doi:10.3969/j.issn.1000-436x.2014.02.005

标准模型下前向安全公钥加密方案的新构造

陆阳，李继国
（河海大学 计算机与信息学院，江苏 南京 211100）

摘 要：针对已有的可证安全的前向安全公钥加密方案仅满足较弱的选择明文安全性，难以满足实际应用的安全需求这一问题，提出了一个新的前向安全公钥加密方案，基于判定性截断 q-ABDHE 问题的困难性，该方案在标准模型下被证明满足选择密文安全性。在该方案中，解密算法的计算代价和密文的长度独立于系统时间周期总数。对比分析表明，该方案的整体性能优于已有的前向安全公钥加密方案。
关键词：公钥加密；前向安全；选择密文安全；标准模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)02-0033-07

Novel construction of forward-secure public-key encryption in the standard model

LU Yang, LI Ji-guo
(College of Computer and Information Engineering, Hohai University, Nanjing 211100, China)

Abstract: All existing provably secure forward-secure public-key encryption schemes in the literature were only proven to be chosen-plaintext secure. A novel forward-secure public-key encryption scheme without random oracles was proposed. Under the hardness of the truncated decision q-augmented bilinear Diffie-Hellman exponent problem, the proposed scheme was proved to be chosen-ciphertext secure in the standard model. In the proposed scheme, the running time of decryption algorithm and the size of ciphertext are both independent on the total number of the time periods. Compared with the previous forward-secure public-key encryption schemes in the literature, the proposed scheme has obvious advantage in security and efficiency.
Key words: public-key encryption; forward security; chosen-ciphertext security; standard model

1 引言

公钥密码体制是实现网络信息安全的重要手段之一。在公钥密码体制中，用于加密或签名验证的公钥可以公开传播，这对公开网络上的保密通信、密钥分配、数字签名以及认证等带来了深远的影响，因此公钥密码体制于 1976 年由 Diffie 和 Hellman[1]提出以来，便得到了广泛的应用。然而，随着计算机网络以及便携式移动设备的广泛应用，密码算法经常需要在不安全的电子设备上运行，私钥泄露的问题变得日益严重。对于攻击者而言，与解决密码系统所基于的数学难题相比，获得不安全的电子设备中的用户私钥则相对容易得多。一旦用户私钥泄露，那么该用户的通信将会失去安全保障。毫无疑问，私钥泄露是公钥密码系统所面临的最致命的威胁。因此，研究如何减轻由于私钥泄漏造成的损害对于构建实用的公钥密码系统是非常必要的。

1997 年，Anderson[2]在第四届 ACM CCS 大会的邀请报告中提出将前向安全的思想[3,4]引入到非交互的公钥密码体制中以解决私钥泄漏这一问题。随后，Bellare 和 Miner[5]给出了非交互的前向安全签名方案及其安全模型的形式化定义，并提出了一个前向安全签名方案。在 Bellare 和 Miner 提出的前向安全签名方案中，用户的私钥不再保持固定不变，而是随着系统时间做不断进化。具体来说，密码系统的生命周期被分成 N 个时间周期，记为 0, 1,…,N–1。在时间周期 0，用户设备生成时间周期 0

收稿日期：2012-11-29；修回日期：2013-03-05

内使用的私钥 SK_0，即初始私钥，该密钥存储在用户设备中。在时间周期 1，该设备以初始私钥 SK_0 作为输入，采用特定的数学方法推导出时间周期 1 的私钥 SK_1，同时删除初始私钥 SK_0。以此类推，在时间周期 $i(1\leqslant i\leqslant N-1)$，该设备以时间周期 $i-1$ 的私钥 SK_{i-1} 为输入，产生时间周期 i 的私钥 SK_i，同时删除 SK_{i-1}。这样，用户的私钥随着系统时间周期的变化而不断进化，而用户的公钥则保持不变。公钥密码方案的前向安全性是指攻击者即使获得了一个用户在时间周期 i 的私钥 SK_i，也无法解密该用户在时间周期 i 之前接收到的所有密文或伪造出该用户在时间周期 i 之前的有效签名，同时也无法由私钥 SK_i 推导出该用户在时间周期 i 之前的所有私钥。因此，前向安全技术能够有效减轻私钥泄漏造成的损害。受到 Bellare 和 Miner 工作[5]的启发，非交互的前向安全技术得到了高度的关注，一系列非交互的前向安全签名方案[6~14]被相继提出。2003 年，Canetti 等人[15]给出了非交互的前向安全公钥加密方案及其安全模型的形式化定义，并首次提出了一个非交互的前向安全公钥加密方案。该方案基于 Gentry 和 Silverberg 的层次化的基于身份加密方案[16]并在标准模型下被证明满足选择明文安全性。2007 年，Canetti 等人[17]提出了二叉树加密的概念并进一步给出了由二叉树加密方案构造前向安全公钥加密方案的一般方法。同年，Jiang 等人[18]提出了一个带有抗篡改证据的前向安全公钥加密方案，并声称所提出的方案在标准模型下满足选择密文安全性。然而，Jiang 等人并没有给出方案的安全性证明。2009 年，李成邦等人[19]提出了一种用普通公钥加密方案构造前向安全公钥加密方案的一般方法。2011 年，Lu 和 Li[20]基于 Boneh 等人的层次化的基于身份加密方案[21]提出了另一个前向安全公钥加密方案，并在标准模型下证明了该方案满足选择明文安全性。与 Canetti 等人的前向安全公钥加密方案[15,17]相比，该方案的优势在于加密时间和密文长度都独立于系统周期总数。该方案的不足在于其安全性是在一个相对较弱的安全模型中证明的。近年来，一些学者还将前向安全思想引入到基于身份密码体制以及基于证书密码体制中，提出了一些具备前向安全性的基于身份密码方案[22~24]和基于证书密码方案[25]。

