ 作为 $\mathcal{A}_{\mathrm{II}}^{1}$ 的谕言机.设安全参数是 k 和泄露参数是 λ,具体执行过程如下:

初始化:$\mathcal{C}$ 运行 $(Params,S_{MSK})\leftarrow Setup(1^k)$ 算法,生成系统公开参数 $Params$ 和主密钥 S_{MSK};发送 $Params$ 和 S_{MSK} 给 $\mathcal{A}_{\mathrm{II}}^{1}$.

阶段 1:与游戏 1 相类似,$\mathcal{A}_{\mathrm{II}}^1$ 可进行多项式有界次的相关询问,并且询问是适应性进行的;但与游戏 1 不同的是,$\mathcal{A}_{\mathrm{II}}^1$ 不能进行公钥替换询问.

挑战:阶段 1 结束后,$\mathcal{A}_{\mathrm{II}}^1$ 选择两个等长的明文消息(M_0,M_1)和两个不同的身份(ID_S,ID_R).$\mathcal{C}$随机选择$b\leftarrow\{0,1\}$,生成 $\sigma_b=Sign_{hybrid}(SK_{ID_S},PK_{ID_R},M_b)$,将挑战密文$\sigma_b$发送给 $\mathcal{A}_{\mathrm{II}}^1$.

阶段 2:该阶段类似于阶段 1,$\mathcal{A}_{\mathrm{II}}^1$ 可对除挑战密文σ_b之外的任意密文σ进行适应性解混合签密询问;但该阶段不允许进行适应性泄露询问.

输出:$\mathcal{A}_{\mathrm{II}}^1$ 输出对随机数 b 的猜测 b',则当 $b=b'$且下述条件都成立时,称敌手 $\mathcal{A}_{\mathrm{II}}^1$ 赢得上述游戏:

① 任意阶段 $\mathcal{A}_{\mathrm{II}}^1$ 对 ID_R 不能进行私钥生成询问.

② 阶段 2 中,$\mathcal{A}_{\mathrm{II}}^1$ 对挑战密文σ_b不能进行解混合签密询问,同时不能对任何身份进行泄露询问.

则对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{II}}^1$,在该游戏中获胜的优势为 $Adv_{LR\text{-}CLHS,\mathcal{C},\mathcal{A}_{\mathrm{II}}^1}^{IND\text{-}KL\text{-}CCA2}(k,\lambda)=\left|\Pr[\mathcal{A}_{\mathrm{II}}^1\text{ wins}]-\frac{1}{2}\right|$.

1.7.2 不可伪造性

不可伪造性要求在选择消息的密钥泄露攻击(unforgeable against key-leakage chosen-message attacks,简称 EUF-KL-CMA)下存在性是不可伪造的,即,对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^2$ 和 $\mathcal{A}_{\mathrm{II}}^2$,在下述游戏 3 和游戏 4 中获胜的优势是可忽略的:

游戏 3:该游戏的参与者有敌手 $\mathcal{A}_{\mathrm{I}}^2$ 和挑战者$\mathcal{C}$,其中,$\mathcal{C}$作为 $\mathcal{A}_{\mathrm{I}}^2$ 的谕言机.设安全参数为 k 和泄露参数为λ,具体执行过程如下:

初始化:$\mathcal{C}$运行$(Params,S_{MSK})\leftarrow Setup(1^k)$算法,生成系统公开参数 $Params$ 和主密钥 S_{MSK};发送 $Params$ 给 $\mathcal{A}_{\mathrm{I}}^2$,且秘密保存 S_{MSK}.

询问:与游戏 1 相类似,$\mathcal{A}_{\mathrm{I}}^2$ 可进行多项式有界次的相关询问,并且询问是适应性进行的.

输出:$\mathcal{A}_{\mathrm{I}}^2$ 输出伪造的身份密文对(ID_S,ID_R,σ^*),当 $UnSign_{hybrid}(PK_{ID_S},SK_{ID_R},\sigma^*)\neq\perp$ 且下述条件都成立时,称敌手 $\mathcal{A}_{\mathrm{I}}^2$ 赢得上述游戏.

① 任意阶段,$\mathcal{A}_{\mathrm{I}}^2$ 对 ID_S 不能进行私钥和部分密钥生成询问;

② 对被替换公钥的任何身份,$\mathcal{A}_{\mathrm{I}}^2$ 不能进行私钥生成询问.

那么,对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^2$,在该游戏中获胜的优势为 $Adv_{LR\text{-}CLHS,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2}^{EUF\text{-}KL\text{-}CMA}(k,\lambda)=\left|\Pr[\mathcal{A}_{\mathrm{I}}^2\text{ wins}]-\frac{1}{2}\right|$.

游戏 4:该游戏的参与者有敌手 $\mathcal{A}_{\mathrm{II}}^2$ 和挑战者$\mathcal{C}$,其中,$\mathcal{C}$作为 $\mathcal{A}_{\mathrm{II}}^2$ 的谕言机.设安全参数为 k 和泄露参数为λ,具体执行过程如下:

初始化:$\mathcal{C}$运行$(Params,S_{MSK})\leftarrow Setup(1^k)$算法,生成系统公开参数 $Params$ 和主密钥 S_{MSK};发送 $Params$ 和 S_{MSK} 给 $\mathcal{A}_{\mathrm{II}}^2$.

询问:与游戏 2 相类似,$\mathcal{A}_{\mathrm{II}}^2$ 可进行多项式有界次的相关询问,并且询问是适应性进行的.

输出:$\mathcal{A}_{\mathrm{II}}^2$ 输出伪造的身份密文对(ID_S,ID_R,σ^*),当 $UnSign_{hybrid}(PK_{ID_S},SK_{ID_R},\sigma^*)\neq\perp$ 且任意时刻 $\mathcal{A}_{\mathrm{II}}^2$ 对 ID_S 不能进行私钥生成询问,称敌手 $\mathcal{A}_{\mathrm{II}}^2$ 赢得上述游戏.

那么,对于任意的 PPT 敌手 $\mathcal{A}_{\mathrm{II}}^2$,在该游戏中获胜的优势为 $Adv_{LR\text{-}CLHS,\mathcal{C},\mathcal{A}_{\mathrm{II}}^2}^{EUF\text{-}KL\text{-}CMA}(k,\lambda)=\left|\Pr[\mathcal{A}_{\mathrm{II}}^2\text{ wins}]-\frac{1}{2}\right|$.

