第42卷第4期 中国科学技术大学学报 Vol. 42, No. 4
2012年4月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Apr. 2012

文章编号:0253-2778(2012)04-0296-06

标准模型中基于身份的匿名加密方案

任艳丽[1],谷大武[2],王朔中[1],张新鹏[1]

(1.上海大学通信与信息工程学院,上海 200072;2.上海交通大学计算机科学与工程系,上海 200240)

摘要:现有基于身份的匿名加密方案在标准模型下的 selective-ID 模型中可证安全,或基于复杂的困难问题假设可证安全.使用阶为合数的双线性群,基于 BDH(bilinear Diffie-Hellman)假设,提出新的基于身份匿名加密方案,在标准模型中是 ANON-IND-ID-CPA 安全的,仅需 2 次双线性对计算.与同类方案相比,该方案同时具备高的安全性与计算效率.

关键词:匿名;基于身份加密;标准模型;BDH 假设

中图分类号:TP309 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2012.04.006

引用格式:任艳丽,谷大武,王朔中,等. 标准模型中基于身份的匿名加密方案[J]. 中国科学技术大学学报,2012,42(4):296-301.

Ren Yanli, Gu Dawu, Wang Shuozhong, et al. Anonymous identity-based encryption scheme without random oracles[J]. Journal of University of Science and Technology of China, 2012,42(4):296-301.

Anonymous identity-based encryption scheme without random oracles

REN Yanli[1], GU Dawu[2], WANG Shuozhong[1], ZHANG Xinpeng[1]

(1. *School of Communication and Information Engineering, Shanghai University, Shanghai* 200072, *China*;
2. *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240, *China*)

Abstract: The anonymous identity-based encryption (IBE) schemes are currently only selective-ID secure without random oracles or provably secure under a complex assumption. An anonymous IBE scheme based on decisional bilinear Diffie-Hellman (BDH) assumption in a group of composite order was proposed, which is ANON-IND-ID-CPA secure without random oracles and only needs two bilinear pairing computations. This scheme is more secure and efficient than the existing ones.

Key words: anonymous; identity-based encryption; without random oracles; decisional bilinear Diffie-Hellman assumption

0 引言

在基于身份的密码系统[1]中,用户的身份直接作为公钥,无需分发公钥证书,PKG(private key generator)为用户生成私钥.基于身份的密码系统简化了公钥管理过程,避免了传统公钥密码体制中因管理用户证书而带来的种种弊端.

2001 年,Boneh 等[2]基于双线性群,提出了第一个有效的基于身份加密(IBE)方案.尽管文献[2]中的方案效率较高,但是仅在随机预言模型[3]下得

收稿日期:2011-05-27;**修回日期**:2011-10-14

基金项目:国家自然科学基金(61071187,61073190),上海市科委重大项目(10DZ1500202),中国博士后科学基金(20100470675),上海市博士后资助计划项目(10R21413200)资助.

作者简介:任艳丽(通讯作者),女,1982 年生,博士/讲师. 研究方向:密码学. E-mail: renyanli1982123@shu.edu.cn

到证明. 而在随机预言模型下可证安全的方案,在实际中却不一定是安全的[4]. Boneh 等[5]不使用随机预言机,提出标准模型中的 IBE 方案,但证明基于比较弱的模型——selective-ID 模型:敌手在系统建立前就需要选择攻击的身份. Waters[6]构造了新的 IBE 方案,并在标准模型下的 adaptive-ID 模型中可证安全,即在询问结束后,敌手可以适应性地选择攻击的身份. 随后,文献[7]又对文献[6]中的方案在效率上进行了改进.

随着现代社会的发展,人们不仅意识到信息保密的重要性,而且越来越注重保护个人的隐私信息. 例如:当 Alice 通过公共信道发送给 Bob 一封加密邮件时,Bob 不希望攻击者 Carol 解密邮件内容,也不希望 Carol 知道加密邮件是发送给自己的. 在大多数基于身份的加密方案中,由密文可以得到接收者的身份,这样即使敌手不能解密,也暴露了接收者的某些私密信息,增加了密文被破译的可能性. 为了更好地保护接收者的隐私和信息安全,方案应该具备匿名性,即由密文不能得到接收者的身份. 匿名加密方案还可用于构造公钥搜索加密方案[8],而公钥搜索加密方案在云存储系统中有广泛的应用[9]. 因此,同时具有匿名性和保密性的公钥加密方案有非常重要的应用价值[10].

