具有多接收者的抗泄露匿名密钥封装机制

周彦伟[1],韩 宇[1],徐 然[1],王 佳[2]
(1. 陕西师范大学计算机科学学院,陕西西安 710119;2. 陕西师范大学信息化建设与管理处,陕西西安 710119)

摘 要: 基于证书的密码体制在继承传统公钥基础设施和身份基密码体制优势的同时,避免了证书管理和密钥托管等不足. 为了向基于证书的密钥封装机制提供匿名性和抗泄露攻击的能力,本文提出具有多接收者的抗泄露匿名密钥封装机制的形式化定义及抵抗泄露攻击的安全模型,并给出具体的实例化构造;同时基于判定的Diffie-Hellman假设的困难性,对上述实例泄露容忍的选择明文攻击安全性进行了证明. 与现有相关构造相比,本文方案不仅具有匿名性、泄露容忍性和多接收者等更优的性能,而且当为多个用户生成封装密钥时具有更优的计算效率.

关键词: 基于证书密码体制;密钥封装机制;多接收者;泄露容忍
基金项目: 国家自然科学基金(No.62272287)
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2023)12-3431-06
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20221124

Leakage-Resilient Key Encapsulation Mechanism with Anonymity and Multi-Receiver

ZHOU Yan-wei[1], HAN Yu[1], XU Ran[1], WANG Jia[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*;
2. *Department of Information Construction and Management, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*)

Abstract: Certificate-based cryptography combines the best aspects of identity-based encryption (implicit certification management) and public key encryption (no key escrow). To provide the ability of broadcast communication and leakage resilience for the certificate-based key encapsulation mechanism, a new cryptographic primitive, called leakage-resilient key encapsulation mechanism with anonymity and multi-receiver, is proposed in this paper; the formal definition and the leakage-resilient security model of our proposal are also described. The concrete construction of the above cryptographic primitive is created, and the corresponding leakage-resilient chosen-plaintext attacks security is proved based on the hardness of the decisional Diffie-Hellman assumption. The corresponding analysis shows that our scheme has better performance in anonymity, leakage resilience, and multi-receiver and so on; also, better computational efficiency can be achieved when generating encapsulation keys for multiple users.

Key words: certificate-based cryptography; key encapsulation mechanism; multi-receiver; leakage resilience
Foundation Item(s): National Natural Science Foundation of China (No.62272287)

1 引言

混合加密机制拥有公钥加密机制中方便快捷的密钥管理模式,同时还具备对称加密机制的高计算效率[1]特点. 在传统密码机制的安全性证明中,往往假设参与运算的秘密信息是完全保密的. 然而,现实存在的各种泄露攻击能协助敌手获得秘密信息的部分内容,导致其完全保密的前提假设是不成立的. 因此,泄露容忍性已成为当前密码原语的一个必备安全属性[2~6]. 近年来,由于基于证书的密码体制巧妙地规避了公钥证书管理和密钥托管等不足而得到研究者的广泛关注[7~10],然而该领域当前的研究主要关注了加密操作的泄露容忍性,缺乏对抗泄露密钥封装机制的讨论. 为进一步增强安全性,需研究具有多接收者的抗泄露匿名的基于证书的密钥封装机制(Certificate-based Key Encapsulation Mechanism,CB-KEM)以满足实际环境对泄露容忍性、匿名性等安全性质的应用需求.

在2003年的欧密会上Gentry提出了基于证书的新

收稿日期:2022-10-09;修回日期:2023-07-30;责任编辑:李勇锋

型公钥密码体制,其中用户自行生成公私钥对后向第三方证书权威(Certificate Authority,CA)申请秘密的证书,该证书在使用中充当了用户的部分私钥(事实上不是私钥),因此它很好地解决了公钥基础设施的证书管理问题,同时避免了身份基密码体制的密钥托管不足. 文献[11]和[12]分别提出了标准模型下安全的CB-KEM;文献[13]提出了带标签的CB-KEM;文献[14]提出了计算效率更优的CB-KEM;文献[15]提出具有多接收者的广播加密方案,但接收者不具有匿名性. 当前关于CB-KEM的相关研究主要存在下述不足:(1)未涉及抗泄露性的研究,导致已有的CB-KEM方案在存在泄露的环境下不再具备其原始的安全性;(2)未满足接收者的匿名性保护需求;(3)未考虑多接收者环境下封装密钥的高效分发需求.

针对现实环境对多接收者、泄露容忍性和接收者匿名性的通信需求,在基于证书的密码体制中,本文提出具有多接收者的抗泄露匿名密钥封装机制. 在定义具体算法和安全模型的基础上,设计了具有多接收者的抗泄露CB-KEM方案,并基于判定性Diffie-Hellman(Decisional Diffie-Hellman,DDH)假设的困难性对该实例泄露容忍的选择明文攻击(Chosen-Plaintext Attacks,CPA)安全性进行了形式化证明.

2 基于证书的多接收者密钥封装机制

结合抗泄露基于证书加密机制的形式化定义和安全模型,本节给出基于证书的多接收者密钥封装机制的形式化定义及抗泄露攻击的安全模型. 特别地,本文中的强随机性提取器、DDH假设等基础知识详见文献[5,6,8~10].

