标准模型下可证安全的通配符基于身份加密方案

明 洋[1],王育民[2]
(1.长安大学信息工程学院,陕西西安 710064;2.西安电子科技大学综合业务网理论及关键技术国家重点实验室,陕西西安 710071)

摘 要: 针对通配符基于身份加密方案中安全归约不紧密以及运算量大的缺陷,利用双线性对和分级基于身份加密的思想提出标准模型下可证安全的通配符基于身份加密方案.新方案取得紧密的安全归约,同时加密算法不需要对运算,解密算法仅仅需要 2 个对运算.安全性分析表明,基于改进判定双线性 Diffie-Hellman 指数假设下,所提方案在适应性选择密文和通配符身份攻击下满足不可区分性.

关键词: 基于身份加密; 标准模型; 通配符; 双线性对
中图分类号: TP918.1 **文献标识码:** A **文章编号:** 0372-2112 (2013) 10-2082-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.10.032

Provably Secure Identity-Based Encryption Scheme with Wildcard in the Standard Model

MING Yang[1], WANG Yu-min[2]
(1. *School of Information Engineering, Chang'an University, Xi'an, Shaanxi* 710064, *China*;
2. *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: Based on the bilinear pairings and hierarchical identity-based encryption, an identity-based encryption with wildcard is proposed to overcome the loose security reduction and computation inefficiency of the known schemes. Our proposed scheme is provably secure in the standard model which captures tight secure reduction. In our scheme, no pairing computation is needed in the encrypt algorithm and the decrypt algorithm requires only two pairings computations. A security analysis shows that the proposed scheme has the indistinguishability against adaptive chosen ciphertext and identity with wildcard attack under the assumption of Decision Modify Bilinear Diffie-Hellman Exponent.

Key words: Identity-based encryption; standard model; wildcard; bilinear pairings

1 引言

1984 年 Shamir[1]提出基于身份公钥密码学(Identity-Based Public Key Cryptography, ID-PKC)的概念,简化公钥证书的管理,避免基于目录公钥认证框架的束缚.该系统直接使用用户身份信息(如 IP 地址,电子邮件地址等)作为公钥,私钥由可信第三方——密钥生成器(Private Key Generator, PKG)生成,自然地解决了公钥和用户身份的绑定问题.2001 年 Boneh 和 Franklin 两位学者[2]利用双线性对提出高效的基于身份加密(Identity-Based Encryption, IBE)方案,在随机预言机模型中证明该方案在适应性选择密文和身份攻击下是不可区分的(IND-ID-CCA2).自从 IBE 提出以来,利用 IBE 思想构建出许多其他密码技术,如:密码共享[3],密钥分配[4]等.

考虑现实场景:Alice 希望发送加密邮件给公司所有职员(邮件地址分别为 A@group.com; B@group.com; C@group.com 等).如果利用传统 IBE 技术,需要分别使用每个职员邮件地址进行加密,那么当职员数量非常庞大时,该方法是不现实的.为了解决该问题,2006 年 Abdalla 等学者[5,6]提出通配符基于身份加密(Identity-Based Encryption with Wildcard, WIBE),该方案中 Alice 使用通配符(用 * 表示)来替换职员身份(邮件地址)的某些部分(* @group.com).利用该邮件地址 Alice 发送加密邮件时,只有特定身份(邮件地址)的职员能够解密,也就是说密文能够被具有相关身份的多个接收者同时解密.

2002 年,Gentry 和 Silverberg 两位学者[7]扩展 IBE 首次提出分级基于身份加密(Hierarchical Identity-based Encryption, HIBE)的思想,且大量 HIBE 方案[8~12]被提出.

收稿日期:2011-12-27;修回日期:2013-05-17;责任编辑:马兰英
基金项目:国家自然科学基金(No.61202438);陕西省自然科学基金(No.2010JQ8017);中国博士后科学基金(No.2011M501427);西安市科技计划项目(No.CX1258③);中央高校基本科研业务费专项基金,长安大学基础研究支持计划专项基金(No.CHD2012JC047)