在基于身份的密码体制中,Boyen 等[11]提出了一个匿名的 IBE 方案,在标准模型下的 selective-ID 模型中可证安全,即在模拟器选择公共参数前,敌手必须选择所要攻击的身份,削弱了敌手的攻击能力. 最近,Liu 等[12]对 Boyen 等的方案进行了分析,指出该方案存在冗余,并提出了简化方案,但是没有对方案安全性进行归约证明. 2006 年,Gentry[13]提出了另一个匿名的 IBE 方案,在标准模型下的 adaptive-ID 模型中可证安全,但证明基于复杂的困难问题假设——ABDHE (augmented bilinear Diffie-Hellman exponent) 假设. 由于困难问题的难度与密码体制的安全强度密切相关[14],而 ABDHE 问题并不是公认的困难问题,难度低于 BDH 问题,因此方案的安全性并不是最理想的. 最近,我们[15]基于 BDH 和线性问题假设,提出了匿名 IBE 方案,在标准模型下的 adaptive-ID 模型中可证安全,但方案效率较低,解密需要 9 次双线性对运算. 除传统匿名 IBE 方案外,国内外学者还做了一些有意义的扩展,如多个接收者的匿名 IBE 方案[16-17]、多个可信中心的匿名 IBE 方案[18]等,但大多仅在随机预言模型中可证安全.

本文继续对传统 IBE 方案进行匿名性研究,基于文献[6]中的 IBE 方案,我们提出新的匿名 IBE 方案. 方案使用阶为合数的双线性群,基于 BDH 假设,在标准模型中是 ANON-IND-ID-CPA 安全的. 由于 BDH 问题是公认的困难问题,难度高于 ABDHE 和线性问题,因此我们的方案具有更高的安全性. 与文献[15]相比,新方案拥有短的私钥和密文长度,解密仅需两次双线性对运算,效率更高. 因此,本文方案同时拥有高的安全性和实现效率.

1　基础知识

本节介绍一些基础知识,包括阶为合数的双线性群、方案基于的复杂性假设及安全模型.

1.1　阶为合数的双线性群

在可证安全的基于身份密码体制中,阶为素数的双线性群得到了广泛的应用[19-21]. 我们将使用阶为合数的双线性群[22]构造基于身份的匿名加密方案. 设 p,p'是两个大素数,$n=pp'$,$\mathbb{G},\mathbb{G}_T$ 是两个阶为 n 的循环群. 如果满足以下条件,$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是一个双线性映射[23]:

① 双线性:对所有 $\tilde{u},\tilde{v}\in\mathbb{G}$, $a_0,b_0\in Z_n$, $e(\tilde{u}^{a_0},\tilde{v}^{b_0})=e(\tilde{u},\tilde{v})^{a_0b_0}$.

②非退化性:存在$\mathbb{G}$ 中生成元 $\tilde{g}$,使得 $e(\tilde{g},\tilde{g})$为$\mathbb{G}_T$ 的生成元.

本文使用$\mathbb{G}_p$ 和$\mathbb{G}_{p'}$分别代表$\mathbb{G}$ 中阶为 p 和 p'的子群,$\mathbb{G}_{T,p}$和$\mathbb{G}_{T,p'}$代表$\mathbb{G}_T$ 中阶为 p 和 p'的子群. 因此,$\mathbb{G}=\mathbb{G}_p\times\mathbb{G}_{p'}$, $\mathbb{G}_T=\mathbb{G}_{T,p}\times\mathbb{G}_{T,p'}$. 如果 $\tilde{g}$ 是$\mathbb{G}$ 中一个生成元,则 $\tilde{g}^{p'}$ 和 $\tilde{g}^{p}$ 分别是$\mathbb{G}_p$ 和$\mathbb{G}_p$ 中的生成元,我们使用 g_p 和 $g_{p'}$分别代表$\mathbb{G}_p$ 和$\mathbb{G}_{p'}$的生成元.

