素数阶群上具有扩展通配符的ABE方案

李作辉 陈性元
(信息工程大学 郑州 450002)

摘 要 叛徒追踪和撤销是基于属性的加密(ABE)在实际应用中需要解决的问题,具有扩展通配符的ABE方案(GWABE)能够方便地解决上述问题。目前自适应安全的GWABE方案均在合数阶群上构造。针对合数阶上双线性映射计算开销过大的问题,以对偶正交基技术为基础,提出了一种素数阶群上自适应安全的GWABE方案,同时将该方案的安全性归约到判定性线性假设。性能分析表明,该方案在达到自适应安全的基础上,具有更好的效率。

关键词 基于属性的加密,叛徒追踪,撤销,自适应安全,素数阶
中图法分类号 TP309.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.042

ABE Scheme with Generalized Wildcards on Prime Order Groups

LI Zuo-hui CHEN Xing-yuan
(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Traitor tracing and revocation are crucial to use of ABE. ABE scheme with generalized wildcards (GWABE) is a convenient way for solving these problems. Previous adaptively secure GWABE scheme suffers from superfluous computation overhead because they are designed on composite order groups. To tackle this problem, an adaptively secure GWABE scheme on prime order groups was proposed when a dual pairing vector space approach was employed. The proposed scheme is proven adaptively secure from the decisional linear assumption. Performance analysis indicates that this scheme is more efficient while achieving the adaptive security.

Keywords Attribute-based encryption, Traitor tracing, Revocation, Adaptive security, Prime order

1 引言

基于属性的加密(ABE)最早源于Sahai和Waters在2005年欧密会上提出的基于模糊身份的加密(FIBE)[1]。随后,Goyal等人在2006年CCS会议上提出了第一个密钥策略ABE方案[2],并根据密文、密钥与访问控制策略、属性的关联关系将ABE方案分为两种类型:密钥策略ABE(KP-ABE)和密文策略ABE(CP-ABE)。KP-ABE密文与属性集合相关联,而密钥与访问控制策略相关联;与此相反,CP-ABE密文与访问控制策略相关联,而密钥与属性集合相关联。Bethencourt等人在2007年S&P会议上提出了第一个CP-ABE方案[3]。一般来说,KP-ABE比较适合数据静态的场景,如付费电视、视频点播等,而CP-ABE适合用户静态的场景,如广播加密等。

在ABE中,密钥仅与用户属性相关,而不与用户的个人信息关联,因此无法跟踪泄露密钥的用户,也难以精确撤销异常用户。Hinek等人2008年提出了基于标号的ABE方案(tk-ABE)[4],该方案在密钥生成过程中引入用户标识,使得密钥代理会暴露用户的隐私信息,对预防密钥克隆起到威慑作用。Yu[5]、Li[6]和Wang[7]也通过引入用户标识,构建能够防止密钥滥用和实现追责的ABE方案。Ostrovsky[8]将用户标识作为一个属性,把密文和被撤销用户标识的"非"相关联,实现了CP-ABE中用户的即时撤销。Attrapadung[9]对Ostrovsky[8]方案进行了改进,降低了撤销的开销。

上述与用户标识相关的ABE方案仅满足选择安全性,也就是说,在安全性证明中,攻击者在游戏之前必须声明攻击目标,即在安全性游戏中要挑战的属性集合或者访问结构。在Waters[10]提出对偶系统加密的证明技术后,Lewko和Waters等人[11]利用对偶系统加密的思想实现了第一个自适应安全的ABE方案。马海英[12]在合数阶群上构造了具有扩展通配符的ABE方案(GWABE),该方案满足自适应安全,能够与完全子树构架[13]结合,实现了密钥滥用追踪和用户撤销。

合数阶群的困难假设通常基于大整数分解的困难性。在同样安全性的情况下,合数阶群中元素的比特长度要大于素数阶群中元素的比特长度,因而合数阶群上的计算开销要高于素数阶群的。由文献[14]可知,在1024比特长的合数阶群上构造的ABE方案,双线性配对运算的计算开销大概是对应安全级别170比特素数阶群上ABE方案的50倍。本文利用文献[15]中的对偶正交基技术,结合马海英方案[12]的系统模型,提出了素数阶群上自适应安全的GWABE方案,该方案也能够与完全子树构架[13]结合,解决追踪和撤销问题,且在达到自适应安全的前提下,具有更高的计算效率。

到稿日期:2015-01-24 返修日期:2015-04-20 本文受国家重点基础研究发展计划(973计划)项目(2011CB311801)资助。
李作辉(1981—),男,博士生,讲师,主要研究方向为公钥密码,E-mail:ForestSpringer@163.com;陈性元(1964—),男,博士,教授,主要研究方向为信息安全。

2 背景知识

2.1 对偶配对空间

定义 1[16] 选取 G 和 G_T 为两个阶为大素数 p 的群，g 是群 G 的一个生成元。定义一个可有效计算的双线性映射 $e:G\times G\to G_T$，其具有以下性质：

1)双线性：对于任意 $a,b\in Z_p$，都有 $e(g^a,g^b)=e(g,g)^{ab}$；

2)非退化性：$e(g,g)\neq 1$。

e 是对称操作，因为 $e(g^a,g^b)=e(g,g)^{ab}=e(g^b,g^a)$。

给定一个 n 维向量 $\vec{v}:=(v_1,v_2,\cdots,v_n)\in Z_p^n$，令 $g^{\vec{v}}:=(g^{v_1},g^{v_2},\cdots,g^{v_n})$，对于任意 $a\in Z_p$，$\vec{v},\vec{w}\in Z_p^n$，定义：

$g^{a\vec{v}}:=(g^{av_1},g^{av_2},\cdots,g^{av_n})$

$g^{\vec{v}+\vec{w}}:=(g^{v_1+w_1},g^{v_2+w_2},\cdots,g^{v_n+w_n})$

定义向量的双线性对映射为：

$$e_n(g^{\vec{v}},g^{\vec{w}}):=\prod_{i=1}^{n}(g^{v_i},g^{w_i})=e(g,g)^{\vec{v}\cdot\vec{w}}$$

定义 2[15] 给定维数 n，如果 Z_p^n 上的两组基：$B=(\vec{b}_1,\vec{b}_2,\cdots,\vec{b}_n)$，$B^*=(\vec{b}_1^*,\vec{b}_2^*,\cdots,\vec{b}_n^*)$，满足：

$$\vec{b}_i\cdot\vec{b}_j^*=\begin{cases}\psi, & i=j\\ 0, & i\neq j\end{cases}\bmod p$$

则称 (B,B^*) 是对偶正交基。类似地，给定群 G 的一个生成元 g，对于 $i\neq j$，有 $e_n(g^{\vec{b}_i},g^{\vec{b}_j^*})=1$，对于 $i=j$，有 $e_n(g^{\vec{b}_i},g^{\vec{b}_j^*})=e_n(g,g)^{\psi}$。用 $Dual(Z_p^n)$ 表示所有 n 维对偶正交基的集合。为了方便，本文与文献[17]一样，令 $\psi=1$。

