doi:10.3969/j.issn.1000-436x.2013.07.010

高效的选择密文安全的单向代理重加密方案

张维纬[1,2]，张茹[1,2]，刘建毅[1,2]，钮心忻[1,2]，杨义先[1,2]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 北京邮电大学 灾备技术国家工程实验室，北京 100876)

摘 要：针对如何构造一个在标准模型下高效的选择密文安全的单向代理重加密方案这个问题，提出了一种新的、高效的单向代理重加密方案，并且在标准模型下证明了方案在自适应攻陷模型下的选择密文安全性。所提方案与 LV 方案相比，在安全性和效率方面都有所提升，与 WJ 方案相比，在同等安全条件下，运算效率有所提高。
关键词：代理重加密；选择密文安全；自适应攻陷模型；标准模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)07-0087-11

Efficient chosen-ciphertext secure proxy re-encryption scheme

ZHANG Wei-wei[1,2], ZHANG Ru[1,2], LIU Jian-yi[1,2], NIU Xin-xin[1,2],YANG Yi-xian[1,2]
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to construct an efficient and chosen-chiphertext secure unidirectional re-encryption scheme in the standard model, a novel and efficient unidirectional proxy re-encryption scheme was proposed, and its chosen-ciphertext security in the adaptive corruption model was proved in the standard model. Compared with LV scheme, this scheme has the advantages of both higher efficiency and stronger curity. Under the same security level, this scheme has lower computational cost than that of WJ scheme.
Key words: proxy re-encryption; chosen-ciphertext security; adaptive corruption model; standard model

1 引言

在 1998 年的欧洲密码学年会上，Blaze 等[1]首次提出了代理重加密(PRE，proxy re-encryption)的概念，在一个代理重加密方案中，一个拥有转换密钥的半可信代理者可以把用 Alice 公钥加密的消息 m 所得的密文转换为用 Bob 公钥加密的消息 m 所得到的密文，但这个过程中半可信代理者不能获得关于消息 m 的任何信息。近年来，PRE 在很多场合得到了应用，如加密电子邮件的转发[1]、此外，代理重加密还可以应用于分布式文件系统[2,3]、DRM 互操作系统中内容加密密钥或多媒体内容的转换[4,5]、云环境中用户文件的加密和传感器网络中用户敏感数据的分类加密[6,7]等。

以分布式文件系统为例，Alice 在不完全可信的服务器上存储了以其公钥加密的文件，允许它在指定的用户访问，但 Alice 可能无法在每次用户进行数据访问时都在线进行密文转换。采用代理重加密方案，Alice 可以使用自己的私钥及指定用户的公钥计算一个重加密密钥，存储于代理服务器上，当用户访问文件时，服务器用相应的重加密密钥将密文重加密成可由用户私钥解密的密文。代理重加密方

收稿日期：2012-06-12；修回日期：2013-01-19
基金项目：国家自然科学基金资助项目(61003284)；北京市自然科学基金资助项目(4122053)；中央高校基本科研业务费专项基金资助项目(BUPT2011RC0210)；新闻出版重大科技工程项目研发“数字版权保护技术研发工程”基金资助项目(GXTC-CZ-1015004/09, GXTC-CZ-1015004/15-1)
Foundation Items: The National Natural Science Foundation of China (61003284); Beijing Municipal Natural Science Foundation(4122053); The Fundamental Research Funds for the l Universities (BUPT2011RC0210); Press and Publication of Major Science and Technology Research and Development Projects “Digital Rights Protection Technology Research and Deve Project” (GXTC-CZ-1015004/09, GXTC-CZ-1015004/15-1)

案的性质保证了代理服务器无法获得明文，也无法得知 Alice 与用户的私钥。

Blaze 等[1]首次提出了双向 PRE 方案。Ateniese 等[2]利用双线性配对构造了 3 种单向 PRE 方案，他们的 PRE 方案都只是在 DBDH 假设的标准模型下满足选择明文安全(CPA, chosen-plaintext attack)的。但实际的应用场合通常都要求密文满足选择密文安全(CCA, chosen-ciphertext attack)。Canetti 等[8]首次利用 CHK (canetti-halevi-katz methodology) [9]技术构造了一种在标准模型下满足 CCA 安全的双向多跳 PRE 方案，但是与 Ateniese 等[2]提出的双向 PRE 方案的缺点一样，该方案也不能抵抗共谋攻击。他们留下了一个公开的问题，即如何构造一个在标准模型下单向 CCA 安全的 PRE 方案。值得注意的是，构造一个单向 PRE 方案比双向 PRE 方案困难，因为任何双向的 PRE 方案都可以通过单向的 PRE 方案实现。Libert 等[10]首次提出了一种在标准模型下能抵抗共谋攻击的单向 PRE 方案，该方案只满足重放选择密文安全(RCCA, replayable chosen ciphertext attack)，RCCA 安全级别比 CCA 低，因为 RCCA 安全模型中不允许敌手询问挑战明文的任何形式的密文解密预言机。Weng 等[11]利用 Hohenberger 等[12]所提出的签名方案中的一个技巧及借助伪随机函数族构造了一个标准模型下 CCA 安全的单向单跳的 PRE 方案。

上述文献[2,8,10,11]所提出的 PRE 方案都需要双线性配对运算，而运行一次双线性对运算的时间至少是椭圆曲线上点乘运算的 20 倍以上[13]。针对这个问题，有学者提出无需双线性配对运算构造的 PRE 方案[14,15]，但这些方案都是在随机预言模型下 CCA 安全的。正如 Canetti 等[16]指出的那样，存在这样的实际签名和加密方案，在随机预言模型中是安全的，但任何具体实现都是不安全的。

近年来，也有学者提出了基于身份的 PRE 方案[17,18]、基于关键词搜索的 PRE 方案[6,7]等。但如何在标准模型下构造一个高效的单向、单跳的 PRE 方案仍然是一个有待解决的重要问题。

本文使用 CHK 技术和随机填充技术构造了一种新的高效的单向、单跳 PRE 方案，并且在无需随机预言机的模型下证明了方案的 CCA 安全性。该方案只需要一次强签名函数以及单向、抗碰撞的散列函数。所提方案在安全性和运算效率方面都优于 LV 方案[10]，而在同等安全性条件下，运算效率优于 WJ 方案[11]。

2 预备知识

2.1 双线性配对

令群G_1和群G_2是 2 个乘法有限循环群，它们的阶为素数 p，双线性配对 $e:G_1\times G_1\to G_2$ 满足如下条件。

1) 双线性：$\forall g,h\in G_1,\forall a,b\in Z_p$，均有 $e(g^a,h^b)=e(g,h)^{ab}$ 成立。

2) 非退化性：存在 $g,h\in G_1$，使 $e(g^a,h^b)\neq 1_{G_2}$ 成立，其中，1_{G_2} 表示群 G_2 的单位元。

3) 可计算性：存在一个有效的算法使得对于 $\forall g,h\in G_1$ 均可计算 $e(g,h)$。

2.2 复杂性假设

本方案的复杂性假设与文献[10,11]相同，即基于 3-弱判定型双线性迪菲-赫尔曼求逆(3-wDBDHI, 3-weak decision bilinear Diffie-Hellman inversion)假设。即给定 $(g,g^a,g^{a^2},g^{a^3},g^b,Q)\in G_1^5\times G_2$，其中，$a,b\in Z_p^*$ 未知，判断 $Q=e(g,g)^{b/a}$ 是否成立。文献[10]已经证明，该问题也等价于给定 $(g,g^{1/a},g^a,g^{a^2},g^b,Q)\in G_1^5\times G_2$，判断 $Q=e(g,g)^{b/a^2}$ 是否成立。

一个概率性多项式时间(PPT, probabilistic polynomial-time)算法B如果满足：

$$|\Pr[\mathrm{B}(g,g^{1/a},g^a,g^{a^2},g^b,Q=e(g,g)^{b/a^2})=1]-\Pr[\mathrm{B}(g,g^{1/a},g^a,g^{a^2},g^b,Q=e(g,g)^{c})=1]|\geq e$$

其中，$a,b,c\in Z_p^*$，则称算法B能够以优势 e 求解群 (G_1,G_2) 中的 3-wDBDHI 问题。

若对于任意 t – 时间的算法B，均无法以优势 e 求解群 (G_1,G_2) 中的 3 – wDBDHI 问题，则称群 (G_1,G_2) 中的 (t,e) – 3 – wDBDHI 假设成立。

