标准模型下安全的基于证书密钥封装方案

李继国,杨海珊,张亦辰
(河海大学计算机与信息学院,江苏南京 211000)

摘 要: 混合加密是将公钥加密与对称加密结合的一种加密技术.将密钥封装机制引入到基于证书加密方案中,提出了基于证书密钥封装机制的形式化定义及安全模型,构造了一个基于证书密钥封装方案.基于判定双线性 Diffie-Hellman 困难问题假定,在标准模型下证明提出的方案是自适应选择密文安全的.

关键词: 密钥封装机制; 基于证书加密; 标准模型; 双线性对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 08-1577-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.08.013

Certificate-Based Key Encapsulation Mechanism Secure in the Standard Model

LI Ji-guo, YANG Hai-shan, ZHANG Yi-chen
(*College of Computer and Information Engineering, Hohai University, Nanjing, Jiangsu* 211000, *China*)

Abstract: A hybrid construction is a formal method of combining asymmetric encryption and symmetric encryption. By introducing key encapsulation mechanism into certificate-based encryption scheme, we propose a formal definition and security model of the certificate-based key encapsulation mechanism. Furthermore, we present a construction of the certificate-based key encapsulation scheme. Based on decision bilinear Diffie-Hellman difficulty assumption, the proposed scheme is provably secure against indistinguishability under adaptive chosen-ciphertext attack in the standard model.

Key words: key encapsulation mechanism; certificate-based encryption; standard model; bilinear pairing

1 引言

2003 年,Gentry[1]在欧密会上提出了一种新型公钥密码系统——基于证书密码系统.与基于身份和传统公钥密码系统相比,克服了基于身份密码体制中的密钥托管和密钥分发问题;基于证书密码体制中的隐含证书机制消除了传统公钥密码系统中对证书状态的第三方询问问题,同时可以使用子集覆盖技术减少传统 PKI 系统中证书撤销的计算量.这种新型公钥密码体制为构建安全、高效的 PKI 提供了有效的方法[1].同时基于证书密码体制还能够为可信计算模块的证书发放和撤销提供新方法,也是可信计算公钥基础设施的重要构件,可用于可信计算平台身份证明方法即隐私 CA 的构造[2].因此,开展对基于证书密码体制的研究具有重要的理论意义和广泛的应用价值.

近年来,许多基于证书加密方案被提出.2004 年,Yum 和 Lee[3]从理论上分析了基于证书加密(CBE)方案、基于身份加密(IBE)方案和无证书加密(CLE)方案之间的归约关系,给出了由双重 IBE 方案获得 CBE 方案和 CLE 方案的通用构造方法.Galindo 等人[4]指出 Yum 和 Lee 的通用构造在选择密文攻击下是不安全的,并给出了具体的攻击方法.2005 年,Al-Riyami 和 Paterson[5]分析了 Gentry[1]提出的 CBE 形式化定义和安全模型,并做了一些补充和修改,提出了从任意选择密文安全的无证书公钥加密方案构造同等安全强度的 CBE 方案的通用方法.以上 CBE 方案的缺陷是只在随机预言模型下证明方案的安全性,而随机预言模型下的安全性证明只是一种启发式证明,这并非是严格意义上的可证安全性.因此,构造标准模型下可证安全的方案成了研究热点.2008 年,Galindo、Morillo 和 Ràfols[6]基于 Waters[7]的 IBE 方案提出了在标准模型下选择密文安全的 CBE 方案.2008 年,Liu 和 Zhou[8]基于 Gentry[9]的 IBE 方案提出了一个在标准模型下自适应选择密文安全的 CBE 方案.

一般情况下,使用公钥密码系统加密,对明文空间

收稿日期:2011-08-23 修回日期:2012-01-19
基金项目:国家自然科学基金(No.60842002,61103183,61103184);中国博士后基金(No.20100471373);江苏省"六大人才高峰"项目 (No.2009182);中央高校基本科研业务费专项资金资助项目(No.2009B21114,2010B07114);河海大学优秀创新人才支持计划

有限制或要求明文属于某个群,这在实际应用中是不实用的.使用公钥密码系统加解密速度比较慢,效率不高.而使用对称密码体制不仅加解密速度快,而且还没有对明文长度限制的优势,但存在密钥管理困难问题.基于速度和安全的考虑,有些学者结合两种密码体制的优点提出了混合密码的思想,即用对称加密算法对需要通信的数据进行加解密,用公钥加密算法对对称加密的密钥进行加密.混合加密的思想虽然简单,但是它的实现方式却各种各样.由于没有精确的形式化定义,许多看似安全的方案[10]被证明是不安全的.

直到 2003 年,Cramer 和 Shoup[11]第一次形式化定义了混合加密的安全模型,即采用密钥封装机制(KEM)与数据封装机制(DEM)进行组合,其模型简记 KEM/DEM.KEM 与公钥加密相似,只是加密的任务变为生成一个随机密钥及对该随机密钥的封装,也就是说加密算法除了一个随机值和接收者的公钥外没有其它输入,生成一个对称密钥以及对该对称密钥的加密.DEM 是一个一次密钥对称加密方案,即每个密钥只用于一条消息的加密.安全的 KEM 是构成安全的混合加密不可或缺的组成部分,因此对它的研究逐渐成为一个热点,许多 KEM 方案及相关的混合加密、混合签密方案也被相继提出[12~14].在 2005 年,Bentahar 等[15]第一次将密钥封装机制与基于身份密码系统和无证书密码系统结合,提出了基于身份的密钥封装机制和无证书密钥封装机制,并给出了在随机预言模型下可证安全的基于身份密钥封装的一般构造和无证书密钥封装的一般构造.随后,Chen 等[16]提出了基于身份密钥封装机制的具体构造.Huang 等[17]首次提出了在标准模型下安全的无证书密钥封装机制的一般构造,并在无证书密钥封装机制中引入了标签,提出了带标签的无证书密钥封装机制,从而将基于标签的密钥封装机制扩展到无证书方案中.到目前,又有许多学者提出高效的或者是标准模型下安全的基于身份或者无证书密钥封装及混合加密[18~20].