2.2 线性秘密共享(LSSS)

定义 3[18] 令 $\Lambda:=\{P_1,P_2,\cdots,P_n\}$ 表示参与方的集合。对于访问结构 $\Phi\subseteq 2^{\Lambda}$，对于任意 A_1,A_2，当 $A_1\in\Phi$ 且 $A_1\subseteq A_2$ 时，有 $A_2\in\Phi$，则称 Φ 是单调的。访问结构 Φ 中的集合称作授权集合，不在 Φ 中的集合称为非授权集合。

定义 4[18] 令 $\Lambda:=\{P_1,P_2,\cdots,P_n\}$ 表示参与方的集合，Λ 上的一个秘密共享方案 Π 是线性的，如果：

1)每个参与方关于秘密 s 的份额是 Z_p 上的一个向量；

2)存在 Π 的一个 o 行 f 列的共享生成矩阵 A，令 ρ 为一个从 $\{1,2,\cdots,o\}$ 到 Λ 的映射，即 ρ 将矩阵 A 的每一行映射到一个参与方，选择一个随机向量 $\vec{v}:=(s,v_2,\cdots,v_f)\in Z_p^f$，则 $A\cdot\vec{v}$ 是 s 关于 Π 的 o 个份额，而且第 j 个份额 λ_j 属于参与方 $\rho(j)$。

文献[18]表明，单调的访问结构与线性秘密共享方案是等价的，且任何一个线性秘密共享方案都具有线性重构的性质。令 (A,ρ) 表示访问结构 Φ，S 为授权集合，令集合 $J:=\{j:\rho(j)\in S\}$，存在常数 $\{c_j\in Z_p\}_{j\in I}$ 使得 $\sum_{j\in I}c_j\lambda_j=s$；对于非授权集合，这样的常数是不存在的。

2.3 系统模型

定义 5[12] 对于长度为 n 的位串，身份模式为 $P:=P_{ip}\parallel *\parallel P_{is}$，其中，$P_{ip}$ 和 P_{is} 分别是长度为 ip 和 is 的位串，通配符 $*$ 的长度为 $n-ip-is$，开始位置为 $ip+1$，终止位置为 $n-is$。

给定用户的身份 id 和身份模式 P，如果 id 可表示为 $P_{ip}\parallel id_*\parallel P_{is}$，则称 id 和 P 相匹配，记作 $id\in_* P$，其中，id_* 为长度为 $n-ip-is$ 的位串。

GWABE 方案[12]由 4 个算法组成：初始化(Setup)，密钥生成(KeyGen)，加密(Enc)，解密(Dec)。

Setup(λ)$\to PK,MSK$：输入系统安全参数 λ，输出系统公钥 PK 和主密钥 MSK。

KeyGen($id,(A,\rho),MSK$)$\to d_{id,(A,\rho)}$：输入用户的身份 id、访问结构 (A,ρ)、主密钥 MSK，输出用户私钥 $d_{id,(A,\rho)}$。

Enc(M,ω,P,PK)$\to CT$：输入消息 M、属性集 ω、身份模式 P 和公钥 PK，输出密文值 CT。

Dec($d_{id,(A,\rho)},CT$)$\to M$：输入用户私钥 $d_{id,(A,\rho)}$、用 ω 和 P 加密的密文值 CT，仅当 $id\in_* P$ 且 ω 满足访问结构 (A,ρ) 时，用户 $(id,(A,\rho))$ 解密密文，否则，解密失败。

可以通过如下挑战者 $\mathcal{S}$ 和攻击者 $\mathcal{A}$ 之间的交互性游戏来定义 GWABE 方案的安全性。

初始化：挑战者 $\mathcal{S}$ 运行系统初始化算法，将 PK 发送给攻击者 $\mathcal{A}$。

阶段 1：攻击者 $\mathcal{A}$ 适应性地询问用户 $(id,(A,\rho))$ 的私钥，挑战者生成私钥并将其发送给攻击者 $\mathcal{A}$，攻击者 $\mathcal{A}$ 可以重复多次询问私钥。

挑战：攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{S}$ 提交等长的 M_0、M_1、挑战属性集 ω 和身份模式 P，挑战者 $\mathcal{S}$ 抛掷一枚公平硬币 $b\in\{0,1\}$，计算 $CT=Enc(M_b,\omega,P,PK)$，并将计算结果 CT 发送给攻击者 $\mathcal{A}$。

阶段 2：重复执行阶段 1。

猜测：攻击者 $\mathcal{A}$ 根据密文 CT 得到一个猜测值 $b'\in\{0,1\}$。

若 $b'=b$，攻击者 $\mathcal{A}$ 从未询问 $id\in_* P$ 且 ω 满足访问结构 (A,ρ) 的用户 $(id,(A,\rho))$ 的密钥，则称攻击者 $\mathcal{A}$ 获胜。在上述游戏中攻击者 $\mathcal{A}$ 获胜的优势为：$adv:=|\Pr[b'=b]-1/2|$。

定义 6[12] 如果任意多项式时间攻击者 $\mathcal{A}$ 在上述游戏中获胜的优势都是可以忽略的，则称该 GWABE 方案是完全安全的。

2.4 子空间困难假设

定义 7[17] 给定一个群生成算法 $\mathfrak{I}$，定义如下分布：

$$C:=(p,G,G_T,e)\xleftarrow{R}\mathfrak{I},g\xleftarrow{R}G,$$

$$\eta,\beta,\tau_1,\tau_2,\tau_3,\mu_1,\mu_2,\mu_3\xleftarrow{R}Z_p,$$

$$(B_1,B_1^*)\xleftarrow{R}Dual(Z_p^{n_1}),\cdots,(B_m,B_m^*)\xleftarrow{R}Dual(Z_p^{n_m}),$$

$$R_{1,i}:=g^{\mu_1\vec{b}_{1,i}+\mu_2\vec{b}_{k_i+1,i}+\mu_3\vec{b}_{2k_i+1,i}},$$

$$R_{2,i}:=g^{\mu_1\vec{b}_{2,i}+\mu_2\vec{b}_{k_i+2,i}+\mu_3\vec{b}_{2k_i+2,i}},$$

$$\cdots,$$

$$R_{k_i,i}:=g^{\mu_1\vec{b}_{k_i,i}+\mu_2\vec{b}_{2k_i,i}+\mu_3\vec{b}_{3k_i,i}},\forall i\in[m],$$

$$V_{1,i}:=g^{\tau_1\eta\vec{b}_{1,i}^*+\tau_2\beta\vec{b}_{k_i+1,i}^*},$$

$$V_{2,i}:=g^{\tau_1\eta\vec{b}_{2,i}^*+\tau_2\beta\vec{b}_{k_i+2,i}^*},$$

$$\cdots,$$

$$V_{k_i,i}:=g^{\tau_1\eta\vec{b}_{k_i,i}^*+\tau_2\beta\vec{b}_{2k_i,i}^*},\forall i\in[m],$$

$$W_{1,i}:=g^{\tau_1\eta\vec{b}_{1,i}^*+\tau_2\beta\vec{b}_{k_i+1,i}^*+\tau_3\beta\vec{b}_{2k_i+1,i}^*},$$

$$W_{2,i}:=g^{\tau_1\eta\vec{b}_{2,i}^*+\tau_2\beta\vec{b}_{k_i+2,i}^*+\tau_3\beta\vec{b}_{2k_i+2,i}^*},$$

$$\cdots,$$

$$W_{k_i,i}:=g^{\tau_1\eta\vec{b}_{k_i,i}^*+\tau_2\beta\vec{b}_{2k_i,i}^*+\tau_3\beta\vec{b}_{3k_i,i}^*},\forall i\in[m],$$