文献[6]分别基于 BB-HIBE[8]和 BBG-HIBE[10]提出随机预言机模型下安全的 WIBE 方案(分别记为 BB-WIBE 和 BBG-WIBE);基于 W-HIBE[9]提出标准模型下安全的 WIBE 方案(记为 W-WIBE).2007 年 Birkeet 等学者[13]扩展 WIBE 方案到混合加密(KEM-DEM)的框架下.2009 年,Ming 等学者[14]基于 CS-HIBE[11]提出标准模型下安全的 WIBE 方案(记为 CS-WIBE),取得短的系统参数和密文.目前已知的 WIBE 方案中,一方面安全性是基于弱 Selective-ID 模型(攻击者在安全性证明之前先确定挑战目标的身份),为了实现强 Adaptive-ID 模型(攻击者可以适应性选取挑战目标的身份)而导致安全归约不紧密;另一方面安全性仅仅满足选择明文攻击(Choose Plaintext Attack,CPA),为了取得选择密文攻击(Choose Ciphertext Attack,CCA)下的安全性,利用 Canetti 技术[15](一次签名),增加了方案的复杂性.

本文基于 HIBE 方案[12],首次提出 Adaptive-ID 模型下可证安全且满足紧密安全归约通配符基于身份加密方案.基于判定性改进的双线性 Diffie-Hellman 指数(Decision Modify Bilinear Diffie-Hellman Exponent,DMBDHE)假设下,证明所提方案在标准模型中适应性选择密文和通配符身份攻击下是不可区分的(IND-WID-CCA2).分析表明所提方案不需要使用 Canetti 等学者[15]技术而直接取得 CCA 安全性,加密算法不需要对运算,解密算法仅仅需要 2 个对运算,因此所提方案更加安全高效.

2　基础知识

2.1　双线性对

设$(G_1,+)$是由 g 生成的加法群,阶数为素数 p,$(G_2,\cdot)$是乘法群,阶数为素数 p.设 $e:G_1\times G_1\rightarrow G_2$ 是一个映射,具有下面的性质:

(1)双线性性:对所有的 $u,v\in G_1$,$a,b\in Z_p$,都有 $e(u^a,v^b)=e(u,v)^{ab}$;(2)非退化性:$e(g,g)\neq 1$;(3)可计算性:对所有的 $u,v\in G_1$,存在有效的算法计算 $e(u,v)$.

那么 e 称为双线性对.

2.2　困难问题

q 改进双线性 Diffie-Hellman 指数(q-MBDHE)问题[10]:给定$(g',g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in G_1^{q+2}$,其中 $\alpha\in Z_p^*$,计算 $e(g',g)^{\alpha^{q+1}}$.

q 判定性改进双线性 Diffie-Hellman 指数(q-DMBDHE)问题:给定$(g',g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q},Z)\in G_1^{q+2}\times G_2$,其中 $\alpha\in Z_p^*$,判定 $e(g',g)^{\alpha^{q+1}}=Z$ 是否成立.

定义算法 B 成功解 q-DMBDHE 问题的优势为:

$$Adv_B=|Pr[B(g',g,g^{\alpha},\cdots,g^{\alpha^q},e(g,g')^{\alpha^{q+1}})=1]-Pr[B(g',g,g^{\alpha},\cdots,g^{\alpha^q},Z)=1]|$$

这里 α 是 Z_p^* 中随机选取,Z 是 G_2 中随机选取.

对于 q-DMBDHE 问题而言,文献[10]中指出如果 q 判定性双线性 Diffie-Hellman 指数问题(q-DBDHE)困难,则 q-DMBDHE 问题是困难的.同时,文献[16]首次提出 q 判定性 Augmented 双线性 Diffie-Hellman 指数问题(q-DABDHE),并证明该问题等价于 q 判定性双线性 Diffie-Hellman 逆问题(q-DBDHI)[8].很显然,如果 q-DMBDHE 问题可解,则 q-DABDHE 问题可解.因此,所提方案基于的 q-DMBDHE 问题至少和 q-DABDHE 问题以及 q-DBDHI 问题具有相同的困难度.

3　通配符基于身份加密方案

通配符基于身份加密(WIBE)方案[6,14]包含 4 个多项式时间算法:系统建立算法,密钥生成算法,加密算法和解密算法.安全性需要满足适应性选择密文和通配符身份攻击下的不可区分性(IND-WID-CCA2).

