一种有效的无证书环签密方案

孙 华[1] 孟 坤[2]

(安阳师范学院计算机与信息工程学院 安阳 455000)[1] (清华大学计算机科学与技术系 北京 100084)[2]

摘 要 环签密是一个重要的密码学术语,它结合了加密和环签名的功能,具有保密性、可认证性和匿名性等安全属性。目前已有的无证书环签密方案大都是在随机预言模型下提出的,然而在该模型下可证安全的方案在哈希函数实例化后有时却并不安全。针对这一问题,设计了一个标准模型下可证安全的无证书环签密方案,并通过计算 Diffie-Hellman (CDH)困难问题假设和判定性 Diffie-Hellman (DBDH)困难问题假设,证明了方案满足适应性选择密文攻击下的不可区分性以及适应性选择消息攻击下存在的不可伪造性,因而方案是安全有效的。

关键词 环签密,无证书公钥密码体制,CDH 问题,DBDH 问题

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.11.041

Efficient Certificateless Ring Signcryption Scheme

SUN Hua[1] MENG Kun[2]

(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[2]

Abstract Ring signcryption is an important cryptographic primitive which combines the functions of encryption and ring signature. It can provide confidentiality, authenticity and anonymity simultaneously. At present, most of existing certificateless ring signcryption schemes are proposed in the random oracle, however, they sometimes are proven to be insecure when the hash functions are instantiated. Aiming at this problem, a certificateless ring signcryption scheme was put forward without random oracles in this paper. Meanwhile, it was proven that this scheme satisfies indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message attacks under the computational Diffie-Hellman assumption and decisional Diffie-Hellman assumption, so the scheme is secure and reliable.

Keywords Ring signcryption, Certificateless public key cryptography, CDH problem, DBDH problem

2003年,Al-Riyami 等人[1]首次提出了无证书公钥密码学的概念。无证书公钥密码体制不仅避免了传统公钥密码体制中复杂的证书管理问题,而且还消除了基于身份密码体制[2,3]中固有的密钥托管问题,故被提出后引起了学者们的广泛兴趣。

1997年,Zheng[4]提出了签密这一密码学术语,它能够在一个逻辑步骤内完成加密和签名两种功能,同时实现保密性和认证性这两个安全目标,而其计算成本却低于传统的先签名后加密方法。匿名性是密码学应用中另一个重要属性,2001年,Rivest 等人[5]提出环签名的概念,它是一种秘密泄露消息的方式,能够实现泄密者身份的匿名性。

2005年,Huang 等人[6]首次提出环签密这一概念,它既能够实现消息的机密性和不可伪造性,还使签密者的身份具有匿名性,可是该方案计算量较大。2008年,Li 等人[8]指出文献[7]中的方案不安全,并提出了一种改进方案,可是其依然是不安全的。Zhun 等人[9]也提出一个基于身份的环签名和环签密方案,但其不能抵抗适应性选择明文攻击。2009年,Zhu 等人[10]提出一可证安全的环签密方案,可是其在适应性选择密文攻击下是不安全的。同年,Sharmila 等人[11]提出一个随机预言模型下基于身份的环签密方案。2013年,Zhao 等人[12]在标准模型下给出一个环签密方案。孙华等人[13]同样在标准模型下给出一个门限环签密方案。

在无证书公钥密码方面,2010年,Zhu 等人[14]在随机预言模型下给出一无证书环签密方案。随后,Qi 等人[15]同样给出一无证书环签密方案,不过该方案仍然是随机预言模型下的。最近覃海生等人[16]在随机预言模型下给出一无对运算的无证书环签密方案。

目前,已有的无证书环签密方案大都是在随机预言模型下提出的,然而在随机预言模型下可证安全的方案在哈希函数实例化后往往并不安全,因此设计标准模型下的无证书环签密方案更有意义。本文首先给出了一个可证明安全的无证书环签密方案(Certificateless Ring Signcryption, CLRSC),

到稿日期:2013-12-21 返修日期:2014-02-23 本文受国家自然科学基金(U1204402),河南省科技厅科技攻关计划项目(112102210370),河南省教育厅科学技术研究重点项目(14A413014)资助。

孙 华(1980-),男,博士,副教授,CCF 会员,主要研究方向为密码学与信息安全;孟 坤(1980-),男,博士后,主要研究方向为计算机网络性能评价、无线网络安全。

然后利用相关的困难问题假设对方案的安全性进行了分析与证明。

1 预备知识

1.1 双线性对

设 G 和 G_T 是阶为素数 p 的两个循环群，群 G 的生成元为 g，双线性对是满足如下性质的映射 $e:G\times G\rightarrow G_T$：