对于任意 $h_p\in\mathbb{G}_p$ 和 $h_{p'}\in\mathbb{G}_{p'}$,存在 $a,b\in Z_n$,满足 $e(h_p,h_{p'})=e(g_p^a,g_{p'}^b)$. 设 $\tilde{g}$ 是$\mathbb{G}$ 中某个生成元,则 $e(g_p^a,g_{p'}^b)=e(\tilde{g}^{p'a},\tilde{g}^{pb})=e(\tilde{g},\tilde{g})^{pp'ab}=1$,因此 $e(h_p,h_{p'})=1$.

1.2　复杂性假设

在基于身份的密码体制中,素数阶群中的 BDH (decisional bilinear Diffie-Hellman)假设[2]已经得到广泛的应用. 我们使用合数阶群中的 BDH 假设构造基于身份的匿名加密方案.

设 $n,p,p',\mathbb{G},\mathbb{G}_T,e$ 如节 1.1 定义. 在群$\mathbb{G}$, $\mathbb{G}_T$ 中,如果不存在 t 时间算法至少能以概率 ε 解决 BDH 问题,我们称(t,ε)-BDH 假设在群$\mathbb{G}$, $\mathbb{G}_T$ 中成立.

$g \leftarrow_R \mathbb{G}_p$, $g_{p'} \leftarrow_R \mathbb{G}_{p'}$, $a,b,c \leftarrow_R Z_n$, $E \leftarrow (g_{p'}, g^a, g^b, g^c)$, $\omega \leftarrow_R \{0,1\}$.

如果 $\omega=0$,令 $Z=e(g,g)^{abc}$;否则取 Z 是 $\mathbb{G}_T$,$_p$ 的一个随机数.我们称 (E,Z) 为 BDH 问题的一个挑战向量,发送这个向量给敌手 A.A 输出 ω',如果 $\omega'=\omega$,A 挑战成功.

我们定义 A 解决 BDH 问题的优势为 $|\Pr[A(E,e(g,g)^{abc})=0]-\Pr[A(E,Z)=0]|$.

1.3 安全模型

Gentry[13]定义了选择密文攻击下匿名 *IBE* 方案的安全模型.安全证明通过下列游戏进行,游戏有两个参与者:敌手 A 和挑战者 B.

Setup:B 执行 Setup 算法,并把参数 params 发给 A.

Phase1:A 适应性地进行下列询问:

Extract query $<$ID$>$:B 对身份 ID 执行 Extract 算法,并把对应的私钥返还给敌手.

Decrypt query $<$ID,C$>$:B 首先对身份 ID 执行 Extract 算法,然后用生成私钥解密密文 C,并把明文 M 或出错信息返还给 A.

Challenge:A 提交身份 ID^0,ID^1 和消息 M_0,M_1 给 B,其中 ID^0,ID^1 均没有在 Phase 1 中执行过 Extract query.B 随机选择 $\beta,\gamma\in\{0,1\}$,计算 $C^*=\text{Encrypt}(\text{params},ID^\beta,M_\gamma)$,并把 C^* 返还给 A.

Phase 2:A 继续适应性地进行询问,但是不能对 ID^0 和 ID^1 进行 Extract query,或对$<ID^0,C^*>$和$<ID^1,C^*>$进行 Decrypt query.

Guess:A 输出 $\beta',\gamma'\in\{0,1\}$.如果 $\beta'=\beta,\gamma'=\gamma$,A 赢得游戏.

我们称 A 为 ANON-IND-ID-CCA2 敌手,其优势定义为 $|\Pr[\beta'=\beta\wedge\gamma'=\gamma]-\frac{1}{4}|$.