自从密钥封装机制提出后,已有不少学者对基于身份密钥封装机制和无证书密钥封装机制进行研究.结合密钥封装机制和基于证书加密方案的优点,本文将密钥封装机制引入到基于证书加密方案中,提出基于证书密钥封装机制的形式化定义和安全模型.在此基础上,构造了一个基于证书密钥封装方案,并在标准模型下证明该方案是自适应选择密文安全的.

2 困难问题假设

定义 1 双线性映射 令 G_1、G_2 是素数 q 阶乘法循环群,g 为群 G_1 的生成元.一个可计算的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 具有以下性质:(1)双线性:对任意 $a, b \in Z_q^*$,有 $e(g^a, g^b) = e(g, g)^{ab}$;(2)非退化性:$e(g, g) \neq 1$;(3)可计算性:存在有效的算法来计算 e.

定义 2 双线性 Diffie-Hellman 问题(BDHP) 给定群元素(g, g^a, g^b, g^c),其中 $a, b, c \in Z_q^*$,计算 $e(g, g)^{abc}$.

概率多项式时间算法 A 解决 $< G_1, G_2 >$ 上的 BDH 问题的优势定义为 $Succ_{A, G_1, G_2}^{BDH} = \Pr[A(g, g^a, g^b, g^c) = e(g, g)^{abc} : a, b, c \in Z_q^*]$.

如果任意的概率多项式时间算法 A 解决 $< G_1, G_2 >$ 上的 BDH 问题的优势都是可忽略的,则称 $< G_1, G_2 >$ 的 BDH 问题是困难的.

定义 3 判定双线性 Diffie-Hellman 问题(DBDHP) 对于 $a, b, c \in Z_q^*$,给定群元素(g, g^a, g^b, g^c)以及 $T \in G_2$,判断 $T = e(g, g)^{abc}$是否成立.如果成立则输出 1,否则输出 0.

概率多项式时间算法 A 解决 $< G_1, G_2 >$ 上的 DBDH 问题的优势定义为 $Succ_{A, G_1, G_2}^{DBDH} = |\Pr[A(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[A(g, g^a, g^b, g^c, T) = 1]|$,其中 $a, b, c \in Z_q^*$.

如果任意的概率多项式时间算法 A 解决 $< G_1, G_2 >$ 上的 DBDH 问题的优势都是可忽略的,则称 $< G_1, G_2 >$ 的 DBDH 问题是困难的.

3 基于证书密钥封装机制的形式化定义及安全模型

3.1 基于证书密钥封装机制的形式化定义

基于证书密钥封装机制由五个算法组成(Setup, UserKeyGen, Certify, Encap, Decap),其中系统参数设置和证书产生算法由证书认证中心(CA)运行,用户密钥生成算法、密钥封装算法和密钥解封装算法由用户执行.

系统参数设置算法(Setup): 以安全参数 k 为输入的概率多项式时间算法,CA 运行此算法产生主密钥 MSK 和系统参数 $params$(包含对串空间的描述以及主公钥 P_{pub}).CA 将系统参数公开.

用户密钥生成算法(UserKeyGen): 用户获得系统参数 $params$ 后,运行此算法生成用户私钥 SK 和用户公钥 PK.

证书产生算法(Certify): 给定用户的身份信息 ID 和用户公钥 PK,以及时间段 τ,输入(MSK, $params$, τ, ID, PK),输出用户在时间 τ 内的证书 $Cert_{ID, \tau}$,并将 $Cert_{ID, \tau}$ 通过公开信道发送给用户.

密钥封装算法(Encap): 该算法输入(τ, $params$, ID, PK),输出密钥封装对(K, C),其中 $K \in \kappa_D$ 为数据封装的加密密钥,C 为对密钥 K 的封装.

密钥解封装算法(Decap): 在时间段 τ 内输入

($params$, $Cert_{ID,\tau}$, SK, C),运行解封装算法,输出密钥 K,或者无效标志⊥.

3.2 基于证书密钥封装机制的安全模型

参考 Cramer 和 Shoup[11]提出的 KEM 的安全模型以及 Li 等人[21~23]提出的基于证书的安全模型,提出了基于证书密钥封装机制的安全模型.

基于证书密钥封装方案包含两类敌手 A_I 和 A_{II}. A_I 模拟了一个不诚实的用户,它不知道系统主密钥,但可以替换公钥以及询问任何用户的私钥,可以获得除目标用户外任意用户的证书,可以进行除目标封装外的其它解封装询问. A_{II}模拟了一个恶意的 CA,它拥有主密钥,可以生成任何用户的证书,但不可以进行替换公钥, A_{II}还可以询问除目标用户外任何用户的私钥,可以对除目标封装外的其它密钥封装进行解封装询问.

基于证书密钥封装方案的安全模型是通过挑战者与敌手之间的游戏来定义的.根据敌手的分类,基于证书密钥封装的安全模型定义如下:

游戏 1

系统参数设置:挑战者运行算法 Setup,返回主密钥 MSK 和系统参数 $params$,保密主密钥 MSK,把系统参数 $params$ 发送给 A_I.

第一阶段询问:在这一阶段中,挑战者维护一个记录用户 ID_i 私钥和公钥的表 $L_0 = \{ID_i, PK_i, SK_i, f_i\}$,该表初始为空, $f_i = 0$ 表示用户公钥没有被替换, $f_i = 1$ 表示公钥被替换. A_I 向挑战者进行如下询问:

(1)公钥询问　敌手 A_I 对 ID_i 进行公钥询问,如果表 L_0 中不存在 ID_i 项,挑战者将运行 UserKeyGen 算法生成 ID_i 的公私钥对(PK_i, SK_i),并将$\{ID_i, PK_i, SK_i, 0\}$加入表 L_0,然后返回 PK_i. 如果表 L_0 中已存在$\{ID_i, PK_i, SK_i, f_i\}$项,则直接返回 PK_i.

