双系统加密技术下带通配符的基于身份加密方案*

张晓敏[1], 赵永斌[1], 刘克智[2]
(1. 石家庄铁道大学 信息与技术学院, 石家庄 050043; 2. 渤海石油职业学院, 河北 沧州 062552)

摘 要: 带通配符的基于身份加密方案(WIBE)大多存在以下缺陷:a)仅达到选择身份(selective-ID)安全,安全系数较低;b)其私钥或密文长度随身份级数呈线性递增,需要耗费大量的存储空间。针对上述问题,运用 Waters 的双系统加密技术,在 Lewko-HIBE 方案的基础上提出了一个密文长度固定的带通配符的分级加密方案。新方案结构紧凑,密钥和密文长度均为常数,加/解密运算速度快,减小了存储空间并提高了计算效率。新方案在标准模型下是适应性选择身份(adaptive-ID)安全的,也叫完全安全,安全级别较选择身份安全更高,并且其安全性可归约为三个静态假设。

关键词: 带通配符的基于身份加密; 双系统加密; 混合阶群; 适应性选择身份安全
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)05-1910-04
doi:10.3969/j.issn.1001-3695.2012.05.083

Wildcarded identity-based encryption using new techniques for dual system encryption

ZHANG Xiao-min[1], ZHAO Yong-bin[1], LIU Ke-zhi[2]
(1. *School of Information Science & Technology, Shijiazhuang Tiedao University, Shijiazhuang* 050043, *China*; 2. *Bohai Pertroleum Vocational College, Cangzhou Hebei* 062552, *China*)

Abstract: Most of the existing wildcarded identity-based encryption(WIBE) scheme have the following shortcomings: a) only to selective-ID secure, its secure factor is lower; b) the private key or the ciphertext length increases linearly with the identity level. To resolve these problems, this paper proposed a WIBE with constant ciphertext which based on Lewko-HIBE scheme by using Waters dual systems encryption. The novel scheme has a compact structure, the length of the key and ciphertext are constans, the encryption/decryption is speeded, which all reduce the storage space and improve the computation efficiency. The scheme is adaptive-ID secure(full secure) in the standard model, whose security level is higher than the selective-ID security, and the security is under three static assumptions.

Key words: WIBE; dual systems encryption; composite-order groups; adaptive-ID secure

0 引言

2002 年,Horwitz 等人[1]提出了基于身份分级加密(HIBE)的概念,解决了在基于身份加密(IBE)系统中 PKG 负担过重的问题。在 HIBE 结构中,用户呈树状分布,每层的用户可以为其下一层的子孙生成私钥。第一个标准模型下的基于身份分级加密方案是 Boneh 等人[2]在 2004 年提出的,但是其安全性证明基于一个较弱安全模型,即 selective-ID 安全模型。随后,Boneh 等人[3]提出了第一个密文长度固定的分级加密方案,但其安全性归约为一个较强的 q-BDHE 假设。

2006 年,Abdalla 等人[4]首次提出了带通配符的基于身份加密(WIBE)的概念,允许对分级结构中满足某种模式的集体身份进行加密。例如, 假设要发送电子邮件给 ECRYTP 工作组中的所有成员,其中包括个人地址 ECRYPT. Nigel、ECRYPR. Dario 和 ECRYPT. John。在传统 HIBE 系统中,需要分别对每个成员加密邮件;而在 WIBE 系统中,可以用"ECRYPT. ＊"对工作组中的所有成员加密邮件。Abdalla 提出的两个带通配符的基于身份加密方案在随机预言机模型下可证明 adaptive-ID 安全(完全安全),但在标准模型下仅能达到 selective-ID 安全,且两种方案的密文长度都不固定,与密文中所含通配符的个数相关。2009 年,Waters[5]提出的双系统加密技术可以使仅达到 selective-ID 安全的 WIBE 方案转换成可以达到 adaptive-ID 安全的 WIBE 方案。2011 年,Luo 等人[6]在 Waters 方案的基础上引入了混合身份机制,构造了一个新的 adaptive-ID 安全的 WIBE 方案,新方案的密文长度固定,但存在私钥长度过长。加/解密运算复杂等问题。