2.1 形式化定义

一个基于证书的多接收者密钥封装机制由下述5个多项式时间算法组成:

(1)初始化. 输入安全参数κ,CA运行算法Setup生成系统公开参数Params和系统主密钥msk.

(2)密钥生成. 用户U_{id}执行随机化的密钥生成算法KeyGen,输入公开参数Params和用户身份$\mathrm{id}\in\mathcal{ID}$,输出用户$U_{\mathrm{id}}$的公私钥对$(\mathrm{pk}_{\mathrm{id}},\mathrm{sk}_{\mathrm{id}})$.

(3)证书生成. CertGen是由CA执行的算法,给定用户U_{id}的身份id和公钥$\mathrm{pk}_{\mathrm{id}}$,CA基于主私钥msk为用户生成证书$\mathrm{Cert}_{\mathrm{id}}$,并将其返回给$U_{\mathrm{id}}$.

(4)多接收者密钥封装. Encap是由发送者执行的随机化算法,输入系统参数Params,接收者身份$\mathrm{ID}=\{\mathrm{id}_1,\cdots,\mathrm{id}_n\}$及公钥集合$\mathrm{pk}=\{\mathrm{pk}_1,\cdots,\mathrm{pk}_n\}$,输出封装密文$C$及对应的封装密钥$k$.

(5)解封装. Decap是由接收者执行的确定性算法,发送者指定的接收者使用各自的私钥$\mathrm{sk}_{\mathrm{id}}$和证书$\mathrm{Cert}_{\mathrm{id}}$对封装密文$C$进行解封装,输出封装密钥$k$或无效符号$\perp$.

2.2 正确性

基于证书的多接收者密钥封装机制的正确性要求对于接收者集合ID中的任意身份$\mathrm{id}_i\in\mathrm{ID}$,有

$$\Pr\left[k\neq k'\ \middle|\ \begin{array}{c}(\mathrm{pk}_i,\mathrm{sk}_i)\leftarrow\mathrm{KeyGen}(\mathrm{id}_i),\\ \mathrm{Cert}_i\leftarrow\mathrm{CertGen}(\mathrm{msk},\mathrm{id}_i,\mathrm{pk}_i),\\ (C,k)\leftarrow\mathrm{Encap}(\mathrm{ID},\mathrm{pk}),\\ k'\leftarrow\mathrm{Decap}(\mathrm{sk}_i,\mathrm{Cert}_i,C).\end{array}\right]\leqslant\mathrm{negl}(\kappa)$$

成立,其中$(\mathrm{Params},\mathrm{msk})\leftarrow\mathrm{Setup}(1^{\kappa})$和$\mathrm{negl}(\kappa)$是安全参数$\kappa$上计算可忽略的值.

2.3 匿名性

密钥封装机制的匿名性要求任意用户都无法获知接收者的身份信息,即使是授权接收者集合的成员同样无法获知其他接收者的身份信息. 则对于任意的多项式时间敌手,任何两个授权接收者集合所对应的消息是不可区分的.

2.4 安全性

在CB-KEM安全模型的基础上,本文提出基于证书的多接收者密钥封装机制的安全模型. 类似地,CB-KEM面临着$\mathcal{A}^1$和$\mathcal{A}^2$两类敌手的攻击,其中$\mathcal{A}^1$能用其已知的信息替换任意用户的公钥;$\mathcal{A}^2$拥有系统主私钥,但不具备替换用户公钥的能力.

2.4.1 敌手$\mathcal{A}^1$攻击下的泄露容忍的CPA安全性

如果不存在多项式时间敌手$\mathcal{A}^1$,能以不可忽略的优势在实验$\mathrm{Exp}^{\text{LR-CPA}}_{\text{KEM},\mathcal{A}^1}(\kappa,\lambda)$中获胜,则在泄露环境下基于证书的多接收者密钥封装机制在$\mathcal{A}^1$的选择明文攻击下具有不可区分性,其中λ是用户私钥的泄露界,其中$\mathcal{O}^{\lambda,\kappa}_{\mathrm{sk}_{\mathrm{id}}}(\cdot)$是泄露谕言机;$\mathcal{O}^{\mathrm{KeyGen}}(\cdot)$是密钥生成谕言机;$\mathcal{O}^{\mathrm{CertGen}}(\cdot)$是证书生成谕言机.