2 抗泄露的无证书混合签密机制

2.1 方案构造

本节提出的抗泄露无证书混合签密方案Π=(*Setup*,*KeyGen*,$Sign_{hybrid}$,$UnSign_{hybrid}$)包含 4 种基本算法,具体细节如下描述.

2.1.1 系统建立阶段

系统初始化阶段,KGC 进行如下操作:

① 循环群 G 的阶为大素数 q,P 为 G 的一个生成元;定义函数 $Ext:G\times\{0,1\}^t\to\{0,1\}^m$ 是平均情况的$(\log q-\lambda,\varepsilon)$强提取器;定义$\lambda$是系统设定的泄露参数;定义对称加密算法 $Enc(k,M)$和解密算法 $Dec(k,c)$.

② 选择抗碰撞哈希函数: $H_1:\{0,1\}^{l_1}\times G\times G\to Z_q^*$,$H_2:\{0,1\}^{l_1}\times\{0,1\}^{l_2}\times G\times Z_q^*\times\{0,1\}^t\to Z_q^*$,其中,$l_1$ 为用户身份标识 ID 的长度,l_2 为明文消息的长度.

③ 定义Γ=($Setup_\Gamma$,$Prove_\Gamma$,$Verify_\Gamma$)是关系$\mathcal{R}'(x,y)$上支持标签的 tSE-NIZK 论证,运行算法$(CRS,TK,EK)\leftarrow Setup_\Gamma(1^k)$;关系$\mathcal{R}'(x,y)$的详细定义见本文第 1.5 节的实例.

④ 随机选取秘密数 $S_{MSK}\in Z_q^*$ 作为系统主密钥,计算系统公钥为 $P_{Pub}=S_{MSK}P$;公开系统公共参数 $Params=\langle q,G,P,P_{Pub},H_1,H_2,Ext,\Gamma,Enc,Dec\rangle$,秘密保存主密钥 S_{MSK}.

2.1.2 用户密钥生成

用户 ID_i 的密钥生成过程如下所述:

① 随机选取秘密值 $x_i\in Z_q^*$,计算 $X_i=x_iP$,发送身份标识 ID_i 和公开参数 X_i 给 KGC.

② 给定用户身份标识 ID_i 及公开参数 X_i,KGC 随机选取秘密数 $r_i\in Z_q^*$,分别计算 $Y_i=r_iP$ 和 $y_i=r_i+S_{MSK}H_1(ID_i,X_i,Y_i)$,通过安全信道将 y_i 和 Y_i 返回给用户 ID_i,其中,y_i 为用户的部分私钥,Y_i 为用户的部分公钥.即:用户 ID_i 的公私钥对为$\langle PK_i=(X_i,Y_i),SK_i=(x_i,y_i)\rangle$,且满足$(SK_i,(Params,PK_i))\in\mathcal{R}'$.

③ 用户 ID_i 通过等式 $y_iP=Y_i+P_{Pub}H_1(ID_i,X_i,Y_i)$验证 KGC 生成的部分私钥 y_i 和部分公钥 Y_i 的正确性,可防止恶意 KGC 的欺骗.

2.1.3 混合签密

设发送者 Alice(身份标识为 ID_A)和接收者 Bob(身份标识为 ID_B)的公私钥对分别为$\langle PK_A=(X_A,Y_A),SK_A=(x_A,y_A)\rangle$和$\langle PK_B=(X_B,Y_B),SK_B=(x_B,y_B)\rangle$.若发送 $m\in\{0,1\}^{l_2}$ 给 Bob,Alice 进行下述操作:

① 均匀随机选取字符串 $S\in\{0,1\}^t$ 和秘密数 $u\in Z_q^*$,计算 $U=uP$ 和 $K=Ext(u(X_B+Y_B+h_1^BP_{Pub}),S)$,其中,$h_1^B=H_1(ID_B,X_B,Y_B)$;生成密文 $C=Enc(K,M)$.

② 计算 $T=u(x_A+y_A)^{-1}$ 和 $\pi=Prove_\Gamma^\alpha(SK_A,(PK_A,Params))$,其中,$\alpha=H_2(ID_A,C,U,T,S)$.

③ 发送密文σ=(π,T,C,S)和 Alice 的身份 ID_A 给接收者 Bob.

2.1.4 解混合签密

Bob 收到密文σ=(π,T,C,S)后进行下述操作.

① 计算 $U'=T(X_A+Y_A+h_1^AP_{Pub})$ (其中,$h_1^A=H_1(ID_A,X_A,Y_A)$)和 $K'=Ext(U'(x_B+y_B)),S)$,恢复明文消息:

$$M=Dec(K',C).$$

② 计算$\alpha'=H_2(ID_A,C,U',T,S)$,若等式 $Verify_\Gamma^{\alpha'}(\pi,(PK_A,Params))=1$ 成立,则 Bob 输出消息 M;否则输出$\perp$,特殊符号表示输入的密文无效.

2.2 正确性分析

2.2.1 密文的可恢复性

由 $U'=u(x_A+y_A)^{-1}(X_A+Y_A+h_1^AP_{Pub})=uP$ 和 $U'(x_B+y_B)=uP(x_B+r_B+S_{MSK}h_1^B)=u(X_B+Y_B+h_1^BP_{Pub})$ (其中,$y_A=r_A+S_{MSK}h_1^A$ 和 $y_B=r_B+S_{msk}h_1^B$),可知 $K'=K$,因此 $M=Dec(K',Enc(K,M))$,即,接收者基于发送者公钥还原出原

始的通信消息;同时,验证了消息发送者的身份.

2.2.2 密文的合法性

由$\alpha'=H_3(ID_a,C,U',T,S)=H_3(ID_a,C,U,T,S)=\alpha$,可知:

$$Verify_T^{\alpha'}(\pi,(PK_A,Params))=1,$$

其中,$\pi=Prove_T^{\alpha}(SK_A,(PK_A,Params))$..因此,接收者能够验证签名的正确性,即 Bob 完成对密文$\sigma=(\pi,T,C,S)$的合法性及完整性的验证.

3 安全性证明

3.1 机密性

引理 5. 如果存在敌手 $\mathcal{A}_{\mathrm{I}}^1$ 能够在多项式时间内赢得游戏 1,那么存在算法$\mathcal{C}$,能够在多项式时间内,以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^1,Leakage}^{IND\text{-}KL\text{-}CCA2}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)},\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}+\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}\right]$解决 CDH 问题.其中,泄露参数$\lambda\leqslant\log q-l_2-\omega\log(k)$,$q_S(q_S<q)$为混合签密询问的次数,$q_{SK}(q_{SK}<q)$为私钥生成询问的次数,$\varepsilon$是敌手 $\mathcal{A}_{\mathrm{I}}^1$ 攻破本文混合签密机制的优势.