$D:=(C,g,g^{\eta},g^{\beta},g^{r_1\eta},g^{r_2\beta},\mu_3,\{S_i\}_{i=1}^m)$，

$S_i=(g^{\vec{b}_{1,i}},g^{\vec{b}_{2,i}},\cdots,g^{\vec{b}_{2k_i,i}},\vec{b}_{3k_i+1,i},\cdots,\vec{b}_{n_i,i},g^{\eta\vec{b}^*_{1,i}},\cdots,g^{\eta\vec{b}^*_{k_i,i}},g^{\beta\vec{b}^*_{k_i+1,i}},\cdots,g^{\beta\vec{b}^*_{2k_i,i}},g^{\vec{b}^*_{2k_i+1,i}},\cdots,g^{\vec{b}^*_{3k_i,i}},\vec{b}^*_{3k_i+1,i},\cdots,\vec{b}^*_{n_i,i},R_{1,i},\cdots,R_{k_i,i})$

攻击者的优势为：$adv:=|\Pr[A(D,\{V_{1,i},\cdots,V_{k_i,i}\}_{i=1}^m)=1]-\Pr[A(D,\{W_{1,i},\cdots,W_{k_i,i}\}_{i=1}^m)=1]|$。

如果对于任意多项式时间算法，此优势是可以忽略的，则假设成立。根据文献[17]，子空间假设可以归约到判定性线性假设。

3 素数阶群上的 GWABE 方案

假设属性集合为 $W:=\{1,2,\cdots,w\}$，w 为属性的个数；假设全体用户的集合为 $\mathcal{N}$，$|\mathcal{N}|$ 为用户的个数，令 $n:=\log_2|\mathcal{N}|$。令 $S(id)$ 为位串 id 中所有值为 1 的位置组成的集合，$x\in S(id)$ 表示 id 第 x 位为 1。

Setup(λ)$\rightarrow PK,MSK$：可信授权机构输入安全参数 λ，调用群生成算法 $\mathfrak{I}$，得到 (p,G,G_T,e)；从 $Dual(Z_p^3)$ 上得到正交基 (B,B^*)，令 $B=(\vec{b}_1,\vec{b}_2,\vec{b}_3)$，$B^*=(\vec{b}_1^*,\vec{b}_2^*,\vec{b}_3^*)$；对于每个属性 $i\in W$，从 $Dual(Z_p^4)$ 上得到正交基组 (B_i,B_i^*)，令 $B_i=(\vec{b}_{1,i},\vec{b}_{2,i},\vec{b}_{3,i},\vec{b}_{4,i})$，$B_i^*=(\vec{b}_{1,i}^*,\vec{b}_{2,i}^*,\vec{b}_{3,i}^*,\vec{b}_{4,i}^*)$；随机选择 a_1，$a_2\in Z_p$，对于每个 $0\leqslant x\leqslant n$，选择随机数 $\{u_x\}_{x=0}^n\in Z_p$，输出系统公开参数为：

$PK:=\{p,\{g^{u_x}\}_{x=0}^n,e(g,g)^{a_1},e(g,g)^{a_2},g^{\vec{b}_1},g^{\vec{b}_2}\{g^{\vec{b}_{1,i}},g^{\vec{b}_{2,i}},g^{\vec{b}_{4,i}}\}_{i\in W}\}$

主密钥为：

$MSK:=\{g,g^{a_1\vec{b}_1^*},g^{a_2\vec{b}_2^*},g^{\vec{b}_1^*},g^{\vec{b}_2^*},\{g^{\vec{b}_{1,i}^*},g^{\vec{b}_{2,i}^*},g^{\vec{b}_{4,i}^*}\}_{i\in W},\{u_x\}_{x=0}^n\}$

在此未使用的 $\vec{b}_3$，$\vec{b}_3^*$ 和 $\vec{b}_{3,i}$，$\vec{b}_{3,i}^*$ 将用于后面构建半功能密文和半功能密钥。为方便理解，本节后续变量定义也跳过了编号 3。

KeyGen($id,(A,\rho),MSK)\rightarrow d_{id,(A,\rho)}$：可信授权机构随机选择 $t_1,t_2\in Z_p$ 和以 t_1,t_2 为首元素的向量 $\vec{v}_1,\vec{v}_2\in Z_p^f$，对于 A 的每一行 A_j，随机选择 $r_{1,j},r_{2,j},r_{4,j}\in Z_p$，令 $f(id):=u_0+\sum_{x\in id}u_x$，如下计算 $d_{id,(A,\rho)}$。

$K^0:=g^{(a_1+t_1)\vec{b}_1^*+(a_2+t_2)\vec{b}_2^*}$

$K_j^1:=g^{r_{1,j}\vec{b}_1^*+r_{2,j}\vec{b}_2^*}$

$K_j^2:=g^{(A_j\cdot\vec{v}_1+r_{1,j})\vec{b}_{1,\rho(j)}^*+(A_j\cdot\vec{v}_2+r_{2,j})\vec{b}_{2,\rho(j)}^*+f(id)r_{4,j}\vec{b}_{4,\rho(j)}^*}$

$K_j^3:=g^{r_{4,j}}$

Enc($M,\omega,P,PK)\rightarrow CT$：算法输入消息 $M\in G_T$、属性集合 $\omega\in W$、身份模式 $P:=P_{ip}\parallel *\parallel P_{is}$ 和系统公钥 PK，随机选择 $s_1,s_2,s_4\in Z_p$，如下计算密文 CT。

$C_0:=Me(g,g)^{a_1s_1+a_2s_2}$

$C_1:=g^{s_1\vec{b}_1+s_2\vec{b}_2}$

$C_{2,i}:=g^{s_1\vec{b}_{1,i}+s_2\vec{b}_{2,i}+s_4\vec{b}_{4,i}},\forall i\in\omega$

$C_3:=(C_{3,ip,is},C_{3,x})$

$C_{3,ip,is}=(g^{u_0}\prod_{x\in S(P_{ip}\parallel 0\cdots 0\parallel P_{is})}g^{u_x})^{s_4}$