2.3 一次性强签名函数[10]

一次强签名函数 $Sig=(G,S,V)$ 包括 3 个算法，即密钥产生算法G、签名算法S和验证算法V。输入安全参数 k，密钥产生算法G输出密钥对 (svk,ssk)，对于消息 m，如果签名值为 $s=\mathrm{S}(ssk,m)$，则验证函数 $V(s,svk,m)$ 输出 1，否则输出 0。

与文献[8,10]一样，提出的方案也需要强的不可伪造的一次签名函数，即要求不存在 PPT 的敌手能够为签名的消息产生一个有效的新签名。

定义 1 $Sig=(G,S,V)$ 是一个强的一次签名函数，如果对于任何的 PPT 函数 F，伪造签名值

成功的概率 Adv^{SIG} 是可忽略的。此处 Adv^{SIG} 的定义为

$$Adv^{\mathrm{SIG}} = \Pr[(ssk, svk) \leftarrow \mathsf{G}(1^k); (m, St) \leftarrow \mathsf{F}(svk); s \leftarrow \mathsf{S}(ssk, m); (m', s') \leftarrow \mathsf{F}(m, s, svk, St): \mathsf{V}(s', svk, m') = 1 \wedge (m', s') \neq (m, s)]$$

其中，St 表示 F 的状态信息。

3　单向 PRE 的模型定义

3.1　单向 PRE 的定义

定义 2　一个单向单跳代理重加密方案包括如下算法。

$\mathrm{Setup}(1^k)$：输入安全参数 1^k，系统参数产生函数输出一个全局公开参数 par。

$\mathrm{KeyGen}(par) \rightarrow (pk, sk)$：输入全局公开参数 par，密钥产生算法 KeyGen 输出公钥 pk 和私钥 sk。

$\mathrm{Enc}_2(par, pk, m) \rightarrow C$：输入公钥 pk、明文 m 和全局公开参数 par，加密算法 Enc_2 输出第 2 层密文 C。

$\mathrm{Enc}_1(par, pk, m) \rightarrow C$：输入公钥 pk、明文 m 和全局公开参数 par，加密算法 Enc_1 输出第 1 层密文 C。

$\mathrm{ReKeyGen}(par, sk_i, pk_j) \rightarrow rk_{i \rightarrow j}$：输入私钥 sk_i、公钥 pk_j 和全局公开参数 par，重加密密钥产生算法 ReKeyGen 输出重加密密钥 $rk_{i \rightarrow j}$。

$\mathrm{ReEnc}(par, rk_{i \rightarrow j}, C_i) \rightarrow C_j$：输入重加密密钥 $rk_{i \rightarrow j}$、密文 C_i 和全局公开参数 par，重加密算法 ReEnc 输出重加密密文 C_j 或者错误符号 $\perp$。

$\mathrm{Dec}_2(par, sk, C) \rightarrow m$：输入私钥 sk、第 2 层密文 C 和全局公开参数 par，解密算法 Dec_2 输出所对应的明文 m 或者错误符号 $\perp$。

$\mathrm{Dec}_1(par, sk, C) \rightarrow m$：输入私钥 sk 和第 1 层密文 C 和全局公开参数 par，解密算法 Dec_1 输出所对应的明文 m 或者错误符号 $\perp$。

正确性：对于明文空间中的明文 m 和任意的两对公私钥对 $(pk_i, sk_i), (pk_j, sk_j) \leftarrow \mathrm{KeyGen}(1^k)$，必须满足以下的条件：

$$\mathrm{Dec}_1(sk_i, \mathrm{Enc}_1(par, pk_i, m)) = m$$

$$\mathrm{Dec}_2(sk_i, \mathrm{Enc}_2(par, pk_i, m)) = m$$

$$\mathrm{Dec}_1(sk_j, \mathrm{ReEnc}(\mathrm{ReKeyGen}(par, sk_i, pk_j), \mathrm{Enc}_2(par, pk_i, m))) = m$$

代理重加密算法应该允许多种类型的加密形式[2]，如第 1 层加密(Enc_1)和第 2 层加密(Enc_2)。第 1 层密文不能被重加密，而第 2 层密文可以被加密成第 1 层密文的形式。这样定义的目的是给发送者选择的余地。发送者可以根据不同的应用场景选择加密算法，即可以加密一个消息只给 Alice 或 Alice 及其下一级的访问用户。

3.2　单向 PRE 的安全性定义

通过 2 个游戏分别定义第 1 层密文和第 2 层密文的安全性。

Game1　Uni-PRE2-CCA：单向代理重加密方案第 2 层密文的 CCA 安全性定义。

阶段 1　敌手A以任何次序询问以下预言机。

公钥产生预言机 $\mathrm{O}_{pk}(i)$：挑战者B输入全局参数 par，运行算法 $\mathrm{KeyGen}(par)$ 得到公私钥对 (pk_i, sk_i)，把 pk_i 返回给敌手A。

注：以下预言机输入均包括全局参数 par。

私钥产生预言机 $\mathrm{O}_{sk}(pk_j)$：敌手A输入公钥 pk_j，挑战者B返回 pk_j 对应的 sk_j 给敌手A。

重加密密钥产生预言机 $\mathrm{O}_{\mathrm{ReKeyGen}}(pk_i, pk_j)$：敌手A输入 (pk_i, pk_j)，挑战者B返回重加密密钥 $rk_{i \rightarrow j} = \mathrm{ReKeyGen}(sk_i, pk_j)$。

重加密预言机 $\mathrm{O}_{\mathrm{ReEnc}}(pk_i, pk_j, C_i)$：敌手A输入 (pk_i, pk_j, C_i)，挑战者B返回重加密密文 $C_j = \mathrm{ReEnc}(\mathrm{ReKeyGen}(sk_i, pk_j), C_i)$。

解密预言机 $\mathrm{O}_{\mathrm{Dec}_1}(pk, C)$：敌手A输入 (pk, C)，C 为第 1 层密文。挑战者B运行 $\mathrm{Dec}_1(sk, C)$，并将结果返回给敌手A。

注释 1　为敌手A提供第 2 层密文的解密预言机是没有必要的，因为A总是可以用获得的重加密密钥加密第 2 层密文从而获得第 1 层密文，再询问第 1 层密文解密预言机得到第 2 层密文对应的明文。

挑战阶段：一旦敌手A决定阶段 1 可以结束了，就会输出 2 个等长的明文 m_0 和 m_1 及一个要挑战的公钥 pk_{i^*}，这里 pk_{i^*} 必须满足：pk_{i^*} 由预言机 O_{pk} 获得且敌手A在阶段 1 没有进行私钥预言机 $\mathrm{O}_{sk}(pk_{i^*})$ 查询。B随机选择 $b \in \{0,1\}$，把 $C_{i^*} = \mathrm{Enc}_2(pk_{i^*}, m_b)$ 发送给敌手A。

阶段 2　A可以任何次序继续询问以下预言机。

公钥产生预言机$O_{pk}(i)$：挑战者B的回答与阶段 1 一样。

私钥产生预言机$O_{sk}(pk_j)$：敌手A输入公钥pk_j，如果$pk_j = pk_{i^*}$或者(pk_{i^*}, pk_j)是预言机O_{ReKeyGen}的输入或者$(pk_{i^*}, pk_j, C_{i^*})$是预言机$O_{\text{ReEnc}}$的输入，则挑战者B输出⊥，否则挑战者和阶段 1 一样回答。

重加密密钥产生预言机$O_{\text{ReKeyGen}}(pk_i, pk_j)$：敌手A输入$(pk_i, pk_j)$，如果$pk_i = pk_{i^*}$并且$pk_j$是$O_{sk}$的一个输入，那么挑战者B输出⊥，否则挑战者和阶段 1 的回答一样。

重加密预言机$O_{\text{ReEnc}}(pk_i, pk_j, C_i)$：敌手A输入$(pk_i, pk_j, C_i)$，如果$(pk_i, C_i)$=$(pk_{i^*}, C_{i^*})$并且$pk_j$是预言机$O_{sk}$的一个输入，那么挑战者B输出⊥，否则挑战者和阶段 1 的回答一样。

