网络出版时间：2016-12-21 08:41:16
网络出版地址：http://www.cnki.net/kcms/detail/11.2127.TP.20161221.0841.004.html

高效的 TPKC→IDPKC 的异构签密方案

李臣意[1], 张玉磊[1], 张永洁[2], 王彩芬[1]
LI Chenyi[1] ,ZHANG Yulei[1] ,ZHANG Yongjie[2],WANG Caifen[1]
1.西北师范大学 计算机科学与工程学院,兰州 730070
2.甘肃卫生职业学院,兰州 730000
1.College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070 China
2. Gansu Health Vocational University ,Lanzhou 730000, China

LI Chenyi,ZHANG Yulei,Zhang Yongjie,WANG Caifen.Efficient PKI→IBC Heterogeneous Signcryption Scheme. Computer Engineering and Application

Abstract: Confidentiality and unforgeability are two main goals of secure communication. In order to solve the aboveproblem of between two heterogeneous cryptographic systems,this paper proposes an efficient TraditionalPublicKeyCryptography(TPKC) to IdentityBased Public Key Cryptography(IDPKC) heterogeneous signcryption scheme. In the signcryption algorithm of this scheme,it does not need to and billinepairing,;inthe un-signcryption algorithm, it only need two of operation, efficiency has been greatly improved; Therefore,it'sefficiencyis higher than the existing same kind of schemes. In the random oracle model, based on the ComputableDiffie-Hellman(CDH)hard problem, it is proved that the scheme has IND-SC-CCA2 security and EUF-SC-CMA security.
Key words: heterogeneous systems;TraditionalPublicKeyCryptography(TPKC);IdentityBased Public Key Cryptography(IDPKC);confidentiality;unforgeability

摘要：机密性和不可伪造性是安全通信的两个主要目标。为了解决异构密码系统之间安全通信问题，本文提出了一个高效从基于传统公钥密码体制到基于身份的公钥密码体制异构签密方案（TPKC→IDPKC）。方法运行签密算法时，不需要对运算；运行解签密算法时，只需要 2 个对运算，与已有同类方案相比较，效率有了较大的提高；同时在随机预言模型下，基于 CDH(ComputableDiffie-Hellman)问题，证明该方案满足 IND-SC-CCA2 安全性和 EUF-SC-CMA 安全性。
关键词:异构系统；传统公钥密码体制；基于身份公钥密码体制；机密性；不可伪造性
doi:10.3778/j.issn.1002-8331.1606-0281 **文献标识码**：A **中图分类号**：TP309

1 引言

现代计算机和通信系统形成了一个全球覆盖的基础设施。不同的计算机和通信系统可能采用不同的安全技术。有些采用传统公钥密码体制（TPKC），有些采用基于身份公钥密码体制（IDPKC），如果要在采用不同密码技术的系统之间进行通信就需要支持异构通信的密码体制；在 PKI 系统中，授权中心（CA）通过颁发证书，提供了一种不可伪造的和可信的公钥，建立了与签名的认证用户身份之间的联系。它的缺点是需要我们对证书进行管理，包括撤销，恢复和发布。另外，在使用证书前，需要鉴别它的有效性。在 IBC 系统中，用户的公钥可以从身份信息中获取，例如电话号码、邮件地址或者 IP 地址；私钥是由可信任的第三方 PKG（私钥生成中心）产生的，无需任何证书，同时消除了与证书相关的问题；但是依靠 PKG 产生用私钥不可避免的造成了密钥托管问题。

机密性和不可伪造性是安全通信的重要目标。为了同时实现这两个目标，传统方法是对消息先签名后加密，或者先加密后签名，虽然实现这两个目标，但是总体而言效率较低，最早的签密概念是由 Zheng[1]提出的，这种签密方案相对应的形式化安全模型被 Baek[2]等人研究发现的。大多数基于传统公钥密码体制（TPKC）的

基金项目:甘肃省高等学校科研基金资助项目(2013A-014)国家自然科学基金资助项目(61262057，61163038，61262056)；

作者介绍：李臣意（1989-），男，硕士研究生，研究方向：异构签密，网络信息安全；张玉磊，男，博士，副教授；张永洁，女，博士、副教授；王彩芬：教授，博士。E-mail: 675989124@qq.com

签密方案[3-7]和基于身份公钥密码体制（IDPKC）的签密方案[8-12]，所解决的都是单一环境下安全通信的问题，并不适用于电子商务，移动通信或者智能卡等多环境领域。为此，Sun 和 Li[13](2010)提出了基于传统公钥密码体制（TPKC）和基于身份公钥密码体制（IDPKC）之间的签密方案,实现异构密码系统之间的通信，但是,这些案效率较低，仅仅满足外部安全性(即攻击者不能是发送者或者接收者)，也不能提供否认性，更不具备内部安全性（即如果发送者的私钥丢失了，攻击者也不能从密文中恢复出消息，如果接收者的私钥丢失了，攻击者也不能伪造一个密文）。Li、Zhang、Takagi[14]提出一个类型 I 的方案(记为 LZT-I 方案)和一个类型 II 的方案(记为 LZT-II 方案）,这两个方案都是基于传统公钥密码体制(TPKC)和基于身份公钥密码体制（IDPKC）两种密码系统，虽然他们所提出方案既满足内部安全性,又满足外部安全性，但是效率较低。因此,两种不同的密码体制都有各自的优缺点，不同的计算机和通信系统都有不同的需求，本文方案利用双线性对构造了高效的 TPKC→IDPKC 异构签密方案，不仅实现异构密码系统之间安全通信问题，同时保证了通信过程中的机密性和不可伪造性，而且在效率上有了一定的提高。

