标准模型下可公开验证的匿名 IBE 方案的安全性分析

杨启良[1,2],周彦伟[1,2],杨坤伟[1],王 涛[1]
(1. 陕西师范大学计算机科学学院,陕西西安 710062;2. 密码科学技术国家重点实验室,北京 100878)

摘 要: 现有的可公开验证的匿名基于身份的加密(Identity-Based Encryption,IBE)机制声称解决了在静态困难性假设之上构造紧的选择密文安全的 IBE 机制的困难性问题. 然而,本文发现,由于该机制的密文不具备防扩展性,使得任何敌手可基于已知的有效密文生成任意消息的合法加密密文,导致该机制无法满足其所声称的选择密文安全性. 我们根据不同的密文相等判定条件分别提出两种方法对原始方案的安全性进行了分析,同时在分析基础上指出原始安全性证明过程中所存在的不足.

关键词: 基于身份的密码学; 基于身份的加密; 公开可验证; 选择密文安全; 判定性双线性 Diffie-Hellman 假设; 标准模型; 双线性映射

中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2020)02-0291-05

电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.02.010

On the Security of Publicly Verifiable Anonymous IBE Scheme in the Standard Model

YANG Qi-liang[1,2], ZHOU Yan-wei[1,2], YANG Kun-wei[1], WANG Tao[1]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *State Key Laboratory of Cryptology, Beijing* 100878, *China*)

Abstract: How to create an identity-based encryption (IBE) scheme with tight chosen-ciphertext attacks (CCA) security based on the static assumption is an open problem. A publicly verifiable anonymous IBE scheme designed in the standard model claimed that the CCA security of proposed scheme was proved based on the classic static assumption. However, in this paper, we demonstrate that the previous IBE scheme cannot achieve the claimed CCA security because the ciphertext was extensile. In other words, a valid encrypted ciphertext can be forged by any adversary from a known ciphertext. To analyze the security of the previous IBE scheme, two methods are proposed based on the criterion of ciphertext equality. Additionally, based on the analysis of the previous IBE scheme, we point out the shortcomings of the original security proof.

Key words: identity-based cryptography; identity-based encryption; anonymous; publicly verifiable; chosen-ciphertext security; decisional bilinear Diffie-Hellman assumption; standard model; bilinear pairing

1 引言

在 Crypto 1985 中,Shamir[1] 创造性地提出了基于身份的密码学(Identity-Based Cryptography,IBC)的概念,用于解决传统基于公钥基础设施密码体制带来的证书的生成、验证、存储和吊销等问题,在 IBC 中,将标示用户身份的唯一信息(如 Email 地址,电话号码,IP 地址等)作为用户的公钥,用户的私钥由可信第三方即私钥生成中心(Key Generation Center,KGC)利用用户的身份信息和自己的主密钥计算得到,IBC 的主要优势是减轻了用户对公钥证书的依赖. 因此,IBC 是一种重要的密码学工具,简化了传统公钥密码系统中公钥证书的生

收稿日期:2019-01-11;修回日期:2019-07-04;责任编辑:覃怀银
基金项目:国家重点研发计划(No. 2017YFB0802000);国家自然科学基金(No. 61802242, No. 61572303, No. 61772326, No. 61872087, No. 61802241, No. 61702259);陕西省自然科学基础研究计划(No. 2018JQ6088);"十三五"国家密码发展基金(No. MMJJ20180217);中央高校基本科研业务费项目(No. GK201803064)

成、管理和吊销等问题. 2001 年,Boneh 和 Franklin[2] 基于双线性映射构建了第一个安全实用的身份基加密(Identity-Based Encryption,IBE)机制,这一开创性工作得到了密码学界的广泛关注,利用双线性映射构造基于身份的加密方案、签名方案、密钥协商协议和数据访问控制机制等各种密码协议[3~12]已经成为信息安全研究中的热点.