自适应选择密文攻击下的不可区分安全性[26](简称选择密文安全性)是公钥加密方案安全性的事实上的标准。然而，已有的可证安全的前向安全公钥加密方案[15,17,20]仅满足较弱的选择明文安全性。尽管可以通过一些密码学方法(如非交互的零知识证明系统[26])将这些方案的安全性增强为选择密文安全性，但会产生额外的计算代价和通信代价。针对这一现状，提出了一个满足选择密文安全性的前向安全公钥加密方案的直接构造。在标准模型下，该方案被证明对自适应选择密文攻击是前向安全的。在方案的效率方面，该方案的加密时间和密文长度独立于系统时间周期总数 N，而其他性能参数的复杂度为 $O(\log N)$。与已有标准模型下可证安全的前向安全公钥加密方案[15,17,20]相比，该方案在整体性能上(综合考虑方案的安全性以及效率)具有明显的优势。

2 双线性对与困难问题假设

令 G_1 和 G_2 是 2 个 p 阶循环群，其中，p 为大素数，g 是群 G_1 的生成元。假设 G_1 和 G_2 这 2 个群中的离散对数问题都是困难问题。一个可接受的双线性对是指满足下列 3 个性质的一个映射 $e:G_1\times G_1\to G_2$。

1) 双线性：对于任意的 $u,v\in G_1$ 和 $a,b\in Z_p^*$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$e(g,g)\neq 1_{G_2}$，其中，1_{G_2} 是群 G_2 的单位元。

3) 可计算性：存在有效的算法计算 $e(u,v)\in G_2$。

本文提出的前向安全公钥加密方案的安全性证明基于如下的判定性截断 q-ABDHE(decision truncated q-augmented bilinear diffie-hellman exponent)问题[27]。

定义 1 判定性截断 q-ABDHE 问题。设 G_1 和 G_2 是 2 个大素数 p 阶循环群，g 是群 G_1 的生成元，$e:G_1\times G_1\to G_2$ 是一个双线性对，则(G_1，G_2)上的判定性截断 q-ABDHE 问题是：对于任意的 $\alpha\in Z_p^*$，给定 $(g,\ g^{\alpha},\cdots,g^{\alpha^q}\ ,g'\ ,g'^{\alpha^{q+2}})\in G_1^{q+3}$ 和 $T\in G_2$，判断 $T=e(g,g')^{\alpha^{q+1}}$ 是否成立。如果成立，输出 1；否则，输出 0。

如果任意概率多项式时间算法 A 解决(G_1,G_2)上的判定性截断 q-ABDHE 问题的优势

$$Adv_A^{q-\mathrm{ABDHE}}=|\Pr[A(g,g^{\alpha},\cdots,g^{\alpha^q},g',g'^{\alpha^{q+2}},e(g,g')^{\alpha^{q+1}})=1]-\Pr[A(g,g^{\alpha},\cdots,g^{\alpha^q},g',g'^{\alpha^{q+2}},T)=1]|$$

都是可忽略的，则称(G_1,G_2)上的判定性截断 q-ABDHE 问题是困难的。

3　前向安全公钥加密方案的形式化定义及安全模型

3.1　前向安全公钥加密方案的形式化定义

前向安全的公钥加密方案由以下 4 个多项式时间算法组成[15]。

1) 用户密钥生成(userkeygen)算法：输入安全参数 k 和系统时间周期总数 N，该算法生成并输出用户的初始私钥 SK_0 和公钥 PK。

2) 密钥进化(keyupd)算法：输入当前时间周期标识 $i(0<i\leqslant N-1)$、用户的公钥 PK 以及时间周期 $i-1$ 的私钥 SK_{i-1}，该算法生成并输出用户在时间周期 i 的私钥 SK_i。

3) 加密(encrypt)算法：输入当前时间周期标识 $i(0\leqslant i\leqslant N-1)$、密文接收者的公钥 PK 以及明文 M，该算法对明文 M 加密，并输出一个密文 C。

4) 解密(decrypt)算法：输入当前时间周期标识 $i(0\leqslant i\leqslant N-1)$、解密者的当前私钥 SK_i 以及密文 C，该算法对密文 C 解密，并输出一个明文 M 或者一个无效标志。

3.2　前向安全公钥加密方案的安全模型

前向安全公钥加密方案的自适应选择密文攻击下的前向安全性安全模型[15]是自适应选择密文攻击下的不可区分性安全模型[26]的一种自然扩展，它允许敌手额外做一次插入询问以获得其指定时间周期的私钥。这个安全模型是通过挑战者(challenger)与一个敌手 A 之间攻击游戏来定义的[15]，攻击游戏描述如下。

1) 系统参数设置：挑战者运行用户密钥生成算法生成一个初始私钥 SK_0 和一个公钥 PK，并将公钥 PK 输出给敌手 A。

2) 第一阶段询问：在这一阶段中，敌手 A 可以向挑战者做一次插入询问以及一系列自适应性的解密询问。

插入询问：敌手 A 输入一个时间周期 $\tau(0<\tau<N)$，挑战者以初始私钥 SK_0 作为初始输入反复运行密钥进化算法生成时间周期 τ 的私钥 SK_τ，并将之输出给敌手 A。