本文所提出的方案，是在参考 Li、Zhang、Takagi[14]所提出的类型 I 的方案(记为 LZT-I 方案)基础上进行改进的方案，不仅满足了外部安全性和内部安全性，而且包含三个更重要的特性：1)方案具有“密钥隐私”的特性，即解密时候，不需要知道发送者 *Alice* 的公钥，实现了发送者身份的匿名性。2)该方案的签名 V 涉及到 E 的计算，在不知道接收者 *Bob* 私钥的情况下，攻击者不能重构签名 V 。如果不知道 E ，即使知道发送者 *Alice* 的私钥也不能构造出签名 V ，这个特点使得方案在适应性选择密文攻击下是安全的。3)在效率方面上，本方案有了较的提高。

2 基础知识

在这一部分中，我们简单描述一下双线性对的基本定义和属性。设 P 、 $Q \in G_1$， P 为生成元，G_1 是由 P 生成的循环加法群，阶为素数 q，G_2 同样也是阶为素数 q 的循环乘法群。存在双线性映射 $e: G_1 \times G_1 \to G_2$，满足：

(1)双线性：$e(aP,bQ)=e(P,Q)$；

(2)非退化性：存在 P 、 $Q \in G_1$，使得 $e(P,Q) \neq 1$；

(3)可计算性：存在有效算法可以计算 $e(P,Q)$。

3TPKC→DPKC 异构签密方案的形式化定义

TPKC→IDPKC 异构签密方案一般包括以下五个算法:系统建立算法、TPKC 密钥生成算法、IDPKC 密钥提取算法、签密算法、解签密算法、验证算法。

(1)TPKC 系统建立算法

该算法通过 CA 来实现，输入参数 1^k，产生系统参数 *params*，并公开，这里的 k 是安全参数。

(2)TPKC 密钥生成算法

TPKC 系统中的用户使用该算法生成公钥 Pk 和相应的私钥 Sk 。CA 需要对者公钥进行签名并生成数字证书。

(3)IDPKC 密钥提取算法

IDPKC 系统中的用户使用这个算法获得自己的私钥。用户提交一个身份 L_2 给 PKG，PKG 计算用户私钥 S_U 并通过安全方式发送给这个用户。用户的公钥是身份 ID_U，这种公钥不需要数字证书。

(4)签密算法

该算法输入系统参数 *params* 、TPKC 环境下发送者的私钥 Sk_s 、IDPKC 环境下接收者的公钥 Pk_r 和消息 m，输出密文 σ，该算法可以表示为 $\sigma = Signcrypt(Sk_s, Pk_r, m)$。

(5)解签密算法

该算法输入系统参数 pk_s 、TPKC 环境下发送者的私钥 pk_s ,IDPKC 环境下的接收者的私钥 Sk_r 和一个密文 σ ,输出消息 m 或者“⊥”（注：表示密文 σ 对于发送者和接收者不合法）。

这些算法必须满足异构签密一致性要求，即如果 $\sigma = Signcrypt(Pk_r, m, Sk_s)$，那么 $m = Unsigncrypt(Pk_{s,} Sk_r, Signcrypt(Pk_r, m, Sk_s))$。

4TPKC→IDPKC 异构签密方案的安全模型

机密性和不可伪造性是签密方案必须满足的两个性质。同样本文异构签密方案也需要满足这两个性质，从而保证攻击者从密文中获取任何明文信息在计算上是不

可行的，或者由它产生一个合法的签密密文在计算上也是不可行的。

4.1 机密性

游戏 4.1.1(IND-SC-CCA2)

TPKC→IDPKC 异构签密方案的适应性选择密文攻击由以下五个阶段组成，挑战者 C 和敌手 A 之间进行以下游戏。

初始阶段：C 运行系统“TPKC 建立算法”，并将产生的系统参数 $params$ 发送给 A。同时运行“TPKC 密钥生成算法”获得发送者的公钥/私钥对 (pk_A, sk_A) 并将其发送给 A。

阶段 1：A 执行多项式有界的密钥提取和解签密询问。在一个秘钥提取询问中，选择一个身份 ID_U，C 运行“IDPKC 密钥提取算法”并将 ID_U 对应的私钥发送给 A。在一个解签密询问中，A 提取一个接收者身份 σ 和一个密文 σ 给 C。C 首先运行“IDPKC 秘钥提取算法”以便获得接收者 S_j，然后利用私钥 S_j 运行解签密算法 $Usigncrypt(pk_{A,}S_j,\sigma)$ 并将产生的结果发送给 A。