$\underline{\mathrm{Exp}^{\text{LR-CPA}}_{\text{CB-BKEM},\mathcal{A}^1}(\kappa,\lambda)}$:

$(\mathrm{Params},\mathrm{msk})\leftarrow\mathrm{Setup}(\kappa)$;

$\mathrm{ID}^*=\{\mathrm{id}_1^*,\cdots,\mathrm{id}_n^*\}\leftarrow(\mathcal{A}^1)^{\mathcal{O}^{\mathrm{KenGen}}(\cdot),\mathcal{O}^{\mathrm{CertGen}}(\cdot),\mathcal{O}^{\lambda,\kappa}_{\mathrm{sk}_{\mathrm{id}}}(\cdot)}(\mathrm{Params})$;

$(C^*,k_1)=\mathrm{Encap}(\mathrm{ID}^*,\mathrm{pk}^*)$ 和 $k_0\leftarrow_R\mathcal{K}$;

$\beta\leftarrow_R\{0,1\}$;

$\beta'\leftarrow(\mathcal{A}^1)^{\mathcal{O}^{\mathrm{KeyGen}}_{\mathrm{id}\notin\mathrm{ID}^*}(\cdot),\mathcal{O}^{\mathrm{CertGen}}_{\mathrm{id}\notin\mathrm{ID}^*}(\cdot)}(C^*,k_\beta)$;

If $\beta'=\beta$, output 1; Otherwise, output 0.

在$\mathrm{Exp}^{\text{LR-CPA}}_{\text{KEM},\mathcal{A}^1}(\kappa,\lambda)$中,$\mathcal{A}^1$获胜的优势为$\mathrm{Adv}^{\text{LR-CPA}}_{\text{CB-BKEM},\mathcal{A}^1}(\kappa,\lambda)=\left|\begin{array}{l}\Pr\left[\mathrm{Exp}^{\text{LR-CPA}}_{\text{CB-BKEM},\mathcal{A}^1}(\kappa,\lambda)=1\right]\\ -\Pr\left[\mathrm{Exp}^{\text{LR-CPA}}_{\text{CB-BKEM},\mathcal{A}^1}(\kappa,\lambda)=0\right]\end{array}\right|$,其中概率来自随机数的使用及敌手的选择.

2.4.2 敌手 $\mathcal{A}^2$ 攻击下的泄露容忍的 CPA 安全性

如果不存在多项式时间敌手 $\mathcal{A}^2$ 能以不可忽略的优势在实验 $\mathrm{Exp}_{\mathrm{KEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)$ 中获胜,则在泄露环境下基于证书的多接收者密钥封装机制在 $\mathcal{A}^2$ 的适应性选择消息攻击下具有不可区分性.

$\underline{\mathrm{Exp}_{\mathrm{CB\text{-}BKEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)}$:

$(\mathrm{Params},\mathrm{msk})\leftarrow\mathrm{Setup}(\kappa)$;

$\mathrm{ID}^*=\{\mathrm{id}_1^*,\cdots,\mathrm{id}_n^*\}\leftarrow(\mathcal{A}^2)^{\mathcal{O}^{\mathrm{KeyGen}}(\cdot),\mathcal{O}_{sk_{id}}^{\lambda,\kappa}(\cdot)}(\mathrm{Params},\mathrm{msk})$;

$(C^*,k_1)=\mathrm{Encap}(\mathrm{ID}^*)$ 和 $k_0\leftarrow_R\mathcal{K}$;

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

$\beta'\leftarrow(\mathcal{A}^2)^{\mathcal{O}_{\mathrm{id}\neq\mathrm{ID}^*}^{\mathrm{KeyGen}}(\cdot)}(C^*,k_\beta)$;

If $\beta=\beta'$, output 1; Otherwise, output 0.

在 $\mathrm{Exp}_{\mathrm{KEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)$ 中,$\mathcal{A}^2$ 获胜的优势为 $\mathrm{Adv}_{\mathrm{CB\text{-}BKEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)=\left|\begin{matrix}\Pr\left[\mathrm{Exp}_{\mathrm{CB\text{-}BKEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)=1\right]\\-\Pr\left[\mathrm{Exp}_{\mathrm{CB\text{-}BKEM},\mathcal{A}^2}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)=0\right]\end{matrix}\right|$,其中概率来自对随机数的使用及敌手的选择.

定义 1　泄露容忍的 CPA 安全性

对于任意的概率多项式时间敌手 $\mathcal{A}^1$ 和 $\mathcal{A}^2$,若在上述实验中获胜的优势是可忽略的,那么基于证书的多接收者密钥封装机制具有泄露容忍的 CPA 安全性.

3　本文方案

本节将提出基于证书的多接收者密钥封装机制的具体构造,并基于 DDH 假设的困难性对该方案的安全性进行形式化证明.

3.1　具体构造

(1) $(\mathrm{Params},\mathrm{msk})\leftarrow\mathrm{Setup}(1^\kappa)$

设 G 是阶为 p 的乘法循环群,g 是群 G 的生成元. 选取三个哈希函数 $H:G\rightarrow\{0,1\}^{l_k}$,$H_1:\mathcal{ID}\rightarrow Z_p^*$ 和 $H_2:\mathcal{ID}\times G\times G\rightarrow Z_p^*$. 令 $\mathrm{Ext}:G_2\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_k}$ 是平均情况的 $(\log q-\lambda,\varepsilon)$ 强随机性提取器,其中 λ 是泄露参数,ε 是 κ 上计算可忽略的值. 选取 $\alpha\leftarrow_R Z_p^*$ 和 $g_1\leftarrow_R G$,并计算 $g_2=g^\alpha$. 令 $\mathrm{Params}=\{p,G,g,g_1,g_2,H,H_1,H_2,\mathrm{Ext}\}$ 和 $\mathrm{msk}=\alpha$.