本文在 Lewko-HIBE[7]方案的基础上,结合双系统加密技术,提出了一个新的带通配符的基于身份加密方案。该方案的密文长度为常数,即密文长度不随模式个数的变化而变化。方案建立在混合阶数双线性群中,安全性归约为三个静态假设,并在标准模型下可证明是 adaptive-ID 安全的。

收稿日期: 2011-09-02; **修回日期**: 2011-10-30

作者简介:张晓敏(1986-),女,河北邯郸人,硕士,主要研究方向为密码学中基于身份密码体制(xiaomin_292@163.com);赵永斌,男,河北石家庄人,副教授,硕导,主要研究方向为网络与信息安全;刘克智,男,河北衡水人.

1　预备知识

1.1　混合阶双线性群

令 G、G_T 是混合阶数为 $N=p_1、p_2、p_3$ 的循环群,其中 p_1、p_2、p_3 为互异的大素数。双线性映射 $e:G\times G\to G_T$ 满足下列性质:

a)双线性。对任何 $g,h\in G;a,b\in Z_N$,总是有 $e(g^a,h^b)=e(g,h)^{ab}$。

b)非退化性。存在 $g\in G$,使得群 G_T 中存在等式 $e(g,g)=N$。

c)可计算性。存在有效算法,对于所有的 $g,h\in G$,均有 $e(g,h)\in G_T$。

令 G_{p_1}、G_{p_2} 和 G_{p_3} 为群 G 中阶数分别为 p_1、p_2 和 p_3 的子群,那么对任意的 $h_i\in G_{p_i}$ 和 $h_j\in G_{p_j}(i\neq j)$,有 $e(h_i,h_j)$ 为群 G_T 的基本元。也就是说,假设 $h_1\in G_{p_1},h_2\in G_{p_2},g$ 为群 G 的生成元,那么 $g^{p_1p_2}$ 可以生成群 G_{p_3},$g^{p_1p_3}$ 可以生成群 G_{p_2},$g^{p_2p_3}$ 可以生成群 G_{p_1}。所以对于任意随机数 $\alpha_1、\alpha_2、h_1=(g^{p_2p_3})^{\alpha_1}$ 和 $h_2=(g^{p_1p_3})^{\alpha_2}$,有 $e(h_1,h_2)=e(g^{\alpha_1},g^{p_3\alpha_2})^{p_1p_2p_3}=1$。称 G_{p_1}、G_{p_2} 和 G_{p_3} 的这一特性为正交性,作为理论工具,将被用来实现方案中私钥和密文的半功能性。

1.2　复杂性假设

本文给出的三个复杂性假设均为静态假设,即不随身份级数或者询问次数的变化而改变。令 $G_{p_1p_2}$ 表示群 G 中 p_1p_2 阶的子群。

假设 1　循环群系统 $(N=p_1p_2p_3,G,G_T,e)$。定义分布如下:$g\leftarrow G_{p_1},X_3\leftarrow G_{p_3},D=(g,X_3),T_1\leftarrow G_{p_1p_2},T_2\leftarrow G_{p_1}$,则定义攻击者 A 攻破假设 1 的优势为

$$\mathrm{Adv1}_A(\lambda)=|\Pr[A(D,T_1)=1]-\Pr[A(D,T_2)=1]|$$

假设 2　循环群系统 $(N=p_1p_2p_3,G,G_T,e)$。定义分布如下:$g,X_1\leftarrow G_{p_1},X_2,Y_2\leftarrow G_{p_2},X_3,Y_3\leftarrow G_{p_3},D=(\Gamma,g,X_1X_2,X_3,Y_2Y_3),T_1\leftarrow G,T_2\leftarrow G_{p_1p_3}$,则攻击者 A 攻破假设 2 的优势为

$$\mathrm{Adv2}_A(\lambda)=|\Pr[A(D,T_1)=1]-\Pr[A(D,T_2)=1]|$$

假设 3　循环群系统 $(N=p_1p_2p_3,G,G_T,e)$。定义分布如下:$\alpha,s\leftarrow Z_N,g,X_1\leftarrow G_{p_1},Y_2,Z_2\leftarrow G_{p_2},X_3\leftarrow G_{p_3},D=(\Gamma,g,g^{\alpha}X_2,X_3,g^sY_2,Z_2),T_1=e(g,g)^{\alpha s},T_2\leftarrow G_T$,则攻击者 A 攻破假设 3 的优势为