Eurocrypt 2006 中,Gentry 提出了两个具有紧规约性质的匿名 IBE 机制[6],分别达到选择明文攻击(Chosen-Plaintext Attacks,CPA)安全和选择密文攻击(Chosen-Ciphertext Attacks,CCA)安全. 方案的公共参数很短,加密过程不需要进行双线性对计算,并基于非静态的安全性假设对该方案的安全性进行了证明,也就是说该方案的安全性强度取决于敌手的询问次数. 同时,Gentry 指出如何基于静态假设构造紧的安全 IBE 机制是一个公开的困难问题.

2016 年,为解决上述困难问题,文献[13]基于判定的双线性 Diffie-Hellman(Decisional Bilinear Diffie-Hellman,DBDH)问题构造了一个在标准模型下安全的、可公开验证的匿名 IBE 方案,并宣称解决了 Gentry 所提出的公开困难问题. 然而,本文通过分析发现该方案并不满足其所声称的 CCA 安全性,并根据不同限制条件给出两种具体的攻击方法;同时,对原始的安全性证明过程进行了详细分析.

2 预备知识

IBE 机制的形式化定义及 CCA 安全模型读者可参考文献[2~6,14].

2.1 双线性映射

群生成算法 $\mathcal{G}(1^\kappa)$ 的输入为安全参数 ,输出是元组(p,g,G_1,G_2,e),其中 G_1 和 G_2 为阶是大素数 p 的乘法循环群,g 为群 G_1 的生成元, $e:G_1\times G_1\to G_2$ 是满足下述性质的双线性映射.

双线性:对于任意的 $a,b\in Z_p^*$,有 $a,b\in Z_p^*$ 成立;

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

可计算性:对于任意的 $P,Q\in G_1$,$e(P,Q)$ 可在多项式时间内完成计算.

2.2 困难性假设

DBDH 假设. 令$(p,g,G_1,G_2,e)\leftarrow\mathcal{G}(1^\kappa)$,对于任意未知的指数 $a,b,c,d\in Z_p^*$ 和给定的两个元组

$$(T,e(g,g)^{abc})\text{和}(T,e(g,g)^{d}),$$

其中 $T=(g,g^a,g^b,g^c)$. DBDH 问题的目标是判断 $e(g,g)^{abc}=e(g,g)^d$ 是否成立. DBDH 假设意味着任意的算法 $\mathcal{A}$ 成功解决 DBDH 问题的优势

$$\mathrm{Adv}_{\mathrm{DBDH}}(\mathcal{A})=\Pr[\mathrm{A}(T,e(g,g)^{abc})=1]-\Pr[\mathrm{A}(T,e(g,g)^{d})=1]$$

是可忽略的,其中概率来源于 a,b,c,d 在 Z_p^* 上的随机选取和算法 A 的随机选择.

特别地,当元组(g,g^a,g^b,g^c,g^d)满足条件 $d=abc$ 时称其是 DBDH 元组;否则称其为非 DBDH 元组.

3 李-杨方案及安全性分析

2016 年,文献[13]基于 DBDH 假设提出一个在标准模型下可公开验证的匿名 IBE 方案(简记为李-杨方案). 为了便于分析,本节首先回顾李-杨方案,并结合 IBE 机制的 CCA 安全模型对该方案进行安全性分析.

3.1 李-杨方案介绍

设 G_1 和 G_2 是阶为 p 的循环群, $e:G_1\times G_1\to G_2$ 是一个双线性映射. g 是群 G 的生成元,随机选取 $a\in Z_p^*$,$g_2\in G_1$,令 $g_1=g^\alpha$,选取了一个抗碰撞的单向哈希函数 $H:\{0,1\}^*\to Z_p^*$,其中 H 的输入空间为 $G_1^3\times G_2$,输出为 $\beta\in Z_p^*$. 具体方案如下:

(1)初始化. 系统建立算法生成相应的公开参数 $\mathrm{Params}=(g,g_1,g_2,e,H)$ 和主密钥为 α.