解密询问：敌手 A 输入一个时间周期 $i(0\leqslant i<N)$ 和一个密文 C，挑战者首先以初始私钥 SK_0 作为初始输入反复运行密钥进化算法生成时间周期 i 的私钥 SK_i，然后通过运行解密算法 $Decrypt(i, SK_i, C)$对密文 C 解密并将结果输出给敌手 A。

a) 挑战阶段：敌手 A 输出一个时间周期 $i^*(0\leqslant i^*<\tau<N)$以及 2 个等长的明文 M_0 和 M_1 进行挑战。挑战者随机选择 $b\in\{0,1\}$，计算密文 $C^*=Encrypt(i^*, PK, M_b)$并输出给敌手 A。

b) 第二阶段询问：敌手 A 继续向挑战者做一系列自适应的解密询问，限制是敌手 A 不可对(i^*, C^*)做解密询问。

c) 猜测：敌手 A 输出对 b 的猜测 b'。如果 $b=b'$，则称敌手 A 赢得游戏。

敌手 A 赢得上述游戏的优势定义为

$$Adv_{\mathrm{A}}^{fs-\mathrm{CCA2}}=\left|\Pr[b=b']-1/2\right|$$

定义 2　自适应选择密文攻击下的前向安全性。对任一前向安全公钥加密方案，如果不存在概率多项式时间敌手以不可忽略的优势赢得上述游戏，则称该方案满足自适应选择密文攻击下的前向安全性，简称 *fs*-CCA2 安全性。

在上述定义中，如果不允许敌手 A 做任何解密询问，则称方案满足自适应选择明文攻击下的前向安全性，简称 *fs*-CPA 安全性。此外，Lu 和 Li[20]提出了一个相对较弱的前向安全公钥加密方案的安全模型。该模型允许敌手 A 在攻击游戏的系统参数设置阶段之前就指定一个目标时间周期 i^*。为了便于区分，本文将基于该模型的自适应选择明文攻击下的前向安全性简称为 *fs*-ST-CPA 安全性。

4　方案的具体描述

假定系统时间周期总数为 N，满足 $N+1=2^{l+1}-1$，其中，l 为整数。本文方案使用一个深度为 l 的标记完全二叉树作为密钥进化树实现用户私钥的进化。该树的树根标记是一个空字符串 ε，而其他节点的标记是一个二进制串。若某个内节点的标记为二进制串 ω，则其左子节点和右子节点的标记分别为 ω_0 和 ω_1。本文采用前序遍历的方式将每个系统时间周期与密钥进化树中的一个非根节点相关联。假定 $\omega^{(i)}$ 表示与时间周期 i 相关联节点的标记，则关联规则定义如下。

1) $\omega^{(0)}=0$，即时间周期 0 与树根的左子节点相关联。

2) 如果 $\omega^{(i)}$ 是一个内节点，则 $\omega^{(i+1)}=\omega_0^{(i)}$。

3) 如果 $\omega^{(i)}$ 是一个叶节点，则 $\omega^{(i+1)}=\omega_1$，其中，ω 满足 $\omega_0=\omega^{(i)}$ 或 ω_0 为 $\omega^{(i)}$ 的最长前缀。

在本文方案中，密钥进化树的每个节点 ω 都需存储一个节点密钥(记为 sk_ω)用于构成用户在特定时间周期内的私钥并且用于私钥的进化。若一个节点的深度为 $d(1\leqslant d\leqslant l)$，则其节点密钥包含了 $l-d+5$

个不同元素。一个用户在时间周期 i 内的私钥是节点密钥的一个集合，由节点$\omega^{(i)}$的节点密钥以及从树根到节点$\omega^{(i)}$的路径上所有节点的右兄弟的节点密钥构成。简化描述起见，本文以堆栈的方式组织用户的私钥。对于用户在时间周期 i 内的私钥 SK_i，其栈顶是节点$\omega^{(i)}$的节点密钥，随后依次是节点$\omega^{(i)}$到树根路径上所有节点的右兄弟节点密钥。

方案的具体描述如下。

用户密钥生成(userkeygen)算法：输入安全参数 k 和系统时间周期总数 N，该算法生成用户的公钥和初始私钥如下。

1) 生成 2 个大素数 p 阶乘法循环群 G_1 和 G_2，以及一个可接受的双线性映射 e:$G_1\times G_1\to G_2$。

2) 随机选择生成元 g、h_1、$h_2\in G_1$ 和α、β_1、$\beta_2\in Z_p^*$，并计算 $g_1=g^{\alpha}$。

3) 随机选择 2 个 l 维向量 $\boldsymbol{U}=(u_1, \cdots, u_l)$, $\boldsymbol{V}=(v_1, \cdots, v_l)\in G^l$。

4) 选择一个抗碰撞散列函数 H:$G_1\times G_2\times G_1\to Z_p^*$。

5) 随机选择 $r\in Z_p^*$，计算节点 0 和节点 1 的节点密钥 sk_0 和 sk_1 如下

$$sk_0=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha},(g^{-\beta_2}h_2)^{1/\alpha},(g^{-1}g_1)^r,z_2^r,\cdots,z_l^r)$$

$$sk_1=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha}z_1^r,(g^{-\beta_2}h_2)^{1/\alpha}z_1^r,(g^{-1}g_1)^r,z_2^r,\cdots,z_l^r)$$

其中，$z_j=u_j^{-1}v_j$ (j=1,2,⋯,l)。依次将节点密钥 sk_1 和 sk_0 压入栈内。栈内节点密钥构成用户的初始私钥。

6) 输出用户的公钥 $PK=(p, G_1, G_2, e, g, g_1, h_1, h_2, U, V, H)$以及初始私钥 $SK_0=(sk_0,sk_1)$。

密钥进化(keyupd)算法：输入当前时间周期标识 i、用户的公钥 PK 以及时间周期 i−1 内的私钥 SK_{i-1}，假设密钥进化树中与时间周期 i−1 相关联的节点为$\omega^{(i-1)}=\omega_1\omega_2\cdots\omega_d\in\{0,1\}^{d\le l}$，且其节点密钥为 $sk_{\omega^{(i-1)}}$，该算法将节点密钥 $sk_{\omega^{(i-1)}}$ 从栈内弹出并产生用户在时间周期 i 内的私钥 SK_i 如下所示。