(2) $(\mathrm{pk}_{\mathrm{id}},\mathrm{sk}_{\mathrm{id}})\leftarrow\mathrm{KeyGen}(\mathrm{id})$

身份为 *id* 的用户选取 $a,b\leftarrow_R Z_p^*$,并设置 $\mathrm{sk}_{\mathrm{id}}=(a,b)$ 为私钥,$\mathrm{pk}_{\mathrm{id}}=g^{aH_1(\mathrm{id})}g_1^b$ 为公钥.

(3) $\mathrm{Cert}_{\mathrm{id}}\leftarrow\mathrm{CertGen}(\mathrm{msk},\mathrm{id},\mathrm{pk}_{\mathrm{id}})$

CA 选取 $t_{\mathrm{id}}\leftarrow_R Z_p^*$,并计算 $T_{\mathrm{id}}=g^{t_{\mathrm{id}}}$;然后计算 $u_{\mathrm{id}}=t_{\mathrm{id}}+\alpha H_2(\mathrm{id},T_{\mathrm{id}},\mathrm{pk}_{\mathrm{id}})$. 最后返回相应的证书 $\mathrm{Cert}_{\mathrm{id}}=\{T_{\mathrm{id}},u_{\mathrm{id}}\}$ 给用户,其中 T_{id} 与 $\mathrm{pk}_{\mathrm{id}}$ 一起公开,u_{id} 是 $\mathrm{Cert}_{\mathrm{id}}$ 的核心部分需秘密保存.

(4) $(C,k)\leftarrow\mathrm{Encap}(\mathrm{ID},\mathrm{PK}_{\mathrm{ID}})$

选取 $r\leftarrow_R Z_p^*$,计算 $U_1=g^r$ 和 $U_2=g_1^r$. 选取 $\eta\leftarrow_R Z_p^*$ 和 $S\leftarrow_R\{0,1\}^{l_t}$,计算 $k=\mathrm{Ext}(U_2^\eta,S)$. 对集合 $\mathrm{ID}=\{\mathrm{id}_1,\cdots,\mathrm{id}_n\}$ 中的每个身份 id_i 计算 $N_i=(\mathrm{pk}_iT_i)^r g_2^{rH_2(\mathrm{id}_i,T_i,\mathrm{pk}_i)}$. 对于 i 从 1 到 n,计算 $k_i=\mathrm{Ext}(N_i,S)$;构造 n 阶多项式 $f(x)=k+\prod_{i=1}^{n}(x-k_i)$,将该式展开后可表示为 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x_n$,其中 $a_{i(i=0,1,\cdots,n-1)}\in Z_p^*$. 令 $\boldsymbol{A}=\{a_0,a_1,\cdots,a_{n-1}\}$. 最后输出封装密文 $C=(U_1,U_2,\boldsymbol{A},S)$ 及封装密钥 k.

(5) $k\leftarrow\mathrm{Decap}(C,\mathrm{sk}_{\mathrm{id}},\mathrm{Cert}_{\mathrm{id}})$

计算 $N_i=U_1^{aH(\mathrm{id}_i)+u_i}U_2^b$. 基于 $\boldsymbol{A}=\{a_0,\cdots,a_{n-1}\}$ 构造多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x_n$. 最后计算 $k_i=\mathrm{Ext}(N_i,S)$,并输出封装密钥 $k=f(k_i)$.

3.2　正确性

$$\begin{aligned}U_1^{aH(\mathrm{id}_i)+u_i}U_2^b&=g^{r(aH(\mathrm{id}_i)+u_i)}g_1^{rb}=g^{raH(\mathrm{id}_i)}g^{ru_i}g_1^{rb}\\&=\left(g^{aH(\mathrm{id}_i)}g_1^b\right)^r g^{r(t_{id}+\alpha H_2(\mathrm{id}_i,T_i,\mathrm{pk}_i))}\\&=\mathrm{pk}_i^r\left(g^{t_i}\right)^r g_2^{rH_2(\mathrm{id}_i,T_i,\mathrm{pk}_i)}\\&=(\mathrm{pk}_iT_i)^r g_2^{rH_2(\mathrm{id}_i,T_i,\mathrm{pk}_i)}\end{aligned}$$

3.3　安全性

定理 1　对于 $\lambda\leqslant\log q-l_k-\omega(\log\kappa)$,若 DDH 假设是困难的,那么本文具有多接收者的匿名密钥封装机制具有泄露容忍的 CPA 安全性.

本文通过下述两个引理完成对定理 1 的证明. 其中引理 1 表明本文构造在敌手 $\mathcal{A}^1$ 的选择明文攻击下具有泄露容忍的 CPA 安全性;引理 2 表明本文构造在敌手 $\mathcal{A}^2$ 的选择明文攻击下具有泄露容忍的 CPA 安全性.