解密预言机$O_{\text{Dec}_1}(pk_j, C_j)$：B输入$(pk_j, C_j)$，若$(pk_j, C_j)$=$(pk_{i^*}, C_{i^*})$或$C_j$=ReEnc($rk_{i^*\to j}, C_{i^*}$)，则挑战者B输出⊥，否则挑战者和阶段 1 的回答一样。

以上输入的公钥pk_i和pk_j都必须由预言机O_{pk}产生。

猜测阶段：敌手A输出一个猜测$b' \in \{0,1\}$。如果$b = b'$，则敌手A赢得了这个游戏。

定义 3 敌手A针对方案 Uni-PRE2-CCA 安全性的优势为

$$Adv_{\text{A}}^{\text{Uni-PRE2-CCA}}(1^k) = |\Pr[b = b'] - \frac{1}{2}|$$

若对于所有多项式t时间的敌手A，分别进行最多q_{pk}、q_{sk}、q_{ReKeyGen}、q_{ReEnc}、q_{Dec_1}次查询后，均有$Adv_{\text{A}}^{\text{Uni-PRE2-CCA}}(1^k) \le e$，则称该单向 PRE 方案是$(t, q_{pk}, q_{sk}, q_{\text{ReKeyGen}}, q_{\text{ReEnc}}, q_{\text{Dec}_1}, e)$ − Uni-PRE2-CCA 安全的。

Game2 Uni-PRE1-CCA :单向代理重加密方案第 1 层密文的 CCA 安全性。

注释 2 在单向单跳的 PRE 中，是无法对第 1 层密文进行再次转换的。所以允许敌手 A 获得任意的重加密密钥(包括从目标公钥到其他已经被敌手获得其私钥对应公钥的重加密密钥)，因此在这个游戏中就没有必要为敌手提供重加密预言机查询，因为 A 可以用获得的重加密密钥进行重加密操作。由注释 1 可知，也没有必要为敌手提供第 2 层密文的解密预言机查询。游戏如下。

阶段 1 除了不询问重加密预言机O_{ReEnc}，其他的与 Game1 的阶段 1 相同。

挑战阶段：一旦敌手A决定阶段 1 可以结束，就会输出 2 个等长的明文m_0和m_1及一个要挑战的公钥pk_{i^*}，这里pk_{i^*}必须满足：pk_{i^*}由预言机O_{pk}获得并且A在阶段 1 没有进行私钥预言机$O_{sk}(pk_{i^*})$查询。B随机选择比特$b \in \{0,1\}$，把$C_{i^*} = \text{Enc}_1(pk_{i^*}, m_b)$发送给敌手A。

阶段 2 敌手A可以任何次序继续询问以下的随机预言机。

公钥产生预言机$O_{pk}(i)$：与阶段 1 相同。

私钥产生预言机$O_{sk}(pk_j)$：敌手A输入公钥pk_j，如果$pk_j = pk_{i^*}$，则挑战者B输出⊥，否则挑战者和阶段 1 一样回答。

重加密密钥产生预言机$O_{\text{ReKeyGen}}(pk_i, pk_j)$：敌手A输入$(pk_i, pk_j)$，挑战者B返回重加密密钥$rk_{i\to j}$ = ReKeyGen(sk_i,pk_j)。

解密预言机$O_{\text{Dec}_1}(pk, C)$：若(pk', C')=(pk_{i^*}, C_{i^*})，则挑战者B输出⊥，否则挑战者和阶段 1 的回答一样。

猜测阶段：敌手A输出一个猜测$b' \in \{0,1\}$。如果$b = b'$，则敌手A赢得了这个游戏。

定义 4 敌手A针对方案 Uni-PRE1-CCA 安全性的优势为

$$Adv_{\text{A}}^{\text{Uni-PRE1-CCA}}(1^k) = |\Pr[b = b'] - \frac{1}{2}|$$

若对于所有多项式t时间的敌手A，分别进行最多q_{pk}、q_{sk}、q_{ReKeyGen}、q_{Dec_1}次查询后，均有$Adv_{\text{A}}^{\text{Uni-PRE1-CCA}}(1^k) \le e$，则称该单向 PRE 方案是$(t, q_{pk}, q_{sk}, q_{\text{ReKeyGen}}, q_{\text{Dec}_1}, e)$ − Uni-PRE1-CCA 安全的。

4 本文提出的 PRE 方案

LV 方案[10]利用 CHK 技术实现了对第 2 层密文有效性的公开验证，但他们第 1 层密文的部分密文$(C_2', C_2'' C_2''')$可以是$(C_2'^s, C_2''^{1/s} C_2'''^s)$($s$是随机数)的任意形式，在第 1 层密文解密时，无法对第 1 层密文的唯一性进行有效验证，因此它们的第 1 层密文只是 RCCA 安全的。构造一个 CCA 安全、单跳、单向的 PRE 方案的关键是对原始密文(第 2 层密文)和

重加密后的密文(第 1 层密文)进行有效性的验证。原始密文有效证的验证保证了该密文是由授权者产生的，而重加密后的密文的有效性验证则保证了该密文是由代理产生的。本文构造的方案基于双线性变换、CHK 变换及密钥填充方案。CHK 技术保证密文转换前后不变密文元素的完整性，并通过随机填充技术及散列函数的单向性和抗碰撞性验证了改变密文的唯一性。本文方案中的第 1 层和第 2 层密文的完整性都可以得到有效验证，实现 CCA 安全。

4.1 方案的构造

填充技术以往用于设计密码方案，例如 RAS-OAEP[19,20]、PSS[21]等。Wang 等[18]首次利用随机填充技术构造基于身份信息的单向代理重加密方案。本文利用 CHK 技术和随机填充技术构造一个单向、单跳的 PRE 方案，包括如下算法。

Setup(1^k)：令明文的空间为 $\mathsf{M}=\{0,1\}^{k_0}$，其中，$k_0<k$ 并且 $\frac{1}{2^{k_0}}$ 与 $\frac{1}{2^{k-k_0}}$ 的值小到可以忽略。令群 G_1 和群 G_2 是 2 个乘法有限循环群，它们的阶为素数 p，设 g_1、g、u、v 为 G_1 的生成元，并且映射 $e:G_1\times G_1\to G_2$ 是一个双线性配对映射。选取一个目标防碰撞的散列函数 $\mathsf{H}:\{0,1\}\to G_1$。选取一个强的不可伪造的一次签名函数 Sig=($G$,$S$,$V$)。最后输出系统的参数：$par=(\mathsf{M},k,k_0,G_1,G_2,g,g_1,p,u,v,e,\mathrm{Sig},\mathsf{H})$。

KeyGen(par)：用户 i 随机选取 $x_i\in Z_p^*$，输出公钥 $pk_i=g^{x_i}$ 和私钥 $sk_i=x_i$。

ReKeyGen(par,sk_i,pk_j)：输入 par 及用户 i 的私钥 $sk_i=x_i$ 和用户 j 的公钥 $pk_j=g^{x_j}$，该算法输出重加密密钥 $rk_{i\to j}=pk_j^{1/sk_i}=g^{x_j/x_i}$。

$\mathrm{Enc}_1(par,pk_j,m)$：输入 par 及公钥 pk_j 和明文 $m\in\mathsf{M}$，该算法按如下步骤产生第 1 层密文。

1) 随机选择一次签名密钥对 $(svk,ssk)\leftarrow G(1^k)$，并且设置 $C_1=svk$。

2) 随机选择 $r\in Z_p^*$ 及 $r_1\in\{0,1\}^{k-k_0}$，然后计算

$C_2=g_1^r$；

$C_3'=\mathrm{e}(pk_j,g)^r$；

$C_4=(m\,\|\,r_1)\cdot\mathrm{e}(g,g)^r$；

$C_5=(u^{svk}\cdot v)^r$；

$C_6=H(m\,\|\,r_1\,\|\,C_5)\cdot C_5^{r_1}$。

3) 对 (C_2,C_4,C_5,C_6) 进行一次签名，得到签名值 $s=\mathsf{S}(ssk,(C_2,C_4,C_5,C_6))$，输出的第 1 层密文 $\boldsymbol{C}_j=(C_1,C_2,C_3',C_4,C_5,C_6,s)$。