① 如果$\omega^{(i-1)}$为叶节点，则栈内剩余节点密钥构成用户在时间周期 i 内的私钥 SK_i。易见，此时栈顶节点密钥为 $sk_{\omega^{(i)}}$。

② 如果$\omega^{(i-1)}$为内节点，随机选择 $s\in Z_p^*$，将节点密钥 $sk_{\omega^{(i-1)}}$ 解析为

$$sk_{\omega^{(i-1)}}=(a_0,a_1,a_2,a_3,a_4,b_{d+1},\cdots,b_l)$$

$$=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r,(g^{-\beta_2}h_2)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r,$$

$$(g^{-1}g_1)^r,z_{d+1}^r,\cdots,z_l^r),$$

计算节点 $\omega_0^{(i-1)}$ 和 $\omega_1^{(i-1)}$ 的节点密钥 $sk_{\omega_0^{(i-1)}}$ 和 $sk_{\omega_1^{(i-1)}}$。

$$sk_{\omega^{(i-1)}\omega_{d+1}}=sk_{\omega_1\cdots\omega_d\omega_{d+1}}$$

$$=(a_0,a_1,a_2b_{d+1}^{\omega_{d+1}}(\prod_{j=1}^{d+1}z_j^{\omega_j})^s,a_3b_{d+1}^{\omega_{d+1}}(\prod_{j=1}^{d+1}z_j^{\omega_j})^s,a_4(g^{-1}g_1)^s,$$

$$b_{d+2}z_{d+2}^s,\cdots,b_lz_l^s)$$

$$=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r z_{d+1}^{r\cdot\omega_{d+1}}(\prod_{j=1}^{d+1}z_j^{\omega_j})^s,(g^{-\beta_2}h_2)^{1/\alpha}\cdot$$

$$(\prod_{j=1}^{d}z_j^{\omega_j})^r z_{d+1}^{r\cdot\omega_{d+1}}(\prod_{j=1}^{d+1}z_j^{\omega_j})^s,$$

$$(g^{-1}g_1)^r(g^{-1}g_1)^s,z_{d+2}^rz_{d+2}^s,\cdots,z_l^rz_l^s)$$

$$=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^{r+s},(g^{-\beta_2}h_2)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^{r+s},$$

$$(g^{-1}g_1)^{r+s},z_{d+2}^{r+s},\cdots,z_l^{r+s})$$

$$=(\beta_1,\beta_2,(g^{-\beta_1}h_1)^{1/\alpha}(\prod_{j=1}^{d+1}z_j^{\omega_j})^{r'},(g^{-\beta_2}h_2)^{1/\alpha}(\prod_{j=1}^{d+1}z_j^{\omega_j})^{r'},$$

$$(g^{-1}g_1)^{r'},z_{d+2}^{r'},\cdots,z_l^{r'}),$$

其中，ω_{d+1}=0，1 且 $r'=r+s$。依次将节点密钥 $sk_{\omega_1^{(i-1)}}$ 和 $sk_{\omega_0^{(i-1)}}$ 压入栈内，则栈内节点密钥构成用户在时间周期 i 内的私钥 SK_i。

加密(encrypt)算法：输入当前时间周期标识 i、接收者的公钥 PK 以及明文 M，假设与时间周期 i 相关联的节点为$\omega^{(i)}=\omega_1\omega_2\cdots\omega_d\in\{0,1\}^{d\le l}$，该算法随机选择 $t\in Z_p^*$，计算 $c_1=(g^{-1}g_1)^t$, $c_2=e(g,g)^t$, $c_3=(\prod_{j=1}^{d}z_j^{\omega_j})^t$, $c_4=M(e(g,h_1)^{\gamma}e(g,h_2))^{-t}$)，并输出密文

$$C=(c_1,c_2,c_3,c_4)$$

其中，$z_j=u_j^{-1}v_j$, $\gamma=H(c_1,c_2,c_3)$。

解密(decrypt)算法：输入当前时间周期标识 i、解密者的当前私钥 SK_i 以及密文 $C=(c_1,c_2,c_3,c_4)$，假设与时间周期 i 相关联的节点为$\omega^{(i)}=\omega_1\omega_2\cdots\omega_d\in\{0,1\}^{d\le l}$，该算法从当前私钥 SK_i 中提取栈顶节点密钥 $sk_{\omega^{(i)}}=(a_0,a_1,a_2,a_3,a_4,b_{d+1},\cdots,b_l)$，计算并输出明文

$$M=\frac{e(c_1,a_2^{\gamma}a_3)c_2^{\gamma a_0+a_1}c_4}{e(a_4,c_3)^{\gamma+1}}$$

其中，$\gamma=H(c_1,c_2,c_3)$。

上述方案的正确性验证如下

$$\frac{e(c_1,a_2^{\gamma}a_3)c_2^{\gamma a_0+a_1}c_4}{e(a_4,c_3)^{\gamma+1}}$$

$$=\frac{e((g^{-1}g_1)^t,((g^{-\beta_1}h_1)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r)^{\gamma}(g^{-\beta_2}h_2)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r)c_2^{\gamma a_0+a_1}c_4}{e((g^{-1}g_1)^r,(\prod_{j=1}^{d}z_j^{\omega_j})^t)^{\gamma+1}}$$

$$=e((g^{-1}g_1)^t,(g^{-\beta_1}h_1)^{\gamma/\alpha}(g^{-\beta_2}h_2)^{1/\alpha})c_2^{\gamma a_0+a_1}c_4$$