引理 1　对于 $\lambda\leqslant\log q-l_k-\omega(\log\kappa)$,若敌手 $\mathcal{A}^1$ 能以优势 $\mathrm{Adv}_{\mathrm{KEM},\mathcal{A}^1}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)$ 攻破本文构造泄露容忍的 CPA 安全性,那么存在算法 $\mathcal{B}$ 能以优势 $\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\kappa)\geqslant\left(1-\frac{n}{Q_1+Q_2+n}\right)\mathrm{Adv}_{\mathrm{KEM},\mathcal{A}^1}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda)$,解决 DDH 困难问题假设的困难性,其中 $\mathcal{A}^1$ 所进行的私钥和证书生成询问的次数分别是 Q_1 和 Q_2,此外 n 是接收者的数量.

证明　算法 $\mathcal{B}$ 与敌手 $\mathcal{A}^1$ 间在进行泄露容忍的 CPA 安全性游戏之前,从 DDH 的挑战者处获得相应的挑战元组 (g,g^x,g^y,Γ) 及公开元组 (p,g,G). 此外,$\mathcal{B}$ 借助列表 L 记录 $\mathcal{A}^1$ 所提交的询问信息及生成的相应应答.

$\mathcal{B}$ 与 $\mathcal{A}^1$ 间的消息交互过程如下所述:

(1)**初始化** 该阶段算法$\mathcal{B}$进行下述操作:选取三个哈希函数$H:G\to\{0,1\}^{l_k}$,$H_1:\mathcal{ID}\to Z_p^*$和$H_2:\mathcal{ID}\times G\times G\to Z_p^*$. 令 Ext:$G_2\times\{0,1\}^{l_t}\to\{0,1\}^{l_k}$是平均情况的$(\log q-\lambda,\varepsilon)$强随机性提取器. 令$g_1=g^x$,随机选取$\alpha\leftarrow_R Z_p^*$计算$g_2=g^{\alpha}$. 发送系统参数 Params=$\{p,G,g,g_1,g_2,H,H_1,H_2,\text{Ext}\}$给$\mathcal{A}^1$,并秘密保存主私钥$\text{msk}=\alpha$.

(2)**阶段 1** 敌手$\mathcal{A}^1$向算法$\mathcal{B}$适应性地提交多项式次下述询问.

① 公钥生成询问. 敌手$\mathcal{A}^1$提交关于 id 的公钥生成询问,若$(\text{id},\text{sk}_{\text{id}},\text{pk}_{\text{id}})\in L$,则$\mathcal{B}$返回$\text{pk}_{\text{id}}$给$\mathcal{A}^1$;否则,算法$\mathcal{B}$选取$a,b\leftarrow_R Z_p^*$,并计算$\text{sk}_{\text{id}}=(a,b)$和$\text{pk}_{\text{id}}=g^{aH_1(\text{id})}g_1^b$,返回$\text{pk}_{\text{id}}$给$\mathcal{A}^1$,并在$L$中添加$(\text{id},\text{sk}_{\text{id}},\text{pk}_{\text{id}})$.

② 私钥生成询问. $\mathcal{A}^1$提交关于 id 的私钥生成询问,若$(\text{id},\text{sk}_{\text{id}},\text{pk}_{\text{id}})\in L$,则$\mathcal{B}$返回$\text{sk}_{\text{id}}$给$\mathcal{A}^1$;否则,对 id 进行公钥生成询问后返回$\text{sk}_{\text{id}}$给$\mathcal{A}^1$.

③ 证书生成询问. 敌手$\mathcal{A}^1$提交关于$(\text{id},\text{pk}_{\text{id}})$的证书生成询问,$\mathcal{B}$随机选取$t_{\text{id}}\leftarrow_R Z_p^*$,计算$T_{\text{id}}=g^{t_{\text{id}}}$和$u_{\text{id}}=t_{\text{id}}+\alpha H_2(\text{id},T_{\text{id}},\text{pk}_{\text{id}})$,然后返回$\text{Cert}_{\text{id}}=(T_{\text{id}},u_{\text{id}})$给$\mathcal{A}^1$.

④ 公钥替换询问. 敌手$\mathcal{A}^1$通过该询问可将身份 id 的公钥pk_{id}替换为pk'_{id}.

⑤ 泄露询问. 敌手$\mathcal{A}^1$向算法$\mathcal{B}$提交泄露询问$(\text{id},f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i})$,其中$f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}$是高效可计算的泄露函数. 若$(\text{id},\text{sk}_{\text{id}},\text{pk}_{\text{id}})\in L$,那么返回$\text{sk}_{\text{id}}$对应的$f_i(\text{sk}_{\text{id}})$给$\mathcal{A}^1$;否则,对$id$进行私钥生成询问后返回$f_i(\text{sk}_{\text{id}})$给$\mathcal{A}^1$. 特别地,在整个生命周期内$\mathcal{A}^1$获得同一私钥$\text{sk}_{\text{id}}$的泄露总量不能超过$\lambda$.

(3)**挑战** 敌手$\mathcal{A}^1$提交挑战身份集合$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$给算法$\mathcal{B}$,其中对$\text{id}_i\in\text{ID}^*$未提交私钥生成询问和证书生成询问. 算法$\mathcal{B}$通过下述操作生成挑战封装密文及对应的封装密钥:

① 令$U_1=g^y$(隐含地设置$r=y$)和$U_2=\Gamma$.