$\mathrm{Enc}_2(par,pk_i,m)$：输入 par 及公钥 pk_i 和明文 $m\in M$，该算法按如下步骤产生第 2 层密文。

1) 随机选择一次签名密钥对 $(svk,ssk)\leftarrow\mathsf{G}(1^k)$ 并且设置 $C_1=svk$。

2) 随机选择 $r\in Z_p^*$ 及 $r_1\in\{0,1\}^{k-k_0}$，然后计算

$C_2=g_1^r$；

$C_3=pk_i^r$；

$C_4=(m\,\|\,r_1)\cdot e(g,g)^r$；

$C_5=(u^{svk}\cdot v)^r$；

$C_6=H(m\,\|\,r_1\,\|\,C_5)\cdot C_5^{r_1}$。

3) 对 (C_2,C_4,C_5,C_6) 进行一次签名，得到签名值 $s=\mathsf{S}(ssk,(C_2,C_4,C_5,C_6))$，输出的第 2 层密文 $\boldsymbol{C}_i=(C_1,C_2,C_3,C_4,C_5,C_6,s)$。

$\mathrm{ReEnc}(par,rk_{i\to j},\boldsymbol{C}_i)$：输入 par、重加密密钥 $rk_{i\to j}$ 及针对公钥 pk_i 的第 2 层密文 $\boldsymbol{C}_i=(C_1,C_2,C_3,C_4,C_5,C_6,s)$，并根据如下的条件判断 $\boldsymbol{C}_i$ 的有效性

$$\mathsf{V}(C_1,s,(C_2,C_4,C_5,C_6))=1 \tag{1}$$

$$\mathrm{e}(C_3,u^{C_1}\cdot v)=\mathrm{e}(pk_i,C_5) \tag{2}$$

若式(1)或式(2)不成立，输出⊥。否则计算 $C_3'=\mathrm{e}(C_3,rk_{i\to j})=\mathrm{e}(pk_j,g)^r$，并输出针对公钥 pk_j 的第 1 层密文：$\boldsymbol{C}_j=(C_1,C_2,C_3',C_4,C_5,C_6,s)$。

$\mathrm{Dec}_1(par,sk_j,\boldsymbol{C}_j)$：用户 j 用私钥 sk_j 按照如下步骤对第 1 层密文 $\boldsymbol{C}_j=(C_1,C_2,C_3',C_4,C_5,C_6,s)$ 进行解密。

1) 验证式(1)是否成立，如果不成立，输出⊥，否则继续以下的步骤。

2) 计算 $m'=\frac{C_4}{C_3'^{(1/sk_j)}}$。

3) 解析 m' 为 $(m\,\|\,r_1)$，m 为 k_0 bit，r_1 为 $(k-k_0)$ bit。

4) 验证 $C_6=H(m'\,\|\,C_5)\cdot C_5^{r_1}$ 是否成立，如果不成立，输出⊥，否则，输出 m。

$\mathrm{Dec}_2(par,sk_i,\boldsymbol{C}_i)$：用户 i 用私钥 sk_i 按如下步骤对第 2 层密文 $\boldsymbol{C}_i=(C_1,C_2,C_3,C_4,C_5,C_6,s)$ 进行解密。

1) 如果式(1)或式(2)不成立，则输出⊥，否则

继续以下的步骤。

2)计算 $m'=\dfrac{C_4}{\mathrm{e}(C_3,g)^{(1/sk_i)}}$。

3)解析 m' 为 $(m\parallel r_1)$，m 为 k_0 bit，r_1 为 $(k-k_0)$ bit，并输出 m。

注释 3 本文利用 CHK 技术保证密文转换前后不变密文元素的完整性，第 2 层密文元素 $C_3=pk_i^r$ 的完整性通过双线性配对运算验证，第 1 层密文元素 $C_3^{'}$ 的完整性通过随机填充技术及散列函数的单向性和抗碰撞性验证。因此本文方案中的第 1 层和第 2 层密文的完整性都可以得到有效验证，实现 CCA 安全，下面将证明方案的 CCA 安全性。

4.2 安全性证明

本文通过定理 1 和定理 2 分别证明所提方案的 CCA 安全性。

定理 1 假设 Sig 是一个不可伪造的一次强签名函数，并且群 (G_1,G_2) 的 $3-\mathrm{wDBDHI}$ 假设成立，那么，本方案是 Uni-PRE2-CCA 安全的。

证明 假设 Sig 是一个不可伪造的一次强签名函数，如果存在一个敌手 A 可以攻破本文所提方案的 $(t,q_{pk},q_{sk},q_{\mathrm{ReKeyGen}},q_{\mathrm{ReEnc}},q_{\mathrm{Dec}_1},e)$-Uni-PRE2-CCA 安全性，则存在一个挑战者 B 可以攻破群 (G_1,G_2) 的 (t',e')-3-wDBDHI 假设，其中 e'，t' 满足

$$e'\geq\left|\pm e\cdot\left(\frac{1}{\mathrm{e}(1+q_{sk}+q_{rk})}\left(1-\frac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}_1}}{p}\right)\right)-Adv^{\mathrm{SIG}}\right|$$

$$t'\leq t+q_{\mathrm{ReEnc}}\cdot(3t_p+3t_e)+q_{\mathrm{Dec}_1}\cdot(1\cdot t_p+3t_e)$$

其中，e 表示自然对数的底。t_p 表示一个双线性配对运算时间，t_e 表示一个模指数运算时间。根据假设，Adv^{SIG} 是可忽略的。

给定 $3-\mathrm{wDBDHI}$ 输入实例 $(g,A_{-1}=g^{1/a},A_1=g^a,A_2=g^{a^2},B=g^b,Q)$，其中，$a,b\in Z_p^*$ 且未知。挑战者 B 的目标是判断 $Q=e(g,g)^{b/a^2}$ 是否成立。挑战者 B 为敌手 A 建立如下的公开参数：B 执行 $G(1^k)\rightarrow(svk^*,ssk^*)$，然后随机选择 a_0，a_1 和 a_2，其中，a_0、a_1、$a_2\in Z_p^*$，设置 $g_1=A_2^{a_0}$，$u=A_1^{a_1}$，$v=A_1^{-a_1\cdot svk^*}\cdot A_2^{a_2}$。挑战者 B 和敌手 A 按照如下的方式进行交互。

阶段 1 B 构造如下预言机。

公钥预言机 $O_{pk}(i)$：挑战者 B 随机选取 $x_i\in Z_p^*$，然后选择随机数 $c_i\in\{0,1\}$，其中，$\Pr[c_i=1]=?$，$\Pr[c_i=0]=1-?$。如果 $c_i=1$，设定 $pk_i=g^{x_i}$，否则设定 $pk_i=A_2^{x_i}$。最后，挑战者 B 将元组 (pk_i,x_i,c_i) 加入列表 T_{PK}，并将 pk_i 返回给敌手 A。

私钥产生预言机 $O_{sk}(pk_i)$：挑战者 B 从列表 T_{PK} 中找出元组 (pk_i,x_i,c_i)。如果 $c_i=1$，将 $sk_i=x_i$ 返回给敌手 A，并把 pk_i 记录在列表 T_{SK} 中；否则 B 输出 Abort 并终止游戏。

重加密密钥产生预言机 $O_{\mathrm{ReKeyGen}}(pk_i,pk_j)$：挑战者 B 从列表 T_{PK} 中找出元组 (pk_i,x_i,c_i) 和 (pk_j,x_j,c_j)，根据如下情况为敌手 A 产生重加密密钥 $rk_{i\rightarrow j}$。

1) 若 $c_i=1$：挑战者 B 设定 $rk_{i\rightarrow j}=pk_j^{1/x_i}$ 并将结果返回给敌手 A，再把 (pk_i,pk_j) 记录在列表 T_{RK} 中。

2) 若 $c_i=c_j=0$：挑战者 B 设定 $rk_{i\rightarrow j}=g^{x_j/x_i}$ 并将结果返回给敌手 A，再把 (pk_i,pk_j) 记录在列表 T_{RK} 中。

3) 若 $c_i=0\wedge c_j=1$：挑战者 B 输出 Abort 并中止游戏。

重加密预言机 $O_{\mathrm{ReEnc}}(pk_i,pk_j,\boldsymbol{C}_i)$：挑战者 B 首先检查 pk_i 和 pk_j 是否都在列表 T_{PK} 中，如果不存在，则 B 输出 $\perp$ 并退出游戏。否则解析 $\boldsymbol{C}_i$，为 $(C_1,C_2,C_3,C_4,C_5,C_6,s)$，按照式(1)和式(2)检查密文的有效性，若式(1)或式(2)不成立，则输出 $\perp$ 并退出模拟游戏，否则 B 进行如下操作。