$$=e((g^{-1}g_1)^t,(g^{-\beta_1}h_1)^{\gamma/\alpha}(g^{-\beta_2}h_2)^{1/\alpha})\cdot e(g,g)^{t(\gamma\beta_1+\beta_2)}M\cdot e(g,h_1^{\gamma}h_2)^{-t}$$

$$=e(g,g)^{-t(\gamma\beta_1+\beta_2)}e(g,h_1^{\gamma}h_2)^t e(g,g)^{t(\gamma\beta_1+\beta_2)}Me(g,h_1^{\gamma}h_2)^{-t}$$

$$=M$$

5　安全性证明

在这一节中，证明本文提出的方案在标准模型下满足自适应选择密文攻击下的前向安全性。根据第 3 节给出的前向安全公钥加密方案的安全模型和定义给出以下证明。

定理 1　若存在概率多项式时间敌手 A，能够在多项式时间内经过最多 q_D 次解密询问后，以 ε 的优势赢得 *fs*-CCA2 游戏，那么存在一个算法 B，在多项式时间内以 ε 的优势解决判定性截断 *q*-ABDHE 问题，其中，$q=q_D+l+1$。

证明　给定判定性截断 *q*-ABDHE 问题的一个随机实例$(p, G, G_T, e, g, g^{\alpha}, \cdots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, T)$，算法 B 模仿 *fs*-CCA2 游戏的挑战者与敌手 A 进行交互，其目标是判定 $T=e(g,g')^{\alpha^{q+1}}$ 是否成立。

系统参数设置：算法 B 置 $g_1=g^{\alpha}$；随机生成 2 个一元 *q* 次多项式 $f_1(x), f_2(x)\in Z_p[x]$，满足 $f_1(0)\neq 0$ 且 $f_2(0)\neq 0$，并基于$(g, g^{\alpha},\cdots,g^{\alpha^q})$分别计算 $h_1=g^{f_1(\alpha)}$ 和 $h_2=g^{f_2(\alpha)}$；随机选择选择 $r_1,\cdots,r_l\in Z_p^*$，分别计算向量 $\boldsymbol{U}=(u_1,\cdots,u_l)=(g^{r_1},\cdots,g^{r_l})$ 和 $\boldsymbol{V}=(v_1,\cdots,v_l)=(g_1^{r_1},\cdots,g_1^{r_l})$；选择一个抗碰撞的散列函数 $H: G_1\times G_2\times G_1\to Z_p^*$；输出公钥 $PK=(p, G_1, G_2, e, g, g_1, h_1, h_2, \boldsymbol{U}, \boldsymbol{V}, H)$给敌手 A。

简化描述起见，定义如下的节点密钥生成(nodekeyextract)算法。算法 B 利用该算法生成密钥进化树中特定节点的节点密钥以便生成特定时间周期内的私钥。

节点密钥生成(nodekeyextract)算法：输入一个公钥 *PK* 和一个非根节点标记 ω，假定 $\omega=\omega_1\omega_2\cdots\omega_d\in\{0,1\}^{d\le l}$，算法 B 随机选择 $r\in Z_p^*$，计算并输出节点 ω 的节点密钥

$$sk_{\omega}=(a_0, a_1, a_2, a_3, a_4, b_{d+1}, \cdots, b_l)=(f_1(0), f_2(0), g^{F_1(\alpha)}(\prod_{j=1}^{d}z_j^{\omega_j})^r, g^{F_2(\alpha)}\cdot(\prod_{j=1}^{d}z_j^{\omega_j})^r, (g^{-1}g_1)^{-r}, z_{d+1}^r,\cdots,z_l^r)$$

其中，$z_j=u_j^{-1}v_j$，$F_1(\alpha)=\frac{f_1(\alpha)-f_1(0)}{\alpha}$，$F_2(\alpha)=\frac{f_2(\alpha)-f_2(0)}{\alpha}$。

易见，算法 B 能够基于$(g, g^{\alpha},\cdots, g^{\alpha^{q-1}})$分别计算出 $g^{F_1(\alpha)}$ 和 $g^{F_2(\alpha)}$。此外，由于

$$a_2=g^{F_1(\alpha)}(\prod_{j=1}^{d}z_j^{\omega_j})^r=g^{\frac{f_1(\alpha)-f_1(0)}{\alpha}}(\prod_{j=1}^{d}z_j^{\omega_j})^r$$

$$=(g^{-f_1(0)}h_1)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r$$

$$a_3=g^{F_2(\alpha)}(\prod_{j=1}^{d}z_j^{\omega_j})^r=g^{\frac{f_2(\alpha)-f_2(0)}{\alpha}}(\prod_{j=1}^{d}z_j^{\omega_j})^r$$

$$=(g^{-f_2(0)}h_2)^{1/\alpha}(\prod_{j=1}^{d}z_j^{\omega_j})^r$$

因此，sk_{ω} 是节点 ω 的有效节点密钥。可见，算法 B 能够生成任意非根节点的节点密钥。

第一阶段询问：在该阶段，敌手 A 向算法 B 做一次插入询问以及一系列的解密询问，算法 B 应答如下。

1) 插入询问：敌手 A 输入一个时间周期 τ，算法 B 首先反复调用上述节点密钥生成算法生成节点 $\omega^{(\tau)}$ 以及从根节点到节点 $\omega^{(\tau)}$ 的路径上所有节点的右兄弟节点密钥，然后组合上述生成的所有节点密钥获得时间周期 τ 的私钥 SK_{τ} 并将之输出给敌手 A。