$C_{3,x}:=(g^{u_x})^{s_4},\forall x\in\{ip+1,\cdots,n-is\}$

其中，位串 $P_{ip}\parallel 0\cdots 0\parallel P_{is}$ 的长度为 n，0 的个数为 $n-ip-is$，即用 $n-ip-is$ 个 0 代替 P 中的通配符。

Dec($d_{id,(A,\rho)},CT)\rightarrow M$：算法收到使用 P 和 ω 加密的密文 CT 时，如果 $id\in *P$ 且 ω 满足 (A,ρ)，首先计算 $C_3':=C_{3,ip,is}\prod_{x\in S(id)\cap\{ip+1,\cdots,n-is\}}C_{3,x}=g^{f(id)s_4}$，然后计算常量 c_j，使得 $\sum_{\rho(j)\in\omega}c_jA_j=(1,0,\cdots,0)$，最后计算：

$X':=\dfrac{e_4(C_{2,\rho(j)},K_j^2)}{e_3(C_1,K_j^1)e(C_3',K_j^3)}$

$X:=\prod_{\rho(j)\in\omega}(X')^{c_i}$

$Y:=e_3(C_1,K^0)$

$M=C_0X/Y$

上述解密是正确的，因为：

$$X':=\frac{e_4(C_{2,\rho(j)},K_j^2)}{e_3(C_1,K_j^1)e(C_3',K_j^3)}$$
$$=\frac{e_4(g^{s_1\vec{b}_{1,\rho(j)}+s_2\vec{b}_{2,\rho(j)}+s_4\vec{b}_{4,\rho(j)}},g^{(A_j\cdot\vec{v}_1+r_{1,j})\vec{b}_{1,\rho(j)}^*+(A_j\cdot\vec{v}_2+r_{2,j})\vec{b}_{2,\rho(j)}^*+f(id)r_{4,j}\vec{b}_{4,\rho(j)}^*})}{e_3(g^{s_1\vec{b}_1+s_2\vec{b}_2},g^{r_{1,j}\vec{b}_1^*+r_{2,j}\vec{b}_2^*})e(g^{f(id)s_4},g^{r_{4,j}})}$$
$$=\frac{e(g,g)^{s_1(A_j\cdot\vec{v}_1+r_{1,j})+s_2(A_j\cdot\vec{v}_2+r_{2,j})+s_4f(id)r_{4,j}}}{e(g,g)^{s_1r_{1,j}+s_2r_{2,j}}e(g,g)^{f(id)s_4r_{4,j}}}$$
$$=e(g,g)^{s_1A_j\cdot\vec{v}_1+s_2A_j\cdot\vec{v}_2}$$

$X=\prod_{\rho(j)\in\omega}(X')^{c_j}$

$=\prod_{\rho(j)\in\omega}(e(g,g)^{s_1A_j\cdot\vec{v}_1+s_2A_j\cdot\vec{v}_2})^{c_j}$

$=e(g,g)^{s_1t_1+s_2t_2}$

$Y=e_3(C_1,K^0)$

$=e_3(g^{s_1\vec{b}_1+s_2\vec{b}_2},g^{(a_1+t_1)\vec{b}_1^*+(a_2+t_2)\vec{b}_2^*})$

$=e(g,g)^{s_1a_1+s_1t_1+s_2a_2+s_2t_2}$

$$C_0X/Y=\frac{Me(g,g)^{a_1s_1+a_2s_2}e(g,g)^{s_1t_1+s_2t_2}}{e(g,g)^{s_1a_1+s_1t_1+s_2a_2+s_2t_2}}=M$$

4 安全性证明

定理 1 如果子空间困难假设成立，则本文的 GWABE 方案是安全的。

本节以文献[10]提出的对偶系统加密证明技术为基础，证明本文方案的安全性。首先定义半功能密文和半功能密钥，半功能密文和半功能密钥只在攻击游戏中用到；然后基于半功能密文与半功能密钥构造一系列攻击游戏；最后，基于子空间困难假设，证明真实的攻击游戏与这些攻击游戏是不可区分的，进而证明攻击者在真实游戏中的攻击优势也是可以忽略的。

半功能密文：首先按本文方案生成密文 $C_0,C_1,C_{2,i},C_3$，然后随机选择 $S_3\in Z_p$，计算半功能密文 $C_0,C_1g^{s_3\vec{b}_3},C_{2,i}g^{s_3\vec{b}_{3,i}},C_3$。

半功能密钥：半功能密钥具有以下两种形式。

第一类半功能密钥：首先生成正常密钥 K^0, K_j^1, K_j^2, K_j^3，然后随机选择 $\gamma, r_{3,j} \in Z_p$ 和 $\vec{v}_3 \in Z_p^f$，计算第一类半功能密钥 $K^0 g^{\gamma \vec{b}_3^*}$，$K_j^1 g^{r_{3,j} \vec{b}_3^*}$，$K_j^2 g^{(A_j \cdot \vec{v}_3 + r_{3,j}) \vec{b}_{3,\rho(j)}^*}$，$K_j^3$。

第二类半功能密钥：首先生成密钥 K^0, K_j^1, K_j^2, K_j^3，然后随机选择 $\gamma \in Z_p$，计算第二类半功能密钥 $K^0 g^{\gamma \vec{b}_3^*}$，$K_j^1, K_j^2, K_j^3$。

半功能密钥可以解密正常的密文，正常的密钥可以解密半功能密文。但是，当用第一类半功能密钥解密半功能密文时，就会多出一个多余的项 $e(g,g)^{t_3 s_3 - \gamma s_3}$，其中 t_3 为 $\vec{v}_3$ 的首元素。也就是说，当 $\gamma = t_3$ 时，第一类半功能密钥能够成功解密半功能密文。此时，称该半功能密钥是象征性的。

利用文献[10]的证明方式，通过一系列两两不可区分的攻击游戏来证明系统的安全性。令 q 表示攻击者 $\mathcal{A}$ 进行密钥查询的最大次数。令 $1 \leqslant l \leqslant q$。定义攻击游戏如下：

Game_{real}：该游戏是一个真实游戏，即挑战密文与密钥都是正常的(以下证明中挑战密文简称密文)。

Game_0：在该游戏中，密文是半功能的，密钥是正常的。

$\mathrm{Game}_{l,1}$：在该游戏中，密文是半功能的，前 $l-1$ 个密钥是第二类半功能密钥，第 l 个密钥是第一类半功能密钥，剩下的密钥是正常的。