定义 1.1 如果所有 t 时间的 ANON-IND-ID-CCA2 敌手经过 q 次询问后,都不能以大于 ε 的优势赢得上述游戏,则基于身份的匿名加密方案是 (t,q,ε)ANON-IND-ID-CCA2 安全的.

Chosen-plaintext security. 在上述游戏中,如果敌手不能进行 Decrypt query, 则被称为 ANON-IND-ID-CPA 敌手.

定义 1.2 如果所有 t 时间的 ANON-IND-ID-CPA 敌手在经过 q 次询问后,都不能以大于 ε 的优势赢得上述游戏,则基于身份的匿名加密方案是 (t,q,ε)ANON-IND-ID-CPA 安全的.

2 基于身份的匿名加密方案

本节我们提出一个基于身份的匿名加密方案,攻击者由密文不能得到接收者身份的任何信息,保护了接收者的隐私,同时增加了破译密文的难度.方案基于合数阶群中的 BDH 假设,在标准模型中是 ANON-IND-ID-CPA 安全的.

构造思想:基于身份加密方案如果具备匿名性,则攻击者由密文不能得到接收者的身份信息.本文方案基于阶为合数的双线性群,公共参数和加密密文取自合数群,PKG 和用户私钥取自素数群.由于攻击者得不到素数群中的元素,从而无法从密文中得到接收者的身份信息,因此,方案可以实现接收者的匿名性.同时,本文方案还具备普通加密方案的特性,即密文的不可区分性.具体方案如下:

(Ⅰ) 系统建立

设用户身份为 l 比特字符串.令 n, p, p', $\mathbb{G}$, $\mathbb{G}_T$, e 如节 1.1 定义,g 和 $g_{p'}$ 分别为 $\mathbb{G}_p$ 和 $\mathbb{G}_{p'}$ 的生成元.PKG 随机选择 $\alpha\in Z_n^*$, g_2, $u'\in\mathbb{G}_p$,向量 $\boldsymbol{u}=(u_i)$, $u_i\in\mathbb{G}_p$, $i\in\{1,2,\cdots,l\}$,及 R_g, R', $R_i\in\mathbb{G}_{p'}$,并计算

$$g_1=g^\alpha, G=gR_g, G'=u'R',$$

$$G_i=u_iR_i, \boldsymbol{U}=(G_i), i\in\{1,2,\cdots,l\}, e(g_1,g_2).$$

则方案公共参数为 $(g_{p'},G,G',\boldsymbol{U},e(g_1,g_2))$,PKG 私钥为 $(g,g_1,g_2,u',\boldsymbol{u})$.

(Ⅱ) 私钥生成

假设用户身份 $\text{ID}=(\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_l)$, $\text{ID}_i\in\{0,1\}$,PKG 随机选择 $r\in Z_n^*$,并计算

$$d_1=g_2^\alpha(u'\prod_{\text{ID}_i=1}u_i)^r, d_2=g^r, d_{\text{ID}}=(d_1,d_2).$$

(Ⅲ) 加密

给定消息 $M\in\mathbb{G}_T$,随机选择 $t\in Z_n^*$, $R_1',R_2'\in\mathbb{G}_{p'}$,其中 $\mathbb{G}_{p'}$ 中的元素可以由 $g_{p'}$ 生成.计算

$$C=(G^t\cdot R_1', (G'\prod_{\text{ID}_i=1}G_i)^t\cdot R_2', M\cdot e(g_1,g_2)^t).$$

(Ⅳ) 解密

令密文 $C=(C_1,C_2,C_3)$,用户 ID 用私钥解密 $C_3\dfrac{e(d_2,C_2)}{e(d_1,C_1)}=M$.

(Ⅴ) 正确性验证

如节 1.1 所述,对于任意 $h_p\in\mathbb{G}_p$ 和 $h_{p'}\in\mathbb{G}_{p'}$, $e(h_p,h_{p'})=1$.