1. 双线性：对于所有的 $P,Q\in G$ 与 $a,b\in Z_p^*$，都有 $e(P^a,Q^b)=e(P,Q)^{ab}$；

2. 非退化性：$e(g,g)\neq 1$；

3. 可计算性：存在一个有效的算法计算 $e(P,Q)$，其中 $P,Q\in G$。

1.2 有关困难问题

1. CDH 问题：已知阶为素数 p 的循环群 G，g 是其生成元，对于任意 $a,b\in Z_p^*$，给定 $g^a,g^b\in G$，计算 g^{ab}。

2. DBDH 问题：已知阶为素数 p 的循环群 G，g 是其生成元，对于任意的 $a,b,c\in Z_p^*$，给定 $g^a,g^b,g^c\in G,h\in G_T$，判定 $h=e(g,g)^{abc}$ 是否成立。

2 CLRSC 的形式化定义和安全要求

2.1 CLRSC 的形式化定义

定义 1 无证书环签密由以下几个算法组成：

1)系统参数产生算法：该算法输入安全参数 k，产生系统公开参数 $params$ 及系统主密钥 msk，其中 msk 保密。

2)部分私钥产生算法：给定系统公开参数 $params$、系统主密钥 msk 及用户身份 ID，该算法产生用户的部分私钥 D_{ID}。

3)设置用户秘密值：输入用户的身份 ID，该算法产生用户的秘密值 x_{ID}。

4)用户公钥产生算法：输入用户的身份 ID 及其秘密值 x_{ID}，该算法产生用户的公钥 pk_{ID}。

5)用户私钥产生算法：输入用户 ID 的部分私钥 D_{ID}、秘密值 x_{ID}，该算法产生用户的私钥 sk_{ID}。

6)签密：给定环成员 $L=(ID_1,\cdots,ID_n)$、待签密消息 m、实际环签密产生者 ID_s 的私钥 sk_{ID_s} 以及环签密接收者 ID_R 的公钥 pk_{ID_R}，该算法产生有效的无证书环签密 C。

7)解密：给定环成员 $L=(ID_1,\cdots,ID_n)$ 及其公钥、环签密接收者 ID_R 的私钥 sk_{ID_R} 以及密文 C，如果 C 是一个有效的无证书环签密，则该算法输出消息 m，否则，输出 $\perp$。

2.2 CLRSC 的安全要求

无证书环签密应该满足下面的安全要求：

1. 正确性：环签密产生者按照签密算法所生成的环签密应能够通过验证算法进行验证。

2. 无条件匿名性：给定有效的环签密密文，任何攻击者(包括环中其它成员)即使知道所有环成员的私钥，也无法确定环签密产生者的真实身份。

3. 不可伪造性：任何攻击者想要伪造环签密产生者而生成有效的签密密文在计算上是不可能的。

4. 机密性：除环签密产生者和接收者之外的任何第三方想要获取签密消息在计算上是不可能的。

5. 消息可恢复性：指定环签密接收者在收到签密密文后，能够验证并解密得到签密消息。

3 本文的 CLRSC 方案

在本部分内容中，我们将给出标准模型下无证书环签密的具体方案，方案描述如下：

给定阶为素数 p 的循环群 G 和 G_T，双线性映射 $e:G\times G\rightarrow G_T$，两个无碰撞的哈希函数 $H_u:\{0,1\}^*\rightarrow\{0,1\}^{n_u}$ 和 $H_m:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$ 分别将任意长度的身份 ID 和消息 m 输出为长为 n_u 和 n_m 的位串。

1)系统参数产生算法

密钥生成中心 KGC 随机选取 G 的生成元 g，$\alpha\in Z_p^*$，计算 $g_1=g^\alpha$。随机选取 $u'\in Z_p,g_2,m'\in G,n_u$ 维向量 $\hat{U}=(u_i)$，n_m 维向量 $\hat{M}=(m_i)$，其中 $u_i\in Z_p,m_i\in G$，计算 $z_1=e(g_1,g_2),z_2=e(g,g_2)$，则系统公开参数为 $params=(G,G_T,e,g,g_1,g_2,u',\hat{U},m',\hat{M},H_u,H_m,z_1,z_2)$，系统主密钥为 $msk=\alpha$。