$$\mathrm{Adv3}_A(\lambda)=|\Pr[A(D,T_1)=1]-\Pr[A(D,T_2)=1]|$$

1.3　WIBE 方案的形式化定义及其安全模型

1.3.1　WIBE 方案的形式化定义

带通配符的基于身份加密方案(WIBE)是基于身份分级加密方案(HIBE)的一种扩展方案,即在加密阶段,发送方可以确保密文能被一组用户解密,该组用户满足一定模式。用向量 $P=(P_1,\cdots,P_L)\in\{0,1\}^*\cup\{*\}^L$ 描述这一模式,其中 $*$ 表示专用的通配符。$I\in P$ 表示身份 $I=(I_1,\cdots,I_l)$ 匹配模式 P,当且仅当 $l\leqslant L$,对所有的 $i=1,\cdots,l$,有 $I_i=P_i$ 或 $P_i=*$。令 $W(P)$ 表示在模式 P 中所有通配符的位置集合,即 $W(P)=\{1\leqslant i\leqslant L:P_i=*\}$。

一个 WIBE 方案由以下五个算法组成:

a)系统建立。输入安全参数 λ,返回主密钥 msk 和公共参数 pk。

b)私钥提取。输入主密钥 msk 和身份 I,生成私钥 sk_I。

c)私钥分发。给出第 k 层身份 $I=(I_1,\cdots,I_k)$ 和其相应的私钥 $\mathrm{sk}_{I|k}$,生成第 $k+1$ 层身份的私钥 $\mathrm{sk}_{I|k+1}$。

d)加密。输入模式 P 和消息 M,输出密文 C。

e)解密。输入匹配模式 P 的身份的私钥 sk_I,返回明文消息 m 或符号"⊥"表示解密失败。

1.3.2　WIBE 方案的安全模型

带通配符的基于身份加密方案的安全性通过追踪私钥的生成方式来定义,即判定私钥是由私钥提取算法直接生成的,还是由私钥分发算法派发的。

初始化:挑战者运行系统建立算法生成公共参数 pk,并发送给攻击者;同时初始化一个集合 $S=\varnothing$,用来记录已创建且未泄露的私钥。

阶段 1　该阶段攻击者发起如下三类询问:

a)Create。攻击者指定一个身份向量 I,挑战者通过调用私钥提取算法为该身份创建私钥,但并不直接发送给攻击者,而是将该私钥添加到集合 S 中,将集合 S 的索引发送给攻击者。

b)Delegate。攻击者指定集合 S 中的某个私钥 sk,并发送给挑战者一个身份 I'。挑战者运行私钥分发算法生成新的私钥,并将其添加到集合 S 中,将更新后的索引发送给攻击者。

c)Reveal。攻击者指定集合 S 中的某个私钥,挑战者把该私钥发送给攻击者,并从集合 S 中删除该私钥。对某私钥进行 reveal 询问后,将不再对该私钥进行 delegate 询问,因为攻击者可以运行私钥分发算法。

挑战:攻击者发送挑战消息 M_0、M_1 和挑战模式 P^* 给挑战者;挑战者随机选取 $b\in\{0,1\}$,加密消息 M_b 和 P^*,并把生成的密文发送给攻击者。

阶段 2　攻击者重复阶段 1 的询问。

猜测:攻击者输出一个猜测值 $b'\in\{0,1\}$。当 $b=b'$ 时,攻击者赢得游戏。

定义攻击者 A 赢得游戏的优势为

$$\mathrm{Adv}_A=\Pr[b^*=b]-1/2$$

1.4　改进的双系统加密技术

在 Waters 的双系统加密技术中,私钥和密文均有两种结构:标准态和半功能态。半功能态的私钥和密文只在安全性证明中使用。其中私钥和密文之间的相互关系如图 1 所示。一个标准私钥可以解密标准态或半功能态密文,同时一个标准密文可以被标准态或半功能态私钥解密。但是,当半功能态私钥解密一个半功能态密文时,解密算法无条件报错,因为私钥和密文中的半功能元素能通过一组随机的交互作用伪装盲化因子。