由于 g, g_2, u', $u_i\in\mathbb{G}_p$, R, R', R_i, R_1', $R_2'\in$

$\mathbb{G}_{p'}$，因此，

$$e(d_2, C_2) = e(g^r, (u'\prod_{\mathrm{ID}_i=1} u_i)^t \cdot (R'\prod_{\mathrm{ID}_i=1} R_i)^t R_2') = e(g^r, (u'\prod_{\mathrm{ID}_i=1} u_i)^t),$$

$$e(d_1, C_1) = e(g_2^a (u'\prod_{\mathrm{ID}_i=1} u_i)^r, g^t R^t R_1') = e(g_2, g_1^t)\, e((u'\prod_{\mathrm{ID}_i=1} u_i)^r, g^t),$$

$$C_3 \frac{e(d_2, C_2)}{e(d_1, C_1)} = M \cdot e(g_1, g_2)^t \cdot \frac{e(g^r, (u'\prod_{\mathrm{ID}_i=1} u_i)^t)}{e(g_1, g_2)^t e((u'\prod_{\mathrm{ID}_i=1} u_i)^r, g^t)} = M.$$

3　安全性和效率分析

本节我们在标准模型中证明方案是 ANON-IND-ID-CPA 安全的，并与其他同类方案进行安全性和效率比较.

3.1　安全性分析

定理 3.1　假定 (t', ε', q)-BDH 假设在 $\mathbb{G}, \mathbb{G}_T$ 中成立，那么文中 IBE 方案是 (t, ε, q)-ANON-IND-ID-CPA 安全的，其中

$$t' = t + O(\varepsilon^{-2}\ln(\varepsilon^{-1})\lambda^{-1}\ln(\lambda^{-1})),$$

$$\varepsilon' = \frac{\varepsilon}{32(l+1)q},\ \lambda = \frac{1}{8(l+1)q}.$$

证明　假定 A 是节 1.3 中定义的 ANON-IND-ID-CPA 敌手，我们可以构建算法 B 解决 BDH 问题. 游戏开始前，给定 B 一个向量 $(g_{p'}, g^a, g^b, g^c, Z) \in \mathbb{G}_{p'} \times \mathbb{G}_p^3 \times \mathbb{G}_T$，判断 $Z = e(g,g)^{abc}$ 是否成立.

Setup：B 计算 $m = 4q$，并随机选择 $k \in \{0,1,\cdots,l\}$，$x' \in \{0,1,\cdots,m-1\}$，一个 l 比特向量 $\boldsymbol{x} = (x_i)$，其中 $x_i \in \{0,1,\cdots,m-1\}$. 令 $X^* = (x', \boldsymbol{x})$，$B$ 随机选择 $y' \in Z_n$ 及一个 l 比特向量 $\boldsymbol{y} = (y_i)$，其中 $y_i \in Z_n$.

对于用户身份 $\mathrm{ID} = (\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_l)$，定义

$$F(\mathrm{ID}) = (n - mk) + x' + \sum_{\mathrm{ID}_i=1} x_i,$$

$$J(\mathrm{ID}) = y' + \sum_{\mathrm{ID}_i=1} y_i,$$

$K(\mathrm{ID})$ 为二值函数，当 $x' + \sum_{\mathrm{ID}_i=1} x_i \equiv 0 \pmod m$ 时，$K(\mathrm{ID}) = 0$；否则 $K(\mathrm{ID}) = 1$. B 定义 $g_1 = g^a$，$g_2 = g^b$，$u' = g_2^{n-km+x'} g^{y'}$，$\boldsymbol{u} = (u_i)$，$u_i = g_2^{x_i} g^{y_i}$，$i \in \{1,\cdots,l\}$，并选择 $R_g, R', R_i \in \mathbb{G}_{p'}$，计算

$$G = gR_g,\ G' = u'R',\ G_i = u_i R_i,$$

$$\boldsymbol{U} = (G_i),\ i \in \{1,2,\cdots,l\},\ e(g_1, g_2).$$

则方案公共参数为 $(G, G', \boldsymbol{U}, e(g_1, g_2))$，PKG 私钥为 $(g, g_1, g_2, u', \boldsymbol{u})$.