2)部分私钥产生算法

给定用户身份 ID，令 $u=H_u(ID)$ 为用户 ID 的长为 n_u 的位串，$u[i]$ 表示该位串中的第 i 位，$\Phi_{ID}\subseteq\{1,2,\cdots,n_u\}$ 为 $u[i]=1$ 的序号 i 的集合，KGC 随机选取 $r\in Z_p$，计算用户 ID 的部分私钥为 $D_{ID}=(d_1,d_2)=(g_2^{\alpha+r(u'+\sum_{j\in\Phi_{ID}}u_j)},z_2^r)$，并将其发送给用户。它在接收到部分私钥 D_{ID} 后，可通过等式 $e(g,d_1)=z_1d_2^{(u'+\sum_{j\in\Phi_{ID}}u_j)}$ 进行验证，若等式成立，则其为有效的部分私钥；否则，重新向 KGC 发出询问。

3)用户秘密值设置

对于用户 ID，其任意选取 $x_{ID}\in Z_p^*$ 作为它的秘密值。

4)用户公钥产生算法

对于用户 ID，其计算 $PK_{ID}=e(g_1,g_2)^{x_{ID}}=z_1^{x_{ID}}$ 作为它的公钥。

5)用户私钥产生算法

对于用户 ID，其私钥为 $SK_{ID}=(s_{ID,1},s_{ID,2},s_{ID,3})=(d_1,d_2,x_{ID})$。

6)签密

设 $L=\{ID_1,\cdots,ID_n\}$ 为 CLRSC 中 n 个成员身份的集合，待签密消息为 $m\in G_T$，不妨设实际产生环签密的用户身份为 ID_s，$ID_s\in L$，环签密接收者的身份为 ID_R，则可以通过如下步骤产生本文的无证书环签密：

①用户 ID_s 计算 $M=H_m(L,m)$，令 $\mathcal{M}\subseteq\{1,2,\cdots,n_m\}$ 为消息 m 的位串中 $M[k]=1$ 的序号 k 的集合。

②令 $U_i=u'+\sum_{j\in\Phi_{ID_i}}u_j(i=1,\cdots,n)$，$U_R=u'+\sum_{j\in\Phi_{ID_R}}u_j$，用户 ID_s 利用其私钥 SK_{ID_s}，随机选取 $l_1,\cdots,l_n,l_m\in Z_p$，计算 $R_i=z_2^{l_i}(i=1,\cdots,n)$，其中 $i\neq s$，$R_s=s_{ID_s,2}\cdot z_2^{l_s}$。令 $C_1=s_{ID_s,1}\cdot(m'\prod_{j\in\mathcal{M}}m_j)^{x_{ID_s}\cdot l_m}\cdot g_2^{\sum_{i=1}^{n}l_i(U_i)}$，$C_2=g^{x_{ID_s}\cdot l_m}$，$C_3=m\cdot PK_{ID_R}^{l_s}=m\cdot z_1^{x_{ID_R}\cdot l_s}$，$C_4=g^{l_s}$，$C_5=l_s(U_R)$，则生成的无证书环签密为 $C=(C_1,C_2,C_3,C_4,C_5,R_1,\cdots,R_n)$。

7)解密

当用户 ID_R 接收到环为 $L=\{ID_1,\cdots,ID_n\}$、消息为 m 的

无证书环签密 C 后，它将进行如下计算：

①用户 ID_R 利用其私钥 SK_{ID_R}，计算 $m=C_3\cdot(s_{ID_R,2})^{C_5\cdot s_{ID_R,3}}\cdot e(s_{ID_R,1},C_4^{s_{ID_R,3}})^{-1}$

②计算 $M=H_m(L,m)$，得到消息 m 的位串中 $M[k]=1$ 的序号 k 的集合 $\mathcal{M}$。

③验证等式 $e(C_1,g)=z_1\cdot e(m'\prod_{j\in\mathcal{M}}m_j,C_2)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$ 是否成立，若等式成立，则 C 是一个有效的无证书环签密。

4 方案分析与证明

4.1 方案正确性

①当签密接收者 ID_R 收到无证书环签密 C 后，其可首先计算：

$$C_3\cdot(s_{ID_R,2})^{C_5\cdot s_{ID_R,3}}\cdot e(s_{ID_R,1},C_4^{s_{ID_R,3}})^{-1}$$
$$=m\cdot z_1^{x_{ID_R}\cdot l_s}\cdot\frac{e(g,g_2)^{r_{ID_R}\cdot l_s(U_R)\cdot x_{ID_R}}}{e(g_2^{a+r_{ID_R}(U_R)},g^{l_s\cdot x_{ID_R}})}$$
$$=m\cdot z_1^{x_{ID_R}\cdot l_s}\cdot z_1^{-x_{ID_R}\cdot l_s}=m$$