① 若 $c_i=0\wedge c_j=1$：挑战者 B 在没有产生转换密钥 $rk_{i\rightarrow j}$ 的情况下为敌手 A 进行重加密操作。如果 $C_1=svk^*$，则 B 输出 Abort 并终止游戏，否则，B 计算

$$\left(\frac{C_5}{C_2^{a_2/a_0}}\right)^{\frac{1}{a_1(svk-svk^*)}}=\left(\frac{(u^{svk}\cdot v)^r}{(g^{a^2\cdot a_0\cdot r})^{a_2/a_0}}\right)^{\frac{1}{a_1\cdot(svk-svk^*)}}$$

$$=\left(\frac{A_1^{a_1\cdot svk\cdot r}\cdot A_1^{-a_1\cdot svk^*\cdot r}\cdot A_2^{a_2\cdot r}}{g^{a^2\cdot a_2\cdot r}}\right)^{\frac{1}{a_1\cdot(svk-svk^*)}}$$

$$=\left(\frac{g^{a\cdot a_1 svk\cdot r}\cdot g^{-a\cdot a_1\cdot svk^*\cdot r}\cdot g^{a^2\cdot a_2\cdot r}}{g^{(a^2\cdot a_2\cdot r)}}\right)^{\frac{1}{a_1\cdot(svk-svk^*)}}$$

$$=(g^{ara_1(svk-svk^*)})^{\frac{1}{a_1\cdot(svk-svk^*)}}=g^{ar}=A_1^r \qquad (4)$$

计算 $\mathrm{e}(A_1^r,A_{-1})^{x_j}=\mathrm{e}(g^{ar},g^{1/a})^{x_j}=\mathrm{e}(pk_j,g)^r=C_3^{'}$。最后将 $\boldsymbol{C}_j=(C_1,C_2,C_3^{'},C_4,C_5,C_6,s)$ 返回给敌手 A，并把 $(pk_i,pk_j,\boldsymbol{C}_i)$ 记录在列表 T_{RE} 中。

② 若 $c_i=0\wedge c_j=1$ 不成立，则按照重加密密

钥预言机O_{ReKeyGen}的方法产生重加密密钥$rk_{i\to j}$，然后运行$\mathrm{ReEnc}(rk_{i\to j},\boldsymbol{C}_i)$并将结果返回给敌手A，并把$(pk_i, pk_j,\boldsymbol{C}_i)$记录在列表$T_{RE}$中。

第 1 层解密预言机$\mathrm{O}_{\mathrm{Dec}_1}(pk_j,\boldsymbol{C}_j)$：挑战者B首先检查$pk_j$是否都在列表$T_{PK}$中，如果不存在，B输出⊥并终止游戏。否则B解析$\boldsymbol{C}_j=(C_1,C_2$，$C_3^{'},C_4,C_5,C_6,s)$，如果$C_1=svk^*$，B输出 Abort 并中止游戏，否则进行如下操作。

1) 若$c_j=1$，则$sk_j=x_j$，则B运行 Dec1($\boldsymbol{C}_j$, sk_j)并将结果返回给敌手 A。

2) 若$c_j=0$，验证式(1)是否成立，如果不成立，输出⊥并退出游戏，否则，由式(4)得到A_1^r，再计算$\mathrm{e}(A_1^r,A_{-1})=\mathrm{e}(g^{ar},g^{1/a})=\mathrm{e}(g,g)^r$，则$m'=\dfrac{C_4}{e(A_1^r,A_{-1})}$，解析$m'$为$(m\,\|\,r_1)$，验证$C_6=H(m^{'}\,\|\,C_5)\cdot C_5^{r_1}$是否成立，如果不成立，输出⊥并退出游戏，否则，输出m。

挑战阶段：一旦敌手 A 决定阶段 1 可以结束，就会输出 2 个等长的明文m_0和m_1及要挑战的公钥pk_{i^*}。如果pk_{i^*}所对应的$c_{i^*}=1$，B 输出 Abort 并中止游戏。否则，B 选择随机数$b\in\{0,1\}$并计算：

$$C_1^*=svk^*$$

$$C_2^*=B^{a_0}=(g^{a^2})^{a_0\cdot\frac{b}{a^2}}=(A_2^{a_0})^{r^*}=g_1^{r^*}$$

$$C_3^*=B^{x_{i^*}}=g^{b\cdot x_{i^*}}=(g^{a^2\cdot x_{i^*}})^{\frac{b}{a^2}}=(pk_{i^*})^{r^*}$$

$$C_4^*=(m_b\,\|\,r_1^*)\cdot Q$$

$$\begin{aligned}C_5^*&=B^{a_2}=(g^b)^{a_2}=(g^{a^2\cdot a_2})^{\frac{b}{a^2}}\\&=(g^{a\cdot a_1(svk^*-svk^*)}\cdot g^{a^2\cdot a_2})^{\frac{b}{a^2}}\\&=(g^{a\cdot a_1 svk^*}\cdot g^{-a\cdot a_1 svk^*}\cdot g^{a^2\cdot a_2})^{\frac{b}{a^2}}\\&=(A_1^{a_1 svk^*}\cdot A_1^{-a_1 svk^*}A_2^{a_2})^{\frac{b}{a^2}}\\&=(u^{svk^*}\cdot v)^{\frac{b}{a^2}}=(u^{svk^*}\cdot v)^{r^*}\end{aligned}$$

$$\begin{aligned}C_6^*&=H(m_b\,\|\,r_1^*\,\|\,B^{a_2})\cdot(B^{a_2})^{r_1^*}\\&=H(m_b\,\|\,r_1^*\,\|\,C_5^*)\cdot(C_5^*)^{r_1^*}\end{aligned}$$

$$s^*=\mathrm{S}(ssk^*,(C_2^*,C_4^*,C_5^*,C_6^*))$$

将挑战密文$\boldsymbol{C}_{i^*}=(C_1^*,C_2^*,C_3^*,C_4^*,C_5^*,C_6^*,s^*)$返回给 A。显然，若$r^*=\dfrac{b}{a^2}$，当$Q=\mathrm{e}(g,g)^{\frac{b}{a^2}}$成立时，$\boldsymbol{C}_{i^*}$必是一个针对$pk_{i^*}$的有效密文。

阶段 2　B构造如下的预言机。

公钥预言机$O_{pk}(i)$：和阶段 1 的回答一样。

私钥产生预言机$O_{sk}(pk_j)$：如果$pk_j=pk_{i^*}$或者(pk_{i^*},pk_j)在列表T_{RK}中或者$(pk_{i^*},pk_j,\boldsymbol{C}_{i^*})$在列表$T_{RE}$中，则挑战者 B 输出⊥并退出游戏。否则和阶段 1 回答一样。

重加密密钥产生预言机$O_{\mathrm{ReKeyGen}}(pk_i,pk_j)$：如果$pk_i=pk_{i^*}$并且$pk_j$在列表$T_{SK}$中，则挑战者 B 输出⊥并退出游戏。否则和阶段 1 回答一样。

重加密预言机$O_{\mathrm{ReEnc}}(pk_i,pk_j,\boldsymbol{C}_i)$：如果$(pk_i,\boldsymbol{C}_i)=(pk_{i^*},\boldsymbol{C}_{i^*})$且$pk_j$在列表$T_{SK}$中，则挑战者 B 输出⊥并退出游戏。否则和阶段 1 回答一样。

第 1 层解密预言机$O_{\mathrm{Dec}_1}(pk_j,\boldsymbol{C}_j)$：如$(pk_{i^*},pk_j,\boldsymbol{C}_{i^*})$在列表$T_{RE}$中，挑战者 B 输出⊥，否则挑战者和阶段 1 的回答一样。

猜测阶段：最后，敌手 A 输出猜测$b^{'}\in\{0,1\}$。如果$b=b^{'}$，那么挑战者 B 输出 1 作为其针对 3-wDBDHI 实例的回答；否则，挑战者 B 输出 0。