Phase1：A 适应性地进行 Extract query. 如果 $K(\mathrm{ID}) = 0$，B 放弃并随机选择 ω'. 否则，随机选择 $r \in Z_n$，计算

$$d = (d_1, d_2) = (g_1^{\frac{-J(\mathrm{ID})}{F(\mathrm{ID})}} (u'\prod_{\mathrm{ID}_i=1} u_i)^r, g_1^{\frac{-1}{F(\mathrm{ID})}} g^r).$$

令 $\bar{r} = r - \frac{a}{F(\mathrm{ID})}$，则

$$d_2 = g^{r - \frac{a}{F(\mathrm{ID})}} = g^{\bar{r}},$$

$$d_1 = g_1^{\frac{-J(\mathrm{ID})}{F(\mathrm{ID})}} (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^r = g_2^a (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^{-\frac{a}{F(\mathrm{ID})}} (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^r = g_2^a (u'\prod_{\mathrm{ID}_i=1} u_i)^{-\frac{a}{F(\mathrm{ID})}} = g_2^a (u'\prod_{\mathrm{ID}_i=1} u_i)^{\bar{r}}.$$

Challenge：A 提交身份 $\mathrm{ID}^0, \mathrm{ID}^1$ 和消息 M_0, M_1 给 B，其中 $\mathrm{ID}^0, \mathrm{ID}^1$ 均没有在 Phase 1 中进行过 Extract query. 如果 $x' + \sum_{\mathrm{ID}_i^0=1} x_i \neq km$ 或 $x' + \sum_{\mathrm{ID}_i^1=1} x_i \neq km$，$B$ 放弃并随机选择 ω'. 否则，$F(\mathrm{ID}^0) \equiv 0 \pmod n$，$F(\mathrm{ID}^1) \equiv 0 \pmod n$ 成立，B 随机选择 $\beta, \gamma \in \{0,1\}$，$R_1', R_2' \in \mathbb{G}_{p'}$，计算 $C^* = (C_1^*, C_2^*, C_3^*) = (g^c \cdot R_1', g^{cJ(\mathrm{ID}^\beta)} \cdot R_2', M_\gamma \cdot Z)$，并把 C^* 返还给 A.

令 $t^* = c$，如果 $Z = e(g,g)^{abc}$，则

$$C_1^* = g^c \cdot R_1' = G^{t^*} \cdot R_1'',$$

$$C_3^* = M_\gamma \cdot e(g_1, g_2)^{t^*},$$

$$C_2^* = g^{t^*(y' + \sum_{\mathrm{ID}_i^\beta=1} y_i)} \cdot R_2' = g^{t^* b(n-km+x' + \sum_{\mathrm{ID}_i^\beta=1} x_i)} g^{t^*(y' + \sum_{\mathrm{ID}_i^\beta=1} y_i)} \cdot R_2' = g^{t^*[b(n-km+x')+y']} \prod_{\mathrm{ID}_i^\beta=1} g^{t^*(bx_i+y_i)} \cdot R_2' = (u'\prod_{\mathrm{ID}_i^\beta=1} u_i)^{t^*} \cdot R_2' = (G'\prod_{\mathrm{ID}_i^\beta=1} G_i)^{t^*} \cdot R_2'',$$

其中，$R_1'', R_2'' \leftarrow_R \mathbb{G}_{p'}$.

因此，C^* 是发送给 ID^β 关于 M_γ 的一个有效密文. 由于 a, b, c 是 Z_n^* 中均匀分布的随机数，C^* 对敌手来说是一个匿名且均匀分布的密文.

Phase 2：A 继续适应性地进行询问，但是不能对 ID_0 和 ID_1 进行 Extract query.

Guess：A 输出 $\beta', \gamma' \in \{0,1\}$. 如果 $\beta' = \beta$，$\gamma' = \gamma$，敌手赢得游戏.

概率分析，时间复杂度：见文献[6].