②用户其次计算 $M=H_m(L,m)$，并进行如下验证：

$$e(C_1,g)$$
$$=e(g_2^{a+(r_{ID_s}+l_s)(U_s)+\sum_{i=1,i\neq s}^{n}l_i(U_i)}(m'\prod_{j\in\mathcal{M}}m_j)^{l_m x_{ID_s}},g)$$
$$=e(g_2^{a},g)\cdot e((m'\prod_{j\in\mathcal{M}}m_j)^{l_m x_{ID_s}},g)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$$
$$=z_1\cdot e(m'\prod_{j\in\mathcal{M}}m_j,C_2)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$$

因此，本文方案是正确的。

4.2 方案安全性

定理 1 本文所提出的 CLRSC 方案满足无条件匿名性。

证明：文中的无证书环签密 C 是由签密产生者 ID_s 利用其私钥生成的，其由随机产生的部分私钥和秘密值构成，故签密者的私钥是随机分布的。其次，无证书环签密 C 中的 $R_1,\cdots,R_n$ 均是随机生成，没有泄露签密者身份的任何信息。对于 $R_s=s_{ID_s,2}\cdot z_2^{l_s}=z_2^{r_{ID_s}+l_s}$ 而言，因 r_{ID_s} 是由 KGC 随机选取，l_s 由签密者随机选取，故 R_s 的分布也是随机的。最后，通过分析 $C_1=g_2^{a+(r_{ID_s}+l_s)(U_s)+\sum_{i=1,i\neq s}^{n}l_i(U_i)}(m'\prod_{j\in\mathcal{M}}m_j)^{l_m x_{ID_s}}$ 可知，g_2 的指数部分也是随机产生的，其没有泄露签密者身份的任何信息。因而即使攻击者获取环 L 中所有成员的私钥，其猜测出实际签密者身份的概率也不超过 $\frac{1}{n-1}$，故本文的 CLRSC 满足无条件匿名性。

定理 2 在 CDH 困难问题假设下，本文方案在第一类攻击者 $\mathcal{A}_I$ 适应性选择消息攻击下满足存在不可伪造性(EUF-CLRSC-CMA)。

证明：假设攻击者 $\mathcal{A}_I$ 能以不可忽略的优势攻击本方案，那么可以构造算法 B，B 能够利用 $\mathcal{A}_I$ 解决 CDH 问题。给定 B 一个 CDH 问题的实例 (g,g^a,g^b)，其目标是计算 g^{ab}。为此算法 B 模仿 $\mathcal{A}_I$ 的挑战者，具体过程如下：

系统初始化：B 设定 $l_u=2(q_e+q_s)$、$l_m=2q_s$，其中 q_e 是 $\mathcal{A}$ 私钥询问次数，q_s 是 $\mathcal{A}$ 签密询问次数。随机选择 k_u 和 k_m，满足 $0\leqslant k_u\leqslant n_u$ 和 $0\leqslant k_m\leqslant n_m$，并假定 $l_u(n_u+1)<p$ 和 $l_m(n_m+1)<p$。B 选取 $x'\in_R Z_{l_u}$ 及长度为 n_u 的向量 $X=(x_i)$，其中 $x_i\in_R Z_{l_u}$；选取 $y'\in_R Z_{l_m}$ 及长度为 n_m 的向量 $Y=(y_i)$，其中 $y_i\in_R Z_{l_m}$；最后选取 $w'\in_R Z_p$，长度为 n_m 的向量 $W=(w_i)$，其中 $w_i\in_R Z_p$。

对于本方案中的哈希函数 $u=H_u(ID)$ 和 $M=H_m(L,m)$ 而言，我们定义以下函数：

$$F(ID)=x'+\sum_{j\in\Phi}x_j-l_u k_u,K(M)=y'+\sum_{j\in\mathcal{M}}y_j-l_m k_m$$
$$L(M)=w'+\sum_{j\in\mathcal{M}}w_j$$

接下来算法 B 构造方案中的公开参数：

$$g_1=g^a,g_2=g^b,u'=x'-l_u k_u,u_i=x_i(1\leqslant i\leqslant n_u)$$
$$m'=g_2^{-l_m k_m+y'}g^{w'},m_i=g_2^{y_i}g^{w_i}(1\leqslant i\leqslant n_m)$$

因此我们可以得到如下等式：

$$g_2^a=g^{ab},F(ID)=u'+\sum_{j\in\Phi}u_j,m'\prod_{j\in\mathcal{M}}m_j=g_2^{K(M)}g^{L(M)}$$