证明:令算法$\mathcal{C}$是一个CDH问题解决者,输入为$\langle P,aP,bP\rangle$,其中,$a,b\in Z_q^*$且未知,目标是计算abP.$\mathcal{C}$以敌手 $\mathcal{A}_{\mathrm{I}}^1$ 为子程序并充当游戏的挑战者.$\mathcal{C}$运行初始化算法,同时发送 $Params$ 给 $\mathcal{A}_{\mathrm{I}}^1$,令 $P_{Pub}=bP$,并秘密保存主密钥 S_{MSK};维持列表 L_1,L_2,L_{SK},L_{PK},分别用于跟踪 $\mathcal{A}_{\mathrm{I}}^1$ 对谕言机 H_1,H_2,私钥生成和公钥生成的询问,初始时各列表均为空.

询问:敌手 $\mathcal{A}_{\mathrm{I}}^1$ 进行下述询问.

H_2 询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$ 对 H_2 的询问$\langle ID,C,U,T,S\rangle$时,若$\langle ID,C,U,T,S,h_2\rangle\in L_2$,则返回相应的 h_2 给 $\mathcal{A}_{\mathrm{I}}^1$;否则,$\mathcal{C}$选取满足条件$\langle *,*,*,*,*,h_2\rangle\notin L_2$(避免哈希函数碰撞的产生)的随机数 $h_2\in Z_q^*$,添加元组$\langle ID,C,U,T,S,h_2\rangle$到 L_2 中,并返回相应的 h_2 给 $\mathcal{A}_{\mathrm{I}}^1$.

公钥生成询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$ 对身份 ID 的公钥生成询问时,$\mathcal{C}$进行下述操作:

① 若$\langle ID,X_{ID},Y_{ID},c_{ID}\rangle\in L_{PK}$,则返回相应的值 $PK_{ID}=\langle X_{ID},Y_{ID}\rangle$给 $\mathcal{A}_{\mathrm{I}}^1$.

② 否则,$\mathcal{C}$选取随机数 $c_{ID}\leftarrow\{0,1\}$,且 $\Pr[c_{ID}=1]=\frac{1}{q_S+1}$. 若 $c_{ID}=0$,则$\mathcal{C}$随机选取 $x_{ID},y_{ID},h_1^{ID}\in Z_q^*$, 计算 $Y_{ID}=y_{ID}P-h_1^{ID}P_{Pub}$ 和 $X_{ID}=x_{ID}P$,使得$\langle *,X_{ID},*,*\rangle\notin L_{PK}$ 和$\langle *,*,Y_{ID},*\rangle\notin L_{PK}$;否则,重新选取相应的随机数.添加$\langle ID,X_{ID},Y_{ID},c_{ID}\rangle$到 L_{PK} 中,添加$\langle ID,x_{ID},y_{ID}\rangle$到 L_{SK} 中,添加 $\langle ID,X_{ID},Y_{ID},h_1^{ID}\rangle$ 到 L_1 中,返回 $PK_{ID}=\langle X_{ID},Y_{ID}\rangle$ 给 $\mathcal{A}_{\mathrm{I}}^1$.若 $c_i=1$,则$\mathcal{C}$随机选取 $r_{Know}^1,r_{Know}^2,h_1^{ID}\in Z_q^*$,计算 $X_{ID}=r_{Know}^1P$ 和 $Y_{ID}=r_{Know}^2P$, 使得$\langle *,X_{ID},*,*\rangle\notin L_{PK}$ 和$\langle *,*,Y_{ID},*\rangle\notin L_{PK}$;否则,重新选取相应的参数.添加$\langle ID,X_{ID},Y_{ID},c_{ID}\rangle$到 L_{PK} 中,添加 $\langle ID,X_{ID},Y_{ID},h_1^{ID}\rangle$ 到 L_1 中,返回 $PK_{ID}=\langle X_{ID},Y_{ID}\rangle$给 $\mathcal{A}_{\mathrm{I}}^1$.

H_1 询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$ 对 H_1 的询问$\langle ID,X_{ID},Y_{ID}\rangle$时,若 $\langle ID,X_{ID},Y_{ID},h_1^{ID}\rangle\in L_1$,则返回 h_1^{ID} 给 $\mathcal{A}_{\mathrm{I}}^1$;否则,$\mathcal{C}$对 ID 进行公钥生成询问后,返回列表 L_1 中元组 $\langle ID,X_{ID},Y_{ID},h_1^{ID}\rangle$ 所对应的 h_1^{ID} 给 $\mathcal{A}_{\mathrm{I}}^1$.

公钥替换:$\mathcal{A}_{\mathrm{I}}^1$ 可选择一个新的公钥 $PK'_{ID}=\langle X'_{ID},Y'_{ID}\rangle$ 替换合法用户 ID 的原始公钥 PK_{ID}.

私钥生成询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$ 对身份 ID 的私钥生成询问时,$\mathcal{C}$进行下述操作:

① 若$\langle ID,x_{ID},y_{ID}\rangle\in L_{SK}$,则返回相应的值 $SK_{ID}=\langle x_{ID},y_{ID}\rangle$给 $\mathcal{A}_{\mathrm{I}}^1$.

② 否则,$\mathcal{C}$对 ID 进行公钥生成询问,并获知相应的应答元组$\langle ID,X_{ID},Y_{ID},c_{ID}\rangle$.若 $c_{ID}=0$,则对 ID 的公钥生成询问已向 L_{SK} 添加了相应的元组$\langle ID,x_{ID},y_{ID}\rangle$,$\mathcal{C}$在 L_{SK} 中查找相应的元组$\langle ID,x_{ID},y_{ID}\rangle$,并返回 $SK_{ID}=\langle x_{ID},y_{ID}\rangle$

给 $\mathcal{A}_{\mathrm{I}}^1$;若 c_{ID}=1,则$\mathcal{C}$选取随机数 $x_{ID}, y_{ID} \in Z_q^*$,并返回 SK_{ID}=〈x_{ID},y_{ID}〉给 $\mathcal{A}_{\mathrm{I}}^1$,并添加相应的元组〈$ID$,$x_{ID}$,$y_{ID}$〉到 L_{SK}中,确保$\mathcal{C}$对 $\mathcal{A}_{\mathrm{I}}^1$关于同一身份私钥生成询问的应答是一致的.