挑战阶段：A 决定阶段 1 何时停止并进入挑战阶段。A 产生两个相同长度的明文 m_0、m_1 和接收者身份 ID_B 并将它们发送者 C。ID_B 不能是已经执行过秘钥提取询问的身份。随机选择一个比特 $\gamma \in \{0,1\}$ 并计算 $\sigma^* = Signcrypt(sk_A, ID_B, m_{\gamma'})$。$C$ 发送 σ^* 给 A 作为挑战密文。

阶段 2：A 可以像阶段 1 那样执行多项式有界的适应性询问。但是在这一阶段，A 不能询问 ID_B 的私钥，也不能提交关于 ID_B 的解签密询问。

猜测阶段：A 输出一个比特 γ'。如果 $\gamma' = \gamma$，那么 A 赢得这个游戏。

A 的优势被定义为 $Adv(A) = \left|\Pr(\gamma' = \gamma) - 1/2\right|$，其中 $\Pr(\gamma' = \gamma)$ 表示 $\gamma' = \gamma$ 的概率。

上述定义允许敌手知道发送者的私钥，这确保了在签密机密性方面的内部安全性，即使发送者的私钥丢失，攻击者也不能从密文中恢复出消息。如果没有任何多项式有界的敌手以一个不可忽略的优势赢得游戏 4.1.1，那么称 TPKC→IDPKC 的异构签密方案在适应性选择密文攻击下具有不可区分性(IND-HSC-CCA2)。下面给出正式的定义。

定义 4.1.1 如果没有任何多项式有界的敌手在 t 时间内，在经过 q_k 次签密和 q_u 解签密询问后，以至少 ε 的优势赢得游戏 4.1.1，那么称本文方案是 $(\varepsilon, t, q_k, q_u) - IND - SC - CCA2$ 安全的。

4.2 不可伪造性

游戏 4.2.1(EUF-SC-CMA)

TPKC→IDPKC 异构签密方案的适应性选择密文攻击游戏由下面三个阶段组成，由一个挑战者 C 和敌手 F 进行游戏。

初始阶段：C 运行系统建立算法，并将产生的系统参数 $params$ 发送给 F。C 同时运行“IBC 密钥提取算法”以获得接收者的公钥/私钥对 (Pk_r, Sk_r) 并将 Pk_r 发送给 F。

攻击阶段：A 执行多项式有界的签密询问和解签密询问。在一个签密询问中，A 提交一个接收者的公钥 Pk_w 和一个消息给 C。如果 Pk_w 不等于 Pk_r 且 Pk_w 是一个合法的公钥，那么 C 运行“签密算法”并返回密文 $\sigma = signcrypt(m, Sk_r, Pk_w)$ 给 A；否则返回错误符号“⊥”。在一个解签密询问中，A 提交一个密文 σ 给 C，输出解签密密文 $Unsigncrypt(Pk_w, Sk_r, \sigma)$

伪造阶段：F 产生新的密文 σ^* 和密钥对 (Pk_r, Sk_r)。当下列两条成立时候，F 赢得这个游戏。

(1) $Unsigncrypt(Pk_w, Sk_r, \sigma)$ 输出 (m, s, Pk_s) 且满足 $\top = Verrify(Pk_s, m, s)$。

(2) F 没有询问过涉及消息 m 和接收者公钥 Pk_w 的签密询问，这个询问会返回密文 σ 并且 (Pk_s, m, s) 成立。这里的 Pk_w 可能不等于 Pk_r。

游戏 4.2.1 如果没有任何多项式有界的敌手以一个不可忽略的优势赢得游戏 4.2.1,那么说明本方案具有秘钥隐私的特性，而且在适应性选择消息攻击下具有存在不可伪造性(EUF-SC-CMA).

定义 4.2.1 如果没有任何多项式有界的敌手在 t 时间内，在经过 q_s 签密询问和 q_u 次解签密询问后，以至少 ε 的优势赢得了游戏 4.2.1，那么就称这个具有密钥隐私性质的 PKI 就称这个异构签密方案 $(\varepsilon, t, q_s, q_u) - EUF - SC - CCA2$（不可伪造性）安全的。

5 具体的 TPKC→IDPKC 异构签密

5.1 方案的构成

TPKC→IDPKC 异构签密方案包括一下算法：TPKC 系统建立算法、IDPKC 秘钥生成算法、IDPKC 秘钥提取算法、签密算法和解签密算法。具体算法如下：

(1)系统建立算法

设 G_1 为 p 生成的循环加法群，阶为 p（p 为 k 比特素数，k 为安全参数），定义生成元 $P\in G_1$，G_2 为具有相同阶的 p 的循环乘法群，存在一个双线性映射 $e:G_1\times G_1\to G_2$。定义三个 *Hash* 函数 $H_1:\{0,1\}^{l_m}\times G_1^3\to Z_p^*$、$H_3:G_2\to\{0,1\}^{l_m}$、$H_3:G_2\to\{0,1\}^{l_m}$，$l_m$ 是签密消息的长度,，PKG 随机选择一个主密钥 $s\in Z_p^*$，计算 $g=e(P,P)$。设 $g=e(P,P)$，PKG 公开系统参数 $\{G_1,G_2,e,P,P_{pub},l_m,g,H_1,H_2,H_3\}$，保密主密钥 s。