4　方案构造

系统建立　PKG 随机选取生成元 $g\in G_1$ 和 $\alpha\in Z_p^*$,计算 $g_1=g^{\alpha}$.随机选取 $g_2,g_3,h_0,h',h_1,\cdots,h_L\in G_1^{L+4}$,选取抗碰撞哈希函数 $H_1:\{0,1\}^*\rightarrow Z_p^*$,$H_2:\{0,1\}^*\rightarrow Z_p^*$.选取一次多项式 $f(x)=ax+b$ 其中 $a,b\in Z_p^*$,如果 $g_2=g_3^{-a}$或 $h_0=g_3^{-b}$,则重新选取 $f(x)$.则系统参数为 $\psi=(g,g_1,g_2,g_3,h_0,h',h_1,\cdots,h_L,H_1,H_2,f(x))$,主密钥为 $\Phi=\alpha$.

密钥生成　对于身份 $ID|_l=(ID_1,ID_2,\cdots,ID_l)$($l\leqslant L$),随机选取 $r',r''\in Z_p^*$,计算私钥为

$$d_{ID|_l}=(d_0,d_{-1},d_{-2},d_{-3},d_{l+1},\cdots,d_L)$$

$$=((h_0g_2^{r'}g_3^{f(r')})^{\alpha}(\prod_{k=1}^{l}h'h_k^{ID_k})^{r''},r',g^{r''},(h')^{r''},h_{l+1}^{r''},\cdots,h_L^{r''})$$

已知身份 $ID|_{l-1}=(ID_1,ID_2,\cdots,ID_{l-1})$的私钥 $d_{ID|_{l-1}}=(d_0,d_{-1},d_{-2},d_{-3},d_l,\cdots,d_L)$,随机选取 $t\in Z_p^*$ 计算 $ID|_l=(ID_1,ID_2,\cdots,ID_l)$的私钥为

$$d_{ID|_l}=(d'_0,d'_{-1},d'_{-2},d'_{-3},d'_{l+1},\cdots,d'_L)$$

$$=(d_0\cdot d_{-3}\cdot d_l^{ID_l}\cdot(\prod_{k=1}^{l}h'h_k^{ID_k})^t,d_{-1},d_{-2}\cdot g^t,d_{-3}\cdot(h')^t,d_l\cdot h_l^t,\cdots,d_L\cdot h_L^t)$$

加密　消息 $m\in G_2$ 在模式 $P=(P_1,P_2,\cdots,P_l)$下加密,随机选取 $s\in Z_p^*$,计算

$$C_1=g^s,C_2=e(g_1,g_2)^s,$$

$$C_3=e(g_1,g_3)^s,(C_{4,i})_{i\in\overline{W}(P)}=(h'\cdot h_i^{P_i})^s,$$

$$(C_{5,i})_{i\in W(P)}=h_i^s,C_6=(h')^s,C_7=m\cdot e(g_1,h_0)^{s+\eta},$$

这里

$$\eta=H_1(C_1,C_2,C_3,(C_{4,i})_{i\in\overline{W}(P)},(C_{5,i})_{i\in W(P)},C_6,e(g_1,h_0)^s),$$

$\xi = H_2(C_1, C_2, C_3, (C_{4,i})_{i\in\overline{W}(P)}, (C_{5,i})_{i\in W(P)}, C_6, C_7, m, m\cdot e(g_1,h_0)^s)$.

则密文为

$C = (C_1, C_2, C_3, (C_{4,i})_{i\in\overline{W}(P)}, (C_{5,i})_{i\in W(P)}, C_6, C_7, \xi)$.

解密 如果身份 $ID|_l = (ID_1, ID_2, \cdots, ID_l)$匹配模式 $P = (P_1, P_2, \cdots, P_l)$,即 $ID|_l \in_* P$,计算

(1) $C_{W,i} = \begin{cases} C_{4,i}, & i\in\overline{W}(P) \\ C_6\cdot C_{5,i}^{ID_i}, & i\in W(P) \end{cases}$.

(2) $\eta = H_1\left(C_1, C_2, C_3, (C_{4,i})_{i\in\overline{W}(P)}, (C_{5,i})_{i\in W(P)}, C_6, \frac{e(d_0, C_1)}{C_{2^{-1}}^d\cdot C_3^{f(d_{-1})}\cdot e\left(\prod_{i=1}^{l} C_{W,i}, d_{-2}\right)}\right)$.

(3) $\frac{C_6}{e(g_1,h_0)^\eta \frac{e(d_0,C_1)}{C_{2^{-1}}^d\cdot C_3^{f(d_{-1})}\cdot e\left(\prod_{i=1}^{l} C_{W,i}, d_{-2}\right)}} = m$.