混合签密询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$对元组〈$ID_S$,$ID_R$,$m$〉($\mathcal{A}_{\mathrm{I}}^1$已完成对 ID_S 和 ID_R 的公钥生成询问)的混合签密询问时,$\mathcal{C}$对 ID_S 进行私钥生成询问、对 ID_R 进行公钥生成询问,获知相应的私钥 $SK_{ID_S}=(x_{ID_S}, y_{ID_S})$ 以及公钥 $PK_{ID_R}=(X_{ID_R}, Y_{ID_R})$,运行混合签密算法 $Sign_{hybrid}$生成相应的密文σ,并将σ返回给 $\mathcal{A}_{\mathrm{I}}^1$.

泄露询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$关于身份 ID 对应私钥 SK_{ID}的泄露询问 f_i()时,检测 $\mathcal{A}_{\mathrm{I}}^1$对 SK_{ID}的所有泄露询问的输出 $f_i(SK_{ID})$总和 $\sum_{k=1}^{i} f_k(SK_{ID})$是否超出系统设定的泄露参数$\lambda$:若 $\sum_{k=1}^{i} f_k(SK_{ID}) > \lambda$,则$\mathcal{C}$忽略 $\mathcal{A}_{\mathrm{I}}^1$的泄露询问;否则,返回相应的泄露信息 $f_i(SK_{ID})$给 $\mathcal{A}_{\mathrm{I}}^1$.

解混合签密询问:当$\mathcal{C}$收到 $\mathcal{A}_{\mathrm{I}}^1$对元组〈$ID_S$,$ID_R$,$\sigma$〉(假设 $\mathcal{A}_{\mathrm{I}}^1$对 ID_S和 ID_R已进行了公钥生成询问)的解混合签密询问时,$\mathcal{C}$在 L_{PK}中查询 ID_R所对应的元组〈$ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}$〉,并进行下述操作.

① 若〈$ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}$〉$\in L_{PK}$且 $c_{ID_R}=0$,则$\mathcal{C}$以 ID_R 和 ID_S 为索引查询 L_{SK} 与 L_{PK},分别获知 SK_{ID_R} 和 PK_{ID_S},并运行解混合签密算法 $UnSign_{hybrid}$,返回相应的结果M给 $\mathcal{A}_{\mathrm{I}}^1$,若输入的密文无效,则$\mathcal{C}$返回特殊符号⊥.

② 若〈$ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}$〉$\in L_{PK}$且 $c_{ID_R}=1$,$\mathcal{C}$以 ID_R 为索引在 L_1 中查询〈$ID_S, X_{ID_R}, Y_{ID_R}, h_1^{ID_R}$〉$\in L_1$,并计算 $U'=T(X_{ID_R}+Y_{ID_R}+h_1^{ID_R}P_{Pub})$,以 ID_S 为索引,在 L_2 中查询〈ID_S,C,U',T,S,h_2〉$\in L_2$:

- 若等式 $Verify_{I'}^{h_2}(\pi,(PK_{ID_S},Params))=1$ 成立,则随机选择 $M\in\{0,1\}^m$,并返回给 $\mathcal{A}_{\mathrm{I}}^1$;
- 否则,$\mathcal{C}$返回特殊符号⊥.

③ 若〈$ID_R, X_{ID_R}, Y_{ID_R}, c_{ID_R}$〉$\notin L_{PK}$(即,公钥被替换),$\mathcal{C}$以 ID_R为索引在 L_{PK},L_1查询〈$ID_R, X'_{ID_R}, Y'_{ID_R}, c_{ID_R}$〉$\in L_{PK}$和〈$ID_R, X'_{ID_R}, Y'_{ID_R}, h_1^{ID_R}$〉$\in L_1$,并计算 $U'=T(X'_{ID_R}+Y'_{ID_R}+h_1^{ID_R}P_{Pub})$:当 $c_{ID_R}=0$ 时,$\mathcal{C}$以 ID_R和 ID_S为索引查询列表 L_{SK}与 L_{PK},分别获知 SK_{ID_R} 和 PK_{ID_S},并运行算法 $UnSign_{hybrid}$返回 M 给 $\mathcal{A}_{\mathrm{I}}^1$;当 $c_{ID_R}=1$时,$\mathcal{C}$以 ID_S为索引在 L_2 中查询〈ID_S,C,U',T,S,h_2〉$\in L_2$,若等式 $Verify_{I'}^{h_2}(\pi,(PK_{ID_S},Params))=1$ 成立,则随机选择 $M\in\{0,1\}^m$,并返 L_2 回给 $\mathcal{A}_{\mathrm{I}}^1$;否则,$\mathcal{C}$返回特殊符号⊥.

挑战:$\mathcal{A}_{\mathrm{I}}^1$输出两个身份($ID_S$,$ID_R$)和两个等长的明文($M_0$,$M_1$),其中,$ID_R$是挑战身份.收到 $\mathcal{A}_{\mathrm{I}}^1$发送的挑战信息后,$\mathcal{C}$对 ID_S和 ID_R进行公钥生成询问后进行下述操作:

① 若 $c_{ID_R}=0$,则$\mathcal{C}$结束,并终止模拟.

② 否则,令 U=aP,$\mathcal{C}$选取满足 $U=T(X_S+Y_S+h_1^S P_{Pub})$ (其中,$h_1^S=H_1(ID_S,X_S,Y_S)$)的随机数 $T\in Z_q^*$,随机选取 $W\in G$,$S\in\{0,1\}^t$和 $f\leftarrow\{0,1\}$,分别计算 K=Ext(W,S)和 C=Enc(K,M_f);计算:

$$\pi = Prove_{I'}^{\alpha}(SK_{ID_S},(PK_{ID_S},Params)).$$

其中,α=H_3(ID_S,C,U,T,S);令σ=(π,T,C,S)是$\mathcal{C}$对 M_f的混合签密密文,发送 ID_S,ID_R和σ给 $\mathcal{A}_{\mathrm{I}}^1$.

输出:收到挑战密文之后,经过多项式次数的上述询问(除了泄露询问)后,$\mathcal{A}_{\mathrm{I}}^1$输出对随机数 f 的猜测 $f'\leftarrow\{0,1\}$,但 $\mathcal{A}_{\mathrm{I}}^1$不能对 ID_R 进行私钥生成询问;对公钥被替换的任何身份都不能进行私钥提取询问;也不能对 ID_S,ID_R和σ进行解混合签密询问.