$\mathrm{Game}_{l,2}$：在该游戏中，密文是半功能的，前 l 个密钥是第二类半功能密钥，剩下的密钥是正常的。

$\mathrm{Game}_{q,2}$：在该游戏中，密文是半功能的，所有的密钥都是第二类半功能密钥。

Game_{final}：在该游戏中，所有的密钥都是第二类半功能密钥，而密文要么是半功能密文，要么是一个随机的消息。

令子空间假设中 $m = w+1$，对于其中一个 i，令 $k_i = 1, n_i = 3$，对于其它的 i，令 $k_i = 1, n_i = 4$。为方便描述，令 $(D, D^*) \in Dual(Z_p^3)$，$(D_1, D_1^*), \cdots, (D_w, D_w^*) \in Dual(Z_p^4)$ 为子空间假设中的对偶正交基。挑战者 $\mathcal{S}$ 可以获得：

$$g, g^{\vec{d}_1}, g^{\vec{d}_2}, \{g^{\vec{d}_{1,i}}, g^{\vec{d}_{2,i}}, g^{\vec{d}_{4,i}}\}_{i \in W}$$

$$g^{\eta \vec{d}_1^*}, g^{\beta \vec{d}_2^*}, g^{\vec{d}_3^*}, \{g^{\eta \vec{d}_{1,i}^*}, g^{\beta \vec{d}_{2,i}^*}, g^{\vec{d}_{3,i}^*}, g^{\vec{d}_{4,i}^*}\}_{i \in W}$$

$$R = g^{\mu_1 \vec{d}_1 + \mu_2 \vec{d}_2 + \mu_3 \vec{d}_3}, \{R_i = g^{\mu_1 \vec{d}_{1,i} + \mu_2 \vec{d}_{2,i} + \mu_3 \vec{d}_{3,i}}\}_{i \in W}$$

$$T, \{T_i\}_{i \in W}$$

其中 $T = g^{\tau_1 \eta \vec{d}_1^* + \tau_2 \beta \vec{d}_2^*}$，$T_i = g^{\tau_1 \eta \vec{d}_{1,i}^* + \tau_2 \beta \vec{d}_{2,i}^*}$，或者 $T = g^{\tau_1 \eta \vec{d}_1^* + \tau_2 \beta \vec{d}_2^* + \tau_3 \vec{d}_3^*}$，$T_i = g^{\tau_1 \eta \vec{d}_{1,i}^* + \tau_2 \beta \vec{d}_{2,i}^* + \tau_3 \vec{d}_{3,i}^*}$。

引理 1 若存攻击者 $\mathcal{A}$ 能够在多项式时间以不可忽略的优势 ε 区分 Game_{real} 与 Game_0，那么就可以构造一个多项式时间算法，挑战者 $\mathcal{S}$ 以同样的优势 ε 攻破子空间假设。

证明：挑战者 $\mathcal{S}$ 将与攻击者 $\mathcal{A}$ 模拟 Game_{real} 或 Game_0。

首先，挑战者 $\mathcal{S}$ 定义对偶正交基 (B, B^*) 和 (B_i, B_i^*) 如下：

$$\vec{b}_1 = \eta \vec{d}_1^*, \vec{b}_2 = \beta \vec{d}_2^*, \vec{b}_3 = \vec{d}_3^*, \vec{b}_1^* = \eta^{-1} \vec{d}_1, \vec{b}_2^* = \beta^{-1} \vec{d}_2, \vec{b}_3^* = \vec{d}_3$$

$$\vec{b}_{1,i} = \eta \vec{d}_{1,i}^*, \vec{b}_{2,i} = \beta \vec{d}_{2,i}^*, \vec{b}_{3,i} = \vec{d}_{3,i}^*, \vec{b}_{4,i} = \vec{d}_{4,i}^*, \vec{b}_{1,i}^* = \eta^{-1} \vec{d}_{1,i}$$

$$\vec{b}_{2,i}^* = \beta^{-1} \vec{d}_{2,i}, \vec{b}_{3,i}^* = \vec{d}_{3,i}, \vec{b}_{4,i}^* = \vec{d}_{4,i}$$

挑战者 $\mathcal{S}$ 随机选择 $\tilde{a}_1, \tilde{a}_2 \in Z_p$，令 $a_1 = \eta \tilde{a}_1$，$a_2 = \beta \tilde{a}_2$，计算 $e(g,g)^{a_1} = e_3(g^{\vec{d}_1}, g^{\eta \vec{d}_1^*})^{\tilde{a}_1}$，$e(g,g)^{a_2} = e_3(g^{\vec{d}_2}, g^{\beta \vec{d}_2^*})^{\tilde{a}_2}$，然后随机选择 $\{u_x\}_{x=0}^n \in Z_p$，计算 g^{u_x} 等项，向攻击者 $\mathcal{A}$ 发布公开参数 PK。

对于攻击者 $\mathcal{A}$ 的密钥询问请求，挑战者 $\mathcal{S}$ 首先随机选择 $\tilde{t}_1, \tilde{t}_2 \in Z_p$ 和以 $\tilde{t}_1, \tilde{t}_2$ 为首元素的向量 $\tilde{v}_1, \tilde{v}_2 \in Z_p^f$，然后对于询问中 A 的每一行，随机选择 $\tilde{r}_{1,j}, \tilde{r}_{2,j}, r_{4,j} \in Z_p$。令 $t_1 = \eta \tilde{t}_1$，$t_2 = \beta \tilde{t}_2$，$\vec{v}_1 = \eta \tilde{v}_1$，$\vec{v}_2 = \beta \tilde{v}_2$，$r_{1,j} = \eta \tilde{r}_{1,j}$，$r_{2,j} = \beta \tilde{r}_{2,j}$，计算密钥如下：

$$K^0 := (g^{\vec{d}_1})^{(\tilde{a}_1 + \tilde{t}_1)} (g^{\vec{d}_2})^{(\tilde{a}_2 + \tilde{t}_2)}$$

$$K_j^1 := (g^{\vec{d}_1})^{\tilde{r}_{1,j}} (g^{\vec{d}_2})^{\tilde{r}_{2,j}}$$

$$K_j^2 := (g^{\vec{d}_{1,\rho(j)}})^{(A_j \cdot \tilde{v}_1 + \tilde{r}_{1,j})} (g^{\vec{d}_{2,\rho(j)}})^{(A_j \cdot \tilde{v}_2 + \tilde{r}_{2,j})} (g^{\vec{d}_{4,\rho(j)}})^{f(id) r_{4,j}}$$

$$K_j^3 := g^{r_{4,j}}$$

挑战阶段，攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{S}$ 提交等长的 M_0, M_1、属性集 ω 和身份模式 P，挑战者抛掷一枚公平硬币 $b \in \{0,1\}$，然后生成 $s_4 \in Z_p$，令 $s_1 = \tau_1, s_2 = \tau_2$，计算半功能密文如下：

$$C_0 := M_b e_3(g^{\vec{d}_1}, T)^{\tilde{a}_1} e_3(g^{\vec{d}_2}, T)^{\tilde{a}_2}$$

$$C_1 := T$$

$$C_{2,i} := T_i (g^{\vec{d}_{4,i}^*})^{s_4}$$

$$C_{3,ip,is} = (g^{u_0} \prod_{x \in id, x \in 1, \cdots, ip, n-is+1, \cdots, n} g^{u_x})^{s_4}$$

$$C_{3,x} := (g^{u_x})^{s_4}$$

当 $T = g^{\tau_1 \eta \vec{d}_1^* + \tau_2 \beta \vec{d}_2^*}$，$T_i = g^{\tau_1 \eta \vec{d}_{1,i}^* + \tau_2 \beta \vec{d}_{2,i}^*}$ 时，加密结果为本文方案的正常密文；当 $T = g^{\tau_1 \eta \vec{d}_1^* + \tau_2 \beta \vec{d}_2^* + \tau_3 \vec{d}_3^*}$，$T_i = g^{\tau_1 \eta \vec{d}_{1,i}^* + \tau_2 \beta \vec{d}_{2,i}^* + \tau_3 \vec{d}_{3,i}^*}$ 时，令 $s_3 = \tau_3$，加密结果为半功能密文。