ANON-IND-ID-CCA2 安全性：根据文献[24]中的方法，一个两层的 HIBE(Hierarchical IBE) 方案[25]可以转化为 CCA2 安全的 IBE 方案. Waters[6] 使用这种方法，把文献[6]和文献[5]中的 IBE 方案分别作为 HIBE 方案的第一、二层，构造了一个 CCA2 安全的 IBE 方案[6]. 同样，我们可以把节 2 中的匿名 IBE 方案和文献[5]中的 IBE 方案分别作为 HIBE 方案的第一、二层，转化为一个两层的 HIBE 方案，再得到达到 ANON-IND-ID-CCA2 安全的匿名 IBE 方案.

3.2 同类方案比较

本文研究传统的匿名 IBE 方案，没有考虑扩展性研究，如多个接收者和多个可信中心的匿名 IBE 方案. 公平起见，在表 1 中，只对传统匿名 IBE 方案进行安全性和效率比较.

由表 1 可以看出，文中方案基于 BDH 假设，在标准模型下的 adaptive-ID 模型可证安全，公钥长度与用户身份长度成正比. 文献[11]中方案虽然具有短的公钥长度，但仅在 selective-ID 模型中可证安全；文献[12]中的方案具有最高的实现效率，但没有对安全性进行归约证明；文献[13]中方案具有短的公钥长度，且在 adaptive-ID 模型中达到 CCA 的安全性，但仅基于 ABDHE 假设可证安全；文献[15]中的方案虽然在 adaptive-ID 模型中可证安全，但基于 BDH 和线性假设可证安全，且解密需要 9 次双线性对运算. 实际上，ABDHE 和线性问题的难度低于 BDH 问题，而 CPA 安全的 IBE 方案可通过文献[24]中的方法转换成 CCA 安全的 IBE 方案，因此与同类方案相比，文中方案同时具有较高的安全性和实现效率.

表 1 匿名 IBE 方案安全性和效率比较

Tab. 1 Comparison among anonymous IBE scheme

方案	复杂性假设	安全性	公钥长度	私钥长度	密文长度	对运算
文献[11]	BDH，线性假设	selective-ID，CPA	8	5	6	5
文献[12]	no	no	3	2	3	2
文献[13]	ABDHE	adaptive-ID，CCA	5	6	4	2
文献[15]	BDH，线性假设	adaptive-ID，CPA	16	9	11	9
本文	BDH	adaptive-ID，CPA	$l+4$	2	3	2

【注】 “l”是一个 hash 函数的输出长度，公钥、私钥和密文长度以群元素的比特数为一个单位.

4 结论

基于阶为合数的双线性群，提出了一个基于身份的匿名加密方案. 方案基于 BDH 假设，在标准模型中是 ANON-IND-ID-CPA 安全的. 与同类方案相比，新方案基于的困难问题难度更强，且在 adaptive-ID 模型中可证安全，而且仅需 2 次双线性对运算，因此同时具有高的安全性和实现效率. 后续工作是对文中方案进行扩展性研究，如构造多个接收者和多个可信中心的匿名 IBE 方案，并在标准模型中可证安全.

参考文献(References)

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Blakley G, Chaum D. Proceedings of CRYPTO'84. California: Springer, 1984: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Kilian J. Proceedings of CRYPTO'01. California: Springer, 2001: 213-229.

[3] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols [C]// Nyberg K. Proceedings of ACM CCS'93. Virginia: ACM, 1993: 62-73.

[4] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited [J]. Journal of the ACM, 2004, 51(4): 557-594.

[5] Boneh D, Boyen X. Efficient selective-ID secure identity based encryption without random oracles [C]// Cachin C, Camenisch J. Proceedings of EUROCRYPT'04. Interlaken: Springer, 2004: 223-238.

[6] Waters B. Efficient identity-based encryption without random oracles [C]// Cramer R. Proceedings of EUROCRYPT'05. Aarhus: Springer, 2005: 114-127.

[7] Naccache D. Secure and practical identity-based encryption [J]. IET Information Security, 2007, 1(2): 59-64.

[8] Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions [C]// Shoup V. Proceedings of CRYPTO'05. California: Springer, 2005: 205-222.