若 f'=f,$\mathcal{C}$输出 $abP=(h_1^{ID_R})^{-1}[W-(r_{know}^1+r_{know}^2)U]$ (其中,$W=(r_{know}^1+r_{know}^2+bh_1^{ID_R})U$)作为 CDH 困难问题的有效解;否则,$\mathcal{C}$没有解决 CDH 困难问题.

若敌手 $\mathcal{A}_{\mathrm{I}}^1$在多项式时间内赢得游戏 1,分两种情况讨论:

① 敌手 $\mathcal{A}_{\mathrm{I}}^1$能够以不可忽略的优势攻破本文机制;

② 任何敌手都无法攻破本文机制,但在泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够赢得游戏 1.

声称 1. 若 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够以不可忽略的优势ε攻破本文机制,则算法$\mathcal{C}$能够以如下优势解决 CDH 问题:

$$Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1}}^{CDH}(k)=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{1}{q(q_{S}+1)}$$

令事件$\mathcal{E}_1$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^{1}$ 对挑战身份 ID_R 未进行私钥生成询问,即 $\Pr[\mathcal{E}_1]=1-\frac{q_{SK}}{2^{k}}$;事件$\mathcal{E}_2$表示询问阶段对 ID_R 未进行混合签密询问,即 $\Pr[\mathcal{E}_2]=1-\frac{q_{S}}{2^{k}}$;事件$\mathcal{E}_3$表示挑战阶段$\mathcal{C}$未终止,即 $\Pr[\mathcal{E}_3]=\frac{1}{q_{S}+1}$;事件$\mathcal{E}_4$表示挑战阶段$\mathcal{C}$输出一个有效的挑战密文,即 $\Pr[\mathcal{E}_4]=\frac{1}{q}$.于是,整个模拟过程中$\mathcal{C}$不终止的概率为

$$\Pr[\mathcal{E}_1\wedge\mathcal{E}_2\wedge\mathcal{E}_3\wedge\mathcal{E}_4]=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{1}{q(q_{S}+1)}.$$

综上所述,忽略信息的泄露,若敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够以不可忽略的优势ε攻破本文混合签密机制,则有算法$\mathcal{C}$能够以不可忽略的优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1}}^{CDH}(k)=\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)}$ 输出 CDH 问题的有效解.

声称 2. 若任意的 PPT 敌手都无法以不可忽略的优势攻破本文混合签密机制,但在相关泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^{1}$ 能够在游戏 1 中获胜,则算法$\mathcal{C}$能够以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1},Leakage}^{CDH}(k)\leqslant\frac{2^{\frac{m+\lambda}{2}-1}}{\sqrt{q}}$ 解决 CDH 问题.

作为敌手,$\mathcal{A}_{\mathrm{I}}^{1}$ 能够从挑战密文、公钥和λ-比特的泄露信息中获知关于私钥的相关信息.令 $Leak_{SK}$ 表示 $\mathcal{A}_{\mathrm{I}}^{1}$ 获得的关于挑战身份 ID_R 私钥 SK_{ID_R} 所有泄露函数 $f_i()(i\geqslant 1)$的输出,则 $Leak_{SK}$ 最多有 2^{λ}个值.有下述关系成立:

$$\begin{aligned}\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},\sigma,Params,Leak_{SK})&=\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},Leak_{SK})\\&=\tilde{H}_{\infty}(x_{ID_R},y_{ID_R}\mid PK_{ID_R},Leak_{SK})\\&\geqslant\tilde{H}_{\infty}(x_{ID_R},y_{ID_R}\mid PK_{ID_R})-\lambda\\&\geqslant\log q-\lambda.\end{aligned}$$

在上述公式中,σ和 $Params$ 与私钥 SK_{ID_R} 无关,并且 $U(x_{ID_R}+y_{ID_R})$ 是关于 SK_{ID_R} 的单向映射.由引理 1 可知,$\mathcal{A}_{\mathrm{I}}^{1}$ 获知 SK_{ID_R} 的概率至多为 $2^{-\tilde{H}_{\infty}(U(x_{ID_R}+y_{ID_R})\mid PK_{ID_R},\sigma,Params,Leak_{SK})}\leqslant\frac{2^{\lambda}}{q}$,则 $\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $K=Ext(U(x_{ID_R}+y_{ID_R}),S)$ 的最大概率为 $\frac{1}{2}\sqrt{2^{l_2}\frac{2^{\lambda}}{q}}=\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$.因此,在相关泄露信息的协助下,$\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $f'=f$ 的概率为 $\Pr[f'=f]_{Under}\leqslant\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$;若未得到泄露信息的协助,则 $\mathcal{A}_{\mathrm{I}}^{1}$ 输出 $f'=f$ 的概率为 $\Pr[f'=f]_{\mathrm{Without}}=\frac{1}{2}$.于是,$\mathcal{C}$解决 CDH 问题的概率为

$$\Pr[f'=f]\leqslant\frac{1}{2}+\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}.$$

因此$\mathcal{C}$解决 CDH 问题的优势为 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^{1},Leakage}^{CDH}(k)=\Pr[f'=f]-\frac{1}{2}\leqslant\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}$,其中,$\lambda\leqslant\log q-l_2-\omega\log(k)$.

由声称 1 和声称 2 可知,引理 5 得证. □

引理 6. 若存在敌手 $\mathcal{A}_{\mathrm{II}}^{1}$ 能够在多项式时间内赢得游戏 2,则存在算法$\mathcal{C}$,能够在多项式时间内以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{II}}^{1},Leakage}^{IND\text{-}KL\text{-}CCA2}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)},\left(1-\frac{q_{SK}}{2^{k}}\right)\left(1-\frac{q_{S}}{2^{k}}\right)\frac{\varepsilon}{q(q_{S}+1)}+\frac{2^{\frac{l_2+\lambda}{2}-1}}{\sqrt{q}}\right]$ 解决 CDH 问题.

证明过程与引理 5 相似,本文不再赘述.

定理 1. 若 CDH 假设成立,则本文混合签密机制Π=(*Setup*,*KeyGen*,$Sign_{hybrid}$,$UnSign_{hybrid}$)在随机谕言机模型下是语义安全的抵抗 IND-KL-CCA2.

由引理 5 和引理 6 可知,定理 1 得证.