(4) $\xi' = H_2\left(C_1, C_2, C_3, (C_{4,i})_{i\in\overline{W}(P)}, (C_{5,i})_{i\in W(P)}, C_6, C_7, m, m\cdot\frac{e(d_0,C_1)}{C_{2^{-1}}^d\cdot C_3^{f(d_{-1})}\cdot e\left(\prod_{i=1}^{l} C_{W,i}, d_{-2}\right)}\right)$,

检验 $\xi' = \xi$ 是否成立.如果成立,则密文是有效的;否则返回错误信息.

5 方案分析

5.1 正确性

$$\frac{e(d_0,C_1)}{C_{2^{-1}}^d\cdot C_3^{f(d_{-1})}\cdot e(\prod_{i=1}^{l} C_{W,i}, d_{-2})}$$

$$= \frac{e\left((h_0 g_2^{r'} g_3^{f(r')})^\alpha\cdot(\prod_{k=1}^{l} h' h_k^{ID_k})^{r''}, g^s\right)}{e(g_1,g_2)^{sr'}\cdot e(g_1,g_3)^{sf(r')}\cdot e\left((\prod_{k=1}^{l} h' h_k^{ID_k})^s, g^{r''}\right)}$$

$$= \frac{e(h_0^\alpha, g^s)\cdot e(g_2^{r'\alpha}, g^s)\cdot e(g_3^{f(r')\alpha}, g^s)\cdot e\left((\prod_{k=1}^{l} h' h_k^{ID_k})^{r''}, g^s\right)}{e(g^\alpha,g_2)^{sr'}\cdot e(g^\alpha,g_3)^{sf(r')}\cdot e\left((\prod_{k=1}^{l} h' h_k^{ID_k})^s, g^{r''}\right)}$$

$$= e(g_1,h_0)^s$$

5.2 安全性

$$\begin{aligned} d_0 &= (g^{\sum_{i=0}^{q-1}(a_i + r' b_i + f(r') c_i)\alpha^{i+1}})\cdot(\prod_{k=1}^{l} h' h_k^{ID_k})^{r''} \\ &= g^{(a_0\alpha + a_1\alpha^2 + \cdots + a_{q-1}\alpha^q) + (b_0\alpha + b_1\alpha^2 + \cdots + b_{q-1}\alpha^q) r' + (c_0\alpha + c_1\alpha^2 + \cdots + c_{q-1}\alpha^q) f(r') + (a_q + b_q r' + c_q f(r'))\alpha^{q+1}} \\ &= g^{(a_0\alpha + a_1\alpha^2 + \cdots + a_{q-1}\alpha^q + a_q\alpha^{q+1}) + (b_0\alpha + b_1\alpha^2 + \cdots + b_{q-1}\alpha^q + b_q\alpha^{q+1}) r' + (c_0\alpha + c_1\alpha^2 + \cdots + c_{q-1}\alpha^q + c_q\alpha^{q+1}) f(r')} \\ &= (g^{a_0 + a_1\alpha + \cdots + a_q\alpha^q} g^{b_0 + b_1\alpha + \cdots + b_q\alpha^q})^{c_0 + c_1\alpha + \cdots + c_q\alpha^q})^\alpha \\ &= (g^{f_1(\alpha)} g^{f_2(\alpha) r'} g^{f_3(\alpha) f(r')})^\alpha \\ &= (h_0 g_2^{r'} g_3^{f(r')})^\alpha. \end{aligned}$$

$d'_{-3} = g^{u' r''} = (h')^{r''}$, $d_{l+1} = g^{u_{l+1} r''} = h_{l+1}^{r''}$, $d_L = g^{u_L r''} = h_L^{r''}$.

解密询问 攻击者 A 对消息 m 在模式 P 下的密文 $C = (C_1, C_2, C_3, (C_{4,i})_{i\in\overline{W}_p}, (C_{5,i})_{i\in W_p}, C_6, C_7, \xi)$ 进行解密询问时,B 首先进行私钥提取询问得到私钥,然后运行解密算法,如果通过验证,B 返回 A 相应的明文,否则输出错误信息.

定理 1 如果攻击者 A 在时间 t' 内,q_k 次私钥询问,q_d 次解密询问后,能够以不可忽略的概率 ε' 攻破所提方案,那么存在一个算法 B 以 $t = t' + O(t_e q L) + O(t_p q)$,$\varepsilon \geqslant \varepsilon' - \frac{1}{p-1}$ 解 q-DMBDHE 问题,这里 t_e 表示群 G_1 中计算一个指数时间,t_p 表示计算一个对的时间.