[9] Kamara S, Lauter K. Cryptographic cloud storage [C]// Dingledine R, Golle P. Proceedings of FC'10. Canary Islands: Springer, 2010: 136-149.

[10] Tian Yuan, Deng Luyao, Zhang Hao. Conditions for anonymity in some generic public-key encryption constructions [J]. Journal on Communications, 2009,

30：8-16.
田园，邓鲁耀，张浩. 几个通用公钥加密方案的匿名性条件[J]. 通信学报，2009，30：8-16.

[11] Boyen X，Waters B. Anonymous hierarchical identity-based encryption（without random oracles）[C]// Dwork C. Proceedings of CRYPTO'06. California：Springer，2006：290-307.

[12] Liu L，Cao Z. Improvements of one anonymous ID-based encryption [C]// Mahadevan V，Tomar G. Proceedings of ICETC'10. Shanghai：IEEE，2010：256-260.

[13] Gentry C. Practical identity-based encryption without random oracles [C]// Vaudenay S. Proceedings of EUROCRYPT'06. Saint Petersburg：Springer，2006：445-464.

[14] Hu Liang，Liu Zheli，Sun Tao，et al. Survey of security on identity-based cryptography [J]. Journal of Computer Research and Development，2009，46(9)：1 537-1 548.
胡亮，刘哲理，孙涛，等. 基于身份密码学的安全性研究综述[J]. 计算机研究与发展，2009，46(9)：1 537-1 548.

[15] Ren Y，Wang S，Zhang X，et al. Fully secure anonymous identity-based encryption under simple assumptions [C]// Chen X. Proceedings of MINES'10. Nanjing：IEEE，2010：428-432.

[16] Wang X，Wang A，Wang L. Efficient ID-based secure encryption scheme for anonymous receivers [J]. Journal of the Networks，2009，4(7)：641-648.

[17] Fan C，Huang L，Ho P. Anonymous multi-receiver identity-based encryption [J]. IEEE transactions on computers，2010，59(9)：1 239-1 249.

[18] Paterson K，Srinivasan S. Security and anonymity of identity-based encryption with multiple trusted authorities [C]// Galbraith S，Paterson K. Proceedings of Pairing'08. London：Springer，2008：354-375.

[19] Zhang Leyou，Hu Yupu，Wu Qing. A new hierarchical identity-based encryption in the standard model [J]. Journal of Electronics & Information Technology，2009，31(4)：937-941.
张乐友，胡予濮，吴青. 标准模型下一种新的基于身份的分级加密方案[J]. 电子与信息学报，2009，31(4)：937-941.

[20] Du Hongzhen，Wen Qiaoyan. Efficient traceable identity-based signature scheme [J]. Journal on Communications，2009，30(8)：56-61.
杜红珍，温巧燕. 高效的可追踪的基于 ID 的签名方案[J]. 通信学报，2009，30(8)：56-61.

[21] Luo Changyuan，Li Wei，Xing Hongzhi，et al. Research on identity-based distributed key management in space network [J]. Journal of Electronics & Information Technology，2010，32(1)：183-188.
罗长远，李伟，邢洪智，等. 空间网络中基于身份的分布式密钥管理研究[J]. 电子与信息学报，2010，32(1)：183-188.

[22] Boneh D，Goh E，Nissim K. Evaluating 2-dnf formulas on ciphertexts [C]// Kilian J. Proceedings of TCC'05. Cambridge：Springer，2005：325-341.

[23] Seo J，Kobayashi T，Ohkubo M，et al. Anonymous hierarchical identity-based encryption with constant size ciphertexts [C]// Jarecki S，Tsudik G. Proceedings of PKC'09. California：Springer，2009：215-234.

[24] Canetti R，Halevi S，Katz J. Chosen-ciphertext security from identity-based encryption [C]// Cachin C，Camenisch J. Proceedings of EUROCRYPT'04. Interlaken：Springer，2004：207-222.

[25] Gentry C，Silverberg A. Hierarchical ID-based cryptography [C]// Zheng Y. Proceedings of ASIACRYPT'02. New Zealand：Springer，2002：548-566.