2) 解密询问：敌手 A 输入一个时间周期 *i* 和一个密文 $C=(c_1,c_2,c_3,c_4)$，假定与时间周期 *i* 相关联的节点为 $\omega^{(i)}=\omega_1\omega_2\cdots\omega_d\in\{0,1\}^{d\le l}$，算法 B 调用上述节点密钥生成算法生成节点 $\omega^{(i)}$ 的节点密钥 $sk_{\omega^{(i)}}=(a_0,a_1,a_2,a_3,a_4,b_{d+1},\cdots,b_l)$，计算明文 $M=\frac{e(c_1,a_2^{\gamma}a_3)c_2^{\gamma a_0+a_1}c_4}{e(a_4,c_3)^{\gamma+1}}$ 并输出给敌手 A，其中，$\gamma=H(c_1, c_2, c_3)$。

挑战阶段：敌手 A 输出(i^*, M_0, M_1)进行挑战。假定与时间周期 i^* 相关联的节点为 $\omega^{(i^*)}=\omega_1^*\omega_2^*\cdots\omega_n^*\in\{0,1\}^{n\le l}$，算法 B 定义一个 *q*+1 次多项式 $F^*(x)=$

$\frac{x^{q+2}-1}{x-1}=\sum_{j=0}^{q+1}F_j^*x^j$，随机选择 $b\in\{0,1\}$，计算 $c_1^*=g'^{\alpha^{q+2}}g'^{-1}$，$c_2^*=T^{F_{q+1}^*}e(\prod_{j=0}^{q}(g^{\alpha^j})^{F_j^*},g')$，$c_3^*=\prod_{j=1}^{n}(c_1^*)^{r_j\cdot\omega_j^*}$，$c_4^*=M_b\left[e(c_1^*,(g^{F_1(\alpha)})^{\gamma^*}g^{F_2(\alpha)})(c_2^*)^{\gamma^*f_1(0)+f_2(0)}\right]^{-1}$，并输出挑战密文 $C^*=(c_1^*,c_2^*,c_3^*,c_4^*)$，其中，$\gamma^*=H(c_1^*,c_2^*,c_3^*)$，$F_1(\alpha)=\frac{f_1(\alpha)-f_1(0)}{\alpha}$，$F_2(\alpha)=\frac{f_2(\alpha)-f_2(0)}{\alpha}$。

第二阶段询问：敌手 A 继续向算法 B 做一系列的解密询问，限制是敌手 A 不可对(i^*,C^*)做解密询问。

猜测：最后敌手 A 输出对 b 的猜测 b'。如果 $b=b'$，则算法 B 输出 1，即表示 $T=e(g,g')^{\alpha^{q+1}}$；否则，算法 B 输出 0。

优势分析：下面分析算法 B 解决给定判定性截断 q-ABDHE 问题的优势。

若 $T=e(g,g')^{\alpha^{q+1}}$ 且置 $s=\log_g b'F^*(\alpha)$，则有

$$c_1^*=g'^{\alpha^{q+2}}g'^{-1}=g'^{\alpha^{q+2}-1}=g^{(\alpha-1)s}=(g^{-1}g_1)^s$$

$$c_2^*=T^{F_{q+1}^*}e(\prod_{j=0}^{q}(g^{\alpha^j})^{F_j^*},g')=e(\prod_{j=0}^{q+1}(g^{\alpha^j})^{F_j^*},g')$$

$$=e(g,g)^{\log_g g'(\sum_{j=0}^{q+1}F_j^*\cdot\alpha^j)}=e(g,g)^s$$

$$c_3^*=\prod_{j=1}^{n}(c_1^*)^{r_j\omega_j^*}=\prod_{j=1}^{n}((g^{-1}g_1)^s)^{r_j\omega_j^*}$$

$$=(\prod_{j=1}^{n}(u_j^{-1}v_j)^{\omega_j^*})^s=(\prod_{j=1}^{n}(z_j)^{\omega_j^*})^s$$

$$c_4^*=M_b\left[e(c_1^*,(g^{F_1(\alpha)})^{\gamma^*}g^{F_2(\alpha)})(c_2^*)^{\gamma^*f_1(0)+f_2(0)}\right]^{-1}$$

$$=M_b\left[e((g^{-1}g_1)^s,g^{\frac{\gamma^*(f_1(\alpha)-f_1(0))+f_2(\alpha)-f_2(0)}{\alpha}})(e(g,g)^s)^{\gamma^*f_1(0)+f_2(0)}\right]^{-1}$$

$$=M_b[e(g,g)^{s[\gamma^*(f_1(\alpha)-f_1(0))+f_2(\alpha)-f_2(0)]}e(g,g)^{s[\gamma^*f_1(0)+f_2(0)]}]^{-1}$$

$$=M_b[e(g,g)^{s(\gamma^*f_1(\alpha)+f_2(\alpha))}]^{-1}$$

$$=M_b(e(g,h_1)^{\gamma^*}e(g,h_2))^{-s}$$

可见，若 $T=e(g,g')^{\alpha^{q+1}}$，则 C^*是 M_b 的有效密文，从而敌手 A 的猜测 b' 满足$|\Pr[b=b']-1/2|\geqslant\varepsilon$。

另一方面，若 T 仅是群 G_T 中的随机元素，则 C^*不是 M_b 的有效密文且不能为敌手 A 的猜测提供任何信息，从而敌手 A 的猜测 b' 满足 $\Pr[b=b']=1/2$。

综上，算法 B 解决给定判定性截断 q-ABDHE 问题的优势满足

$$\left|\Pr[B(g,g^{\alpha},\cdots,g^{\alpha^q},g',g'^{\alpha^{q+2}},e(g,g')^{\alpha^{q+1}})=1]-\Pr[B(g,g^{\alpha},\cdots,g^{\alpha^q},g',g'^{\alpha^{q+2}},T)=1]\right|\geqslant|(1/2\pm\varepsilon)-1/2|=\varepsilon$$