(2)TPKC 密钥生成算法

PKI 系统中的用户随机选择 $Sk_u\in Z_p^*$，作为自己的私钥，并且设置自己的公钥 $Pk_u=Sk_u P$。

(3)IDPKC 密钥提取算法

IBC 系统中的用户提交身份 ID_v 给 PKG，PKG 计算用户的用户的私钥 $Sk_v=\dfrac{1}{H_1(ID_v)+s}P$。

(4)签密算法

假设用户 *Alice* 属于 TPKC 系统，作为发送者，它的公钥为 $Pk_A=Sk_A P$，私钥为 Sk_A；用户 *Bob* 属于 IDPKC 系统，作为接收者，它的公钥就是身份信息 $Q_B=H_2(ID_B)$，私钥 Sk_B。当 *Alice* 希望通过签密方式发送消息 m 交给 *Bob* 时，执行以下步骤：

①随机选择 $r\in Z_p^*$，并计算 $W=rP$ 和 $Q_B=H_2(ID_B)$。

②计算 $V=Sk_A H_1(m,W,Q_B)$。

③计算 $x=g^r$ 和 $c=m\oplus H_3(x)$。

④计算 $T=r[H_1(ID_B)P+P_{pub}]$。

⑤消息 m 的签密密文：$\sigma=(c,T,W,V)$。

5)解签密算法

①计算 $x=e(T,Sk_B)$ 和 $m=c\oplus H_3(x)$

②计算 $N=H_1(m,W,Q_B)$ 和 $Q_B=H_2(ID_B)$

③如果 $Pk_A\notin G_1$，那么输出错误符号“⊥”，检查等式 $e(Pk_A,N)=e(P,V)$，是否成立，如果成立，那么输出 $(m,(W,Q_B,V),Pk_A)$，否则输出错误符号“⊥”。

5.2 方案的正确性

本方案满足一致性要求:接收者 Bob 可以正确的解密，签名也可以被正确的验证。

(1)正确的解密：当 Bob 收到密文 $\sigma=(c,T,W,V)$ 时，可以正确的解密。

$$e(T,Sk_B)=e(r(H_1(ID_B)P+P_{pub}),Sk_B)$$

$$e(T,Sk_B)=e(r(H_1(ID_B)P+P_{pub}),\frac{1}{H_1(ID_B)+s}P)$$

$$e(T,Sk_B)=e(rP,P)$$

$$e(T,Sk_B)=g^r=x$$

(2)正确的验证：当 Bob 收到密文 $e(Pk_A,N)=e(P,V)$ 和 *Alice* 的公钥，从检查验证等式：$e(Pk_A,N)=e(P,V)$。

$$e(Pk_A,N)=e(P,V)$$

$$e(Pk_A,N)=e(Sk_A P,H_1(m,W,Q_B))$$

$$e(Pk_A,N)=e(P,Sk_A H_1(m,W,Q_B))$$

$$e(Pk_A,N)=e(P,V)$$

5.3 方案的不可伪造性

定理 5.3 在随机预言模型中，若存在一个敌手 F 能够以 ε 的优势攻破本方案 EUF-SC-CMA 的安全性，则存在一个算法 C，以 $(1-q_u 2^{-poly(k)})(1-q_{H1}q_s 2^{-poly(k)})$ 的优势解决 CDH 问题。其中，q_u 表示最大的解签密询问次数；q_{H_1} 表示最大的 H_1 询问次数；q_s 表示最大的签密询问次数，$ploy$ 表示一个多项式；k 为安全参数。

证明：假设存在敌手 F 能以一个不可忽略的优势赢得游戏 4.1.1，那么可以得出一个算法 C 来解决 CDH 问题。C 接收一个随机的 CDH 问题实例（P，aP，bP），它的目标计算出 abP。C 把 F 作为游戏 4.1 中 F 的挑战者。

初始阶段：C 运行“系统建立算法”将系统参数发送给 F，同时将主密钥 s 也发送给 F，同时运行“TPKC 密钥生成算法”获得发送者的公钥/私钥 (Pk_A,Sk_A) 发送给 F 并且设 $Pk_r=Pk_B=bP$ 为挑战公钥。

阶段 1：C 维护 L_1 和 L_2 两个不同的列表，分别用于跟踪 F 对预言机 H_1 和

H_2的询问，这些回答是随机产生的，但要维持一致性冲突。

H_1询问：对于一个$(P_1,P_2,\perp)$询问，C首先检查元组(m,P_1,P_2,P_3)是否已经存在于列表L_1中。如果已经存在，那么返回存在的结果。如果不存在并且等式$e(P_1,P_2)=e(P,P_3)$成立和$(P_1,P_2,\perp)$已经存在列表L_1中，C用P_3代替“$\perp$”并将存在的结果返回给F。对其他的情况，C随机选择$t\in Z_p$并返回taP给F。询问的元素和返回的值都将存储在列表L_1中。为了便于以后模拟时能得到t的值，t也将存储在列表L_1中。