(2)私钥询问　敌手 A_I 询问身份 ID_i 的私钥. 如果表 L_0 中不存在 ID_i 项,则挑战者运行 $UserKeyGen$ 算法生成用户 ID_i 的公私钥对(PK_i, SK_i),并将$\{ID_i, PK_i, SK_i, 0\}$加入表 L_0,然后返回 SK_i. 若 L_0 中已存在$\{ID_i, PK_i, SK_i, f_i\}$项,则直接返回 SK_i.

(3)公钥替换询问　敌手 A_I 随机选择公钥 PK_i' 对 ID_i 进行公钥替换询问. 如果表 L_0 中不存在 ID_i 项,则挑战者将(ID_i, PK_i',⊥,1)加入. 否则挑战者将表 L_0 中 ID_i 项更新为(ID_i, PK_i',⊥,1).

(4)证书询问　敌手 A_I 询问 ID_i 的证书,如果表 L_0 中不存在 ID_i 项,则挑战者运行算法 UserKeyGen 生成 ID_i 的公私钥对(PK_i, SK_i),并将$\{ID_i, PK_i, SK_i, 0\}$加入表 L_0. 否则挑战者获取 PK_i. 两种情况下挑战者都以($params$, MSK, ID_i, PK_i)为输入运行 Certify 算法,返回 $Cert_{ID_i}$.

(5)解封装询问　敌手 A_I 对(ID_i, C_i)进行解封装询问. 挑战者利用解封装算法解封装 C_i,返回密钥 K_i.

挑战阶段　敌手 A_I 选择目标身份 ID^* 并将目标身份发送给挑战者. 挑战者对目标身份运行密钥封装算法产生密钥及封装 Encap($params$, ID^*, PK^*)→(K_1, C^*),同时选取 $K_0 \in \kappa_D$. 然后随机选取 $b \in \{0,1\}$并将(K_b, C^*)返回给敌手.

第二阶段询问　A_I 继续进行询问,但不能询问目标用户 ID^* 的证书以及对(ID^*, C^*)的解封装询问.

猜测　A_I 输出 b'. 如果 $b' = b$,则称 A_I 赢得游戏.

A_I 赢得游戏的优势定义为

$$Adv^{A_I}_{CB-KEM} = |2\Pr[b' = b] - 1|.$$

定义 4(对第一类攻击者在自适应选择密文攻击下的不可区分性)　如果不存在概率多项式时间的敌手 A_I,能以不可忽略的优势赢得游戏 1,那么就称基于证书密钥封装方案对第一类敌手在自适应选择密文攻击下是不可区分的.

游戏 2

系统参数设置　挑战者运行算法 Setup,返回主密钥 MSK 和系统参数 $params$,并把主密钥 MSK 和系统参数 $params$ 都发送给 A_{II}.

第一阶段询问　在这一阶段中,挑战者维护一个记录用户 ID_i 私钥和公钥的表 $L_0 = \{ID_i, PK_i, SK_i\}$,该表初始为空. A_{II}向挑战者进行如下询问:

(1)公钥询问　敌手 A_{II}对 ID_i 进行公钥询问,如果表 L_0 中不存在 ID_i 项,挑战者将运行 UserKeyGen 算法生成 ID_i 的公私钥对(PK_i, SK_i),并将$\{ID_i, PK_i, SK_i\}$加入表 L_0,然后返回 PK_i. 如果表 L_0 中已存在$\{ID_i, PK_i, SK_i\}$项,则直接返回 PK_i.

(2)私钥询问　敌手 A_{II}询问身份 ID_i 的私钥. 如果表 L_0 中不存在 ID_i 项,则挑战者运行 UserKeyGen 算法生成用户 ID_i 的公私钥对(PK_i, SK_i),并将$\{ID_i, PK_i, SK_i\}$加入表 L_0,然后返回 SK_i. 若 L_0 中已存在$\{ID_i, PK_i, SK_i\}$项,则直接返回 SK_i.

(3)解封装询问　敌手 A_{II}对(ID_i, C_i)进行解封装询问. 挑战者利用解封装算法解密 C_i,返回密钥 K_i.

挑战阶段　敌手 A_{II}选择目标身份 ID^* 并将目标身份发送给挑战者. 挑战者对目标身份运行密钥封装算法产生密钥及封装 Encap($params$, ID^*, PK^*)→(K_1, C^*),同时选取 $K_0 \in \kappa_D$. 然后随机选取 $b \in \{0,1\}$并将(K_b, C^*)返回给敌手.

第二阶段询问　A_{II}继续像第一阶段那样询问,但不能对目标身份 ID^* 进行私钥询问,也不能对(ID^*, C^*)进行解封装询问.

猜测 A_{II}输出 b'. 如果 $b'=b$,则称 A_{II}赢得游戏. A_{II}赢得游戏的优势定义为

$$Adv_{CB-KEM}^{A_{II}}=|2\Pr[b'=b]-1|.$$

定义 5(对第二类攻击者在自适应选择密文攻击下的不可区分性) 如果不存在概率多项式时间攻击者 A_{II},能以不可忽略的优势赢得游戏 2,那么就称基于证书密钥封装方案对第二类攻击者在自适应选择密文攻击下是不可区分的.

4 基于证书密钥封装方案的构造

在这部分中,首次提出了标准模型下安全的基于证书密钥封装方案,并对它进行正确性分析. 该方案由以下五个算法组成:

系统参数设置算法(Setup) 该算法由 CA 执行如下:G_1, G_2 为素数 q 阶循环群,g 为群 G_1 的生成元,存在可计算的双线性映射 $e: G_1\times G_1\rightarrow G_2$. 随机选取 $\alpha\in Z_q^*$,计算 $g_1=g^\alpha$. 在群中选取 $g_2\in G_1$,向量$(u', u_1, \cdots, u_n)\in G_1^{n+1}$,$(v', v_1, \cdots, v_n)\in G_1^{n+1}$,计算函数 $F_u(Q)=u'\prod_{j=1}^{n}u_j^{i_j}$,其中 $Q=i_1i_2\cdots i_n$; $F_v(w)=v'\prod_{j=1}^{n}v_j^{w_j}$,其中 $w=w_1w_2\cdots w_n$. 选择两个 Hash 函数 $H_1:\{0,1\}^*\rightarrow\{0,1\}^n$, $H_2:\{0,1\}^*\rightarrow\{0,1\}^n$. 则系统主私钥 $MSK=g_2^\alpha$ 且由 CA 保存,并将系统参数 $params=\{G_1, G_2, q, e, g, g_1, g_2, u', u_1, \cdots, u_n, v', v_1, \cdots, v_n, H_1, H_2\}$公开.