(2)密钥生成. 为身份 id 生成对应的私钥. 可信第三方 KGC 选取一个随机数 $r\in Z_p^*$,输出私钥$\mathrm{sk}_{\mathrm{id}}=(d_1,d_2,d_3)=(g_2^\alpha g_1^{\mathrm{id}\cdot r},g^r,g^{\mathrm{id}\cdot r})$.

(3)加密. 使用身份 id 加密消息 $m\in G_2$,发送者选择两个随机数 $t,s\in Z_p^*$,并输出

$$\begin{aligned}C&=(c_1,c_2,c_3,c_4,c_5)\\&=(e(g_1,g_2)^t m,g_1^{\mathrm{id}\cdot(t+s)},g_1^s,g^t,e(g,g_1)^{\beta\cdot(s+t)})\end{aligned}$$

其中 $\beta=H(c_1,c_2,c_3,c_4)$. 由于 $e(g_1,g_2)$ 和 $e(g,g_1)$ 可提前运算,则加密不需要任何对运算.

(4)解密. 收到密文 $C=(c_1,c_2,c_3,c_4,c_5)$ 后,接收者首先计算 $\beta=H(c_1,c_2,c_3,c_4)$,若验证等式 $c_5=e(g^\beta,c_3)e(c_4,g_1)^\beta$ 成立,则接收者输出

$$m=c_1\frac{e(d_2,c_2)}{e(d_1,c_4)e(d_3,c_3)}.$$

3.2 李-杨方案的安全性分析

在 IBE 机制中,CCA 安全游戏的第二阶段敌手对除挑战身份密文对之外的任何身份密文对进行解密询问,也就是说,除挑战密文之外,敌手能够对关于挑战身份的其他任意密文进行解密询问. 对于 CCA 安全的 IBE 机制而言,有效密文不能具有扩展性,即任何敌手均无法基于现有的合法密文生成一个新的合法密文,否则在 CCA 安全游戏的第二阶段,敌手能够基于挑战密文为挑战身份伪造一个新的合法密文,并向挑战者提出关于新密文的解密询问,由于伪造的密文跟挑战密文并不相同,因此挑战者将返回新密文所对应的明文,进而敌手能够基于该明文猜出挑战密文所对应的

明文.

CCA 安全游戏中涉及不同密文的概念. 在李-杨方案中,密文包含多个元素,根据强度不同的两种条件对不同密文进行定义:(1)不同的密文中至少有一个互不相同的元素;(2)不同密文中的所有元素均不相同.

3.2.1　攻击方法一

针对不同密文的第一种定义,本节给出一种具体的攻击方法,指出李-杨方案不满足其所声称的 CCA 安全性,具体过程如下:

对于身份消息对(id,m)的合法密文$C=(c_1,c_2,c_3,c_4,c_5)$,其中$c_1=e(g_1,g_2)^t m$,$c_2=g_1^{\mathrm{id}\cdot(t+s)}$,$c_3=g_1^s$,$c_4=g^t$ 和$c_5=e(g,g_1)^{\beta\cdot(s+t)}$,敌手 A 进行下述伪造操作:

(1)计算$\beta=H(c_1,c_2,c_3,c_4)$和$\gamma=c_5^{\frac{1}{\beta}}$,即有$\gamma=e(g,g_1)^{s+t}$;

(2)选取随机值$m'\in G_2$,计算$c_1'=c_1\cdot m'$;

(3)令$c_2'=c_2$,$c_3'=c_3$ 和$c_4'=c_4$;

(4)计算$\beta'=H(c_1',c_2',c_3',c_4')$和$c_5'=\gamma^{\beta'}$.

(5)输出密文$C'=(c_1',c_2',c_3',c_4',c_5')$给接收者 id,其中$c_1=e(g_1,g_2)^t m\cdot m'$,$c_2'=g_1^{\mathrm{id}\cdot(t+s)}$,$c_3'=g_1^s$,$c_4'=g^t$ 和$c_5'=e(g,g_1)^{\beta'\cdot(s+t)}$.