证明 算法 B 把 A 作为子程序来解决一个随机 q-DMBDHE 问题的实例,即给定 $(g', g, g^\alpha, g^{\alpha^2}, \cdots, g^{\alpha^q}, Z)$ 下判定 $e(g',g)^{\alpha^{q+1}} = Z$ 是否成立.

算法 B 模拟不可区分性中的挑战者和攻击者 A 交互如下:

系统建立 B 随机选取 $u', u_1, u_2, \cdots, u_L \in (Z_p^*)^{L+1}$,$q$ 次多项式 $f_1(x), f_2(x), f_3(x) \in Z_p^*[x]$,满足 $f_1(x) = \sum_{i=0}^{q} a_i x^i$, $f_2(x) = \sum_{i=0}^{q} b_i x^i$, $f_3(x) = \sum_{i=0}^{q} c_i x^i$. 令 $g_1 = g^\alpha$, $h_0 = g^{f_1(\alpha)}$, $g_2 = g^{f_2(\alpha)}$, $g_3 = g^{f_3(\alpha)}$, $h' = g^{u'}$, $h_1 = g^{u_1}, g^{u_2}, \cdots, h_L = g^{u_L}$, $f(x) = -\frac{b_q}{c_q}x - \frac{a_q}{c_q}$. 如果 $g_2 = g_3^{\frac{b_q}{c_q}}$ 或者 $h_0 = g_3^{\frac{a_q}{c_q}}$,则重新选择 $f_1(x), f_2(x), f_3(x)$. B 返回系统参数 $\psi = (g, g_1, g_2, g_3, h_0, h', f(x), h_1, h_2, \cdots, h_L)$给 A.

阶段 1 攻击者 A 适应性进行多项式有界次以下询问.

私钥询问 当 A 询问 $ID|_l = (ID_1, ID_2, \cdots, ID_l)$ $(l \leqslant L)$的私钥时,B 执行操作:

(1)如果 $ID = \alpha$,B 直接使用 α 解 q-DMBDHE 问题.

(2)如果 $ID \neq \alpha$,B 随机选取 $r', r'' \in Z_p^*$,计算

$$\begin{aligned} d_{ID|_l} &= (d_0, d_{-1}, d_{-2}, d_{-3}, d_{l+1}, \cdots, d_L) \\ &= \left(g^{\sum_{i=0}^{q-1}(a_i + r' b_i + f(r') c_i)\alpha^{i+1}} \cdot (\prod_{k=1}^{l} h' h_k^{ID_k})^{r''}, r', g^{r''}, g^{u' r''}, g^{u_{l+1} r''}, \cdots, g^{u_L r''}\right) \end{aligned}$$

正确性 由 $f(r') = -\frac{b_q}{c_q}r' - \frac{a_q}{c_q}$可知 $a_q + b_q r' + c_q f(r') = 0$,

挑战 当 A 决定结束阶段 1 后,发送 $P^* = (P_1^*, P_2^*, \cdots, P_l^*)$以及 m_0, m_1 给 B,B 随机选取 $b \in \{0,1\}$计算

$C_1^* = g'$, $C_2^* = Z^{b_0} e(g',g)^{\sum_{i=0}^{q-1} b_i \alpha^{i+1}}$,

$$C_3^* = Z^{c_q} e(g', g)^{\sum_{i=0}^{q-1} c_i \alpha^{i+1}},$$

$$(C_{4,i}^*)_{i \in \overline{W}(P^*)} = (g')^{u'} \cdot (g'^{u_i})^{P_i}, (C_{5,i}^*)_{i \in W(P^*)} = (g')^{u_i},$$

$$C_{W,i}^* = \begin{cases} \text{malignmark} / > C_{4,i}^*, & i \in \overline{W}(P^*) \\ C_6^* \cdot (C_{5,i})^{P_i^*}, & i \in W(P^*) \end{cases},$$

$$C_6^* = (g')^{u'}, C_7^* = m_b \cdot Z^{a_q} e(g', g)^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}} \cdot e(g_1, h_0)^{\eta^*},$$