用户密钥生成算法(UserKeyGen) 用户在 Z_q^* 中随机选取 x,利用系统参数生成自己的公钥 $PK=(PK_1, PK_2)=(g^x, g_1^x)$,用户私钥 $SK=x$.

证书产生算法(Certify) 认证中心 CA 为当前用户计算证书. 输入$(params, MSK, ID, PK)$,计算 $Q_{ID}=H_1(ID, PK)$,随机选取 $r\in Z_q^*$,则用户的证书 $Cert=(Cert_1, Cert_2)=(g_2^\alpha F_u(Q_{ID})^r, g^r)$.

密钥封装算法(Encap) 发送者使用接收者的公钥 PK 和身份 ID 生成对称密钥和对该密钥的封装. 首先,发送者验证 $e(PK_1, g_1)=e(PK_2, g)$是否成立. 若不成立,输出$\perp$并终止. 否则,发送者计算 $Q_{ID}=H_1(ID, PK)$,随机选取 $s\in Z_q^*$,计算:(1) $K=e(g_2, PK_2)^s$;(2) $C_1=g^s$, $C_2=F_u(Q_{ID})^s$, $C_3=F_v(w)^s$,其中 $w=H_2(C_1, C_2, ID, PK)$. 返回对密钥 K 的封装 $C=(C_1, C_2, C_3)$.

密钥解封装算法(Decap) 接收者收到封装 $C=(C_1, C_2, C_3)$后,用证书及私钥解封装如下:计算 $w=H_2(C_1, C_2, ID, PK)$,若 $e(C_1, F_u(Q_{ID})F_v(w))=e(g, C_2C_3)$, C 是正确的封装,计算 $K=\dfrac{e(C_1, Cert_1^{SK})}{e(C_2, Cert_2^{SK})}$;否则 C 是无效的.

正确性分析:

$$K=\frac{e(C_1, Cert_1^{SK})}{e(C_2, Cert_2^{SK})}=\frac{e(g^s, (g_2^\alpha F_u(Q_{ID})^r)^x)}{e(F_u(Q_{ID})^s, g^{rx})}$$

$$=\frac{e(g, g_2^\alpha)^{sx}e(g, F_u(Q_{ID})^r)^{sx}}{e(g, F_u(Q_{ID})^r)^{sx}}=e(PK_2, g_2)^s$$

5 安全性证明

在这一部分中,证明本文提出的基于证书密钥封装方案在标准模型下是安全的. 根据第 3 节的基于证书密钥封装的安全模型和定义,给出以下证明.

定理 1 如果存在概率多项式时间敌手 A_I,经过最多 q_C 次证书询问,最多 q_D 次解封装询问后,以概率 ε 在游戏 1 中区分出 K_b. 那么存在一个算法 B,在多项式时间内以 $\varepsilon'\geqslant\dfrac{\varepsilon}{16(n+1)^2q_Cq_D}$ 概率解决 DBDH 困难问题.

证明 我们构造算法 B 来解决 DBDH 问题,以$(G_1, G_2, e, q, g, g^a, g^b, g^c, T)$为输入,其目的是判定 $T=e(g, g)^{abc}$是否成立. B 将扮演挑战者与敌手 A_I 进行交互,并利用 A_I 实现目标.

系统参数设置 挑战者选取 $k_u\in\{0,1,\cdots,n\}$, $k_v\in\{0,1,\cdots,n\}$. 整数 t_u, t_v 满足不等式 $t_u(n+1)<q$, $t_v(n+1)<q$,且随机选取 $x_u'\in Z_{t_u}$, $x_v'\in Z_{t_v}$,向量$(\boldsymbol{x}_{u,1}, \boldsymbol{x}_{u,2}, \cdots, \boldsymbol{x}_{u,n})$,其中 $\boldsymbol{x}_{u,j}\in\boldsymbol{Z}_{t_u}$ $(j\in\{1,\cdots,n\})$,向量$(\boldsymbol{x}_{v,1}, \boldsymbol{x}_{v,2}, \cdots, \boldsymbol{x}_{v,n})$,其中 $\boldsymbol{x}_{v,j}\in\boldsymbol{Z}_{t_v}$ $(j\in\{1,\cdots,n\})$. 选取 $\boldsymbol{y}_u'\in\boldsymbol{Z}_q$, $\boldsymbol{y}_v'\in\boldsymbol{Z}_q$,向量$(\boldsymbol{y}_{u,1}, \boldsymbol{y}_{u,2}, \cdots, \boldsymbol{y}_{u,n})$,其中 $\boldsymbol{y}_{u,j}\in\boldsymbol{Z}_q$ $(j\in\{1,\cdots,n\})$,向量$(\boldsymbol{y}_{v,1}, \boldsymbol{y}_{v,2}, \cdots, \boldsymbol{y}_{v,n})$,其中 $\boldsymbol{y}_{v,j}\in\boldsymbol{Z}_q$ $(j\in\{1,\cdots,n\})$. 令 $u'=g_2^{x_u'-k_ut_u}g^{y_u'}$, $u_j=g_2^{x_{u,j}}g^{y_{u,j}}$,其中 $1\leqslant j\leqslant n$; $v'=g_2^{x_v'-k_vt_v}g^{y_v'}$, $v_j=g_2^{x_{v,j}}g^{y_{v,j}}$, $1\leqslant j\leqslant n$. 为了分析方便,我们定义了四个函数: $J_u(Q)=x_u'+\sum_{j=1}^{n}i_jx_{u,j}-k_ut_u$, $K_u(Q)=y_u'+\sum_{j=1}^{n}i_jy_{u,j}$,其中 $Q=i_1i_2\cdots i_n$; $J_v(w)=x_v'+\sum_{j=1}^{n}w_jx_{v,j}-k_vt_v$, $K_v(w)=y_v'+\sum_{j=1}^{n}w_jy_{v,j}$,其中 $w=w_1w_2\cdots w_n$. 则系统参数为 $F_u(Q)=u'\prod_{j=1}^{n}u_j^{i_j}=g_2^{J_u(Q)}g^{K_u(Q)}$, $F_v(w)=v'\prod_{j=1}^{n}v_j^{w_j}=g_2^{J_v(w)}g^{K_v(w)}$, g, $g_1=g^a$, $g_2=g^b$. 主私钥为 $MSK=g_2^a$,但是未知.