敌手 A 输出伪造密文C'后,挑战者对密文C'的解密过程具体描述如下:

(1)验证等式$c_5'=e(g^{\beta'},c_3')e(c_4',g_1)^{\beta'}$是否成立,其中

$$\begin{aligned}c_5'&=e(g,g_1)^{\beta'\cdot(s+t)}=e(g^{\beta'},g_1)^s e(g,g_1)^{\beta'\cdot t}\\&=e(g^{\beta'},g_1^s)e(g^t,g_1)^{\beta'}=e(g^{\beta'},c_3')e(c_4',g_1)^{\beta'}.\end{aligned}$$

(2)输出相应的解密结果

$$\begin{aligned}&c_1'\frac{e(d_2,c_2')}{e(d_1,c_4')e(d_3,c_3')}\\&=(e(g_1,g_2)^t m\cdot m')\frac{e(g^r,g_1^{\mathrm{id}\cdot(t+s)})}{e(g_2^\alpha g_1^{\mathrm{id}\cdot r},g^t)e(g^{\mathrm{id}\cdot r},g_1^s)}\\&=(e(g_1,g_2)^t m\cdot m')\frac{e(g^r,g_1^{\mathrm{id}\cdot t})e(g^r,g_1^{\mathrm{id}\cdot s})}{e(g_2^\alpha,g^t)e(g_1^{\mathrm{id}\cdot r},g^t)e(g^{\mathrm{id}\cdot r},g_1^s)}\\&=(e(g_1,g_2)^t m\cdot m')\frac{1}{e(g_2^\alpha,g^t)}\\&=(e(g_1,g_2)^t m\cdot m')\frac{1}{e(g_1,g_2)^t}=m\cdot m',\end{aligned}$$

其中$\mathrm{sk}_{\mathrm{id}}=(d_1,d_2,d_3)=(g_2^\alpha g_1^{\mathrm{id}\cdot r},g^r,g^{\mathrm{id}\cdot r})$.

综上所述,基于消息m的合法密文C,敌手 A 为接收者 id 伪造的密文C'是关于消息$m\cdot m'$的合法密文,其中$c_1'\neq c_1$ 和$c_5'\neq c_5$.

3.2.2　攻击方法二

针对不同密文的第二种定义,本节给出一种具体的攻击方法,指出李-杨方案不满足其所声称的 CCA 安全性,具体过程如下:

收到关于身份消息对(id,m)的合法密文$C=(c_1,c_2,c_3,c_4,c_5)$后,敌手 A 进行下述操作:

(1)计算$\beta=H(c_1,c_2,c_3,c_4)$和$\gamma=c_5^{\frac{1}{\beta}}$,即有$\gamma=e(g,g_1)^{s+t}$;

(2)选取随机的$m'\in G_2$和$x,y\in Z_p^*$,计算$c_1'=c_1\cdot e(g_1,g_2)^x\cdot m'$;

(3)计算$c_2'=c_2 g_1^{\mathrm{id}\cdot(x+y)}$,$c_3'=c_3 g_1^y$ 和$c_4'=c_4 g^x$;

(4)计算$\beta'=H(c_1',c_2',c_3',c_4')$和$c_5'=\gamma^{\beta'}e(g,g_1)^{\beta'\cdot(x+y)}$.

(5)输出密文$C'=(c_1',c_2',c_3',c_4',c_5')$给接收者 id,其中$c_1=e(g_1,g_2)^{t+x}m\cdot m'$,$c_2'=g_1^{\mathrm{id}\cdot(t+s+x+y)}$,$c_3'=g_1^{s+y}$,$c_4'=g^{t+x}$和$c_5'=e(g,g_1)^{\beta'\cdot(s+t+x+y)}$.