最后算法 B 将公开参数发送给攻击者 $\mathcal{A}_I$。

询问阶段：攻击者 $\mathcal{A}_I$ 可适应性地发起如下一系列询问，算法 B 维护列表 L_1,L_2,L_3，它们在初始状态下都是空表，当 $\mathcal{A}_I$ 发起询问时，B 进行如下响应：

①部分私钥询问：当 $\mathcal{A}_I$ 询问身份 ID 的部分私钥 D_{ID} 时，如果条件 $F(ID)\neq 0 \bmod p$ 成立，则 B 可以构造出其 D_{ID}。B 任选 $r\in Z_p$，计算

$$D_{ID}=(d_1,d_2)$$
$$=(g_1^{-1}(gg_2)^{r(u'+\sum_{j\in\Phi_{ID}}u_j)},e(gg_2,g^r g_1^{-1/(u'+\sum_{j\in\Phi_{ID}}u_j)}))$$

然后把 (ID,D_{ID}) 添加到列表 L_1 中，同时将其发送给攻击者 $\mathcal{A}_I$，$\mathcal{A}_I$ 可通过等式 $e(g,d_1)=z_1 d_2^{(u'+\sum_{j\in\Phi_{ID}}u_j)}$ 进行验证；如果 $F(ID)=0 \bmod p$，那么 B 将失败退出。

②用户公钥询问：当 $\mathcal{A}_I$ 询问身份 ID 的公钥 PK_{ID} 时，如果列表 L_2 中存在 $(ID,x_{ID},PK_{ID},0)$，则返回 PK_{ID}，这里列表 L_2 中的数字 0 或 1 分别代表公钥是否被替换；否则，B 任选 $x_{ID}\in Z_p^*$ 计算 $PK_{ID}=e(g_1,g_2)^{x_{ID}}$，然后把 $(ID,x_{ID},PK_{ID},0)$ 添加到列表 L_2 中，同时将其发送给 $\mathcal{A}_I$。

③用户私钥询问：当 $\mathcal{A}_I$ 询问身份 ID 的私钥 SK_{ID} 时，如果列表 L_3 中存在 (ID,SK_{ID})，则返回 SK_{ID}；否则，算法 B 首先从列表 L_1、L_2 中查询 ID 所对应的 (ID,D_{ID}) 和 (ID,x_{ID},PK_{ID})，令 $SK_{ID}=(D_{ID},x_{ID})$，然后把它添加到列表 L_3 中，同时将其发送给 $\mathcal{A}_I$。

④公钥替换询问：当 $\mathcal{A}_I$ 对身份 ID 进行公钥替换询问时，算法 B 任选 $x'_{ID}\in Z_p^*$，计算 $PK'_{ID}=e(g_1,g_2)^{x'_{ID}}$，然后把 $(ID,x'_{ID},PK'_{ID},1)$ 添加到列表 L_2 中，同时将其发送给 $\mathcal{A}_I$。

⑤签密询问：当攻击者 $\mathcal{A}_I$ 询问环为 $L=\{ID_1,\cdots,ID_n\}$、消息为 m、签密者为 ID_s、签密接收者为 ID_R 的无证书环签密时，如果条件 $F(ID_s)\neq 0 \bmod p$ 成立，那么算法 B 可以使用前面的方法构造出其私钥，并利用签密算法产生无证书环签密 C。

如果条件 $F(ID_s)=0 \bmod p$ 且 $F(ID_R)\neq 0 \bmod p$ 成立，那么算法 B 按照如下方法来构造该无证书环签密。假定 $K(M)\neq 0 \bmod p$，B 随机选择 $l_1,\cdots,l_n,l_m\in Z_p$，计算 $R_1=z_2^{l_1},\cdots,R_n=z_2^{l_n}$，$C_1'=g_2^{a+\sum_{i=1}^{n}l_i(U_i)}g_1^{-L(M)/K(M)}(m'\prod_{j\in\mathcal{M}}m_j)^{l_m}=g_2^{a+\sum_{i=1}^{n}l_i(U_i)}(m'\prod_{j\in\mathcal{M}}m_j)^{\bar{l}_m}$，$C_2'=g_1^{-1/K(M)}g^{l_m}=g^{\bar{l}_m}$，$C_3'=m\cdot e(g_1,g_2)^{x_{ID_R}\cdot l_s}$，$C_4'=g^{l_s}$，$C_5'=l_s(U_{ID_R})$，其中 $\bar{l}_m=l_m-a/K(M)$。可见 $C'=(C_1',C_2',C_3',C_4',C_5',R_1,\cdots,R_n)$ 是一个有