② 对$\text{id}_i\in\text{ID}^*$,计算身份$\text{id}_i$相对应的公钥$\text{pk}_i=g^{a_iH_1(id_i)}g_1^{b_i}$和私钥$sk_i=(a_i,b_i)$;对$\text{id}_i\in\text{ID}^*$,选取$t_i\leftarrow_R Z_p^*$,计算$id_i$相对应的证书$\text{Cert}_i=(T_i,u_i)=(g^{t_{\text{id}}},t_i+\alpha H_2(\text{id},T_i,\text{pk}_i))$.

③ 随机选取$\eta\leftarrow_R Z_p^*$和$S\leftarrow_R\{0,1\}^{l_t}$,计算$k_\beta=\text{Ext}(U_2^\eta,S)$. 对集合$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$中的每个身份$\text{id}_i$计算$N_i=U_1^{a_iH(\text{id}_i)+u_i}U_2^{b_i}$.

④对于i从 1 到n,计算$k_i=\text{Ext}(N_i,S)$;构造n阶多项式$f(x)=k+\prod_{i=1}^{n}(x-k_i)$,其展开后为$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x_n$,其中$a_{i(i=0,1,\cdots,n-1)}\in Z_p^*$. 令$\boldsymbol{A}=\{a_0,a_1,\cdots,a_{n-1}\}$. 最后输出封装密文$C=(U_1,U_2,\boldsymbol{A},S)$及封装密钥$k_\beta$.

当$\Gamma=g^{xy}$时,$U_2=g^{xy}=g_1^y$,则k_β是与挑战密文$C=(U_1,U_2,\boldsymbol{A},S)$相对应的封装密钥;当$\Gamma\leftarrow_R G$时,则由随机性提取器的安全性可知$k_\beta$是封装密钥空间上的一个随机值.

(4)**阶段 2** 算法$\mathcal{B}$使用与阶段 1 相同的方式应答敌手$\mathcal{A}^1$提出的相关询问. 特别地,集合$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$的身份都不能在$\mathcal{A}^1$的私钥和证书的生成询问中出现;并且$\mathcal{A}^1$也不能提交泄露询问.

(5)**输出** 敌手$\mathcal{A}$输出对β的猜测β'. 若$\beta'=1$,$\mathcal{B}$输出 1,意味着$\Gamma=g^{xy}$;否则,$\mathcal{B}$输出 0,意味着$\Gamma\leftarrow_R G$.

令事件$\mathcal{E}$表示$\mathcal{A}^1$对集合$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$中的任何身份未进行私钥和证书的生成询问,那么有$\Pr[\mathcal{E}]=1-\frac{n}{Q_1+Q_2+n}$. 特别地,对于$\mathcal{A}^1$而言,挑战身份的私钥和证书是不允许其掌握的,一旦挑战身份在相应的询问中出现过,那么$\mathcal{B}$将终止该游戏. 上述询问中$\mathcal{A}^1$共提交了Q_1+Q_2+n个不同的身份.

由底层强随机性提取器 Ext 的安全性可知$\lambda\leqslant\log q-l_k-\omega(\log\kappa)$,其中$\omega(\log\kappa)$表示计算过程中的额外泄露量. 若$\mathcal{A}^1$能以优势$\text{Adv}_{\text{KEM},\mathcal{A}^1}^{\text{LR-CPA}}(\kappa,\lambda)$攻破本文构造泄露容忍的 CPA 安全性,且$\mathcal{A}^1$对$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$中的身份未进行私钥和证书的生成询问,那么$\mathcal{B}$以不可忽略的优势$\text{Adv}_{\mathcal{B}}^{\text{DDH}}(\kappa)\geqslant\left(1-\frac{n}{Q_1+Q_2+n}\right)\text{Adv}_{\text{KEM},\mathcal{A}^1}^{\text{LR-CPA}}(\kappa,\lambda)$解决 DDH 假设的困难性.

引理 2 对于$\lambda\leqslant\log q-l_k-\omega(\log\kappa)$,若存在敌手$\mathcal{A}^2$能以优势$\text{Adv}_{\text{KEM},\mathcal{A}^2}^{\text{LR-CPA}}(\kappa,\lambda)$攻破本文构造泄露容忍的 CPA 安全性,那么存在算法$\mathcal{B}$能以优势$\text{Adv}_{\mathcal{B}}^{\text{DDH}}(\kappa)\geqslant\left(1-\frac{n}{Q_1+n}\right)\text{Adv}_{\text{KEM},\mathcal{A}^2}^{\text{LR-CPA}}(\kappa,\lambda)$,解决 DDH 假设的困难性.

在引理 1 的证明中,由于算法$\mathcal{B}$持有完整的主私钥,因此该方法依然可用于对引理 2 的证明. 由于已知晓主私钥,$\mathcal{A}^2$无需进行证书生成询问,因此$\mathcal{A}^2$对$\text{ID}^*=\{\text{id}_1,\cdots,\text{id}_n\}$中的身份未进行私钥生成询问的概率为$1-\frac{n}{Q_1+n}$.