定理 1 证明完毕。

6 性能评价

本节从方案的安全性和效率 2 个方面来评价本文方案的性能。方案的效率通过方案中主要性能参数(包括密钥进化时间、加密时间、解密时间、公钥长度以及密文长度)的复杂度进行评价。表 1 给出了本文方案与已有的标准模型下可证安全的前向安全公钥加密方案[15,17,20]的性能对比，其中，N 为系统的时间周期总数。

首先简要分析一下本文方案中主要性能参数的复杂度。密钥进化算法在进化用户私钥时至多需要计算 2 个密钥进化树的节点密钥。由于生成一个节点密钥需要计算 $l+d+5(\leqslant 2l+5)$个群 G_1 中的指数，因此密钥进化至多需要计算 $4l+10$ 个群 G_1 中的指数，从而其时间复杂度为 $O(\log N)$。加密算法在加密明文时需要计算 $d+2(\leqslant l+2)$个群 G_1 中的指数，3 个群 G_2 中的指数以及 3 个双线性对，因此，其时间复杂度为 $O(\log N)$。此外，解密算法在解密密文时仅需计算 1 个群 G_1 中的指数、2 个群 G_2 中的指数以及 2 个双线性对，因此解密时间的复杂度为 $O(1)$。对于方案的通信复杂度，用户公钥含有 2 个 l 维的群 G_1 中的元素向量，因此数据量为 $O(\log N)$ bit；而密文仅包含 3 个群 G_1 中的元素和 1 个群 G_2 中的元素，长度独立于 N，因此数据量为 $O(1)$ bit。

从表 1 可以看出，本文方案的性能明显优于文献[15,17]中的方案。尽管文献[20]中方案的各性能

表 1 性能对比

方案	安全性	计算复杂度			通信复杂度	
		密钥进化	加密	解密	公钥	密文
方案 1[15,17]	*fs*-CPA	$O(\log N)$	$O(\log N\cdot(\log\log N)^2)$	$O(\log N)$	$O(\log N)$	$O(\log N)$
方案 2[20]	*fs*-ST-CPA	$O(\log N)$	$O(\log N)$	$O(1)$	$O(\log N)$	$O(1)$
本文方案	*fs*-CCA2	$O(\log N)$	$O(\log N)$	$O(1)$	$O(\log N)$	$O(1)$

参数的复杂度与本文方案相同，但其安全性要弱于本文方案。因此，本文方案的总体性能(综合考虑方案的安全性和效率)要优于已有的标准模型下可证安全的前向安全公钥加密方案。

7　结束语

本文提出了一个直接选择密文安全的前向安全公钥加密方案，并在标准模型下证明了其安全性。在所提出的方案中，解密算法的计算时间和密文的长度都独立于系统时间周期总数 N，而其他的主要性能参数的复杂度至多为 $O(\log N)$。对比分析表明，所提出方案的总体性能优于已有的标准模型下可证安全的前向安全公钥加密方案。与已有的前向安全公钥加密方案一样，本文方案也仅能支持有限的系统时间周期总数，并且假设系统时间周期总数在系统初始化时已知。此外，方案的一些性能参数的复杂度也与系统时间周期总数相关。然而，在实际应用中，一些系统的时间周期总数可能非常巨大，甚至是无限，那么仅能支持有限系统时间周期总数的前向安全公钥密码方案的应用将受到限制。因此，高效的能够支持无限系统时间周期总数的前向安全公钥加密方案的构造是下一步的工作重心。此外，可以将本文方案中的密钥进化方法直接应用于已有的基于身份加密方案[27]，构造出标准模型下满足选择密文安全性的前向安全基于身份加密方案；或者将本文方案与已有的基于证书加密方案[28]相结合，构造出标准模型下满足选择密文安全性的前向安全基于证书加密方案[25]。

参考文献：

[1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654.

[2] ANDERSON R. Two Remarks on Public Key Cryptology[R]. Invited Lecture at the 4th ACM Conference on Computer and Communications Security, 1997.

[3] GÜNTHER C G. An identity-based key-exchange protocol[A]. Proc of the Eurocrypt 1989[C]. Heidelberg: Springer-Verlag, 1990. 29-37.

[4] DIFFIE W, VAN-OORSCHOT P C, WEINER M J. Authentication and authenticated key exchanges[J]. Designs, Codes and Cryptography, 1992, 2(2):107-125.

[5] BELLARE M, MINER S K. A forward-secure digital signature scheme[A]. Proc of the Crypto 1999[C]. Heidelberg:Springer-Verlag, 1999.431-448.

[6] KRAWCZYK H. Simple forward-secure signatures from any signature scheme[A]. Proc of 7th ACM Conference on Computer and Communications Security[C]. New York, USA, 2000.108-115.

[7] ABDALLA M, REYZIN L. A new forward-secure digital signature scheme[A]. Proc of the Asiacrypt 2000[C]. Heidelberg: Springer-Verlag, 2000.116-129.

[8] ABDALLA M, MINER S K, NAMPREMPRE C. Forward-secure threshold signature schemes[A]. Proc of the CT-RSA 2001[C]. Heidelberg:Springer-Verlag, 2001.441-456.

[9] ITKIS G, REYZIN L. Forward-secure signatures with optimal signing and verifying[A]. Proc of the Crypto 2001[C]. Heidelberg: Springer-Verlag, 2001.499-514.

[10] KOZLOV A, REYZIN L. Forward-secure signatures with fast key update[A]. Proc of the SCN 2002[C]. Heidelberg: Springer-Verlag, 2002. 247-262.

[11] MALKIN T, MICCIANCIO D, MINER S K. Efficient generic forward-secure signatures with an unbounded number of time periods[A]. Proc of the Eurocrypt 2002[C]. Heidelberg: Springer-Verlag, 2002. 400-417.