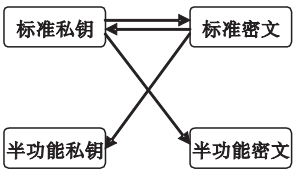

图1　Waters双系统加密技术

在 Waters 的双系统加密技术的基础上,Lewko 等人[7]提出一个新的概念——象征性(nominally)半功能态私钥。Lewko 改进后的双系统加密技术中私钥和密文之间的相互作用如图

2 所示。象征性半功能态私钥与半功能态私钥有相同的分布，但它能与半功能态密文发生交互作用，这样当一个象征性半功能私钥解密一个半功能密文时，两者的半功能成分的交互作用就会抵消，因此解密成功。

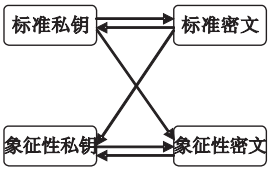

图2 Lewko双系统加密技术

2 新方案的构造

2.1 具体方案构造

在 Lewko-HIBE 方案基础上，本文设计了一个新的带通配符的分级加密方案，新方案由以下五个算法组成：

a）系统建立。混合阶数双线性群 G 的阶数为 $N=p_1p_2p_3$，令 L 为 WIBE 的最大级数。随机选取 $g,h,u_1,\cdots,u_L\in G_{p_1}$，$X_3\in G_{p_3}$ 和 $\alpha\in Z_N$，公共参数 $\mathrm{pk}=(N,g,h,u_1,\cdots,u_L,X_3,e(g,g)^{\alpha})$，主密钥为 α。

b）私钥提取。首先随机选取 $r\in Z_N$ 和 $R_3,R'_3,R_{k+1},\cdots,R_L\in G_{p_3}$，则身份 $I=(I_1,\cdots,I_k)$ 对应私钥 $\mathrm{sk}_{I|k}=(K_1,K_2,E_{k+1},\cdots,E_L)$ 的计算过程为

$$K_1=g^rR_3$$

$$K_2=g^{\alpha}(h\prod_{i=1}^{k}u_i^{I_i})^rR'_3$$

$$E_{k+1}=u_{k+1}^rR_{k+1},\cdots,E_L=u_L^rR_L$$

c）私钥分发。给出第 k 层身份 $I'=(I_1,\cdots,I_k)$ 及其相应的私钥 $\mathrm{sk}_{I|k}=(K'_1,K'_2,E'_{k+1},\cdots,E'_L)$，首先随机选取 $r'\in Z_N$，$\tilde{R}_3,\tilde{R}'_3,\tilde{R}_{k+1},\cdots,\tilde{R}_L\in G_{p_3}$，则第 $k+1$ 层身份 $I=(I_1,\cdots,I_k,I_{k+1})$ 的私钥生成过程为

$$K_1=K'_1g^{r'}\tilde{R}_3$$

$$K_2=K'_2(h\prod_{i=1}^{k}u_k^{I_k})^{r'}(E'_{k+1})^{I_{k+1}}u_{k+1}^{r'I_{k+1}}\tilde{R}'_3$$

$$E_{k+2}=E'_{k+2}u_{k+2}^{r'}\tilde{R}_{k+2},\cdots,E_L=E'_Lu_L^{r'}\tilde{R}_L$$

d）加密。令 M 为加密的消息，模式 $P=(P_1,\cdots,P_k)$，然后随机选取 $s\in Z_N$，那么计算密文 $C=(P,C_0,C_1,C_2)$ 如下：

$$C_0=Me(g,g)^{\alpha s}$$

$$C_1=(h_{i=1,i\notin W(P)}^{k}u_i^{P_i}\prod_{i\in W(P)}^{k}u_i)^s$$

$$C_2=g^s$$

e）解密。假设一个合法用户收到的密文 $C=(P,C_0,C_1,C_2)$ 是有效的，并且与其私钥 $\mathrm{sk}_{I|k}=(K_1,K_2,E_{k+1},\cdots,E_L)$ 相匹配。首先计算 $C''_1=(h_{i=1,i\notin W(P)}^{k}u_i^{P_i}\prod_{i=1,i\in W(P)}^{k}u_i^{I_i})^s$，然后计算盲因子 $e(g,g)^{\alpha s}=\dfrac{e(K_2,C_2)}{e(K_1,C''_1)}$。