H_2询问：这些询问用一个计数器v来标记，其初始值为 1。对于一个$H_1(ID_v)$询问，C返回e_v作为回答，将(ID_v,e_v)存进列表L_2并将计数器v的值的加 1。

H_3询问：当A询问$H_3(x_i)$时，C首先检查列表L_3是否已经存在这个询问的条目，如果存在，那么返回相同的回答；否则，C从$\{0,1\}^{l_m}$中随机选取$h_{3,i}$作为回答，将元组$(x_i,h_{3,i})$存入列表L_3。

签密询问：F提交一个接收者的公钥Pk_w和一个消息m给C。如果Pk_w不合法或者等于Pk_s，那么返回一个错误符号“$\perp$”；否则C随机选择$r\in Z_p$，计算$W=rP$。如果$(m,W,Pk_\omega,rPk_\omega)$经存在于$L_1$中且相应的$Hash$值是$taP$，那么$C$失败并停止。否则，$C$随机选择$t'\in Z_p$并返回$t'P$作为$H_1(m,W,Pk_\omega,rPk_\omega)$的值，询问元组、返回值和$t'$都被存进列表$L_1$中。$C$计算$(W,Pk_s,\lambda)$，同理可以获得$H_2(m,W,Pk_\omega,rPk_\omega)$并计算$T=(m\|Pk_s\|t'Pk_s)\oplus H_2(W,Pk_\omega,rPk_\omega)$得到密文$\sigma=(T,W)$。

解签密询问：F提交一个签密密文$\sigma=(T,W)$给挑战者C，得出解签密密文$Unsigncrypt(Sk_s,\sigma)$。执行下面的步骤：

(1)在列表L_2中查找元组(W,Pk_s,λ)使得$e(P,\lambda)=e(U,Pk_s)$成立或$\lambda=\perp$。如果列表L_2中不存在元组$\lambda=\perp$，那么在L_2中插入一个新的条目，这个条目以$(U,Pk_s,\perp)$为询问元组。符号“$\perp$”表示(P,U,Pk_s)的 CDH 问题的解。这一步确保了$(P,\lambda)=(W,Pk_s)$在σ解签密前确定下来。如果元组(W,Pk_s,λ)已经存在于L_2中，那么存在的结果将为$H_2(W,Pk_s,\lambda)$的值。

(2)计算$(m\|Pk_A\|\gamma)\oplus T\oplus H_2(W,Pk_s,\lambda)$并在列表$L_1$中查找$(m,W,Pk_s,\lambda)$使得$(P,\lambda)=(W,Pk_s)$成立或者$\lambda=\perp$。如果$L_1$中不存在$H_1(m,W,Pk_s,\lambda)$，那么$L_1$中插入一个新的条目，这个条目以$(m,W,Pk_s,\lambda)$为询问元组，以一个随机值$taP$为返回值。这里$t\in Z_p$。值得注意的是，$\lambda$可能已经从上面的$L_2$获得，等式$e(P,\lambda)=e(W,Pk_s)$可能成立。如果元组$(m,(W,Pk_s,\lambda,V)$已经存在于$L_1$中并且等式$e(P,\lambda)=e(W,Pk_s)$成立，那么存在的值作$H_1(m,W,Pk_s,\lambda)$的值，$\lambda$也用于更新$L_2$中相应的条目。如果$abP=t^{-1}V$存在于$L_1$中。如果$\lambda$可以从$L_2$中获得，那么$(m,W,Pk_s,\perp)$也应该被更新为$(m,W,Pk_s,\lambda)$。

(3)检查等式$e(Pk_A,H_1(m,W,Pk_s,\lambda))=e(P,V)$否成立。若不成立，则输出错误符号“$\perp$”否则进一步检查等式$e(P,\lambda)=e(W,Pk_s)$是否成立。若成立，则输出消息/签名$(m,(W,Pk_s,\lambda,V)$发送者的公钥$Pk_A$。若$\lambda=\perp$，则$C$失败并停止。

伪造阶段：当F产生一个密文σ和一个密钥对(Sk_r,Pk_r)时，$V=taP$按照上述解签密模拟的步骤对密文进行解签密。如果这个伪造是合法的，那么有$e(Pk_s,H_1(U,Pk_s,\lambda,V))=e(P,V)=e(bP,taP)$$C$可以得到$V=taP$并解决 CDH 问题$abP=t^{-1}V$，$C$输出$abP$并停止。

由上面的解签密模拟可以看出，L_1中必定存在一个针对$H_1(m,W,Pk_r,\lambda)$的条目且相应的返回值一定是taP形式。如果说$H_1(m,W,Pk_r,\lambda)$的值为$t'P$，即从签密询问中生成，那么Z也应该在签密询问阶段生成。这于游戏 4.2 中的限制条件（σ不是由签密预言机输出的）相矛盾。