[12] BOYEN X, SHACHAM H, SHEN E, *et al*. Forward-secure signatures with untrusted update[A]. Proc of 13th ACM Conference on Computer and Communications Security[C]. New York, USA, 2006.191-200.

[13] LIBERT B, QUISQUATER J, YUNG M. Forward-secure signatures in untrusted update environments[A]. Proc of the 14th ACM Conference on Computer and Communications Security[C]. New York, USA,2007. 266-275.

[14] YU J, KONG F Y, CHENG X G, *et al*. Construction of yet another forward-secure signature scheme suing bilinear maps[A]. Proc of the 2nd International Conference on Provable Security[C]. Heidelberg: Springer-Verlag, 2008. 83-97.

[15] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[A]. Proc of the Eurocrypt 2003[C]. Heidelberg: Springer-Verlag, 2003. 255-271.

[16] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography[A]. Proc of the Asiacrypt 2002[C]. Heidelberg: Springer-Verlag, 2002. 548-566.

[17] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[J]. Journal of Cryptology, 2007, 20:265-294.

[18] JIANG H, XU Q L, HOU M B. Forward-secure public-key encryption scheme with tamper evidence[A]. Proc of the 2007 International Conference on Computational Intelligence and Security Workshops[C]. IEEE Press, 2007. 656-659.

[19] 李成邦, 胡珂流, 许春香. 一种构造前向安全公钥加密算法的一般方法[J]. 信息安全与通信保密, 2009, 8:313-315.
LI C B, HU K L, XU C X. Forward-secure public cryptosystem based on a simple public cryptosystem[J]. China Information Security, 2009, 8:313-315.

[20] LU Y, LI J G. A practical forward-secure public-key encryption scheme[J]. Journal of Networks, 2011, 6(9):1254-1261.

[21] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[A]. Proc of the Eurocrypt 2005[C]. Heidelberg: Springer-Verlag, 2005. 440-456.

[22] YAO D, FAZIO N, DODIS Y, *et al*. ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption[A]. Proc of the 11th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, USA, 2004. 354-363.

（下转第 45 页）

[3] DIFFIE W, HELLMAN M. Exhaustive cryptanalysis of the NBS data encryption standard[J]. Computer, 1977,10(6):74-84.

[4] AOKI K, SASAKI Y. Preimage attacks on one-block MD4, 63-step MD5 and more[A]. SAC 2008[C]. New Brunswick, Canada, 2008. 103-119.

[5] National Institute of Standards and Technology. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family[EB/OL]. http://csrc.nist.gov/ groups/ST/hash/ documents/ FR_ Notice_Nov07.pdf, 2008.

[6] SM3 hash function[EB/OL]. http://www.oscca.gov.cn/UpFile/2010 1222141857786.pdf/, 2010.

[7] ZOU J, WU W, WU S, *et al*. Preimage attacks on step-reduced SM3 hash function[A]. ICISC 2011[C]. Seoul Korea, 2011.375-390.

[8] KIRCANSKI A, SHEN Y, WANG G, *et al*. Boomerang and slide-rotational analysis of SM3 hash function[A]. SAC 2012[C]. Windsor, Canada, 2012.305-321.

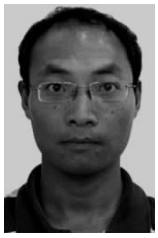
[9] WANG G, SHEN Y. Preimage and pseudo-collision attacks on step-reduced SM3 hash function[EB/OL]. http://eprint.iacr.org/2012/640/, 2012.

[10] MENEZES A J, OORSCHOT P C, VANSTONE S. Handbook of Applied Cryptography[M]. CRC Press,1996.

[11] LI J, ISOBE T, SHIBUTANI K. Converting meetin-the-middle preimage attack into pseudo collision attack: application to SHA-2[A]. FSE 2012[C]. Washington DC, USA, 2012.264-286.

作者简介：

王高丽（1982-），女，安徽宿州人，博士，东华大学副教授、硕士生导师，主要研究方向为密码学、对称密码算法的分析与设计。



申延召（1984-），男，河南汝州人，东华大学硕士生，主要研究方向为散列函数设计与分析。

（上接第 39 页）

[23] YU J, KONG F Y, CHENG X G, *et al*. Forward-secure identity-based public-key encryption without random oracles[J]. Fundamenta Informaticae, 2011, 111(2): 241-256.

[24] 杨浩淼, 孙世新, 李洪伟. 前向安全的基于身份加密方案[J]. 电子科技大学学报, 2007, 36(3):534-537.
YANG H M, SUN S X, LI H W. Forward-secure identity-based encryption scheme[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(3):534-537.

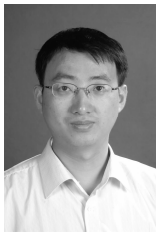
[25] LU Y, LI J G. Forward-secure certificate-based encryption and its generic construction[J]. Journal of Networks, 2010, 5(5):527-534.

[26] RACKOFF C, SIMON D. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[A]. Proc of the Crypto 1991[C]. Heidelberg:Springer-Verlag, 1991. 433-444.

[27] GENTRY C. Practical identity-based encryption without random oracles[A]. Proc of the Eurocrypt 2006[C]. Heidelberg: Springer-Verlag, 2006. 445-464.

[28] LIU J K, ZHOU J Y. Efficient certificate-based encryption in the standard model[A]. Proc of the 6th International Conference on Security and Cryptography for Networks[C]. Heidelberg:Springer-Verlag, 2008. 144-155.

作者简介：



陆阳（1977-），男，江苏扬州人，博士，河海大学副教授、硕士生导师，主要研究方向为信息安全、密码学理论与技术。

李继国（1970-），男，黑龙江富裕人，博士，河海大学教授、博士生导师，主要研究方向为信息安全、密码学理论与技术。