效的无证书环签密，如果 $K(M)=0 \bmod p$，那么算法 B 将失败退出。

⑥解签密询问：当攻击者 $\mathcal{A}_I$ 发起在环为 L 、环签密接收者为 ID_R 以及密文为 C 的解签密询问时，算法 B 首先从列表 L_3 中获取 ID_R 的私钥 SK_{ID_R}，然后通过运行解密算法恢复出消息 m 并将其发送给 $\mathcal{A}_I$。

伪造阶段：攻击者 $\mathcal{A}_I$ 输出在环 $L^*=\{ID_1^*,\cdots,ID_z^*\}$、消息 m^* 及环签密接收者为 ID_R^* 下的伪造无证书环签密 C^*。如果以下两个 i^* 条件同时成立：

①$F(ID_i^*)=0 \bmod p$ 对于所有 $ID_i^* \in L^*$ 都成立；

②$K(M^*)=0 \bmod p$，其中 $M^*=H_m(L^*,m^*)$。

且算法 B 在整个询问过程中没有失败退出，那么 B 可计算 $\dfrac{C_1^*}{(C_2^*)^{L(M^*)}}=\dfrac{g_2^{a+\sum_{i=1}^{n} l_i(U_i^*)}(m'\prod_{j\in M} m_j)^{l_m^*}}{g^{l_m^*\cdot L(M^*)}}=g_2^a=g^{ab}$，此即 CDH 问题的解。

因此如果存在一个攻击者 $\mathcal{A}_I$ 能以不可忽略的概率伪造一个有效的 CLRSC，那么就存在一个有效的算法能以不可忽略的概率解决 CDH 问题，而这与 CDH 问题是一个困难问题相矛盾，故方案是 EUF-CLRSC-CMA 安全的。

定理 3 在 CDH 困难问题假设下，本文方案在第二类攻击者 $\mathcal{A}_{II}$ 攻击下满足 EUF-CLRSC-CMA。

证明：对于第二类攻击者 $\mathcal{A}_{II}$ 而言，它知道系统主密钥，但不能替换用户的公钥。证明过程与定理 2 中相类似，限于篇幅原因，此处省略。

定理 4 在 DBDH 困难问题假设下，本文方案在第一类攻击者 $\mathcal{A}_I$ 适应性选择密文攻击下满足不可区分性（IND-CLRSC-CCA2）。

证明：假设攻击者 $\mathcal{A}_I$ 能以不可忽略的优势攻击本方案，那么可以构造算法 B，B 能够利用 $\mathcal{A}_I$ 解决 DBDH 问题。给定 B 一个 DBDH 问题的实例 (g^a,g^b,g^c,h)，其目标是判定等式 $h=e(g,g)^{abc}$ 是否成立。为此算法 B 模仿 A_I 的挑战者，具体过程如下：

系统初始化：算法 B 如同定理 2 证明中那样构造系统参数，这里的区别在于，B 随机选取 $\beta\in Z_p$，令 $g_1=g^a$，$g_2=g^\beta$，然后将 g_1、g_2 以及其它系统参数发送给攻击者 $\mathcal{A}_I$。

阶段 1：攻击者 $\mathcal{A}_I$ 可如同定理 2 证明中那样，发起一定数量的询问，算法 B 然后进行响应。

挑战阶段：攻击者 $\mathcal{A}_I$ 任意选取两个相同长度的消息 m_0 和 m_1、环 $L^*=\{D_1^*,\cdots,ID_z^*\}$ 以及环签密接收者身份 ID_R^* 并将它们发送给算法 B。如果在 $\mathcal{A}_I$ 第一阶段询问了 ID_R^* 的私钥，那么 B 将失败退出。B 任选一位 $b\in(0,1)$，如果 $K(M_b)=0 \bmod p$，那么 B 将失败退出。如果 $F(ID_R^*)\neq 0 \bmod p$，那么 B 同样将失败退出。否则，B 任选 $l_1,\cdots,l_n,l_m\in Z_p$，进行如下构造：

$$C_1^*=g_2^{\sum_{i=1}^{n} l_i(U_i)}\, g_1^{-L(M_b)/K(M_b)}(m'\prod_{j\in M} m_j)^{l_m}$$