2.2 正确性

假设 $C=(P,C_0,C'_1,C_2)$ 是合法密文，计算

$$\frac{e(K_2,C_2)}{e(K_1,C''_1)}=\frac{e(g^{\alpha}(h\prod_{i=1}^{k}u_i^{I_i})^r\cdot R'_3,g^s)}{e(g^rR_3,h_{i=1,i\notin W(P)}^{k}(u_i^{P_i})^s\cdot\prod_{i=1,i\in W(P)}^{k}u_i^{sI_i})}=$$

$$\frac{e(g,g)^{\alpha s}e((h\prod_{i=1}^{k}u_i^{I_i})\cdot R'_3,g)^{rs}}{e(g,(h\prod_{i=1}^{k}u_i^{I_i})\cdot R_3)^{rs}}=e(g,g)^{\alpha s}$$

3 安全性证明

首先定义半功能态的私钥和密文。

a）半功能态密文。令 g_2 为子群 G_{p_2} 的生成元，首先设置标准密文为 $C'=(P,C'_0,C'_i,C'_2)$，然后随机选取 $x,z_c\in Z_N$，设置

$$C_0=C'_0,C_1=C'_1g_2^{xz_c},C_2=C'_2g_2^x$$

b）半功能态私钥。调用私钥提取算法生成一个标准私钥 $\mathrm{sk}'_{I|k}=(K'_1,K'_2,E'_{k+1},\cdots,E'_L)$，然后随机选取 $\gamma,z_k,z_{k+1},\cdots,z_L\in Z_N$，设置：

$$K_1=K'_1g_2^{\gamma},K_2=K'_2g_2^{\gamma z_k}$$

$$E_{k+1}=E'_{k+1}g^{\gamma z_{k+1}},E_L=E'_Lg_2^{\gamma z_L}$$

方案的安全性证明使用游戏序列（game order）证明技术，定义攻击者 A 和挑战者 C 之间的相互游戏如下：

$\mathrm{Game}_{\mathrm{real}}$，真实的 WIBE 安全游戏。

$\mathrm{Game}'_{\mathrm{real}}$，与 $\mathrm{Game}_{\mathrm{real}}$ 相似，但要求由私钥提取算法来响应所有的私钥询问（挑战者在一定方式下不能调用私钥分发算法）。

$\mathrm{Game}_{\mathrm{restricted}}$，与 $\mathrm{Game}'_{\mathrm{real}}$ 相似，但限制攻击者不能对 $P^*\bmod N$ 的模式进行私钥询问，其中 P^* 为挑战模式，并将此限制运用到随后的游戏中。

Game_k，其中 $0\leqslant k\leqslant q$，要求攻击者 A 获得的密文是半功能态的，而前 k 个私钥也是半功能态的，剩余的为标准私钥。即 Game_0 中所有的挑战密文均为半功能态的，Game_q 中挑战密文和所有的私钥都是半功能态的。

$\mathrm{Game}_{\mathrm{final}}$，与 Game_q 相似，但要求半功能态密文是对某个随机消息加密所得，而标准密文为对挑战消息加密所得。

通过以下五个引理来证明上述各个游戏之间是两两不可区分的。

引理 1 对于任意算法 A，总是存在等式 $\mathrm{Game}_{\mathrm{real}}\mathrm{Adv}_A=\mathrm{Game}_{\mathrm{real}'}\mathrm{Adv}_A$。

证明 对于任意一个身份，有两种方式为其生成私钥，一种是运行私钥提取算法，另一种是运行私钥分发算法（需要其上级身份的密钥）。无论运行哪个算法，其私钥都有相同分布。从攻击者的角度无法区分上述游戏。