敌手 A 输出伪造密文C'后,挑战者对密文C'的解密过程具体描述如下:

(1)验证等式$c_5'=e(g^{\beta'},c_3')e(c_4',g_1)^{\beta'}$是否成立,其中

$$\begin{aligned}c_5'&=e(g,g_1)^{\beta'\cdot(s+t+x+y)}=e(g^{\beta'},g_1)^{s+y}e(g,g_1)^{\beta'\cdot(t+x)}\\&=e(g^{\beta'},g_1^{s+y})e(g^{t+x},g_1)^{\beta'}\\&=e(g^{\beta'},c_3')e(c_4',g_1)^{\beta'}.\end{aligned}$$

(2)输出相应的解密结果

$$\begin{aligned}&c_1'\frac{e(d_2,c_2')}{e(d_1,c_4')e(d_3,c_3')}\\&=(e(g_1,g_2)^{t+x}m\cdot m')\frac{e(g^r,g_1^{\mathrm{id}\cdot(t+s+x+y)})}{e(g_2^\alpha g_1^{\mathrm{id}\cdot r},g^{t+x})e(g^{\mathrm{id}\cdot r},g_1^{s+y})}\\&=(e(g_1,g_2)^{t+x}m\cdot m')\frac{e(g^r,g_1^{\mathrm{id}\cdot(t+x)})e(g^r,g_1^{\mathrm{id}\cdot(s+y)})}{e(g_2^\alpha,g^{t+x})e(g_1^{\mathrm{id}\cdot r},g^{t+x})e(g^{\mathrm{id}\cdot r},g_1^{s+y})}\\&=(e(g_1,g_2)^{t+x}m\cdot m')\frac{1}{e(g_2^\alpha,g^{t+x})}\\&=(e(g_1,g_2)^{t+x}m\cdot m')\frac{1}{e(g_1,g_2)^{t+x}}=m\cdot m'.\end{aligned}$$

其中$\mathrm{sk}_{\mathrm{id}}=(d_1,d_2,d_3)=(g_2^\alpha g_1^{\mathrm{id}\cdot r},g^r,g^{\mathrm{id}\cdot r})$.

综上所述,敌手 A 基于消息m的合法密文C为接受者 id 伪造了关于消息$m\cdot m'$的合法密文C',其中$c_i'\neq c_i(i=1,2,3,4,5)$.

3.3　李-杨方案安全性证明过程分析

在文献[13]中,作者对所提方案的安全性进行了详细的形式化证明. 本节将对原始证明过程的正确性进行分析. 为方便分析,首先简述原始的证明过程(简单起见,下述描述中省略了匿名性的证明内容),具体描述如下:

(1)初始化. 模拟者 C 从 DBDH 假设的挑战者处收到相应的挑战元组(g,g^a,g^b,g^c,Z). 令$g_1=g^a$(隐含的设置未知的随机数a是系统主私钥)和$g_2=g^b$,并将相应的系统公开参数 Params$=(g,g_1,g_2,e,H)$发给敌手 A,其中$H:\{0,1\}^*\to Z_p^*$是抗碰撞哈希函数.

(2)阶段 1. 该阶段敌手 A 可适应性的进行多项式次的密钥生成询问和解密询问.

密钥生成询问. 对每一个用户身份 id,$\mathcal{C}$ 选取一个随机数 $r\in Z_p^*$,生成相应的秘密钥:

$$\begin{aligned}\mathrm{sk}_{\mathrm{id}}&=(d_1,d_2,d_3)\\&=(g_1^{r\cdot\mathrm{id}},g^r g_2^{-\frac{1}{\mathrm{id}}},g^{r\cdot\mathrm{id}}g_2^{-1}).\end{aligned}$$