3.4 匿名性

在传统具备广播通信功能的协议中,为确保接收者能够从参数向量中准备定位属于自己的元素,发送者通常会将授权的接收者集合随通信信息一起发送,导致相关构造[15]无法满足接收者的匿名性需求. 然而

在本文构造中,接收者的身份集合是不随封装密文一起发送的,授权的接收者基于自己的私钥即可恢复出原始的封装密钥,因此本文的密钥封装机制具有接收者匿名性.

3.5　连续泄露容忍性

在实际环境中,敌手往往会发起持续的泄露攻击,这要求密码原语应具备抗连续泄露攻击的能力. Dodis等[16]指出在保持公开信息不变的情况下可通过定期更新私有秘密的方式能够将密码机制的有界泄露容忍性转换为连续泄露容忍性. 因此,下面将通过改进本文基础构造的密钥生成算法为其提供抵抗连续泄露攻击的能力.

(1)密钥生成. 身份为id的用户选取 $a_1,b_1,a_2,b_2\leftarrow_R Z_p^*$,令 $\mathrm{sk}_{\mathrm{id}}=(a_1,b_1,a_2,b_2)$ 为私钥,$\mathrm{pk}_{\mathrm{id}}=g^{(a_1+a_2)H_1(\mathrm{id})}g_1^{b_1+b_2}$ 为公钥. 特别地,将原始解封装算法中 N_i 的计算过程更改为 $N_i=U_1^{(a_1+a_2)H(\mathrm{id}_i)+u_i}U_2^{b_1+b_2}$,封装算法和解封装算法的其他计算均保持不变.

(2)密钥更新. 身份为id的用户随机选取 $c,d\leftarrow_R Z_p^*$,对原始的用户私钥 $\mathrm{sk}_{\mathrm{id}}=(a_1,b_1,a_2,b_2)$ 进行更新操作,产生更新后的私钥 $\mathrm{sk}'_{\mathrm{id}}=(a'_1,b'_1,a'_2,b'_2)$,其中 $a'_1=a_1+c,b'_1=b_1+d,a'_2=a_2-c$ 和 $b'_2=b_2-d$.

密钥封装机制的公开参数和功能在上述更新过程中保持不变. 此外,随机数的使用确保更新后的私钥与原始私钥是不可区分的. 由上述构造可知,连续泄露容忍性的核心本质是要构建私钥与公钥间的多对一映射关系,那么私钥在更新过程中其对应的公钥依然保持不变.

3.6　性能对比

由于目前尚未有具有多接收者的抗泄露匿名密钥封装机制的相关研究,本节将对本文构造与相应CB-KEM[12~14]同时生成 n 个封装密钥时的计算效率进行对比. 为清晰地展示计算效率间的对比结果,本文在个人电脑(配置为Intel(R) Core i3-2310,CPU@2.10 GHz,4 GB内存和Ubuntu 14.04操作系统)上对基础密码操作的运行时间进行了模拟,通过统计10次运行时间的平均值,可知双线性映射的运算时间为2.483 ms,群上的指数运算时间为0.316 ms,群上的乘运算时间为0.059 ms和群上的加运算时间为0.001 ms. 针对不同的接收者数量,本文与相关构造[12~14]的计算效率比较结果如表1所示;计算效率随接收者数量 n 的变化情况如图2所示. 由图1可知,本文方案具有更优的计算效率. 由图2可知,文献[12]的计算效率受接收者数量影响最大,文献[13]的方案次之,接着是文献[14],本文方案受接收者数量的影响最小.

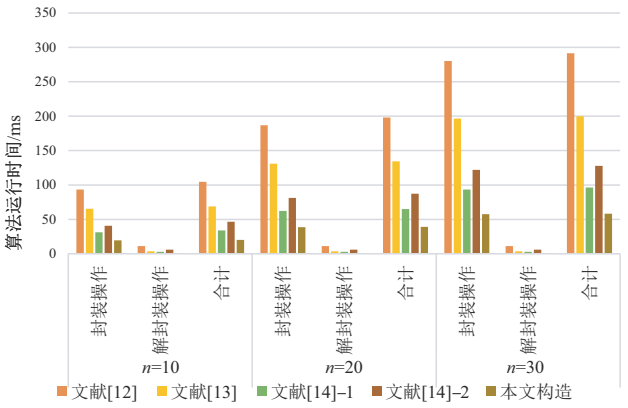


图1　CB-KEM的计算效率比较结果

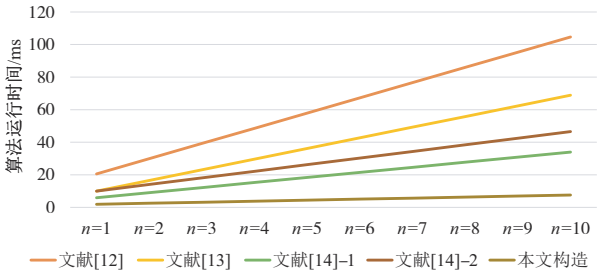


图2　CB-KEM中计算效率随接收者数量的变化情况

4　结论

针对现实环境对密钥封装机制的多接收者、抵抗泄露攻击和匿名性等性能的真实需求,在基于证书的密码体制下,本文设计了具有多接收者的抗泄露匿名密钥封装机制,并基于DDH假设的困难性对本文方案的安全性进行了证明. 与现有相关方案的对比结果表明,本文构造在性能和计算效率等方面均具有一定的优势. 现有广播加密机制的密文长度与接收者数量呈线性关系,下一阶段在保证性能和计算效率的基础上,我们将基于本文CB-KEM的构造,研究具有固定密文长度的广播加密机制,进一步提高广播加密机制的传输效率. 此外,还将考虑高效实现CB-KEM的选择密文攻击安全性.