第一阶段询问 在该阶段中,B 与敌手 A_I 进行交互,过程如下:

(1)公钥询问 B 维持一个记录用户私钥和公钥的表 $L_0=\{ID_i, PK_i=(PK_{i1}, PK_{i2}), SK_i, f_i\}$, $f_i=0$ 表示用户公钥没有被替换, $f_i=1$ 表示公钥被替换,该表初始为空. A_I 询问用户 ID_i 的公钥,若表 L_0 中有 ID_i 项,B 直接

返回 ID_i 的公钥 PK_i 给 A_I;若表 L_0 中没有 ID_i 项,B 随机选取 $x_i \in Z_q^*$,计算 $PK_i = (PK_{i1}, PK_{i2}) = (g^{x_i}, g_1^{x_i})$,返回 PK_i 给 A_I,并将元组$(ID_i, PK_i, x_i, 0)$添加到表 L_0.

(2)私钥询问　A_I 询问用户 ID_i 的私钥,B 检查 $\{ID_i, PK_i, SK_i, f_i\}$是否在 L_0 表中.若 ID_i 对应的元组在 L_0 表中且 $f_i = 1$,B 拒绝回答 A_I 的询问,若 ID_i 对应的元组在 L_0 表中且 $f_i = 0$,B 返回私钥 SK_i;若 ID_i 对应的元组不在 L_0 表中,B 随机选取 $x_i \in Z_q^*$,计算 $PK_i = (PK_{i1}, PK_{i2}) = (g^{x_i}, g_1^{x_i})$,返回 $SK_i = x_i$ 给 A_I,并将元组$(ID_i, PK_i, x_i, 0)$添加到表 L_0 中.

(3)公钥替换询问　敌手 A_I 提交公钥替换询问(ID_i, PK_i').B 检查 $e(P_{pub}, PK_{i1}') = e(P, PK_{i2}')$是否成立.若不成立,返回无效的公钥;否则,B 检查表 L_0 中是否存在 ID_i 项.若不存在,则 B 将$(ID_i, PK_i', \perp, 1)$加入.否则 B 将表 L_0 中的 ID_i 项更新为$(ID_i, PK_i', \perp, 1)$.

(4)证书询问　敌手 A_I 对(ID, PK)询问证书,挑战者 B 计算 $Q = H_1(ID, PK)$,如果 $J_u(Q) = 0 \bmod t_u$,B 失败并退出;否则 $J_u(Q) \neq 0 \bmod t_u$,也即 $J_u(Q) \neq 0 \bmod q$,挑战者随机选取 $r \in Z_q^*$,计算 $Cert_1 = F_u(Q)^r g_1^{-K_u(Q)/J_u(Q)} = g_2^a F_u(Q)^{r'}$, $Cert_2 = g^r g_1^{-1/J_u(Q)} = g^{r'}$, $r' = r - \frac{a}{J_u(Q)}$,并将证书返回给敌手.

(5)解封装询问　敌手 A_I 对(ID, PK)的封装 $C = (C_1, C_2, C_3)$进行解封装询问.B 计算 $w = H_2(C_1, C_2, ID, PK)$,如果 $J_v(w) = 0 \bmod t_v$,B 失败并退出;否则 $J_v(w) \neq 0 \bmod q$,对于 $s \in Z_q^*$,有 $C_1 = g^s$, $C_3 = (F_v(w))^s = (g_2^{J_v(w)} g^{K_v(w)})^s$,所以挑战者可以得到 $g_2^s = (C_3 / C_1^{K_v(w)})^{1/J_v(w)}$,由此可得 $K = e(PK_2, (C_3 / C_1^{K_v(w)})^{1/J_v(w)})$.

挑战阶段　当敌手 A_I 决定第一阶段询问结束时,敌手选取目标用户 ID^* 发送给 B,B 运行如下:如果 $J_u(Q^*) \neq 0 \bmod q$ 或者 $J_v(w^*) \neq 0 \bmod q$ 时,B 失败并退出;否则 $J_u(Q^*) = J_v(w^*) = 0 \bmod q$ 时,计算 $C_1^* = g^c$, $C_2^* = C_1^{*K_u(Q^*)} = (g^c)^{K_u(Q^*)}$, $C_3^* = C_1^{*K_v(w^*)} = (g^c)^{K_v(w^*)}$,其中,$Q^* = H_1(ID^*, PK^*)$, $w^* = H_2(C_1^*, C_2^*, ID^*, PK^*)$.B 将封装 $C^* = (C_1^*, C_2^*, C_3^*)$及 $K_b^* = T^{x^*} \in G_1$(x^*为目标用户的私钥)返回给 A_I.

第二阶段询问　敌手 A_I 继续进行一系列询问,但不能询问目标用户 ID^* 的证书以及对(C^*, ID^*, PK^*)的解封装.B 的回答方式和第一阶段询问相同.

猜测　敌手 A_I 输出对 b 的猜测 $b' \in \{0,1\}$,猜测 $b' = 1$ 意味着 K_b^* 是正确密钥.算法 B 推断如下:B 将 b'作为它的输出 b'', $b'' = 1$ 意味着 B 猜测出 $T = e(g,g)^{abc}$.