$$\eta^* = H_1\Big(C_1^*, C_2^*, C_3^*, (C_{4,i}^*)_{i \in \overline{W}(P^*)}, (C_{5,i}^*)_{i \in W(P^*)}, C_6^*, \frac{e(d_0^*, C_1^*)}{(C_2^*)^{d_{-1}^*} \cdot (C_3^*)^{f(d_{-1}^*)} \cdot e(\prod_{i=1}^{l} C_{W,i}^*, d_{-2}^*)} \Big),$$

$$\xi^* = H_2\Big(C_1^*, C_2^*, C_3^*, (C_{4,i}^*)_{i \in \overline{W}(P^*)}, (C_{5,i}^*)_{i \in W(P^*)}, C_6^*, C_7^*, m_b, m_b \cdot \frac{e(d_0^*, C_1^*)}{(C_2^*)^{d_{-1}^*} \cdot (C_3^*)^{f(d_{-1}^*)} \cdot e(\prod_{i=1}^{l} C_{W,i}^*, d_{-2}^*)} \Big)$$

B 返回

$C^* = (C_1^*, C_2^*, C_3^*, (C_{4,i}^*)_{i \in \overline{W}(P^*)}, (C_{5,i}^*)_{i \in W(P^*)}, C_6^*, C_7^*, \xi^*)$ 给攻击者 A.

正确性　令 $s^* = \log_g g'$,如果 $Z = e(g, g')^{\alpha^{q+1}}$,则

$$C_1^* = g' = g^{s^*}$$

$$C_2^* = Z^{b_q} e(g', g)^{\sum_{i=0}^{q-1} b_i \alpha^{i+1}}$$

$$= e(g', g)^{b_q \alpha^{q+1}} e(g', g)^{b_0 \alpha + b_1 \alpha^2 + \cdots + b_{q-1} \alpha^q}$$

$$= e(g', g)^{b_q \alpha^{q+1} + b_0 \alpha + b_1 \alpha^2 + \cdots + b_{q-1} \alpha^q} = e(g', g)^{f_2(\alpha)\alpha}$$

$$= e(g', g_2)^{\alpha} = e(g^{s^*}, g_2)^{\alpha} = e(g_1, g_2)^{s^*}$$

$$C_3^* = Z^{c_q} e(g', g)^{\sum_{i=0}^{q-1} c_i \alpha^{i+1}} = e(g_1, g_3)^{s^*}$$

$$(C_{4,i}^*)_{i \in \overline{W}(P^*)} = (g')^{u'} \cdot (g'^{u_i})^{P_i^*} = (g^{s^*})^{u'} (g^{s^* u_i})^{P_i^*}$$

$$= (g^{u'} g^{u_i P_i^*})^{s^*} = (h' h_i^{P_i^*})^{s^*}$$

$$(C_{5,i}^*)_{i \in W(P^*)} = (g')^{u_i} = g^{s^* u_i} = h_i^{s^*}$$

$$C_6^* = (g')^{u'} = g^{s^* u'} = (h')^{s^*}$$

$$C_7^* = m_b \cdot Z^{a_q} e(g', g)^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}} \cdot e(g_1, h_0)^{\eta^*}$$

$$= m_b \cdot e(g_1, h_0)^{s^*} \cdot e(g_1, h_0)^{\eta^*} = m_b \cdot e(g_1, h_0)^{s^* + \eta^*}$$

$$\frac{e(d_0^*, C_1^*)}{(C_2^*)^{d_{-1}^*} \cdot (C_3^*)^{f(d_{-1}^*)} \cdot e(\prod_{i=1}^{l} C_{W,i}, d_{-2}^*)}$$

$$= \frac{e\Big((h_0 g_2^{r'^*} g_3^{f(r'^*)})^{\alpha} \cdot (\prod_{i=1}^{l} h' h_i^{P_i^*})^{r'^*}, g^{s^*} \Big)}{e(g_1, g_2)^{s^* r'^*} \cdot e(g_1, g_3)^{s^* f(r'^*)} \cdot e\Big((\prod_{i=1}^{l} h' h_i^{P_i^*})^{s^*}, g^{r'^*} \Big)}$$

$$= e(g_1, h_0)^{s^*}$$

阶段 2　和阶段 1 相同,除了 A 不能对 $P^* = (P_1^*, P_2^*, \cdots, P_l^*)$ 以及前缀进行私钥询问;不能对 (P^*, C^*) 进行解密询问.

猜测　A 输出 b'. 如果 $b' = b$,B 输出 1;否则输出 0.