引理 2 若存攻击者 $\mathcal{A}$ 能够在多项式时间以不可忽略的优势 ε 区分 $\mathrm{Game}_{l-1,2}$ 与 $\mathrm{Game}_{l,1}$，那么就可以构造一个多项式时间算法，挑战者 $\mathcal{S}$ 以同样的优势 ε 攻破子空间假设。

证明：挑战者 $\mathcal{S}$ 将与攻击者 $\mathcal{A}$ 模拟 $\mathrm{Game}_{l-1,2}$ 或 $\mathrm{Game}_{l,1}$。

挑战者 $\mathcal{S}$ 将 (D, D^*) 和 $(D_1, D_1^*), \cdots, (D_w, D_w^*)$ 作为模拟构造的对偶正交基，随机选择 $\tilde{a}_1, \tilde{a}_2 \in Z_p$，令 $a_1 = \eta \tilde{a}_1$，$a_2 = \beta \tilde{a}_2$，计算 $e(g,g)^{a_1} = e_3(g^{\vec{d}_1}, g^{\eta \vec{d}_1^*})^{\tilde{a}_1}$，$e(g,g)^{a_2} = e_3(g^{\vec{d}_2}, g^{\beta \vec{d}_2^*})^{\tilde{a}_2}$，然后随机选择 $\{u_x\}_{x=0}^n \in Z_p$，计算 g^{u_x} 等项，向攻击者 $\mathcal{A}$ 发布公开参数 PK。

对于攻击者 $\mathcal{A}$ 的前 $l-1$ 次密钥询问请求，挑战者 $\mathcal{S}$ 首先随机选择 $\tilde{t}_1, \tilde{t}_2, \gamma \in Z_p$ 和以 $\tilde{t}_1, \tilde{t}_2$ 为首元素的向量 $\tilde{v}_1, \tilde{v}_2 \in Z_p^f$，然后对于询问中 A 的每一行，随机选择 $\tilde{r}_{1,j}, \tilde{r}_{2,j}, r_{4,j} \in Z_p$。令 $t_1 = \eta \tilde{t}_1$，$t_2 = \beta \tilde{t}_2$，$\vec{v}_1 = \eta \tilde{v}_1$，$\vec{v}_2 = \beta \tilde{v}_2$，$r_{1,j} = \eta \tilde{r}_{1,j}$，$r_{2,j} = \beta \tilde{r}_{2,j}$，计算第二类半功能密钥如下：

$$K^0 := (g^{\eta \vec{d}_1^*})^{(\tilde{a}_1 + \tilde{t}_1)} (g^{\beta \vec{d}_2^*})^{(\tilde{a}_2 + \tilde{t}_2)} (g^{\vec{d}_3^*})^{\gamma}$$

$$K_j^1 := (g^{\eta \vec{d}_1^*})^{\tilde{r}_{1,j}} (g^{\beta \vec{d}_2^*})^{\tilde{r}_{2,j}}$$

$$K_j^2 := (g^{\eta \vec{d}_{1,\rho(j)}^*})^{(A_j \cdot \tilde{v}_1 + \tilde{r}_{1,j})} (g^{\beta \vec{d}_{2,\rho(j)}^*})^{(A_j \cdot \tilde{v}_2 + \tilde{r}_{2,j})} (g^{\vec{d}_{4,\rho(j)}^*})^{f(id) r_{4,j}}$$

$$K_j^3 := g^{r_{4,j}}$$

对于攻击者 $\mathcal{A}$ 的第 l 次密钥询问请求，挑战者 $\mathcal{S}$ 随机选

择$\tilde{v}_1,\tilde{v}_2,\tilde{v}_3\in Z_p^l$，其中$\tilde{v}_1,\tilde{v}_2$的首元素为0，$\tilde{v}_3$的首元素为1，对于询问中$A$的每一行，随机选择$\tilde{r}_{1,j},\tilde{r}_{2,j},\tilde{r}_{3,j},r_{4,j}\in Z_p$，令$t_1=\eta\tau_1,t_2=\beta\tau_2,\vec{v}_1=\eta\tau_1\tilde{v}_3+\eta\tilde{v}_1,\vec{v}_2=\beta\tau_2\tilde{v}_3+\beta\tilde{v}_2,r_{1,j}=\eta\tau_1\tilde{r}_{3,j}+\eta\tilde{r}_{1,j},r_{2,j}=\beta\tau_2\tilde{r}_{3,j}+\beta\tilde{r}_{2,j}$，计算密钥如下：

$K^0:=(g^{\eta\vec{d}_1^*})^{\tilde{a}_1}(g^{\beta\vec{d}_2^*})^{\tilde{a}_2}T$

$K_j^1:=(g^{\eta\vec{d}_1^*})^{\tilde{r}_{1,j}}(g^{\beta\vec{d}_2^*})^{\tilde{r}_{2,j}}T^{\tilde{r}_{3,j}}$

$K_j^2:=(g^{\eta\vec{d}_{1,\rho(j)}^*})^{(A_j\cdot\tilde{v}_1+\tilde{r}_{1,j})}(g^{\beta\vec{d}_{2,\rho(j)}^*})^{(A_j\cdot\tilde{v}_2+\tilde{r}_{2,j})}(g^{\vec{d}_{4,\rho(j)}^*})^{f(id)r_{4,j}}T_{\rho(j)}^{(A_j\cdot\tilde{v}_3+\tilde{r}_{3,j})}$

$K_j^3:=g^{r_{4,j}}$

当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*}$，$T_{\rho(j)}=g^{\tau_1\eta\vec{d}_{1,\rho(j)}^*+\tau_2\beta\vec{d}_{2,\rho(j)}^*}$时，该密钥为正常密钥；当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*+\tau_3\vec{d}_3^*}$，$T_{\rho(j)}=g^{\tau_1\eta\vec{d}_{1,\rho(j)}^*+\tau_2\beta\vec{d}_{2,\rho(j)}^*+\tau_3\vec{d}_{3,\rho(j)}^*}$时，令$\gamma=\tau_3,\vec{v}_3=\tau_3\vec{v}_3,r_{3,j}=\tau_3\tilde{r}_{3,j}$，该密钥为第一类半功能密钥。由于$\tau_3$与$\tau_3\vec{v}_3$的首元素相等，此半功能密钥是象征的。根据文献[17]，在属性不重复使用的情况下，τ_3对于攻击者$\mathcal{A}$是完全不可知的，因此该密钥可以看作普通的第一类半功能密钥。