概率分析：定义 Abort 为敌手 A 在与挑战者 B 交互时发生的中断事件。

假设敌手 A 最多进行了q_{sk}、q_{ReKeyGen}、q_{ReEnc}、q_{Dec_1}次预言机O_{sk}、O_{ReKeyGen}、O_{ReEnc}、O_{Dec_1}查询。在阶段 1 和阶段 2 对预言机O_{sk}、O_{ReKeyGen}查询中关于c_i的 Abort 不会发生的概率分别为$?^{q_{sk}}$及$(?+(1-?)^2)^{q_{rk}}$。由于在进行O_{ReEnc}、O_{Dec_1}查询中，出现$C_1=svk^*$最大的概率为$1/p$，因此查询O_{ReEnc}，O_{Dec_1}中 Abort 不会发生的概率为$\left(1-\dfrac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}_1}}{p}\right)$。在挑战阶段关于$c_i$的 Abort 不会发生的概率为$(1-?)$。因此，在模拟中，关于 coin 的 Abort 不会发生的概率为

$$\Pr[\neg\mathrm{Abort}]=?^{q_{sk}}(?+(1-?)^2)^{q_{rk}}(1-?)\cdot\left(1-\frac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}_1}}{p}\right)\geq?^{q_{sk}+q_{rk}}(1-?)\left(1-\frac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}_1}}{p}\right)$$

当$?=\dfrac{q_{sk}+q_{rk}}{1+q_{sk}+q_{rk}}$时，$?^{q_{sk}+q_{rk}}(1-?)$取得最大值，最大值为$\dfrac{1}{\mathrm{e}(1+q_{sk}+q_{rk})}$。从而得出

$$\Pr[\neg\mathrm{Abort}]\geq\frac{1}{\mathrm{e}(1+q_{sk}+q_{rk})}\left(1-\frac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}_1}}{p}\right)$$

其中，e 表示自然对数的底。

当 Abort 不会发生并且 $T=\mathrm{e}(g,g)^{b/a^2}$ 时，由于挑战密文恰好是对 m_b 的有效加密密文。此时，

$$\begin{aligned}&\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q=\mathrm{e}(g,g)^{b/a^2})=1]\\&=\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q=\mathrm{e}(g,g)^{b/a^2})=1\mid\mathrm{Abort}]\cdot\\&\Pr[\mathrm{Abort}]+\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q=\mathrm{e}(g,g)^{b/a^2})\\&=1\mid\neg\mathrm{Abort}]\cdot\Pr[\neg\mathrm{Abort}]\\&=(1/2)\cdot\Pr[\mathrm{Abort}]+\Pr[b=b'\mid\neg\mathrm{Abort}]\cdot\Pr[\neg\mathrm{Abort}]\end{aligned}$$

当 Abort 不会发生且 Q 是 G_2 的一个随机元素时，挑战密文是对 G_2 上一个随机元素的加密密文。此时敌手 A 的优势是伪造一次签名。此时

$$\begin{aligned}&\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q\neq\mathrm{e}(g,g)^{b/a^2})=1]\\&=\frac{1}{2}+Adv^{\mathrm{SIG}}\end{aligned}$$

综上，根据假设及敌手 A 的优势定义：

$$\begin{aligned}&|\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q=\mathrm{e}(g,g)^{b/a^2})=1]-\\&-\Pr[\mathsf{B}(g,\mathrm{g}^{1/a},\mathrm{g}^{a},\mathrm{g}^{a^2},\mathrm{g}^{b},Q\neq\mathrm{e}(g,g)^{b/a^2})=1]|\\&=|\frac{1}{2}\cdot\Pr[\mathrm{Abort}]+\Pr[b=b'\mid\neg\mathrm{Abort}]\cdot\Pr[\neg\mathrm{Abort}]-\\&(\frac{1}{2}+Adv^{\mathrm{SIG}})|=|\frac{1}{2}-\frac{1}{2}\Pr[\neg\mathrm{Abort}]+\\&\Pr[b=b'\mid\neg\mathrm{Abort}]\cdot\Pr[\neg\mathrm{Abort}]-(\frac{1}{2}+Adv^{\mathrm{SIG}})|\\&=|(\Pr[b=b'\mid\neg\mathrm{Abort}]-\frac{1}{2})\cdot\Pr[\neg\mathrm{Abort}]-Adv^{\mathrm{SIG}}|\\&\geq|(\pm e+\frac{1}{2}-\frac{1}{2})\cdot\Pr[\neg\mathrm{Abort}]-Adv^{\mathrm{SIG}}|\\&\geq|\pm e(\frac{1}{\mathrm{e}(1+q_{sk}+q_{rk})}\cdot(1-\frac{q_{\mathrm{ReEnc}}+q_{\mathrm{Dec}}}{p}))-Adv^{\mathrm{SIG}}|\end{aligned}$$

时间复杂度：挑战者 B 与敌手 A 的交互过程中，其主要的计算代价是在回答 A 的重加密和第 1 层密文解密查询所需的双线性映射运算和模指数运算。假设一次双线性映射运算所需的时间为 t_p，一次模指数运算运算所需的时间为 t_e，那么可得

$$t'\leq t+q_{\mathrm{ReEnc}}(3t_p+3t_e)+q_{\mathrm{Dec}_1}(t_p+3t_e)$$

证毕。

定理 2 假设 Sig 是一个不可伪造的一次强签名函数，并且群 (G_1,G_2) 的 3-wDBDHI 假设成立，那么，本方案是 Uni-PRE1-CCA 安全的。

证明 假设 Sig 是一个不可伪造的一次强签名函数，如果存在一个敌手 A 可以攻破本文所提方案的 $(t,q_{pk},q_{sk},q_{\mathrm{ReKeyGen}},q_{\mathrm{Dec}_1},e)-$Uni-PRE1-CCA 安全性，则存在一个挑战者 B 可以攻破群 (G_1,G_2) 的 (t',e')-3-wDBDHI 假设，其中，e'，t' 满足

$$e'\geq\left|\pm e\left(\frac{1}{\mathrm{e}(1+q_{sk})}\cdot\left(1-\frac{q_{\mathrm{Dec}_1}}{p}\right)\right)-Adv^{\mathrm{SIG}}\right|$$
$$t'\leq t+q_{\mathrm{Dec}_1}(t_p+3t_e)$$

给定 3-wDBDHI 输入实例 $(g,A_{-1}=g^{1/a},A_1=g^{a},A_2=g^{a^2},B=g^{b},Q)$，其中，$a,b\in Z_p^*$ 且未知。挑战者 B 的目标是判断 $Q=\mathrm{e}(g,g)^{b/a^2}$ 是否成立。挑战者 B 为 A 建立如下的公开参数：B 执行 $\mathsf{G}(1^k)\rightarrow(svk^*,ssk^*)$，然后，随机选择 a_0、a_1 和 a_2 $(a_0,a_1,a_2\in Z_p^*)$，设置 $g_1=A_2^{a_0}$，$u=A_1^{a_1}$，并且 $v=A_1^{-a_1\cdot svk^*}A_2^{a_2}$。挑战者 B 和敌手 A 按照如下的方式进行交互。

阶段 1 B 构造如下预言机。

公钥预言机 $O_{pk}(i)$：挑战者 B 随机选取 $x_i\in Z_p^*$，然后选择一个随机数 $c_i\in\{0,1\}$，其中，$\Pr[c_i=1]=?$，$\Pr[c_i=0]=1-?$。如果 $c_i=1$，设定 $pk_i=g^{x_i}$；否则设定 $pk_i=A_1^{x_i}$。最后，挑战者 B 将元组 (pk_i,x_i,c_i) 加入列表 T_{PK}，并将 pk_i 返回给敌手 A。

私钥产生预言机 $O_{sk}(pk_i)$：挑战者 B 从列表 T_{PK} 中找出元组 (pk_i,x_i,c_i)。如果 $c_i=1$，将 $sk_i=x_i$ 返回给敌手 A，并把 pk_i 记录在列表 T_{SK} 中；否则 B 输出 Abort 并终止游戏。

重加密密钥产生预言机 $\mathsf{O}_{\mathrm{ReKeyGen}}(pk_i,pk_j)$：B 从列表 T_{PK} 中找出元组 (pk_i,x_i,c_i) 和 (pk_j,x_j,c_j)，根据如下情况为敌手 A 产生重加密密钥 $rk_{i\rightarrow j}$。

1) 若 $c_i=1$ 挑战者 B 设定 $rk_{i\rightarrow j}=pk_j^{1/x_i}$ 并将结果返回给敌手 A，并把 (pk_i,pk_j) 记录在列表 T_{RK} 中。