C失败的情况有两种。第一种在签密询问中，选择了$r\in Z_p$，$(m,W=rp,Pk_\omega,Pk_\omega)$已经询问过了$H_1$了，这种事件发生的概率为$q_{H_1}q_s/l_1$。$C$不失败的概率

至少为 abP。第二种在解签密询问中，同理也可以得出 C 在解签密询问中不失败的概率至少为 $1-q_u 2^{-poly(k)}$。如果 C 不失败并且 F 赢得了这个游戏，那么 C 能够解决 CDH 问题。因此，Pr[F 赢得游戏∧不失败]$\geq(1-q_u 2^{-poly(k)})(1-q_{H_1}q_u 2^{-poly(k)})\varepsilon$。

5.4 方案的机密性

定理 5.4 在随机预言模型中，若存在一个敌手 A 能够在 t 时间内，以 q_{H_1} 的优势解决游戏 4.2.1[他(她)最多能进行 q_{H_1} 次 H_1 询问、q_{H_2} 次 H_2 询问、q_{H_3} 次 H_3 询问和 q_u 次解签密询问]，则存在一个算法 C，能够在 $t' \leq t+O(q_u)t_p+O(q^2H_1)t_m+O(q_uq_{H_2})t_e$ 时间内，以 $\varepsilon' \geq \frac{\varepsilon}{q_{H_1}(q_{H_2}+q_{H_3})}(1-\frac{q_u}{2^k})$ 的优势解决 n-BDHI 问题，其中 t_p 表示计算一次双线性对运算所需要的时间，G_1 表示 G_1 中计算一次点乘运算所需要的时间，t_e 表示 G_2 中计算一次指数运算所需要的时间。

证明：假设存在一个敌手 ε 能够以一个能够以一个不可忽略的优势赢得 4.2.1，那么构造一个算法 C 来解决 n-BDHI 问题。C 接收一个随机的 n-BDHI 问题实例 (P,aP,bP)，它的目标是计算出 abP。

初始阶段：C 随机选择 $\tau\in\{1,...,q_{H_1}\}$，$e\in Z_p^*$ 和 ω_1，…，$\omega_{\tau-1}$，$\omega_{\tau+1}$，$\omega_n\in Z_p^*$。对于 $i=1$，…，$\tau-1$，$\tau+1$，…，n，C 计算 $e_i=e_\tau-\omega_i$，并使用它的输入计算一个生成元 $Q\in G_1$ 和 $X=\alpha Q\in G_1$ 以至于它知道 $n-1$ 对 $(\omega_i, Vi=\frac{1}{\alpha+\omega_i}Q)$，$i\in\{1,...,n\}\backslash\{\tau\}$。$C$ 为了获得这样的元素，C 展开多项式：$f(z)=\prod_{i=1,i\neq\tau}^{n}(z+\omega_i)=\sum_{j=0}^{n-1}c_jz^j$ 生成元 Q 和元素 X 可以分别通过 $Q=\sum_{j=0}^{n-1}c_j(\alpha^jP)=f(\alpha)P$ 和 $X=\sum_{j=1}^{n}c_{j-1}(\alpha^jP)=\alpha f(\alpha)=\alpha Q$ 得到。同时 (ω_i,V_i) 可以通过 $f_i(z)=\frac{f(z)}{z+\omega_i}=\sum_{j=0}^{n-2}d_jz^j$ 并计算 $Vi=\sum_{j=0}^{n-2}d_j(\alpha^jP)=fi(\alpha)P=\frac{f(\alpha)}{\alpha+\omega_i}P=\frac{1}{\alpha+\omega_i}Q$ 得到。PKG 的公钥设为 $Q_{pub}=-X-e_\tau Q=(-\alpha-e_\tau)Q$，相应的私钥为 $s=-\alpha-e_\tau\in Z_p^*$。对于 $i\in\{1,...,n\}\backslash\{\tau\}$，这里有 $(e_i,-V_i)=(e_i,\frac{1}{e_i+s}Q)$。

C 将系统参数[包括 Q、$Q_{pub}=(-\alpha-e_\tau)Q$]和 $g=e(Q,Q)$]发送给 (Pk_A,Sk_A)。C 同时运行秘钥生成算法以获得发送者的公钥/私钥对 (Pk_A,Sk_A) 并发送给 A

阶段 1：C 模拟游戏 4.2.1 中 A 的挑战者。C 维护 L_1、L_2、L_3 三张列表，分别用于跟踪 A 对预言机 H_1、H_2、H_3 的询问，这些回答是随机产生的，但要维持一致性并避免冲突。这里假设每次 H_1 询问是不同的，目标身份 ID_B 在某个时候被询问过 H_1 和身份 ID 在被使用到其它询问之前已经询问过 H_1 预言机。

H_1 询问：对于一个 $C=(m,P_1,P_2,P_3)$ 询问，C 首先检查元组 (m,P_1,P_2,P_3) 是否已经存在于列表 L_1 中。如果已经存在，那么返回存在的结果。如果不存在并且等式 $e(P_1,P_2)=e(P,P_3)$ 成立和 $(P_1,P_2,\top)$ 已经存在列表 L_1 中，C 用 P_3 代替“$\top$”并将存在的结果返回给 F。对其他的情况，C 随机选择 $t\in Z_p$ 并返回 tP 给 F。询问的元素和返回的值都将存储在列表 L_1 中。为了便于以后模拟时能得到 t 的值，t 也将存储在列表 L_1 中。