分析　$C^* = (C_1^*, C_2^*, C_3^*)$的封装密钥 $K_1^* = e(PK_2^*, g_2)^c = e(g,g)^{abcx^*}$,而 $K_0^* \in G_2$ 是挑战者随机选取的.B 将 $K_b^* = T^{x^*} \in G_1$ 返回给敌手.敌手 A_I 输出对 b 的猜测 $b' \in \{0,1\}$, $b' = 1$ 意味着 $T = e(g,g)^{abc}$, $b' = 0$ 意味着 T 为随机值.此时 B 将 b'作为它的输出 b'', $b'' = 1$ 也即 B 猜测出 $T = e(g,g)^{abc}$成立,否则不成立.如果 A_I 在游戏中能区分出 K_b^*,则 B 可以根据敌手解决 DBDH 困难问题.

概率计算　记事件 E 为算法 B 没有终止游戏,事件 E_1 为在证书询问阶段 $J_u(Q) \neq 0 \bmod t_u$,事件 E_2 为在解封装询问中 $J_v(w) \neq 0 \bmod t_v$,事件 E_3 为挑战阶段中 $J_u(Q^*) = J_v(w^*) = 0 \bmod q$.则 $\Pr[E] = \Pr[E_1 \wedge E_2 \wedge E_3] = \Pr[E_3]\Pr[E_1 \wedge E_2 \mid E_3] \geqslant \frac{1}{t_u(n+1)} \frac{1}{t_v(n+1)} (1 - \frac{q_D}{t_v})(1 - \frac{q_C}{t_u})$, $t_u \leqslant 2q_C$, $t_v = 2q_D$,所以 $\Pr[E] \geqslant \frac{1}{16(n+1)^2 q_C q_D}$. B 解决困难问题的概率 $\varepsilon' \geqslant \frac{\varepsilon}{16(n+1)^2 q_C q_D}$.

定理 2　如果存在概率多项式时间敌手 A_{II},经过最多 q_{SK}次私钥询问,最多 q_D 次解封装询问后,以概率 ε 在游戏 2 中区分出 K_b.那么存在算法 B,在多项式时间内以概率 $\varepsilon' \geqslant \frac{\varepsilon}{16(n+1)^2 q_{SK} q_D}$解决 DBDH 困难问题.

证明　我们构造算法 B 来解决 DBDH 问题,以$(G_1, G_2, e, q, g, g^a, g^b, g^c, T)$为输入,其目的是判定 $T = e(g,g)^{abc}$是否成立.B 将扮演挑战者与 A_{II}进行交互,并利用 A_{II}实现目标.为了使对 A_{II}询问回答前后一致,B 需要维持初始为空的表 L_0,用于记录 B 对敌手 A_{II}询问的回答.

系统参数设置　挑战者选取 $k_u \in \{0,1,\cdots,n\}$, $k_v \in \{0,1,\cdots,n\}$.整数 t_u, t_v 满足不等式 $t_u(n+1) < q$, $t_v(n+1) < q$,且随机选取 $x_u' \in Z_{t_u}$, $x_v' \in Z_{t_v}$,向量$(\boldsymbol{x}_{u,1}, \boldsymbol{x}_{u,2}, \cdots, \boldsymbol{x}_{u,n})$,其中 $\boldsymbol{x}_{u,j} \in \boldsymbol{Z}_{t_u}$ $(j \in \{1,\cdots,n\})$,向量$(\boldsymbol{x}_{v,1}, \boldsymbol{x}_{v,2}, \cdots, \boldsymbol{x}_{v,n})$,其中 $\boldsymbol{x}_{v,j} \in \boldsymbol{Z}_{t_v}$ $(j \in \{1,\cdots,n\})$.选取 $\boldsymbol{y}_u' \in \boldsymbol{Z}_q$, $\boldsymbol{y}_v' \in \boldsymbol{Z}_q$,向量$(\boldsymbol{y}_{u,1}, \boldsymbol{y}_{u,2}, \cdots, \boldsymbol{y}_{u,n})$,其中 $\boldsymbol{y}_{u,j} \in \boldsymbol{Z}_q$ $(j \in \{1,\cdots,n\})$,向量$(\boldsymbol{y}_{v,1}, \boldsymbol{y}_{v,2}, \cdots, \boldsymbol{y}_{v,n})$,其中 $\boldsymbol{y}_{v,j} \in \boldsymbol{Z}_q$ $(j \in \{1,\cdots,n\})$.令 $u' = g_2^{x_u' - k_u t_u} g^{y_u'}$, $u_j = g_2^{x_{u,j}} g^{y_{u,j}}$,其中 $1 \leqslant j \leqslant n$; $v' = g_2^{x_v' - k_v t_v} g^{y_v'}$, $v_j = g_2^{x_{v,j}} g^{y_{v,j}}$, $1 \leqslant j \leqslant n$.为了分析方便,我们定义了四个函数: $J_u(Q) = x_u' + \sum_{j=1}^{n} i_j x_{u,j} - k_u t_u$, $K_u(Q) = y_u' + \sum_{j=1}^{n} i_j y_{u,j}$,其中 $Q = i_1 i_2 \cdots i_n$; $J_v(w) = x_v' + \sum_{j=1}^{n} w_j x_{v,j} - k_v t_v$, $K_v(w) = y_v' + \sum_{j=1}^{n} w_j y_{v,j}$,其中 w

$= w_1 w_2 \cdots w_n$，则 $F_u(Q) = u' \prod_{j=1}^{n} u_j^{i_j} = g_2^{J_u(Q)} g^{K_u(Q)}$，$F_v(w) = v' \prod_{j=1}^{n} v_j^{w_j} = g_2^{J_v(w)} g^{K_v(w)}$. B 随机选取 $\alpha \in Z_q^*$，$g_1 = g^\alpha$，$g_2 = g^b$，$A = g^a$. 则 B 将系统参数和主私钥 $MSK = g_2^\alpha$ 发送给 A_{II}.