3.2 不可伪造性

引理 7. 若存在敌手 $\mathcal{A}_{\mathrm{I}}^2$ 能够在多项式时间内赢得游戏 3,则存在算法$\mathcal{C}$,能够在多项式时间内以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2,Leakage}^{EUF\text{-}KL\text{-}CMA}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)},\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}+\frac{2^{\lambda}}{q-q_d+1}\right]$ 解决 DL 困难问题.其中,泄露参数$\lambda\leqslant\log q-l_2-\omega\log(k)$,$q_S(q_S<q)$为混合签密询问的次数,$q_{SK}(q_{SK}<q)$为私钥生成询问的次数,$q_d(q_d<q)$为解混合签密询问的次数,$\varepsilon$是敌手 $\mathcal{A}_{\mathrm{I}}^2$ 攻破本文混合签密机制的优势.

证明:算法$\mathcal{C}$是一个 DL 问题的解决者,输入为$\langle P,bP\rangle$,其中,$b\in Z_q^*$ 且未知,目标是计算 b.$\mathcal{C}$以 $\mathcal{A}_{\mathrm{I}}^2$ 为子程序并充当游戏的挑战者.$\mathcal{C}$运行 Setup 算法,并发送 *Params* 给 $\mathcal{A}_{\mathrm{I}}^2$,令 $P_{Pub}=bP$,并秘密保存主密钥 S_{MSK};维持列表 L_1,L_2,L_{SK},L_{PK} 分别用于跟踪 $\mathcal{A}_{\mathrm{I}}^2$ 对谕言机 H_1,H_2,私钥生成和公钥生成的询问.初始时,各列表为空.

询问:敌手 $\mathcal{A}_{\mathrm{I}}^2$ 执行多项式有界次的 H_1 询问、H_2 询问、私钥提取、公钥提取、公钥替换、混合签密、泄露询问和解混合签密询问,$\mathcal{C}$按引理 5 中的应答方式对相关询问进行应答.但在该游戏中,挑战身份是 ID_S 而不是 ID_R.

伪造: $\mathcal{A}_{\mathrm{I}}^2$ 选择 $u\in Z_q^*$,并计算 $U=uP$,选取满足 $U=T(X_S+Y_S+h_1^S P_{Pub})$ (其中,$h_1^S=H_1(ID_S,X_S,Y_S)$)的随机数 $T\in Z_q^*$,随机选取 $S\in\{0,1\}^t$,并计算 $K=Ext(u(X_{ID_R}+Y_{ID_R}+h_1^{ID_R}P_{Pub}),S)$ 和 $C=Enc(K,M)$,选取随机数 $\pi\in Z_q^*$,则 $\sigma=(\pi,T,C,S)$是 $\mathcal{A}_{\mathrm{I}}^2$ 伪造的关于 ID_S,ID_R 和 M 的混合签密密文,其中,对 M 未进行混合签密询问. $\mathcal{A}_{\mathrm{I}}^2$ 发送 ID_S,ID_R 和σ给$\mathcal{C}$.伪造阶段, $\mathcal{A}_{\mathrm{I}}^2$ 可进行概率多项式时间次数的上述询问,但 $\mathcal{A}_{\mathrm{I}}^2$ 不能对 ID_S 进行私钥生成询问,对公钥被替换的任何身份都不能进行私钥生成询问.

当$\mathcal{C}$接收到 $\mathcal{A}_{\mathrm{I}}^2$ 所发送的伪造信息后,以 ID_S 为索引查询 L_{PK},获知相应的元组$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle$并进行下述操作:

① 若 $c_{ID_S}=0$,则$\mathcal{C}$结束,并终止模拟.

② 否则,$\mathcal{C}$输出 $b=(Th_1^{ID_S})^{-1}[u-T(r_{know}^1+r_{know}^2)]$ (其中,$T=u(r_{know}^1+r_{know}^2+bh_1^{ID_S})^{-1}$)作为 DL 问题的有效解.

声称 3. 若 PPT 敌手 $\mathcal{A}_{\mathrm{I}}^2$ 能够以不可忽略的优势ε伪造合法的混合签密密文,则算法$\mathcal{C}$能够以优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2}^{DL}(k)=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q_S+1}$ 解决 DL 问题.

令事件$\mathcal{E}_1$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^2$ 对挑战身份 ID_S 未进行私钥生成询问,即 $\Pr[\mathcal{E}_1]=1-\frac{q_{SK}}{2^k}$;事件$\mathcal{E}_2$表示询问阶段 $\mathcal{A}_{\mathrm{I}}^2$ 对挑战身份 ID_S 未进行混合签密询问,即 $\Pr[\mathcal{E}_2]=1-\frac{q_S}{2^k}$;事件$\mathcal{E}_3$表示挑战阶段$\mathcal{C}$未终止,即 $\Pr[\mathcal{E}_3]=\frac{1}{q_S+1}$;事件$\mathcal{E}_4$表示敌手 $\mathcal{A}_{\mathrm{I}}^2$ 输出了有效的伪造信息,即 $\Pr[\mathcal{E}_4]=\frac{1}{q}$.于是,整个模拟过程中$\mathcal{C}$不终止的概率为

$$\Pr[\mathcal{E}_1\wedge\mathcal{E}_2\wedge\mathcal{E}_3\wedge\mathcal{E}_4]=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{1}{q(q_S+1)}.$$

综上所述,忽略信息的泄露,若 $\mathcal{A}_{\mathrm{I}}^2$ 能够以不可忽略的优势ε攻破本文机制,则算法$\mathcal{C}$能够以不可忽略的优势 $Adv_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2}^{DL}(k)=\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}$ 输出 DL 问题的有效解.

声称 4. 若任意的 PPT 敌手都无法以不可忽略的优势攻破本文机制的不可伪造性,但在相关泄露信息的协助下,敌手 $\mathcal{A}_{\mathrm{I}}^2$ 能够在游戏 3 中获胜,即 $\mathcal{A}_{\mathrm{I}}^2$ 输出了有效的伪造签名,则算法 $\mathcal{C}$ 能够以优势 $Adv^{DL}_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^2,Leakage}(k)\leqslant \frac{2^{\lambda}}{q-q_d+1}$ 解决 DL 问题.

令 $Leak'_{SK}$ 表示 $\mathcal{A}_{\mathrm{I}}^2$ 选择的所有关于身份 ID_S 私钥 SK_{ID_S} 的泄露信息,则 $Leak'_{SK}$ 最多有 2^{λ}个值.有关系 $\tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S},\sigma,Params,Leak'_{SK})\geqslant \tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S})-\lambda\geqslant \log q-\lambda$ 成立,式中,σ和 $Params$ 与私钥 SK_{ID_S} 无关.根据引理 1 可知,$\mathcal{A}_{\mathrm{I}}^2$ 获知 SK_{ID_S} 的概率最多为 $2^{-\tilde{H}_{\infty}(SK_{ID_S}\mid PK_{ID_S},\sigma,Leak'_{SK})}\leqslant \frac{2^{\lambda}}{q}$.