$$=g_2^{a+\sum_{i=1}^{n} l_i(U_i)}(m'\prod_{j\in M} m_j)^{\tilde{l}_m}$$

$$C_2^*=g_1^{-1/K(M_b)}g^{l_m}=g^{\tilde{l}_m}$$

$$C_3^*=m_b\cdot PK_{ID_R^*}^{c}=m_b\cdot(e(g^a,g^\beta)^b)^c=m_b\cdot h^\beta$$

$$C_4^*=g^c$$

$$C_5^*=c(U_{ID_R^*})=cF(ID_R^*)=0$$

$$R_1=z_2^{l_1},\cdots,R_n=z_2^{l_n}$$

其中，$\tilde{l}_m=l_m-a/K(M)$。如果 $h=e(g,g)^{abc}$，则 $C'=(C_1',C_2',C_3',C_4',C_5',R_1,\cdots,R_n)$ 是一个有效的无证书环签密，且由 C_3^* 可知这里 ID_R^* 的秘密值为 $x_{ID_R^*}=b$，又由于 g^b 是给定 B 的 DBDH 问题实例中属于群 G 的任意随机元素，因此 b 对 B 而言是未知的（这是一个有限群上的 DLP 困难问题）。

阶段 2：攻击者 $\mathcal{A}_I$ 可如同阶段 1 那样，发起一定数量的询问，但是 $\mathcal{A}_I$ 不能询问 ID_R^* 的私钥。

猜测阶段：攻击者 $\mathcal{A}_I$ 输出对 b 的猜测 b'，如果 $b=b'$，那么算法 B 输出 True，并将 $h=e(g,g)^{abc}$ 作为 DBDH 问题的解；否则，B 输出 False，并终止游戏。因此如果存在一个攻击者 $\mathcal{A}_I$ 能以不可忽略的概率成功地对本方案进行适应性选择密文攻击，那么就存在一个有效的算法能以不可忽略的概率解决 DBDH 问题，而这与 DBDH 问题是一个困难问题相矛盾，故方案是 IND-CLRSC-CCA2 安全的。

定理 5 在 DBDH 困难问题假设下，本文方案在第二类攻击者 $\mathcal{A}_{II}$ 攻击下满足 IND-CLRSC-CCA2。

证明：该证明过程与定理 4 中相类似，限于篇幅原因，此处省略。

5 性能分析

我们将从方案的计算开销和对方案进行安全性证明所采用的安全模型两个方面入手，通过表 1 将本文所提出的方案与现有的几个基于身份的环签密方案[11,12]及无证书环签密方案[14,15]进行比较。对于群元素的计算而言，因群元素的标量乘和指数运算等计算，其开销要远小于双线性对的计算开销，故这里仅考虑双线性对的运算量。此外，在本方案中可以通过对 $z_1=e(g_1,g_2)$ 和 $z_2=e(g,g_2)$ 进行预计算来提高本方案的计算效率，这里在与文献[12]进行对比时也采取了相同的处理方法。

表 1 几个环签密方案比较

	签密	解密	安全模型
文献[11]	1	3	随机模型
文献[12]	0	3	标准模型
文献[14]	n+1	n	随机模型
文献[15]	1	n+2	随机模型
本文方案	0	3	标准模型

通过上表可知，现有的环签密方案大都是在随机预言模型下进行安全性证明的，其计算开销较大，而本文所提出的方案不仅具有无证书公钥密码体制的优点，同时也具有较低的计算开销。

结束语 基于环签密特定的安全属性，在实际生活中有着广泛的应用。针对现有的无证书环签密大多是在随机预言模型下提出的这一现状，本文设计了一个标准模型下的无证书环签密方案，并通过 CDH 和 DBDH 困难问题假设对方案的安全性进行了分析与证明。该方案在整个实现过程中仅需要 3 次双线性对运算，因而具有较高的效率。如何设计密文

（下转第 238 页）

参 考 文 献

[1] 李慧颖,瞿裕忠. 基于关键词的语义网数据查询研究综述[J]. 计算机科学,2011,38(7):18-23

[2] 金强. 基于 Hase 的 RDF 存储系统的研究与设计[D]. 杭州:浙江大学,2011

[3] 王鑫,冯志勇,杜朴风,等. Jingwei:一种分布式大规模 RDF 数据服务器[J]. 计算机研究与发展,2011,48(Suppl.):451-455

[4] Li L,Song Y. Distributed Storage of Massive RDF Data Using HBase[J]. Journal of Communication and Computer, 2011, 8(5):325-328

[5] Sun J,Jin Q. Scalable rdf store based on hbase and mapreduce [C]// 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE,2010:633-636

[6] Husain M F, Doshi P, Khan L, et al. Storage and retrieval of large rdf graph using hadoop and mapreduce[M]. Cloud Computing. Springer Berlin Heidelberg,2009:680-686