令 $r'=r-\dfrac{b}{\mathrm{id}}$,则有:

$$\begin{aligned}d_1&=g_1^{r\cdot\mathrm{id}}=g_2^{\alpha}g_1^{-b}g_1^{r\cdot\mathrm{id}}=g_2^{\alpha}g_1^{r\cdot\mathrm{id}-b}\\&=g_2^{\alpha}g_1^{\mathrm{id}\cdot(r-\frac{b}{\mathrm{id}})}=g_2^{\alpha}g_1^{\mathrm{id}\cdot r'};\\d_2&=g^r g_2^{-\frac{1}{\mathrm{id}}}=g^{r-\frac{b}{\mathrm{id}}}=g^{r'};\\d_3&=g^{r\cdot\mathrm{id}}g_2^{-1}=g^{r\cdot\mathrm{id}-b}=g^{\mathrm{id}\cdot(r-\frac{b}{\mathrm{id}})}=g^{\mathrm{id}\cdot r'}.\end{aligned}$$

解密询问. 对身份和密文对(id,C)的解密询问. $\mathcal{C}$ 首先对身份 id 进行秘密钥生成询问,产生与 id 对应的秘密钥$\mathrm{sk}_{\mathrm{id}}$,再运行解密算法,用$\mathrm{sk}_{\mathrm{id}}$解密密文 C,并将相应的明文 m 发送给 A.

(3)挑战 敌手 A 提交一个挑战身份id^*和两个等长的挑战消息 m_0,m_1. C 选取随机比特 $v\in\{0,1\}$,并按阶段 1 的过程计算身份id^*对应私钥$\mathrm{sk}_{\mathrm{id}^*}=(d_1^*,d_2^*,d_3^*)$,然后选取两个随机数 $c,p\in Z_p^*$ 构造对应的密文如下:

$$\begin{aligned}C_b^*&=(c_1,c_2,c_3,c_4,c_5)\\&=(Zm_v,g_1^{\mathrm{id}^*\cdot(c+p)},g_1^p,g^c,e(g,g_1)^{\beta\cdot(c+p)}),\end{aligned}$$

其中 $\beta=H(c_1,c_2,c_3,c_4)$.

如果模拟器 C 的输入是 DBDH 元组时,即 $Z=e(g,g)^{abc}$,则密文 C 的形式为:

$$\begin{aligned}C_v^*&=(c_1,c_2,c_3,c_4,c_5)\\&=(e(g,g)^{abc}m_v,g_1^{\mathrm{id}^*\cdot(c+p)},g_1^p,g^c,e(g,g_1)^{\beta\cdot(c+p)})\\&=(e(g_1,g_2)^c m_v,g_1^{\mathrm{id}^*\cdot(c+p)},g_1^p,g^c,e(g,g_1)^{\beta\cdot(c+p)}).\end{aligned}$$

显然,C_v^* 是明文 m_v 的一个有效加密密文.

如果模拟器 C 的输入是非 DBDH 元组时,即 Z 是 G_2 中的一个随机元素. 这种情况下,模拟器 C 的输出密文是一个随机消息的加密密文.

(4)阶段 2 敌手 A 继续发起私钥生成询问和解密询问,模拟器 C 按阶段 1 的方式进行应答,但是该阶段中 A 不能对挑战身份进行密钥生成询问,也不能对挑战身份和挑战密文对(id^*,C_v^*)进行解密询问.

(5)猜测 最终,敌手 A 输出对随机数 v 的猜测 $v'\in\{0,1\}$,如果 $v'=v$,则敌手 A 攻击成功.

分析发现,上述证明过程的挑战阶段出现了问题,模拟器 C 通过计算 $c_1=Zm_v$ 隐含的设置使用随机数 c 对消息 m_v 进行加密,并且密文元素 c_2,c_4 和 c_5 计算所需的随机数 c 与 $Z=e(g,g)^{abc}$中的 c 是相同的,而对于模拟器 C 而言,随机数 c 是未知的,因为 c 是来自 DBDH 困难问题的随机数. 因此证明过程的随机数 c 是不能由模拟器 C 随机选取. 由于 $g_1=g^a$,那么在计算 $c_2=g_1^{\mathrm{id}^*\cdot(c+p)}$ 时,模拟器 C 将面临计算 g^{ac},而对于 C 而言是无能力计算 g^{ac}的,因此原始的证明过程是不成立的. 综上所述,虽然文献[13]给出了基于 DBDH 假设的证明过程,但是该过程是不严谨的,导致原始方案并不满足其所声称的 CCA 安全性.