H_2 询问：这些询问用一个计数器 v 来标记，其初始值为 1。对于一个 $H_1(ID_v)$ 询问，C 返回 e_v 作为回答，将 (ID_v,e_v) 存进列表 L_2 并将计数器 v 的值的加 1。

H_3 询问：当 A 询问 $H_3(x_i)$ 时，C 首先检查列表 L_3 是否已经存在这个询问的条目，如果存在，那么返回相同的回答；否则，C 从 $\{0,1\}^{l_m}$ 中随机选取 $h_{3,i}$ 作为回答，将元组 $(x_i,h_{3,i})$ 存入列表 L_3。

密钥提取询问：当 A 询问 ID_i 的私钥时，如果 $i=\tau$，那么 C 失败并停止；否

则 C 知道 $H_1(ID_i)e_i$，并返回 $-V_i=\frac{1}{e_i+s}Q$ 给 A。

解签密询问：A提交一个接收者身份 ID_j 和一个密文给挑战者 C。如果 $j=\tau$，那么 C 知道接收者的私钥 $S_j=-V_j$，可以按照正常的解签密步骤来回答这个询问。如果 $j=\tau$，那么对于所有合法的密文，有 $\log_{Sk_A}(V-hSk_A)=\log_{e_jQ+Q_{pub}}T$，这里这里的 $h=H_2(m,$ 。因此，等式 $e(T,Sk_A)=e(e_jQ+Q_{pub},V-hSk_A)$ 成立。C 首先计算 $\xi=e(V,e_jQ+Q_{pub})$ 并在 L_2 中查找形式为 $\{mi,xi,h2,i,c,\xi\}$ 的条目，这里 $i\in\{1,...,q_{H_2}\}$。如果没有这样的条目，那么 C 拒绝回答 σ 的解签密询问；否则 C 进一步检查等式 $\frac{e(T,Sk)}{e(e_jQ+Q_{pub},V}=e(e_jQ+Q_{pub},V-hS_j$。如果唯一满足上述方程的 $i\in\{1,...,q_{H_2}\}$ 已找到，那么 C 返回匹配的消息 m_i；否则 C 拒绝回答的解签密询问。容易看出，对于所有的解签密询问，拒绝一个合法密文的概率不会超过 $\frac{q_u}{2_k}$。

挑战阶段：A产生两个相同长度的明文 m_0 和 m_1 和接收者身份 $ID_B\neq ID_\tau$ 并将他们发送给 C。如果 $ID_B\neq ID_\tau$，那么 C 终止；否则 C 随机选择 $c^*\in\{0,1\}$、$V^*\in G_1$ 和 $T^*=-\lambda Q$ 并计算 $T^*=-\lambda Q$。C 返回密文 $\sigma^*=(c^*,V^*,T^*,W$ 给 A。如果定义 H_2 且 $s=-\alpha-e_\tau$，那么就有 $T^*=-\lambda Q=-\rho\alpha Q$ $T^*=-\lambda Q=-\rho\alpha Q$ $\rho e_\tau Q+\rho Q_{pub}$ 除非 A对进行 σ^* 和 H_3 询问，否则他（她）不能辨别出 σ^* 是一个不合法的密文。

阶段 2：A可以像阶段 1 那样执行多项式有界的适应性询问。但是在这一阶段，ID_B 不能询问 $ID_B\sigma^*$ 的私钥，也不能执行 σ^* 关于 ID_B 的解签密询问。Pr 按照阶段 1 的方法进行回答。

猜测阶段：A输出一个比特 $Y`$，C 忽略这个输出。

C 从列表 L_2 或者 L_3 中提取一个随机的条目 $(m_i,x_i,h_{2,i}c_i,\xi_i)$ 或者 $(x_i,h_{3,i})$。既然 L_3 包含的条目至多为 $2q_{H_2}+q_{H_3}$，那么随机选择的条目包含了正确元素 $x_i=e(Q,Q)^\rho=e(P.P)^{f(\alpha)^2\lambda/\alpha}$ 的概率为 $\frac{1}{2q_{H_2}+q_{H_3}}$。如果 $\xi^*=e(P,P)^{1/\alpha}$，那么 n-BDHI 问题可以通过下式解决：

$$e(Q,Q)^{1/\alpha}=\xi^{*(c_2^0)}e(\sum_{j=0}^{n-2}c_{j+1}(\alpha^jP),c_0P)e(Q,\sum_{j=0}^{n-2}c_{j+1}(\alpha_j)P)$$