对于大于l次的密钥询问请求，挑战者$\mathcal{S}$以与前$l-1$次询问相似的方式返回正常密钥。

挑战阶段，挑战者$\mathcal{S}$随机选择$s_4\in Z_p$，令$s_1=\mu_1,s_2=\mu_2,s_3=\mu_3$，计算半功能密文如下：

$C_0=M_be_3(R,g^{\eta\vec{d}_1^*})^{\tilde{a}_1}e_3(R,g^{\beta\vec{d}_2^*})^{\tilde{a}_2}$

$C_1=R$

$C_{2,i}=R_i(g^{\vec{d}_{4,i}^*})^{s_4}$

$C_{3,ip,is}=(g^{u_0}\prod_{x\in id,x\in 1,\cdots,ip,n-is+1,\cdots,n}g^{u_x})^{s_4}$

$C_{3,x}:=(g^{u_x})^{s_4}$

引理3 若存攻击者$\mathcal{A}$能够在多项式时间以不可忽略的优势ε区分$\mathrm{Game}_{l,1}$与$\mathrm{Game}_{l,2}$，那么就可以构造一个多项式时间算法，挑战者$\mathcal{S}$以同样的优势ε攻破子空间假设。

证明：挑战者$\mathcal{S}$将与攻击者$\mathcal{A}$模拟$\mathrm{Game}_{l,1}$或$\mathrm{Game}_{l,2}$。

除了生成第l次询问的密钥K^0时，挑战者多生成一个随机数γ，计算$K^0:=(g^{\eta\vec{d}_1^*})^{\tilde{a}_1}(g^{\beta\vec{d}_2^*})^{\tilde{a}_2}T(g^{\vec{d}_3^*})^{\gamma}$而不是$K^0:=(g^{\eta\vec{d}_1^*})^{\tilde{a}_1}(g^{\beta\vec{d}_2^*})^{\tilde{a}_2}T$，其它部分与引理2相同。

当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*}$时，挑战者$\mathcal{S}$第$l$次询问生成的密钥为第二类半功能密钥；当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*+\tau_3\vec{d}_3^*}$时，有$K^0=g^{(a_1+t_1)\vec{b}_1^*+(a_2+t_2)\vec{b}_2^*}g^{(\tau_3+\gamma)\vec{b}_3^*}$，由于$\gamma'=\tau_3+\gamma$，对攻击者$\mathcal{A}$也是随机的，因此挑战者$\mathcal{S}$第$l$次询问生成的密钥为第一类半功能密钥。

引理4 若存攻击者$\mathcal{A}$能够在多项式时间以不可忽略的优势ε区分$\mathrm{Game}_{q,2}$与Game_{final}，那么就可以构造一个多项式时间算法，挑战者$\mathcal{S}$以同样的优势ε攻破子空间假设。

证明：挑战者$\mathcal{S}$将与攻击者$\mathcal{A}$模拟$\mathrm{Game}_{q,2}$或Game_{final}。

首先，挑战者$\mathcal{S}$将(D,D^*)和$(D_1,D_1^*),\cdots,(D_w,D_w^*)$作为模拟构造的对偶正交基，令$a_1=\eta\tau_1,a_2=\beta\tau_2$，计算$e(g,g)^{a_1}=e_3(g^{\vec{d}_1},T),e(g,g)^{a_2}=e_3(g^{\vec{d}_2},T)$，然后随机选择$\{u_x\}_{x=0}^n\in Z_p$，计算$g^{u_x}$等项，向攻击者$\mathcal{A}$发布公开参数$PK$。

对于密钥询问请求，挑战者$\mathcal{S}$随机选择$\tilde{t}_1,\tilde{t}_2,\gamma\in Z_p$，令$t_1=\eta\tilde{t}_1,t_2=\beta\tilde{t}_2$，计算$K^0:=(g^{\eta\vec{d}_1^*})^{\tilde{\tau}_1}(g^{\beta\vec{d}_2^*})^{\tilde{\tau}_2}T(g^{\vec{d}_3^*})^{\gamma}$，然后如引理2前$l-1$次询问计算$K_j^1,K_j^2,K_j^3$。由于$\gamma$和$\gamma+\tau_3$对于攻击者$\mathcal{A}$均是随机的，因此结果为第二类半功能密钥。

挑战阶段，挑战者$\mathcal{S}$随机选择$s_4\in Z_p$，令$s_1=\mu_1,s_2=\mu_2,s_3=\mu_3$，计算$C_0=M_be_3(R,T)$，然后如引理2计算$C_1,C_{2,i},C_3$。

当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*}$，$T_i=g^{\tau_1\eta\vec{d}_{1,i}^*+\tau_2\beta\vec{d}_{2,i}^*}$时，加密结果为半功能密文；当$T=g^{\tau_1\eta\vec{d}_1^*+\tau_2\beta\vec{d}_2^*+\tau_3\vec{d}_3^*}$，$T_i=g^{\tau_1\eta\vec{d}_{1,i}^*+\tau_2\beta\vec{d}_{2,i}^*+\tau_3\vec{d}_{3,i}^*}$时，$C_0=M_be(g,g)^{\mu_3\tau_3}e(g,g)^{a_1s_1+a_2s_2}$，对于攻击者$\mathcal{A}$，$e(g,g)^{\mu_3\tau_3}$为$G_T$上的随机值，加密结果为随机值。

如果攻击者$\mathcal{A}$能够以不可忽略的优势区分ε区分$\mathrm{Game}_{q,2}$与Game_{final}，那么挑战者$\mathcal{S}$就可以以不可忽略的优势ε攻破子空间假设。至此，定理1得证。

5 性能分析

令I表示解密时所用的属性集合。根据定义可知，计算e_n需完成n次双线性配对运算。本文方案解密时：对于每个$\rho(j)\in I$，得到X'时，计算$e_4(C_{2,\rho(j)},K_j^2)$、$e_3(C_1,K_j^1)$、$e(C_3',K_j^3)$需完成4+3+1=8次双线性配对运算，因此得到X需完成$8|I|$次双线性配对运算；得到Y时，计算$e_3(C_1,K^0)$需完成3次双线性配对运算。由此可知，本文方案解密时共需完成$8|I|+3$次双线性配对运算。根据相似分析，文献[12]方案解密时需完成$3|I|$次双线性配对运算。根据文献[14]，在80比特AES安全性上，1024比特超奇异椭圆曲线上合数阶群Tate双线性对运算开销大约是170比特Miyaji-Nakabayashi-Takano椭圆曲线上素数阶群Tate双线性对运算开销的50倍。令素数阶群双线性配对计算时间为t，合数阶群双线性配对计算时间则为$50t$。本文方案与文献[12] GWABE方案解密时双线性配对运算次数、解密计算开销以及是否在素数阶群上构造3个方面的比较关系如表1所列。由于双线性对计算在实现效率方面要远远低于其他运算[19]，表1中解密计算开销按照双线性配对的开销进行比较。