引理 2 假设存在一个概率算法 A 可以使 $\mathrm{Game}_{\mathrm{real}'}\mathrm{Adv}_A-\mathrm{Game}_{\mathrm{restricted}}\mathrm{Adv}_A=\varepsilon$，那么可以构建一个算法 C，其攻破假设 1 的优势至少为 $\varepsilon/2$。

证明 输入 g、X_3，算法 A 以概率 ε 生成身份 I 和 I^*，其中 $I\neq I^*\bmod n$，有 p_2 整除 $(I-I^*)$。C 通过计算 $a=\gcd(I-I^*,n)$，得到 n 的一个非平凡因子。令 $b=n/a$，由于 p_2 整除 a，并且有 $n=ad=p_1p_2p_3$。因此可能存在两种情况：p_1 整除 b，p_3 整除 b。

至少一种可能性发生的概率大于等于 $\varepsilon/2$。在每种可能性中，C 打破假设 1 的方式如下：给定 g,X_3,T,C 通过验证 g^b 是否为基元来判定 p_i 是否整除 b，其中 $i\in\{1,3\}$，进而判断 T^b 是否为基元。如果是，则 $T\in G_{p_i}$，否则 $T\in G_{p_ip_2}$。因此，C 能通过 A 的输出来区分 T 的可能值。

引理 3 假设存在一个概率算法 A 使得 $\mathrm{Game}_{\mathrm{restricted}}\mathrm{Adv}_A-\mathrm{Game}_0\mathrm{Adv}_A=\varepsilon$，那么可以构建一个算法 C，其攻破假设 1 的优势为 ε。

证明　算法 C 接收到 g、X_3、T,然后随机选取 $\alpha,a_1,\cdots,a_L$,$b\in Z_N$,设 $g=g$,$h=g^b$,$u_i=g^{a_i}$,其中 $1\leqslant i\leqslant L$。算法 C 发送给攻击者 A 公共参数$\{N,g,u_1,\cdots,u_L,h,e(g,g)^\alpha\}$。对于任何一个身份 $I|k=(I_1,\cdots,I_k)$,算法 C 按以下方式计算私钥:随机选取 $r,t,\omega,v_{k+1},\cdots,v_L\in Z_N$,计算私钥 $K_1=g^rX_3^t$,$K_2=g^\alpha(u_1^{I_1}u_k^{I_k}h)^r\times X_3^\omega$,$E_{k+1}=u_{k+1}^rX_3^{v_{k+1}}$,$\cdots$,$E_L=u_L^rX_3^{v_L}$。

攻击者 A 发送消息 M_0、M_1 和挑战模式 $P^*=(P_1^*,\cdots,P_k^*)$给算法 C。算法 C 随机选取 $\beta\in\{0,1\}$,然后计算密文如下:

$$C_0=M_\beta e(T,g)^\alpha,C_1=T^{(\sum_{i=1,i\notin W(P)}^{k}a_iP_i^*)+(\sum_{i=1,i\in W(P)}^{k}a_i)+b},C_2=T$$

如果 $T\in G_{p1p2}$,那么密文为半功能态并且满足 $z_c=b+(\sum_{i=1,i\notin W(P)}^{k}a_iP_i^*)+(\sum_{i=1,i\in W(P)}^{k}a_i)$;如果 $T\in G_{p_1}$,则为标准密文。因此,C 能通过 A 的输出值来区分 T 的可能值。

引理 4　假设存在一个概率算法 A 总能使 $\mathrm{Game}_{k-1}\mathrm{Adv}_A-\mathrm{Game}_k\mathrm{Adv}_A=\varepsilon$,那么可以构建一个算法 C,其攻破假设 2 的优势为 ε。