概率分析　如果 Z 是群 G_1 中的随机元素,B 模拟的挑战密文和真实密文具有相同的概率分布,因此 A 正确猜测比特 b 的概率为 $\frac{1}{2} + \varepsilon'$,即 $\Pr[B(g', g, g^{\alpha}, \cdots, g^{\alpha^q}, Z) = 1] \geqslant \frac{1}{2} + \varepsilon'$.

如果 $Z = e(g, g')^{\alpha^{q+1}}$ 时,$s^* = \log_g g'$ 是随机元素,η^* 是随机元素,则 $s^* + \eta^* = 0$ 的概率为 $\frac{1}{p-1}$,因此 A 正确猜测比特 b 的概率为 $\frac{1}{2} + \frac{1}{p-1}$,即

$$Pr[B(g', g, g^{\alpha}, \cdots, g^{\alpha^q}, e(g, g')^{\alpha^{q+1}}) = 1] = \frac{1}{2} + \frac{1}{p-1}.$$

因此,算法 B 解 q-DMBDHE 问题的优势为

$$|Pr[B(g', g, g^{\alpha}, \cdots, g^{\alpha^q}, e(g, g')^{\alpha^{q+1}}) = 1] - Pr[B(g', g, g^{\alpha}, \cdots, g^{\alpha^q}, Z) = 1]|$$

$$\geqslant |\frac{1}{2} + \frac{1}{p-1} - \frac{1}{2} - \varepsilon'| \geqslant \varepsilon' - \frac{1}{p-1}.$$

时间分析　B 的运行时间为解困难问题的时间以及回答私钥询问和解密询问的时间. 每次私钥询问需要群 G_1 中 $O(L)$次指数运算,每次解密询问需要群 G_1 中 $O(L)$次指数运算和 $O(1)$次对运算. A 最多进行 $q-1$ 次询问,则 $t = t' + O(t_e q L) + O(t_p q)$. 证毕.

5.3　效率分析

表 1 中从安全模型,系统参数长度,密钥长度,密文长度,对运算量,安全归约以及是否使用随机预言机模型 7 个方面比较所提 WIBE 方案和目前已知的 WIBE 方案[6,14],其中 L 表示最大分级,n 表示身份比特长度,q_H 表示哈希函数询问次数,q_k 表示私钥询问次数,$O(\cdot)$ 表示高阶无穷小,*RO* 表示随机预言机模型,Loose 表示不紧密安全归约,Tight 表示紧密安全归约. 从表 1 中可

表 1　通配符基于身份加密方案效率和安全性质比较

方案	安全模型	系统参数长度	密钥长度	密文长度	对运算	RO	安全归约(损失因子)
[6]BB-WIBE	IND-WID-CPA	$O(L)$	$O(L)$	$O(L)$	$O(L)$	√	Loose $O(\frac{1}{(Lq_H)^L})$
[6]BBG-WIBE	IND-WID-CPA	$O(L)$	$O(L)$	$O(L)$	$O(1)$	√	Loose $O(\frac{1}{(Lq_H)^L})$
[6]W-WIBE	IND-WID-CPA	$O(nL)$	$O(L)$	$O(nL)$	$O(L)$	×	Loose $O(\frac{1}{2^L})$
[14]CS-WIBE	IND-WID-CPA	$O(L)$	$O(L)$	$O(L)$	$O(L)$	×	Loose $O(\frac{1}{(q_k n)^L})$
本文方案	IND-WID-CCA2	$O(L)$	$O(L)$	$O(L)$	$O(1)$	×	Tight $O(1)$

以看出和标准模型下安全的 W-WIBE[6] 和 CS-WIBE[14] 方案相比,所提方案具有短系统参数和密文长度,以及少量的对运算,同时取得 CCA 安全性和紧密安全归约.

6 结论

通配符基于身份加密(WIBE)是基于身份加密(IBE)的泛化形式,具有更加广泛的应用.本文利用双线性对和分级基于身份加密的思想提出标准模型下可证安全的 WIBE 方案.基于 q-DMBDHE 假设下,证明所提方案在适应性选择密文和通配符身份攻击下是安全的,同时取得紧密安全归约,加密算法中不需要使用对运算,解密算法中仅仅需要 2 个对运算,因此本文所提方案效率更高,更加适合现实中的应用.

参考文献

[1] A Shamir. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology-Crypto 1984[C]. LNCS 0196, Berlin: Springer-Verlag, 1984. 47 – 53.