这就完成了模拟的描述。

下面分析 C 的优势，定义了三个事件：E_1、E_2 和 E_3。

ID_τ：A在挑战阶段没有选择 ID_τ 为接收者的身份。

E_2：A对身份 ID_τ 进行了秘钥提取询问。

E_3：A由于在解签密询问中拒绝了一个合法的的密文而终止。

由上面的分析来看：不终止的概率为 $Pr[\neg终止]=Pr[\neg E_1\wedge\neg E_2\wedge\neg E_3]$，$Pr[\neg E_1]=1/q_{H_1}$ 和 $r[E_3]\leq q_u/2^k$。此外，$\neg E_1$ 意味着 $\neg E_2$。所以，有 $Pr[\neg终止]\geq\frac{1}{q_{H_1}}(1-\frac{q_u}{2^k})$。另外，$C$ 从 L_3 或者 L_3 中选择正确元素的概率为 $\frac{1}{2q_{H_2}+q_{H_3}}$。因此有 $\varepsilon'\geq\frac{\varepsilon}{q_{H_1}(2q_{H_2}+q_{H_3})}(1-\frac{q_u}{2^k})$。

5.5 方案的效率分析

在异构签密方案中，衡量方案率的优劣主要参照对运算和幂运算的运算量，所以，本方案在尽量减少对的使用对和幂的运算。在表 1 中，列出了该文方案与文章[14]方案中所需要的运算量，其中 p 表示对运算，e 表示幂运算。分析表 1 数据可知，该文方案的效率是比较高。

表 1 该文方案与其他方案所需的运算量

方案	签密	解签密
文献[14]	1e	2p+1e
本文方案	1e	1p

6 结束语

异构签密是一个很重要的研究方向，在计算机通信网络中具有很重要的应用价值。本文提出的 TPKC→IDPKC 异构签密方案是在随机预言机模型下设计的， 实现在安全通信过程中机密性和不可伪造性两个目标。本方案虽然基于不同的公钥密码

系统实现的，但是两种系统所采用的参数都是相同的，得出的效果并不是很理想，所以在以后异构签密的研究中，不同的密码系统采用不同的参数，努力使得结论有很大的对比性和可参照性；虽然该文方案效率上有了较大的提高，但是总体而言没有达到预期的结果，如果以后在异构签密的研究中，将离散对数或者椭圆曲线等知识应用到异构签密中，效率将会大大的提高。但是，在未来的工作，将继续对方案的效率进行改进，而且可能设计标准模型下安全的异构签密[15]，或者特殊性质的异构签密。此外，还可以设计发送者属于基于身份的公钥密码系统、接收者属于无证书密码系统或者发送者属于无证书密码系统[16]、接收者属于基于身份公钥系统的异构签密。

参考文献：

[1]李发根. 数字签密原理与技术[M]. 科学出版社, 2014.

[2]Baek J, Steinfeld R, Zheng Y. Formal Proofs for the Security of Signcryption[J]. Journal ofCryptology, 2002, 20(2):80-98.

[3]Bao F, Deng R H. A Signcryption Scheme with Signature Directly Verifiable by Public Key.[C]// Public Key Cryptography, First International Workshop on Practice and Theory in Public Key Cryptography, PKC '98, Pacifico Yokohama, Japan, February 5-6, 1998, Proceedings. 1998:55-59.

[4]Gamage C, Leiwo J, Zheng Y. Encrypted Message Authentication by Firewalls[C]// Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, March 1-3, 1999, Proceedings. 1999:69-81.

[5]Zheng Y, Imai H. How to construct efficient signcryption schemes on elliptic curves[J]. Information Processing Letters, 1998, 68(5):227-233.

[6]Malonelee J, Mao W. Two Birds One Stone: Signcryption Using RSA[M]// Topics in Cryptology — CT-RSA 2003. Springer Berlin Heidelberg, 2003:211-226.

[7]Li C K, Yang G, 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.

[8]Libert B, Quisquater J J. A new identity based signcryption scheme from pairings[J]. IEEE Information Theory Workshop, 2003:155--158.

[9] Chow S S M, Yiu S M, Hui L C K, et al. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity[M]// Information Security and Cryptology - ICISC 2003. 2004:352-369.

[10]Boyen X. Multipurpose Identity-Based Signcryption - A Swiss Army Knife for Identity-Based Cryptography[C]// CRYPTO. 2003:383--399.

[11] Chen L, Malonelee J. Improved Identity-Based Signcryption[M]// Public Key Cryptography - PKC 2005. Springer Berlin Heidelberg, 2005:362-379.

[12]Barreto P S L M, Libert B, Mccullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]// International Conference on Theory and Application of Cryptology and Information Security. Springer-Verlag, 2005:515--532.

[13]YinXia, LI, Hui. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. Sciece China Information Sciences, 2010, 53(3):557-566.

[14] Li F, Zhang H, Takagi T. Efficient Signcryption for Heterogeneous Systems[J]. IEEE Systems Journal, 2013, 7(3):420-429.

[15] Huang Q, Wong D S, Yang G. Heterogeneous Signcryption with Key Privacy[J]. Computer Journal, 2011, 54(4):525-536.

[16]张玉磊, 李臣意, 周冬瑞,等. 高效的可撤销无证书签名方案[J]. 计算机工程, 2015, 41(7):157-162.