证明　算法 C 首先接收 g、X_1X_2、X_3、Y_2Y_3、T,然后随机选取 $a_1,\cdots,a_L,b\in Z_N$,设置公共参数如下:$g=g$,$h=g^b$,$u_i=g^{a_i}$,$e(g,g)^\alpha$。算法 C 把这些公共参数发送给 A。当攻击者 A 询问身份 $I|k=(I_1,\cdots,I_k)$的第 i 个私钥时分为以下几种:

a)如果 $i<k$,算法 C 生成一组半功能态私钥。随机选取 $r,z,t,z_{k+1},\cdots,z_L\in Z_N$,计算私钥如下:

$$K_1=g^r(Y_2Y_3)^t,K_2=g^\alpha(h\prod_{i=1}^{k}u_i^{I_i})^r(Y_2Y_3)^z$$

$$E_{k+1}=u_{k+1}^r(Y_2Y_3)^{z_{k+1}},\cdots,E_L=u_L^r(Y_2Y_3)^{z_L}$$

b)如果 $i>k$,算法 C 调用私钥提取算法生成一组标准私钥。

c)如果 $i=k$,算法 C 设置 $z_k=(\sum_{i=1}^{k}a_iI_i)+b$,随机选取 $w_k,w_{k+1},\cdots,w_L\in Z_N$,并计算 $K_1=T$,$K_2=g^\alpha T^{z_k}X_3^{w_k}$,$E_{k+1}=T^{a_{k+1}}X_3^{w_{k+1}},\cdots,E_L=T^{a_L}X_3^{w_L}$。如果 $T\in G_{p1p3}$,则为标准私钥;如果 $T\in G$,则为半功能态私钥。

然后,A 发送给 C 消息 M_0、M_1 和挑战模式 $P^*=(P_1^*,\cdots,P_k^*)$,C 随机选取 $\beta\in\{0,1\}$,然后生成密文如下:

$$C_0=M_\beta e(X_1X_2,g)^\alpha$$

$$C_1=(X_1X_2)^{(\sum_{i=1,i\notin W(P)}^{k}a_iP_i^*)+(\sum_{i=1,i\in W(P)}^{k}a_i)+b},C_2=X_1X_2$$

如果 $I_k=I \bmod p_2$,则私钥询问无效,因为盲化因子被 $e(g,g)^{xy(z_k-z_c)}$ 所掩盖。若 $z_k=z_c$,继续运行解密算法。如果 $T\in G_{p1p3}$,那么算法 C 模拟的是游戏 Game_{k-1};如果 $T\in G$,那么算法 C 模拟的是游戏 Game_k。因此,B 可以通过 A 的输出来区分 T 的可能值。

引理 5　假设存在一个概率算法 A 总能使得 $\mathrm{Game}_q\mathrm{Adv}_A-\mathrm{Game}_{\mathrm{final}}\mathrm{Adv}_A=\varepsilon$,那么可以构建一个算法 C,其攻破假设 3 的优势为 ε。

证明　C 收到 g、$g^\alpha X_2$、X_3、g^sY_2、Z_2、T,然后随机选取 $a_1,\cdots,a_L,b\in Z_N$,设置公共参数如下:$g=g$,$h=g^b$,$u_i=g^{a_i}$,$e(g,g)^\alpha=e(g^\alpha X_2,g)$,算法 C 把这些公共参数发送给 A。当 A 发起对身份 $I|k$ 的私钥询问时,算法 C 随机选取 $c,r,t,w,z,z_{k+1},\cdots,z_L,w_{k+1},\cdots,w_L\in Z_N$,生成半功能态私钥如下:

$$K_1=g^rZ_2^zX_3^t,K_2=g^\alpha X_2Z_2^c(h\prod_{i=1}^{k}u_i^{I_i})^rX_3^w$$

$$E_{k+1}=u_{k+1}^rZ_2^{zk+1}X_3^{wk+1},\cdots,E_L=u_L^rZ_2^{zL}X_3^{wL}$$

然后,A 发送给 C 消息 M_0、M_1 和挑战模式 $P^*=(P_1^*,\cdots,P_k^*)$,C 首先随机选取 $\beta\in\{0,1\}$,然后计算密文:

$$C_0=M_\beta T,C_1=(g^sY_2)^{(\sum_{i=1.i\notin W(P)}^{k}a_iP_i^*)+(\sum_{i=1,i\in W(P)}^{k}a_i)+b}$$

$$C_2=g^sY_2$$

设置 $z_c=(\sum_{i=1}^{k}a_iI_i^*)+b$,若 $T=e(g,g)^{\alpha s}$,则该密文为消息 M_β 的半功能态密文;若 T 是 G_T 中的随机值,则该密文为随机消息的半功能态密文。