[2] D Boneh, M Franklin. Identity-based encryption from the Weil pairing[A]. Advances in Cryptology-Crypto 2001[C]. LNCS 2139, Berlin: Springer-Verlag, 2001. 213 – 229.

[3] 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 Geng, ZHU Li. An ID based verifieable secret sharing scheme[J]. Acta Electronica Sinica, 2010, 38(9): 2059 – 2065. (in Chinese)

[4] 杨庚,等.基于身份加密的无线传感器网络密钥分配方法[J].电子学报,2007,35(1):180 – 184.
YANG Geng, et al. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms[J]. Acta Electronica Sinica, 2007, 35(1): 180 – 184. (in Chinese)

[5] M Abdalla, D Catalano, A. W Dent, et al. Identity-based encryption gone wild[A]. Proceedings of International Colloquium on Automata, Languages and Programming-ICALP 2006 [C]. LNCS 4052, Berlin: Springer-Verlag, 2006. 300 – 311.

[6] M Abdalla, D Catalano, A W Dent, et al. Identity-Based encryption gone wild [J/OL]. http://eprint. iacr. org/2006/304, 2009 – 12 – 20.

[7] C Gentry, A Silverberg. Hierarchical ID – based cryptography [A]. Advances in Cryptology-Asiacrypt 2002 [C]. LNCS 2501, Berlin. Springer-Verlag, 2002. 548 – 566.

[8] D Boneh, X Boyen. Efficient selective-ID secure identity based encryption without random oracles[A]. Advances in Cryptology-Eurocrypt 2004[C]. LNCS 3027, Berlin. Springer-Verlag, 2004. 223 – 238.

[9] B Waters. Efficient Identity-based encryption without random oracles[A]. Advances in Cryptology-Eurocrypt 2005 [C]. LNCS 3494, Berlin: Springer-Verlag, 2005. 114 – 127.

[10] D Boneh, X Boyen, E.-J Goh. Hierarchical identity based encryption with constant size ciphertext[A]. Advances in Cryptology-Eurocrypt 2005[C]. LNCS 3494, Berlin. Springer-Verlag, 2005. 440 – 456.

[11] S Chatterjee, P Sarkar. HIBE with short public parameters without random oracle[A]. Advances in Cryptology-Asiacrypt 2006[C]. LNCS 4284, Berlin. Springer-Verlag, 2006. 145 – 160.

[12] REN Yan-li, GU Da-wu. Secure hierarchical identity based encryption scheme in the standard model [A]. Progress in Cryptology-INDOCRYPT 2008 [C]. LNCS 5365, Berlin. Springer-Verlag, 2008. 104 – 115.

[13] J Birkett, A. W Dent, G Neven, et al. Efficient chosen-ciphertext secure identity-based encryption with wildcards[A]. Proceedings of Australasian Conference on Information Security and Privacy-ACISP 2007[C]. LNCS 4586, Berlin. Springer-Verlag, 2007. 274 – 292.

[14] MING Yang, SHEN Xiao-qin, WANG Yu-min. Identity-based encryption with wildcards in the standard model [J]. The Jounal of China Universities of Posts and Telecommunications, 2009, 16(1): 64 – 68.

[15] R Canetti, S Halevi, J Kate. A forward-secure public key encryption scheme[A]. Advances in Cryptology-Eurocrypt 2003 [C]. LNCS 2656, Berlin. Springer-Verlag, 2003. 255 – 271.

[16] C Gentry. Practical identity-based encryption without random oracles[A]. Advances in Cryptology-Eurocrypt 2006 [C]. LNCS 4004, Berlin. Springer-Verlag, 2006. 445 – 464.

作者简介

明 洋 男,1979 年 12 月生,陕西人.2002、2005 年在西安理工大学获理学学士、硕士学位,2008 年获西安电子科技大学工学博士学位.现为长安大学信息工程学院副教授,硕士生导师.主要从事密码学与信息安全研究.
E-mail: yangming@chd.edu.cn

王育民 男,1936 年 2 月生,北京人.现为西安电子科技大学通信工程学院教授、博士生导师.中国电子学会会士,中国密码学会荣誉理事,IEEE 高级会员,中国电子学会信息论学会委员,中国自然科学基金研究会会员,中山大学兼职教授.曾任全国高等学校通信和信息工程专业教学指导委员会主任,陕西省电子学会副理事长.主要从事通信、信息论、编码、密码理论与应用研究.
E-mail: ymwang@xidian.edu.cn