2) 若 $c_i=c_j=0$：挑战者 B 设定 $rk_{i\rightarrow j}=g^{x_j/x_i}$ 并将结果返回给敌手 A 并把 (pk_i,pk_j) 记录在列表 T_{RK} 中。

3) 若 $c_i=0\wedge c_j=1$：挑战者 B 设定 $rk_{i\rightarrow j}=A_{-1}^{x_j/x_i}$ 并将结果返回给敌手 A，并把 (pk_i,pk_j) 记录在列表 T_{RK} 中。

第 1 层解密预言机 $\mathsf{O}_{\mathrm{Dec}_1}(pk_j,\boldsymbol{C}_j)$：挑战者 B 首先检查 pk_j 是否都在列表 T_{PK} 中。如果不存在，挑战者 B 输出 $\perp$ 并终止游戏。否则挑战者 B 解析 $\boldsymbol{C}_j=(C_1,C_2,C_3',C_4,C_5,C_6,s)$，若 $C_1=svk^*$，B 输出 Abort 并终止游戏，否则进行如下操作。

1) 若 $c_j = 1$，由于 $sk_j = x_j$，B 运行 $\mathrm{Dec}_1(\boldsymbol{C}_j, sk_j)$ 并将结果返回给敌手A。

2) 若 $c_j = 0$，验证式(1)是否成立，如果不成立，输出⊥并退出游戏，否则，由式(4)得到 A_1^r，再计算 $\mathrm{e}(A_1^r, A_{-1}) = \mathrm{e}(g^{ar}, g^{1/a}) = \mathrm{e}(g,g)^r$，则 $m' = \dfrac{C_4}{\mathrm{e}(A_1^r, A_{-1})}$，解析 m' 为 $(m \| r_1)$，验证 $C_6 = H(m' \| C_5) \cdot C_5^{r_1}$ 是否成立，如果不成立，输出⊥并退出游戏，否则，输出 m。

挑战阶段：一旦敌手A决定阶段 1 可以结束，就会输出 2 个等长的明文 m_0 和 m_1 及要挑战的公钥 pk_{i^*}。如果 pk_{i^*} 所对应的 $c_{i^*} = 1$，B 输出 Abort 并终止游戏。否则，B 选择随机数 $b \in \{0,1\}$ 并计算

$$C_1^* = svk^*$$

$$C_2^* = B^{a_0} = (g^{a^2})^{a_0 \cdot \frac{b}{a^2}} = (A_2^{a_0})^{r^*} = g_1^{r^*}$$

$$C_3'^* = \mathrm{e}(A_{-1}, B)^{x_{i^*}} = \mathrm{e}(g^{1/a}, g^b)^{x_{i^*}} = \mathrm{e}(g^{a \cdot x_{i^*}}, g)^{\frac{b}{a^2}}$$
$$= \mathrm{e}(pk_{i^*}, g)^{r^*}$$

$$C_4^* = (m_b \| r_1^*) Q$$

$$C_5^* = B^{a_2} = (g^b)^{a_2} = (g^{a^2 \cdot a_2})^{\frac{b}{a^2}}$$
$$= (g^{a \cdot a_1 (svk^* - svk^*)} \cdot g^{a^2 \cdot a_2})^{\frac{b}{a^2}}$$
$$= (g^{a \cdot a_1 svk^*} \cdot g^{-a \cdot a_1 svk^*} \cdot g^{a^2 \cdot a_2})^{\frac{b}{a^2}}$$
$$= (A_1^{a_1 svk^*} \cdot A_1^{-a_1 svk^*} A_2^{a_2})^{\frac{b}{a^2}}$$
$$= (u^{svk^*} \cdot v)^{\frac{b}{a^2}} = (u^{svk^*} \cdot v)^{r^*}$$

$$C_6^* = H(m_b \| r_1^* \| B^{a_2}) \cdot (B^{a_2})^{r_1^*}$$
$$= H(m_b \| r_1^* \| C_5^*) \cdot (C_5^*)^{r_1^*}$$

$$s^* = \mathrm{S}(ssk^*, (C_2^*, C_4^*, C_5^*, C_6^*))$$

将挑战密文 $\boldsymbol{C}_{i^*} = (C_1^*, C_2^*, C_3'^*, C_4^*, C_5^*, C_6^*, s^*)$ 返回给A。显然，若 $r^* = \dfrac{b}{a^2}$，当 $Q = \mathrm{e}(g,g)^{\frac{b}{a^2}}$ 成立时，$\boldsymbol{C}_{i^*}$ 必是一个针对 pk_{i^*} 的有效密文。

阶段 2　B 构造如下的预言机。

公钥预言机 $\mathrm{O}_{pk}(i)$：和阶段 1 的回答一样。

私钥产生预言机 $\mathrm{O}_{sk}(pk_j)$：如果 $pk_j = pk_{i^*}$ 或者 (pk_{i^*}, pk_j) 在列表 T_{RK} 中，则 B 输出⊥并退出游戏；否则和阶段 1 回答一样。

重加密密钥产生预言机 $O_{\mathrm{ReKeyGen}}(pk_i, pk_j)$：如果 $pk_i = pk_{i^*}$ 并且 pk_j 在列表 T_{SK} 中，则 B 输出⊥并退出游戏。否则和阶段 1 的回答一样。

第 1 层解密预言机 $\mathrm{O}_{\mathrm{Dec}_1}(pk_j, \boldsymbol{C}_j)$：如果 $\boldsymbol{C}_j = \mathrm{ReEnc}(rk_{i^* \to j}, \boldsymbol{C}_{i^*})$，B 输出⊥，否则挑战者和阶段 1 的回答一样。

猜测阶段：最后，A输出一个猜测 $b' \in \{0,1\}$。如果 $b = b'$，那么 B 输出 1 作为其针对 3-wDBDHI 实例的回答；否则，B 输出 0。

概率分析：定义 Abort 为敌手A在与挑战者 B 交互时发生的中断事件。假设A最多进行了 q_{sk}，q_{Dec_1} 次查询。在阶段 1 和阶段 2 对预言机 O_{sk} 查询中关于 c_i 的 Abort 不会发生的概率为 $?^{q_{sk}}$。由于在进行 $\mathrm{O}_{\mathrm{Dec}_1}$ 查询中，出现 $C_1 = svk^*$ 的概率为 $1/p$，因此查询 $\mathrm{O}_{\mathrm{Dec}_1}$ 中 Abort 不会发生的概率为 $(1 - \dfrac{q_{\mathrm{Dec}_1}}{p})$。在挑战阶段关于 c_i 的 Abort 不会发生的概率为 $(1-?)$。因此，在模拟中，关于 coin 的 Abort 不会发生的概率为

$$\Pr[\neg \mathrm{Abort}] = ?^{q_{sk}}(1-?)\left(1 - \frac{q_{\mathrm{Dec}_1}}{p}\right)$$

当 $? = \dfrac{q_{sk}}{1+q_{sk}}$ 时，$?^{q_{sk}}(1-?)$ 取得最大值，最大值为 $\dfrac{1}{\mathrm{e}(1+q_{sk})}$，即 $\Pr[\neg \mathrm{Abort}] \geq \dfrac{1}{\mathrm{e}(1+q_{sk})}\left(1 - \dfrac{q_{\mathrm{Dec}_1}}{p}\right)$。

与定理 1 的证明同理，根据假设及敌手 A 的优势定义可得

$$|\Pr[\mathrm{B}(g, g^{1/a}, g^a, g^{a^2}, g^b, Q = \mathrm{e}(g,g)^{b/a^2}) = 1] -$$
$$\Pr[\mathrm{B}(g, g^{1/a}, g^a, g^{a^2}, g^b, Q \neq \mathrm{e}(g,g)^{b/a^2}) = 1]|$$
$$\geq |\pm e \cdot \left(\frac{1}{\mathrm{e}(1+q_{sk})}\left(1 - \frac{q_{\mathrm{Dec}_1}}{p}\right)\right) - Adv^{\mathrm{SIG}}|$$