4 结论

文献[13]提出了一种在标准模型下可证明安全的可公开验证的 IBE 方案,并基于静态假设 DBDH 假设证明了该方案的安全性. 然而,本文在 IBE 机制的安全模型下对该方案进行了分析,发现该方案并不满足其所声称的 CCA 安全性,即任意敌手能够基于合法密文伪造出一个关于新消息的合法密文,给出了具体的攻击方法,并指出了原文安全性证明中的不合理之处.

参考文献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Annual International Cryptology Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg:Springer,1985. 47 – 53.

[2] BONEH D,FRANKLIN M. Identity-based encryption from the weil pairing[A]. Annual International Cryptology Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2001. 213 – 229.

[3] BONEH D,BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles[A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2004. 223 – 238.

[4] BONEH D, BOYEN X. Secure identity-based encryption without random oracles[A]. Annual International Cryptology Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2004. 443 – 459.

[5] WATERS B. Efficient identity-based encryption without random oracles[A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg:Springer,2005. 114 – 127.

[6] GENTRY C. Practical identity-based encryption without random oracles[A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg:Springer,2006. 445 – 464.

[7] 李大伟,杨庚,朱莉. 一种基于身份加密的可验证秘密共享方案[J]. 电子学报,2010,38(9):2059 – 2065.
LI Da-wei,YANG Gen,ZHU Li. An ID-based verifiable secret sharing scheme[J]. Acta Electronica Sinica,2010,38

(9):2059 – 2065. (in Chinese)
[8] 明洋,王育民. 标准模型下可证安全的通配符基于身份加密方案[J]. 电子学报,2013,41(10):2082 – 2086.
MING Yang, WANG Yu-min. Provably secure identity-based encryption scheme with wildcard in the standard model[J]. Acta Electronica Sinica, 2013, 41(10): 2082 – 2086. (in Chinese)
[9] HU M X, Ye Q, Tang Y L. Efficient batch identity-based fully homomorphic encryption scheme in the standard model[J]. IET Information Security, 2018, 12(6): 475 – 483.
[10] LI X G, XIANG T, CHEN F, GUO S W. Efficient biometric identity-based encryption[J]. Information Sciences, 2018, 465: 248 – 264.
[11] WU L B, ZHANG Y B, CHOO K K, HE D B. Efficient and secure identity-based encryption scheme with equality test in cloud computing[J]. Future Generation Computer Systems, 2017, 73: 22 – 31.
[12] HAN S, LIU S L, QIN B D, GU D W. Tightly CCA-secure identity-based encryption with ciphertext pseudorandomness[J]. Designs, Codes and Cryptography, 2018, 86(3): 517 – 554.
[13] 李顺东,杨坤伟,巩林明,毛庆,刘新. 标准模型下可公开验证的匿名 IBE 方案[J]. 电子学报,2016,44(3),673 – 678.
LI Shun-dong, YANG Kun-wei, GONG Lin-ming, MAO Qing, LIU Xin. A publicly verifiable anonymous IBE scheme in the standard model[J]. Acta Electronica Sinica, 2016, 44(3), 673 – 678. (in Chinese)

作者简介

杨启良　男,1991 年 6 月出生于陕西省西安市. 现为陕西师范大学计算机科学学院博士生. 从事密码学、信息安全的研究工作
E-mail:yangqiliang@ snnu. edu. cn

周彦伟(通信作者)　男,1986 年 4 月出生于甘肃省通渭县. 博士,硕士研究生导师. 现为陕西师范大学计算机科学学院高级工程师,从事密码学、信息安全的研究工作.
E-mail:zyw@ snnu. edu. cn