第一阶段询问 在该阶段中，B 与敌手 A_{II}进行交互，过程如下：

(1)公钥询问 B 维持一个记录用户私钥和公钥的表 $L_0 = \{ID_i, PK_i = (PK_{i1}, PK_{i2}), SK_i, J_i\}$，$J_i = J_u(H_1(PK_i, ID_i))$，该表初始为空. A_{II}询问用户 ID_i 的公钥，若表 L_0 中有 ID_i 项，B 直接返回 ID_i 的公钥 PK_i 给 A_{II}；若表 L_0 中没有 ID_i 项，B 随机选取 $x_i \in Z_q^*$，计算 $PK_i = (PK_{i1}, PK_{i2}) = (A^{x_i}, A^{\alpha x_i})$，$J_i = J_u(H_1(PK_i, ID_i))$，返回 PK_i 给 A_{II}，将元组(ID_i, PK_i, x_i, J_i)添加到表 L_0.

(2)私钥询问 A_{II}询问用户 ID_i 的私钥，B 检查$\{ID_i, PK_i, SK_i, J_i\}$是否在 L_0 表中. 若 ID_i 对应的元组在 L_0 表中且 $J_i = 0 \bmod q$，B 拒绝回答 A_{II}的询问，若 ID_i 对应的元组在 L_0 表中且 $J_i \neq 0 \bmod q$，B 返回私钥 SK_i；若 ID_i 对应的元组不在 L_0 表中，B 随机选取 $x_i \in Z_q^*$，计算 $PK_i = (PK_{i1}, PK_{i2}) = (A^{x_i}, A^{\alpha x_i})$，$J_i = J_u(H_1(PK_i, ID_i))$，若 $J_i \neq 0 \bmod q$，返回 $SK_i = x_i$ 给 A_{II}，并将元组(ID_i, PK_i, x_i, J_i)添加到表 L_0 中；若 $J_i = 0 \bmod q$，B 拒绝回答 A_{II}的询问.

(3)解封装询问 敌手 A_{II}对(ID, PK)的封装 $C = (C_1, C_2, C_3)$进行解封装询问. B 计算 $w = H_2(C_1, C_2, ID, PK)$，如果 $J_v(w) = 0 \bmod t_v$，B 失败并退出；否则 $J_v(w) \neq 0 \bmod q$，对于 $s \in Z_q^*$，有 $C_1 = g^s$，$C_3 = (F_v(w))^s = (g_2^{J_v(w)} g^{K_v(w)})^s$，所以挑战者可以计算得 $g_2^s = (C_3 / C_1^{K_v(w)})^{1/J_v(w)}$，由此可得 $K = e(PK_2, (C_3 / C_1^{K_v(w)})^{1/J_v(w)})$.

挑战阶段 当敌手 A_{II}决定第一阶段询问结束时，敌手选取目标用户 ID^* 发送给 B，B 运行如下：如果 $J_u(Q^*) \neq 0 \bmod q$ 或者 $J_v(w^*) \neq 0 \bmod q$ 时，B 失败并退出；否则 $J_u(Q^*) = J_v(w^*) = 0 \bmod q$ 时，计算 $C_1^* = g^c$，$C_2^* = C_1^{*K_u(Q^*)} = (g^c)^{K_u(Q^*)}$，$C_3^* = C_1^{*K_v(w^*)} = (g^c)^{K_v(w^*)}$，其中，$Q^* = H_1(ID^*, PK^*)$，$w^* = H_2(C_1^*, C_2^*, ID^*, PK^*)$. B 将封装 $C^* = (C_1^*, C_2^*, C_3^*)$及 $K_b^* = T^{\alpha x^*} \in G_1$($x^*$为目标用户的私钥)返回给 A_{II}.

第二阶段询问 敌手 A_{II}继续进行一系列询问，但不能对目标用户 ID^* 进行私钥询问，也不能对(C^*, ID^*, PK^*)进行解封装询问. B 的回答方式和第一阶段询问相同.

猜测 敌手 A_{II}输出对 b 的猜测 $b' \in \{0,1\}$. B 将 b' 作为它的输出 b''，$b'' = 1$ 意味着 B 猜测出 $T = e(g, g)^{abc}$.

分析 $C^* = (C_1^*, C_2^*, C_3^*)$的封装密钥 $K_1^* = e(PK_2^*, g_2)^c = e(g, g)^{abc\alpha x^*}$，而 $K_0^* \in G_2$ 是挑战者随机选取的. B 将 $K_b^* = T^{\alpha x^*} \in G_1$ 返回给敌手. 敌手 A_{II}输出对 b 的猜测 $b' \in \{0,1\}$，$b' = 1$ 意味着 $T = e(g, g)^{abc}$，$b' = 0$ 意味着 T 为随机值. 此时 B 将 b' 作为它的输出 b''，$b'' = 1$ 也即 B 猜测出 $T = e(g, g)^{abc}$ 成立，否则不成立. 如果 A_{II}在游戏中能区分出 K_b^*，则 B 可以根据敌手解决 DBDH 困难问题.

概率计算 记事件 E 为算法 B 没有终止游戏，事件 E_1 为在证书询问阶段 $J_i \neq 0 \bmod t_u$，事件 E_2 为在解封装询问中 $J_v(w) \neq 0 \bmod t_v$，事件 E_3 为挑战阶段中 $J_u(Q^*) = J_v(w^*) = 0 \bmod q$. $\Pr[E] = \Pr[E_1 \wedge E_2 \wedge E_3] = \Pr[E_3]\Pr[E_1 \wedge E_2 \mid E_3] \geqslant \frac{1}{t_u(n+1)} \frac{1}{t_v(n+1)} (1 - \frac{q_D}{t_v})(1 - \frac{q_{SK}}{t_u})$，$t_u \leqslant 2q_{SK}$，$t_v = 2q_D$，所以 $\Pr[E] \geqslant \frac{1}{16(n+1)^2 q_{SK} q_D}$. B 解决困难问题的概率 $\varepsilon' \geqslant \frac{\varepsilon}{16(n+1)^2 q_{SK} q_D}$.