时间复杂度：假设一次双线性映射运算所需的时间为 t_p，一次模指数运算运算所需的时间为 t_e，可得

$$t' \leq t + q_{\mathrm{Dec}_1}(t_p + 3t_e)$$

证毕。

4.3　方案比较

本文方案与 LV 方案[10]和 WJ 方案[11]都是单向单跳的 PRE 方案。表 1 为本文方案与 LV 方案和 WJ 方案的比较。表 1 中，$|Z_p|$ 和 l 分别表示 WJ 方案中密文元素 t 和安全参数位长度。$|G_1|$ 和 $|G_2|$

表 1 本文方案与 LV 方案及 WJ 方案的比较

方案指标		WJ 方案	LV 方案	本文方案
密文长度	第 1 层	$\|Z_p\|+2\|G_1\|+\|G_2\|+l$	$\|svk\|+4\|G_1\|+\|G_2\|+\|s\|$	$\|svk\|+3\|G_1\|+2\|G_2\|+\|s\|$
	第 2 层	$\|Z_p\|+3\|G_1\|+l$	$\|svk\|+2\|G_1\|+\|G_2\|+\|s\|$	$\|svk\|+4\|G_1\|+\|G_2\|+\|s\|$
运算代价	Enc_1	$6t_e$	$6t_e+t_s$	$6t_e+t_s$
	Enc_2	$6t_e$	$4t_e+t_s$	$6t_e+t_s$
	ReEnc	$3t_p+6t_e$	$2t_p+4t_e+t_v$	$3t_p+t_e+t_v$
	Dec_1	$2t_p+2t_e$	$5t_p+2t_e+t_v$	$2t_e+t_v$
	Dec_2	$3t_p+7t_e$	$3t_p+2t_e+t_v$	$3t_p+2t_e+t_v$
	总运算代价	$8t_p+27t_e$	$10t_p+18t_e+2t_s+3t_v$	$6t_p+17t_e+2t_s+3t_v$
PRE 类型		单向单跳	单向单跳	单向单跳
随机预言机		无需	无需	无需
困难假设		3-wDBDHI	3-wDBDHI	3-wDBDHI
安全性		CCA	RCCA	CCA
攻陷模型		自适应	非自适应	自适应

分别表示 3 种方案中群G_1和G_2中一个元素的位长度。$|svk|$和$|s|$分别表示 LV 方案和本文方案中所采用的一次强签名函数的验证密钥位长度和签名位长度。t_p 表示一个双线性配对运算时间，t_e 表示一个模指数运算时间，t_s 表示一次签名运算时间，t_v 表示一次签名验证运算所需的时间。

假设本文方案和 LV 方案的一次强签名函数都是采用 1 024 bit 的 RSA。3 种方案采用的双线性配对都是 Tate 双线性配对。要达到 1 024 bit RSA 的安全级别，需要 512 bit 的 Tate 双线性配对操作[22]。根据文献[22]的实验结果，执行一次 Tate 双线性操作需要 20.04 ms，一次模指数运算为 5.31 ms。而 RSA 的签名时间约为执行一次模指数运算的时间，RSA 的验证时间相对于签名时间可忽略。因此，可分别估算 WJ 方案、LV 方案和本文方案的总运算时间为 303.69 ms，306.6 ms 和 221.13 ms，由此得出本文方案总运算时间分别是 WJ 方案的 72.81%，是 LV 方案的 72.12%。

表 1 的比较结果还表明，本文方案是 CCA 安全的，而 LV 方案只能达到 RCCA 安全，并且在同等困难假设、同样无需随机预言模型下进行证明方案安全性时，本文方案是自适应攻陷模型下 CCA 安全的，而 LV 方案是非自适应攻陷模型下 RCCA 安全的。与 WJ 方案相比，本文方案与 WJ 方案所达到的安全级别相同，但具有更高的运算效率。

5 结束语

针对实际应用中需要高效的标准模型下 CCA 安全的单向 PRE 方案，本文使用 CHK 技术和随机填充技术构造了一种新的高效的单向、单跳的 PRE 方案，并且在无需借助随机预言机的模型下证明了方案的 CCA 安全性。

构造单跳单向 PRE 方案的进一步研究工作主要是：1)在保证同等安全级别的情况下如何有效减少密文的长度；2)如何实现第 1 层密文完整性的公开验证。

参考文献：

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[A]. EUROCRYPT'98, International Conference on the Theory and Application of Cryptographic echniques[C]. Espoo, Finland, 1998.127-144.

[2] ATENIESE G, FU K, GREEN M, *et al*. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information System Security, 2006, (9):1-30.

[3] SHAO J, LIU P, ZHOU Y. Achieving key privacy without losing CCA security in proxy re-encryption[J]. The Journal of Systems and Software, 2012, 85:655-665.

[4] TABAN G, CÁRDENAS A A, GLIGOR V D. Towards a secure and interoperable DRM architecture[A]. Proceedings of the ACM Workshop on Digital Rights Management[C]. New York, USA, 2006. 69-78.

[5] LEE S, HEEJIN P, JONG K. A secure and mutual-profitable DRM interoperability scheme[A]. Proceedings of the IEEE Symposium on Computers and Communications[C]. Riccione, Italy, 2010. 75-80.

[6] SHAO J, CAO Z, LIANG X H, *et al.* Proxy re-encryption with keyword search[J]. Information Sciences, 2010, 180(4):2576-2587.
[7] WANG X A, HUANG X Y, YANG X Y, *et al.* Further observation on proxy re-encryption with keyword search[J]. The Journal of Systems and Software, 2012, 85:643-654.
[8] CANETTI R, HOHENBERGER S. Chosen-ciphertext secure proxy re-encryption[A]. Proceedings of the 14th ACM Conference on Computer and Communications Security[C]. Alexandria, VA, USA, 2007. 185-194.
[9] CANETTI R, HALEVI S, KATZ J. Chosen-ciphertext security from identity-based encryption[A]. EUROCRYPT'04[C]. Alexandria, VA, USA, 2007. 185-194.
[10] LIBERT B, VERGNAUD D. Unidirectional chosen-ciphertext secure proxy re-encryption[J]. IEEE transactions on Information theory, 2011, 57(3):1786-1802.
[11] WENG J, CHEN M R, YANG Y J, *et al.* CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles[J]. Science China(Information Sciences), 2010, 53(3):593-606.
[12] HOHENBERGER S, WATERS B. Realizing hash-and-sign signatures under standard assumptions[A]. EUROCRYPT '09[C]. 2009.333-350.
[13] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. Journal of Information Security, 2007, 6(4):213-241.
[14] SHAO J, CAO Z F. CCA-secure proxy re-encryption without pairings[A]. PKC 2009[C]. California, USA, 2009. 357-376.
[15] WENG J, DENG R H, LIU S L, *et al.* Chosen-ciphertext secure bidirectional proxy re-encryption schemes without pairings[J]. Information Sciences, 2010, 180:5077-5089.
[16] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4):557- 594.
[17] SHAO J, CAO Z F. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption[J]. Information Sciences, 2012,206(5):83-95.
[18] WANG H B, CAO Z F, WANG L C. Multi-use and unidirectional identity-based proxy re-encryption schemes[J]. Information Sciences, 2010, 180:4042-4059.
[19] BELLARE M, ROGAWAY P. Optimal asymmetric encryption[A]. EUROCRYPT'94[C]. Perugia, Italy, 1995.92-111.
[20] BONEH D. Simplified OAEP for the RSA and Rabin functions[A]. CRYPTO 2001[C]. California, USA, 2001. 275-291.
[21] BELLARE M, ROGAWAY P. The exact security of digital si natures-how to sign with RSA and rabin[A]. EUROCRYPT'96[C]. Zaragoza, Spain, 1996. 399-416.
[22] HE D B, CHEN J H, HU J. An ID-based proxy signature schemes without bilinear pairings[J]. Ann Telecommun, 2011, 66:657-662.

作者简介：

张维纬（1982-），男，福建泉州人，北京邮电大学博士生，主要研究方向为数字版权管理与数字水印。

张茹（1976-），女，山东济南人，北京邮电大学副教授、硕士生导师，主要研究方向为数字水印、数字图像取证与密码学等。

刘建毅（1980-），男，山西原平人，北京邮电大学副教授、硕士生导师，主要研究方向为信息内容安全、智能信息处理等。

钮心忻（1963-），女，浙江湖州人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、信息隐藏与数字水印、数字内容安全、软件无线电等。

杨义先（1961-），男，四川绵阳人，北京邮电大学教授、博士生导师、主要研究方向为网络与信息安全、密码学、编码理论等。