表1 性能比较

方案	解密配对次数	解密计算开销(80 bit AES)	合数/素数
文献[12]方案	3|I|	150|I|·t	合数
本文方案	8|I|+3	8|I|·t+3·t	素数

如表1所列，虽然本文方案解密时使用了约3倍于文献[12]方案的双线性配对次数，但是解密计算开销依然只是该方案的1/15左右，因此，本文方案效率更高。

结束语 本文在合数阶群GWABE方案的基础上，利用文献[15]中的对偶正交基技术，提出了素数阶群上自适应安全的GWABE方案；然后通过一系列两两不可区分的攻击游戏证明了方案的安全性；最后通过性能分析说明了该方案比文献[12]方案计算开销低。

参考文献

[1] Sahai A, Waters B. Fuzzy identity-based encryption[C]// EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

(下转第210页)

参 考 文 献

[1] Petzold C. Windows 程序设计(第 5 版 珍藏版)[M]. 方敏,张胜,梁路平,等译. 北京:清华大学出版社,2010:333-382

[2] Zaidan A A, Zaidan B B, Alanazi O H, et al. Novel approach for high (secure and rate) data hidden within triplex space for executable file[J]. Scientific Research and Essayss, 2010, 5(15): 1965-1977

[3] Long Fei-yu, Liu Jia-yong, Yuan Xi Software watermark based on structure transform of PE file import table[J]. Journal of Computer Applications, 2010, 30(1): 217-219(in Chinese)
龙飞宇,刘嘉勇,袁熹. 一种变换 PE 文件引入表结构的软件水印[J]. 计算机应用,2010,30(1):217-219

[4] Duanmu Qing-feng, Wang Yan-bo, Zhang Xiong-wei, et al. A spread spectrum software watermarking scheme based on the improt functions[J]. Journal of Computer Research and Development, 2009, 46(Suppl.): 88-92(in Chinese)
端木庆峰,王衍波,张雄伟,等. 基于导入函数引用次数的扩频软件水印方案[J]. 计算机研究与发展,2009,46(Suppl.):88-92

[5] Zhou Qing-lei, Li bin. Double software watermark scheme based on tamper-proofing[J]. Computer Engineering, 2013, 39(7): 185-188(in Chinese)
周清雷,李斌. 基于防篡改的双重软件水印方案[J]. 计算机工程,2013,39(7):185-188

[6] Zhang Meng, Chen Gou-xi, Zhang Peng-cheng. Executable file backdoor steganographic algorithm with highly efficient[J]. Application Research of Computers, 2013, 30(4): 1198-1200(in Chinese)
张萌,陈够喜,张鹏程. 高效可执行文件后门隐写算法[J]. 计算机应用研究,2013,30(4):1198-1200

[7] Jang J, Ji H, Hong J M, et al. Protecting Android applications with steganography-based software watermarking[C]// Proceedings of the 28th Annual ACM Symposium on Applied Computing. Coimbra, 2013: 1657-1658

[8] Wei Wei-min, Liu Kun, Wan Xiao-peng. High capacity information hiding based on PE file format[J]. Journal of Nanjing University of Science and Technology, 2015, 39(1): 45-49(in Chinese)
魏为民,刘锟,万晓鹏. PE 文件格式的大容量信息隐藏技术[J]. 南京理工大学学报,2015,39(1):45-49

[9] 刘家超. 基于行为分析的未知 PE 病毒检测技术研究[D]. 北京:北京邮电大学,2014

[10] Ji Yi-mu, Zhu Tong-hui, Chai Bo-zhou, et al. Hybrid encryption scheme and performance analsysi for user's privacy in cloud[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2015, 27(5): 631-638(in Chinese)
季一木,朱曈晖,柴博周,等. 云环境下用户隐私混合加密方案及其性能分析[J]. 重庆邮电大学学报(自然科学版),2015,27(5):631-638

(上接第 190 页)

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]// CCS2006. Alexandria, Virginia: ACM, 2006: 89-98

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy 2007. Berkeley, CA: IEEE, 2007: 321-334

[4] Hinek J, Jiang S, Safavi R, et al. Attribute-Based Encryption with Key Cloning Protection: Report 2008/478[R]. 2008

[5] Yu Shu-cheng, Ren Kui, Lou Wen-jing, et al. Defending Against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems[C]// Proceedings of the Security and Privacy in Communication Networks. Athens, Greece, 2009: 311-329

[6] Li Jin, Ren Kui, Zhu Bo, et al. Privacy-aware Attribute-based Encryption with User Accountability[C]// Proceedings of the Information Security Conference 2009. 2009: 347-362

[7] Wang Yong-tao, Chen Ke-fei, Chen Jian-hong. Attribute-Based Traitor Tracing[J]. Journal of Information Science and Engineering, 2011, 27(1): 181-195

[8] Ostrovsky R, Sahai A, Waters B. Attribute Based Encryption with Non-Monotonic Access Structures[C]// Proceedings of the 14th ACM Conference on Computer and Communication Security. Alexandria, New York, USA, 2007: 195-203

[9] Attrapadung N, Imai H. Conjunctive broadcast and attribute-based encryption[C]// Proceedings of the Pairing-Based Cryptography-Pairing 2009. Palo Alto, USA, 2009: 248-265

[10] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]// Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009: 619-636

[11] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]// Advances in Cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 62-91

[12] Ma Hai-ying, Zeng Guo-sun. An Attribute-Based Encryption Scheme for Traitor Tracing and revocation together[J]. Chinese Journal of Computers, 2012, 35(9): 1845-1855(in Chinese)
马海英,曾国荪. 可追踪并撤销叛徒的属性基加密方案[J]. 计算机学报,2012,35(9):1845-1855

[13] Naor D, Naor M, Lotspiech J. Revocation and Tracing Schemes for Stateless Receivers[C]// Proceedings of the CRYPTO 2001. Santa Barbara, California, USA, 2001: 41-62

[14] Freeman M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[C]// EUROCRYPT 2010. Berlin: Springer, 2010: 44-61

[15] Lewko A. Tools for simulating features of composite order bilinear groups in the prime order setting[C]// EUROCRYPT-2012. Berlin: Springer, 2012: 318-335

[16] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// CRYPTO 2001. Berlin: Springer, 2001: 213-229

[17] Lewko A, Waters B. Functional Encryption: New Proof Techniques and Advancing Capabilities[D]. The University of Texas at Austin, 2012

[18] Beimel A. Secure Schemes for Secret Sharing and Key Distribution[D]. Haifa, Israel: Israel Institute of Technology, Technion, 1996

[19] Feng Deng-guo, Chen Cheng. Research on Attribute-based Cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 1-12 (in Chinese)
冯登国,陈成. 属性密码学研究[J]. 密码学报,2014,1(1):1-12