[7] Myung J,Yeon J,Lee S G. SPARQL Basie Graph Pattern Processing with Iterative MapReduce [C] // Proceedings of the Workshop on Massive Data Analytics on the Cloud (MDAC' 10). 2010:6-12

[8] Husain M, McGlothlin J, Masud M M, et al. Heuristics-Based Query Processing for Large RDF Graphs Using Cloud Computing[J]. IEEE Transactions on Knowledge and Data Engineering,2011,23(9):1312-1327

[9] Cheng J,Wang W,Gao R. Massive RDF Data Complicated Query Optimization Based on MapReduce [J]. Physics Procedia, 2012,25:1414-1419

[10] Wu B,Jin H,Yuan P. Scalable SAPRQL querying processing on large RDF data in cloud computing environment[C]// Pervasive Computing and the Networked World. Berlin Heidelberg: Springer,2013:631-646

[11] Liu L,Yin J,Gao L. Efficient Social Network Data Query Processing on MapReduce[C]// Proc of the 5th ACM workshop. New York:ACM,2013:27-32

[12] 刘翔宇,吴刚. 基于 Prôfer 序列的 RDF 数据索引与查询[J]. 计算机学报,2011,34(10):1997-2008

[13] Dean J,Ghemawat S. MapReduce:simplified data processing on large clusters[J]. Communications of the ACM, 2008, 51(1): 107-113

[14] 袁平鹏,刘谱,张文娅,等. 高可扩展的 RDF 数据存储系统[J]. 计算机研究与发展,2012,49(10):2131-2141

(上接第 211 页)

长度为固定值的无证书环签密,且进一步提高方案的效率,是笔者下一步将继续展开的工作,同时对它的研究也具有重要的理论和现实意义。

参 考 文 献

[1] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Proceedings of ASIACRYPT 2003. Berlin:Springer-Verlag,2003:452-473

[2] Waters B. Efficient identity-based encryption without random oracles[C]// Proceedings of EUROCRYPT 2005. Berlin:Springer-Verlag,2005:114-127

[3] Gentry C. Practical identity-based encryption without random oracles[C]// Proceedings of EUROCRYPT 2006. Berlin:Springer-Verlag,2006:445-464

[4] Zheng Y L. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature)+cost(encryption)[C]// Proceedings of CRYPTO 1997. Berlin: Springer-Verlag, 1997: 165-179

[5] Rivest R L,Shamir A,Tauman Y. How to leak a secret[C]// Proceedings of ASIACRYPT 2001. Berlin: Springer-Verlag, 2001:552-565

[6] Huang X Y,Susilo W,Mu Y,et al. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[C]// Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Washington DC,IEEE Computer Society,2005:649-654

[7] Zhang M, Yang B, Zhu S, et al. Efficient secret authenticatable anonymous signcryption scheme with identity privacy[C]// Proceedings of Intelligence and Security Informatics(ISI 2008). Berlin:Springer-Verlag,2008:126-137

[8] Li F G, Masaaki S, Tsuyoshi T. Analysis and improvement of authenticatable ring signcryption scheme[J]. Journal of Shanghai Jiaotong University(Science),2008,13(6):679-683

[9] Zhun L J,Zhang F T. Efficient id-based ring signature and ring signcryption schemes [C] // Proceedings of CIS 2008. IEEE Press,2008:303-307

[10] Zhu Z C,Zhang Y Q,Wang F J. An efficient and provable secure identity-based ring signcryption scheme[J]. Computer Standards & Interfaces,2009,31(6):1092-1097

[11] Sharmila D S S,Sree V S,Pandu R C. On the security of identity based ring signcryption schemes[C]// Proceedings of ISC 2009. Berlin:Springer-Verlag,2009:310-325

[12] Zhao Z M, Yu T, Ren X F. Efficient identity-based ring signcryption scheme in the standard model[EB/OL]. [2013-03-20]. http://www.joics.com/publishedpapers/2013_10_5_1471_1478.pdf

[13] Sun H,Wang A M,Zheng X F. Provably secure identity-based threshold ring signcryption scheme in standard model[J]. Computer Science,2013,40(5):131-135

[14] Zhu L J, Zhang F T, Miao S Q. A provably secure parallel certificateless ring signcryption scheme[C]// Proceedings of 2010 International Conference on Multimedia Information Networking and Security. IEEE Press,2010:423-427

[15] Qi Z H,Yang G,Ren X Y. Provably secure certificateless ring signcryption scheme[J]. China Communications,2011,8(3):99-106

[16] Qin H S,Zhang L,Feng Y Q,et al. Certificateless ring signcryption scheme without paring design[J]. Computer Engineering and Design,2013,34(3):841-844