6 结束语

本文首次将密钥封装机制引入到基于证书加密体制中，提出了基于证书密钥封装机制(CB-KEM)的形式化定义及安全模型. 在此基础上构造了一个基于证书密钥封装方案，并证明该方案在标准模型下是自适应选择密文不可区分的. 在标准模型下证明安全的方案，效率一般比随机预言机模型下的方案要低，本文也不例外. 因此，构造标准模型下安全的高效的基于证书密钥封装方案是下一步研究的重点. 此外，针对不同的应用背景，可以进一步将基于证书密码体制拓展到具有特殊性质的基于证书加密或签名方案，如群签名[24]、环签名[25]和环签密[26]等.

参考文献

[1] Gentry C. Certificate-based encryption and the certificate revocation problem[A]. Eurocrypt'2003[C]. Berlin: Springer-Verlag, 2003. 272 - 293.

[2] Balfe S, Gallery E, Mitchell C J. Challenges for trusted computing[J]. IEEE Security & Privacy, 2008, 6(6): 60 - 66.

[3] Yum D H, Lee P J. Identity-based cryptography in public key management[A]. EuroPKI'2004[C]. Berlin: Springer-Verlag, 2004. 71 - 84.

[4] Galindo D, Morillo P, Ràfols C. Breaking Yum and Lee generic constructions of certificateless and certificate-based encryption

schemes[A]. EuroPKI'2006[C]. Berlin: Springer-Verlag, 2006.81 – 91.
[5] Al-Riyami S S, Paterson K. CBE from CL-PKE: A generic construction and efficient schemes[A]. PKC'2005[C]. Berlin: Springer-Verlag, 2005.398 – 415.
[6] Galindo D, Morillo P, Rùfols C. Improved certificate-based encryption in the standard model[J]. Journal of Systems and Software, 2008, 81(7): 1218 – 1226.
[7] Waters B. Efficient identity-based encryption without random oracles[A]. Eurocrypt'2005[C]. Berlin: Springer-Verlag, 2005. 114 – 127.
[8] Liu J K, Zhou J Y. Efficient certificate-based encryption in the standard model[A]. SCN'2008[C]. Berlin: Springer-Verlag, 2008.144 – 155.
[9] Gentry C. Practical identity-based encryption without random oracles[A]. Eurocrypt'2006[C]. Berlin: Springer-Verlag, 2006. 445 – 464.
[10] Boneh D, Joux A, Nguyen A. Why textbook ElGamal and RSA encryption are insecure[A]. Aisacrypt' 2000[C]. Berlin: Springer-Verlag, 2000.30 – 43.
[11] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack[J]. SIAM Journal on Computing, 2003, 33(1): 167 – 226.
[12] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme[A]. Crypto'2004[C]. Berlin: Springer-Verlag, 2004.426 – 442
[13] Abe M, Gennaro R, Kurosawa K. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM[A]. Eurocrypt' 2005[C]. Berlin: Springer-Verlag, 2005.128 – 146.
[14] Dent A. A designer's guide to KEMs[A]. Cryptography and Coding 2003[C]. Berlin: Springer-Verlag, 2003.133 – 151.
[15] Bentahar K, Farshim P, Malone-Lee J. Generic constructions of identity-based and certificateless KEMs[J]. Journal of Cryptology, 2008, 21(2): 178 – 199.
[16] Chen L, Cheng Z, Malone-Lee J. An efficient ID-KEM based on the Sakai-Kasahara key construction[J]. IEE Proceedings-Information Security, 2006, 153(1): 19 – 26.
[17] Huang Q, Wong D S. Generic certificateless key encapsulation mechanism[A]. ACISP'2007[C]. Berlin: Springer-Verlag, 2007.215 – 229.
[18] Kiltz E, Galindo D. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles[A]. ACISP'2006[C]. Berlin: Springer-Verlag, 2006.336 – 347.
[19] Long Y, Li X X, Chen K F. Distributed certificateless key encapsulation mechanism secure against the adaptive adversary [J]. Shanghai Jiaotong Univ. (Sci.), 2009, 14(1): 102 – 106.
[20] Nieto J G, Lippold G, Boyd C. Efficient certificateless KEM in the standard model[A]. ICISC'2009[C]. Berlin: Springer-Verlag, 2010.34 – 46.
[21] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Constructions of certificate-based signature secure against key replacement attacks[J]. Journal of Computer Security, 2010, 18(3): 421 – 449.
[22] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Certificate-based signature: security model and efficient construction[A]. EuroPKI'2007[C]. Berlin: Springer-Verlag, 2007.110 – 125.
[23] Li J G, Huang X Y, Zhang Y C, Xu L Z. An efficient short certificate-based signature scheme[J]. Journal of Systems and Software, 2012, 85(2): 314 – 322.
[24] 李继国,孙刚,张亦辰.标准模型下可证安全的本地验证者撤销群签名方案[J].电子学报,2011,20(7):1618 – 1623.
Li J G, Sun G, Zhang Y C. Provably secure group signature scheme with verifier-local revocation in the standard model [J]. Acta Electronica Sinica, 2011, 20(7): 1618-1623. (in Chinese)
[25] 桑永宣,曾吉文.两种无证书的分布环签名方案[J].电子学报,2008,36(7):1468-1472.
Sang Y X, Zeng J W. Two certificateless distributed ring signature schemes[J]. Acta Electronica Sinica, 2008, 36(7): 1468-1472. (in Chinese)
[26] 黄欣沂,张福泰,伍玮.一种基于身份的环签密方案[J].电子学报,2006,34(2):263 – 266.
Huang X Y, Zhang F T, Wu W. An identity-based ring signcryption scheme[J]. Acta Electronica Sinica, 2006, 34(2): 263-266. (in Chinese)

作者简介

李继国　男,1970 年生于黑龙江省富裕县,博士,教授,博士生导师,主要研究领域为信息安全、密码学理论与技术、可信计算等.
E-mail: ljg1688@163.com

杨海珊　女,1985 年生于山西省吕梁市,硕士,主要研究领域为密码学理论与技术.