参考文献

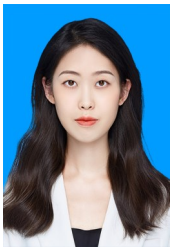
[1] CHOW S S M, LIU J K, ZHOU J Y. Identity-based online/offline key encapsulation and encryption[C]//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2011: 52-60.

[2] LYU L, LIU S L, GU D W. Structure-preserving public-key encryption with leakage-resilient CCA security[J]. Theoretical Computer Science, 2019, 795: 57-80.

[3] LI J G, YU Q H, ZHANG Y C. Identity-based broadcast encryption with continuous leakage resilience[J]. Information Sciences, 2018, 429: 177-193.
[4] LI J G, YU Q H, ZHANG Y C. Key-policy attribute-based encryption against continual auxiliary input leakage[J]. Information Sciences, 2019, 470: 175-188.
[5] ZHOU Y W, YANG B. Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing[J]. Information Processing Letters, 2018, 130: 16-24.
[6] ZHOU Y W, YANG B. Continuous leakage-resilient certificateless public key encryption with CCA security[J]. Knowledge-Based Systems, 2017, 136: 27-36.
[7] LU Y, LI J G. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds [J]. Future Generation Computer Systems, 2016, 62: 140-147.
[8] LU Y, LI J G. A provably secure certificate-based encryption scheme against malicious CA attacks in the standard model[J]. Information Sciences, 2016, 372: 745-757.
[9] GUO Y Y, LI J G, LU Y, et al. Provably secure certificate-based encryption with leakage resilience[J]. Theoretical Computer Science, 2018, 711: 1-10.
[10] ZHOU Y W, YANG B, WANG T, et al. Continuous leakage-resilient certificate-based encryption scheme without bilinear pairings[J]. The Computer Journal, 2020, 63(4): 508-524.
[11] 李继国, 杨海珊, 张亦辰. 标准模型下安全的基于证书密钥封装方案[J]. 电子学报, 2012, 40(8): 1577-1583.
LI J G, YANG H S, ZHANG Y C. Secure certificate-based key encapsulation scheme under standard model[J]. Acta Electronica Sinica, 2012, 40(8): 1577-1583. (in Chinese)
[12] 陆阳, 李继国. 标准模型下高效安全的基于证书密钥封装机制[J]. 计算机研究与发展, 2014, 51(7): 1497-1505.
LU Y, LI J G. Efficient and provably-secure certificate-based key encapsulation mechanism in the standard model [J]. Journal of Computer Research and Development, 2014, 51(7): 1497-1505. (in Chinese)
[13] 李继国, 杨海珊, 张亦辰. 带标签的基于证书密钥封装机制[J]. 软件学报, 2012, 23(8): 2163-2172.
LI J G, YANG H S, ZHANG Y C. Certificate-based key encapsulation mechanism with tags[J]. Journal of Software, 2012, 23(8): 2163-2172. (in Chinese)
[14] LU Y, LI J G. Efficient constructions of certificate-based key encapsulation mechanism[J]. International Journal of Internet Protocol Technology, 2014, 8(2/3): 96-106.
[15] 赖建昌, 黄欣沂, 何德彪. 一种基于商密SM9的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897-907.
LAI J C, HUANG X Y, HE D B. An efficient identity-based broadcast encryption scheme based on SM9[J]. Chinese Journal of Computers, 2021, 44(5): 897-907. (in Chinese)
[16] DODIS Y, HARALAMBIEV K, LOPEZ-ALT A, et al. Cryptography against continuous memory attacks[C]// 2010 IEEE 51st Annual Symposium on Foundations of Computer Science. Piscataway: IEEE, 2010: 511-520.

作者简介

周彦伟 男, 1986年4月出生于甘肃省通渭县. 现为陕西师范大学计算机科学学院副教授、硕士生导师. 在国内外学术期刊发表论文80余篇. 主要研究方向为密码学、信息安全.
E-mail: zyw@snnu.edu.cn



韩 宇 女, 2000年4月出生于山西省太原市. 现为陕西师范大学计算机科学学院硕士研究生.

徐 然 女, 1999年10月出生于山东省泰安市. 现为陕西师范大学计算机科学学院硕士研究生.

王 佳(通讯作者) 女, 1988年11月出生于陕西省榆林市. 现为陕西师范大学信息化建设与管理处工程师.
E- mail: wangjia@snnu.edu.cn