如果混合签密密文 $\sigma=(\pi,T,C,S)$ 满足等式 $Verify_T^{\alpha}(\pi,(PK_{ID_S},Params))=1$ (其中,$\alpha=H_3(ID_a,C,U,T,S)$ 和 $U=T(X_{ID_S}+Y_{ID_S}+h_1^{ID_S}P_{Pub})$),则称密文 σ 为有效密文;否则,称 σ 为无效密文.伪造攻击过程中,$\mathcal{A}_{\mathrm{I}}^2$ 可至多向解混合签密谕言机 $UnSign^{\mathcal{O}}_{hybrid}()$ 提出 q_d 次询问.在上述询问应答的帮助下,$\mathcal{A}_{\mathrm{I}}^2$ 输出最终的伪造密文.

令 σ' 是 $\mathcal{A}_{\mathrm{I}}^2$ 向 $UnSign^{\mathcal{O}}_{hybrid}()$ 询问的第 1 个密文,则 $UnSign^{\mathcal{O}}_{hybrid}()$ 接收 σ' 的优势至多是 $\frac{2^{\lambda}}{q}$;若 $UnSign^{\mathcal{O}}_{hybrid}()$ 拒绝了该密文 σ',则 $\mathcal{A}_{\mathrm{I}}^2$ 可获知关于私钥的相关信息,此时,$\mathcal{A}_{\mathrm{I}}^2$ 生成有效密文的优势至多是 $\frac{2^{\lambda}}{q-1}$.综合考虑所有的 q_d 次解混合签密询问,可知 $\mathcal{A}_{\mathrm{I}}^2$ 伪造有效密文的优势至多是 $\frac{2^{\lambda}}{q-q_d+1}$.于是,算法 $\mathcal{C}$ 解决 DL 问题的优势为

$$Adv^{CDH}_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{I}}^1,Leakage}(k)\leqslant \frac{2^{\lambda}}{q-q_d+1}.$$

其中,$\lambda\leqslant \log q-l_2-\omega\log(k)$.

由声称 3 和声称 4 证明可知,引理 7 得证. □

引理 8. 若存在敌手 $\mathcal{A}_{\mathrm{II}}^2$ 能够在多项式时间内赢得游戏 4,则存在算法 $\mathcal{C}$,能在多项式时间内,以优势 $Adv^{EUF\text{-}KL\text{-}CMA}_{\Pi,\mathcal{C},\mathcal{A}_{\mathrm{II}}^2,Leakage}(k,\lambda)\in\left[\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)},\left(1-\frac{q_{SK}}{2^k}\right)\left(1-\frac{q_S}{2^k}\right)\frac{\varepsilon}{q(q_S+1)}+\frac{2^{\lambda}}{q-q_d+1}\right]$ 解决 DL 问题.

证明过程与引理 7 类似,本文不再赘述.

定理 2. 若 DL 假设成立,则本文混合签密机制 $\Pi=(Setup,KeyGen,Sign_{hybrid},UnSign_{hybrid})$ 在随机谕言机模型下是存在性不可伪造的抵抗 EUF-KL-CMA.

由引理 7 和引理 8 可知,定理 2 得证.

3.3 公开验证性

本文方案中,当发送者和接收者关于密文的有效性发生争执,需要公开验证发送者身份时,第三方无需收发双方的任何私有信息,只需验证等式 $Verify_T^{\alpha}(\pi,(PK_{ID_S},Params))=1$ (其中,参数 α 均可由相关公开信息计算得到)是否成立即可,因此,本文方案具有公开验证性.

3.4 不可否认性

本文方案中,密文消息是不可伪造的.因此,若发送者确实生成了签密密文,该发送者就不能否认;同时,由公开验证性可知,任何第三方均可公开验证密文发送者的身份,因此,本文方案具有不可否认性.

3.5 前/后向安全性

本文方案中,即使在某次签密密文的收发过程中,攻击者获得签密发送者或密文接收者的相关参数,由于密文生成参数是随机选取的,具有较强的新鲜性,因此,攻击者无法获知先前的密文及相关参数,则攻击者无法获得先前的明文消息.同时,攻击者也无法猜测发送者即将发送的签密密文及其相关参数,所以也无法获知即将要

发送的明文消息.因此,本文方案具有完美的前/后向安全性.

4 性能分析

与现有的混合签密方案[7−11]进行比较时,计算开销主要取决于混合签密和签密验证算法的计算量,且计算量主要统计双线性映射及群上点乘运算和指数运算的执行次数,但未统计可提前准备的相关计算及混合签密中必须进行的对称加解密运算;通信开销主要通过密文的长度来衡量;而安全属性主要讨论方案的不可伪造性、机密性和抗泄露性等.

表 1 中相关符号的含义如下:$\mathcal{O}_M$表示群上的点乘运算,$\mathcal{O}_E$表示群上的指数运算,$\mathcal{O}_B$表示双线性映射运算,$\mathcal{O}_{Ext}$表示随机提取器运算,$\mathcal{O}_P$表示 tSE-NIZK 论证的 Prove 运算,$\mathcal{O}_V$表示 tSE-NIZK 论证的 Verify 运算,$|M|$表示明文消息 M 的长度,$|G|$表示群 G 上相应元素的长度,$|Z|$表示 Z_q^* 上相应元素的长度,$|\{0,1\}^n|$表示字符串$\{0,1\}^n$的长度.