定理 1　若假设 1 ~ 3 成立,那么本文的 WIBE 方案是 adaptive-ID 安全的。

证明　若假设 1 ~ 3 均成立,通过上述引理已证实真实游戏与游戏 $\mathrm{Game}_{\mathrm{final}}$ 是不可区分的,因为 β 值对攻击者是完全隐藏的(信息论意义上),所以攻击者在 $\mathrm{Game}_{\mathrm{final}}$ 中的优势为 0,从而得知在 $\mathrm{Game}_{\mathrm{real}}$ 中攻击者的优势是可忽略的。

4　方案比较

本文构造的带通配符的基于身份加密方案具有两点优势:a)密文长度为常数,这一点无论是与基于身份分级加密方案相比,还是与带通配符的基于身份分级加密方案相比,都不失为可取之处;b)在标准模型下可证明达到了完全安全,即 adaptive-ID 安全,这一特点打破了带通配符的基于身份分级加密方案大多仅达到 selective-ID 安全的局限。

将 Abdalla 提出的两个带通配符的基于身份分级加密方案分别简称为 BB-WIBE 和 BBG-WIBE。由表 1 可以看出,本文方案加密算法中 $e(g,g)$ 可以预计算,不需要其他对运算,形成的密文长度固定,只含有四个群元素且不需要身份标签的介入,而解密算法中仅使用两个对运算,因而具有较高的运算效率。新方案的安全性基于静态假设,在标准模型下达到 adaptive-ID 安全。与以往方案相比,新方案无论在结构、效率还是在安全性方面,均具有更大的优势。

表 1　本文方案与同类方案的性能比较

方案	公钥长度	私钥长度	密文长度	对运算	假设	安全模型
BB-WIBE	$2L+3$	$L+1$	$2L+2$	$L+1$	非静态	s-ID
BBG-WIBE	$L+4$	$L+2$	$L+3$	2	非静态	s-ID
本文方案	$L+4$	$L+2$	4	2	静态	a-ID

5　结束语

本文构造了一个带通配符的基于身份加密方案,新方案在标准模型下被证明达到 adaptive-ID 安全。本方案较突出的贡献在于使密文长度固定,而不随密文中所含模式 P 个数的变化而变化。新方案的构造使用了混合阶双线性群,而混合阶群中对运算的速度低于素阶群中对运算的速度。因此,本文留下一个问题:如何在素阶群中构造简单高效的 WIBE 方案[8,9],或者如何把混合阶群中的方案转换成素阶群中的方案[10]。

参考文献:

[1] HORWITZ J, LYNN B. Toward hierarchical identity-based encryption [C]//Proc of International Conference on the Theory and Application of Cryptographic Techniques. London: Springer-Verlag, 2002: 466-481.

(下转第 1917 页)

(上接第 1913 页)

[2] BONEH D, BOYEN X. Efficient selective-ID secure identity based encryption without random oracles[C]//Proc of International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer-Verlag,2004:223-238.

[3] BONEH D, BOYEN X, GOH E. Hierarchical identity based encryption with constant size ciphertext[C]//Proc of the 24th International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer-Verlag, 2005:440-456.

[4] ABDALLA M, CATALANO D, DENT A W, *et al*. Identity-based encryption gone wild[C]//Proc of the 33rd International Conference on Automata, Languages and Programming. Berlin: Springer, 2006: 300-311.

[5] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]//Proc of the 29th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag,2009:619-636.

[6] LUO Song, CHEN Yu, HU Jian-bin, *et al*. New fully secure hierarchical identity-based encryption with constant size ciphertext[C]// Proc of the 7th IEEE International Conference on Information Security Practice and Experience. Berlin: Springer-Verlag,2011:55-70.

[7] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[C]//Proc of the 7th International Conference on Theory of Cryptography. Berlin: Springer, 2010:455-479.

[8] ABDALLA M, BIRKETT J, CATALANO D, *et al*. Wildcarded identity-based encryption[J]. Journal of Cryptology, 2011, 24(1):42-82.

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

[10] FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order group[C]//Proc of the 29th International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer-Verlag, 2010:44-61.