Table 1 Comparison of computational efficiency

表 1 效率比较结果

混合签密机制	计算效率		通信开销	安全属性				
	混合签密	解混合签密	密文长度	不可伪造性	机密性	公开验证性	不可否认性	抗泄露性
文献[7]	$2\mathcal{O}_M+\mathcal{O}_B$	$5\mathcal{O}_B$	$2\|G\|+\|M\|$	√	√	√	√	×
文献[8]	$2\mathcal{O}_M$	$\mathcal{O}_M+3\mathcal{O}_B$	$\|\{0,1\}^n\|+2\|G\|+\|M\|$	√	√	√	√	×
文献[9]	$\mathcal{O}_M+\mathcal{O}_B$	$\mathcal{O}_M+\mathcal{O}_B$	$\|Z\|+\|M\|$	√	√	×	×	×
文献[11]	$\mathcal{O}_M+2\mathcal{O}_E+2\mathcal{O}_B$	$\mathcal{O}_M+\mathcal{O}_E+6\mathcal{O}_B$	$\|Z\|+\|G\|+\|M\|$	√	√	×	√	×
本文方案	$\mathcal{O}_M+\mathcal{O}_{Ext}+\mathcal{O}_P$	$\mathcal{O}_M+\mathcal{O}_{Ext}+\mathcal{O}_V$	$2\|Z\|+\|M\|$	√	√	√	√	√

√表示方案具有该属性,×表示方案不具有该属性

如表 1 所示,在计算效率方面,由于运行一次双线性对运算的时间较大,因此相对于现有的使用双线性映射的混合签密机制[7−11]而言,不使用双线性映射的混合签密机制具有更大的效率优势,即本文方案在效率方面有明显的优势;在安全性方面,文献[7–9,11]的方案不具有抗泄露性,在信息可泄露的环境中,上述机制[7−11]无法满足其所声称的安全性,而本文机制依然保持其原有的安全性;文献[9,11]中方案不满足公开验证性;文献[9]的方案不具有不可否认性.综上所述,现有的混合签密机制[7−11]在计算效率或安全性方面存在一定的不足.相对于上述机制,本文机制的计算和通信效率及安全性更优.

5 结束语

签密作为一种较为理想的数据信息安全传输方法,其安全性和计算开销对其实际应用有着至关重要的作用.本文针对传统混合签密方案[7−11]无抗泄露的能力和存在计算效率低的不足,在不使用双线性映射的基础上提出了安全、高效的抗泄露无证书混合签密机制,并在随机谕言机模型下基于 CDH 和 DL 问题对本文机制的机密性和不可伪造性进行了证明;同时,分析了本文方案的公开验证性、前/后向安全性和不可否认性等安全属性.与现有的无证书混合签密机制[7−11]相比,本文机制不仅具有更优的计算效率和安全性,而且在信息可泄露的环境中依然保持其所声称的安全性,即本文方案具有抵抗秘密信息泄露的能力.

由于随机提取器的运算必须有随机种子的参与,在一定程度上会增加密文的传输负载.下一阶段,本文将构造不使用随机提取器的抗泄露无证书混合签密机制.

References:

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption). In: Proc. of the Advances in Cryptology—CRYPTO'97. Berlin, Heidelberg: Springer-Verlag, 1997. 165–179. [doi: 10.1007/BFb0052234]

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the Advances in Cryptology—ASIACRYPT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 452–473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1985. 47−53. [doi: 10.1007/3-540-39568-7_5]
[4] Dent AW. Hybrid signcryption schemes with outsider security. In: Proc. of the Information Security. Berlin, Heidelberg: Springer-Verlag, 2005. 203−217. [doi: 10.1007/11556992_15]
[5] Dent AW. Hybrid signcryption schemes with insider security. In: Proc. of the Information Security and Privacy. Berlin, Heidelberg: Springer-Verlag, 2005. 253−266. [doi: 10.1007/11506157_22]
[6] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003,33(1):167−226. [doi: 10.1137/S0097539702403773]
[7] Li F, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Proc. of the Information Security Practice and Experience. Berlin, Heidelberg: Springer-Verlag, 2009. 112−123. [doi: 10.1007/978-3-642-00843-6_11]
[8] Li F, Shirase M, Takagi T. Identity-Based hybrid signcryption. In: Proc. of the Int'l Conf. on Availability, Reliability and Security (ARES 2009). IEEE, 2009. 534−539. [doi: 10.1109/ARES.2009.44]
[9] Sun YX, Li H. Efficient certificateless hybrid signcryption. Ruan Jian Xue Bao/Journal of Software, 2011,22(7):1690−1698 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/SP.J.1001.2011.03825]
[10] Selvi SSD, Vivek SS, Pandu Rangan C. Breaking and re-building a certificateless hybrid signcryption scheme. Lecture Notes in Computer Science, 2010:294−307. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=F4BD72725754665BBCB2010D8E30910B?doi=10.1.1.215.5905&rep=rep1&type=pdf
[11] Yu HF, Yang B. Provably secure certificateless hybrid signcryption. Chinese Journal of Computers, 2015,38(4):804−813 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2015.00804]
[12] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proc. of the Advances in Cryptology—CRYPTO'96. Berlin, Heidelberg: Springer-Verlag, 1996. 104−113. [doi: 10.1007/3-540-68697-5_9]
[13] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: Proc. of the Advances in Cryptology—CRYPTO'97. Berlin, Heidelberg: Springer-Verlag, 1997. 513−525. [doi: 10.1007/BFb0052259]
[14] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proc. of the Advances in Cryptology—CRYPTO'99. Berlin, Heidelberg: Springer-Verlag, 1999. 388−397. [doi: 10.1007/3-540-48405-1_25]
[15] Halderman JA, Schoen SD, Heninger N, Clarkson W, Paul W, Calandrino JA, Feldman AJ, Appelbaum J, Felten EW. Lest we remember: Cold-Boot attacks on encryption keys. Communications of the ACM, 2009,52(5):91−98. [doi: 10.1145/1506409.1506429]
[16] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Efficient public-key cryptography in the presence of key leakage. In: Proc. of the Advances in Cryptology—ASIACRYPT 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 613−631. [doi: 10.1007/978-3-642-17373-8_35]
[17] Li SJ, Zhang FT, Sun YX, Shen LM. Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013,16(4):797−806. [doi: 10.1007/s10586-013-0253-z]
[18] Liu SL, Weng J, Zhao YL. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks. In: Proc. of the Topics in Cryptology—CT-RSA 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 84−100. [doi: 10.1007/978-3-642-36095-4_6]
[19] Naor M, Segev G. Public-Key cryptosystems resilient to key leakage. SIAM Journal on Computing, 2012,41(4):772−814. [doi: 10.1137/100813464]

附中文参考文献:

[9] 孙银霞,李晖.高效无证书混合签密.软件学报,2011,22(7):1690−1698. http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/SP.J.1001.2011.03825]
[11] 俞惠芳,杨波.可证安全的无证书混合签密.计算机学报,2015,38(4):804−813. [doi: 10.3724/SP.J.1016.2015.00804]

周彦伟(1986－),男,甘肃通渭人,博士生,工程师,主要研究领域为密码学,匿名通信技术,可信计算.

王青龙(1970－),男,博士,副教授,主要研究领域为密码学及其应用.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.