·安全技术· 文章编号：1000-3428(2016)08-0096-05 文献标志码：A 中图分类号：TP309

具有扩展通配符的快速解密 ABE 方案

李作辉，陈性元

（信息工程大学 密码工程学院，郑州 450000）

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）能够较好地解决上述问题。针对现有 GWABE 方案解密计算开销随参与解密属性的数量线性增长的问题，利用双线性群上的数学性质，提出一种快速解密 ABE 方案，并将该方案的安全性归约到判定性 q-BDHE 假设。分析结果表明，该方案解密时双线性配对为常数次，在参数解密属性数量为 1 时，与基于属性的叛徒追踪方案和 GWABE 方案相同，随着参数解密属性数量增加，性能优势逐步变大。

关键词： 基于属性的加密；叛徒追踪；撤销；快速解密；双线性群

中文引用格式： 李作辉，陈性元. 具有扩展通配符的快速解密 ABE 方案[J]. 计算机工程，2016，42(8)：96-100.

英文引用格式： Li Zuohui，Chen Xingyuan. ABE Scheme of Fast Decryption with Generalized Wildcards[J]. Computer Engineering，2016，42(8)：96-100.

ABE Scheme of Fast Decryption with Generalized Wildcards

LI Zuohui，CHEN Xingyuan

（School of Security Engineering，Information Engineering University，Zhengzhou 450000，china）

【Abstract】 Traitor tracing and revocation are crucial to the use of Attribute-based Encryption（ABE）. ABE scheme with Generalized Wildcards（GWABE） is a convenient way to solve the problems. Since the decryption cost of existing GWABE scheme increases linearly with the number of attributes used in decryption，an ABE scheme with Fast decryption and Generalized wildcards（FGWABE） is proposed with the assistance of mathematical properties of bilinear group. This scheme is proven secure from the decisional *q*-parallel Bilinear Diffie-hellman Exponent（*q*-BDHE） assumption. Performance analysis result shows that the ciphertexts of this scheme can be decrypted with a constant number of pairings. When one attribute is used in decryption，this number in FGWABE is the same as that of Attribute-based Traitor Tracing（ABTT） scheme and GWABE scheme. FGWABE is more efficient as the number of attributes increases.

【Key words】 Attribute-based Encryption（ABE）；traitor tracing；revocation；fast decryption；bilinear group

DOI： 10.3969/j.issn.1000-3428.2016.08.018

1 概述

基于属性的加密（Attribute-based Encryption，ABE）自 Sahai 等[1]在欧洲密码学年度会议提出后受到广泛的关注。Goyal 等[2]提出了第 1 个密钥策略 ABE（Key-Policy Attribute-based Encryption，KP-ABE）方案，并根据密文、密钥与访问策略、属性的关联关系将 ABE 方案分为两类：密钥策略 ABE 和密文策略 ABE（Ciphertext-Policy Attribute-based Encryption，CP-ABE）。文献[3]提出一个 CP-ABE 方案，文献[4]提出了基于动态属性的加密方案。

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[5]于 2008 年提出了基于标号的 ABE 方案（token-based Attribute-Based Encryption，tk-ABE），该方案在密钥生成过程中引入用户标识，可有效防止密钥克隆。文献[6-7]分别提出了防滥用 ABE 方案和可追责的匿名 ABE 方案。文献[8]使用唯一身份标识用户，提出了基于属性的叛徒追踪方案（Attribute-based Traitor Tracing，ABTT），实现了密钥滥用者的身份追踪。文献[9]将撤销用户标识的“非”作为访问策略的一部

基金项目： 国家“973”计划基金资助项目(2011CB311801)。

作者简介： 李作辉(1981－)，男，副研究员、博士研究生，主研方向为公钥密码、网络安全；陈性元，教授、博士。

收稿日期： 2015-08-14 **修回日期：** 2015-09-18 **E-mail：** forestspringer@163.com

分,构建了支持即时撤销的 CP-ABE 方案。文献[10]构造了具有扩展通配符的 ABE 方案(ABE scheme with Generalized Wildcards, GWABE),并实现了叛徒追踪和撤销。

由于双线性配对开销是 ABE 方案解密开销的主要部分,上述 ABE 方案解密所需双线性配对次数均随参与属性数量呈线性增长,因此需要解密时双线性配对为常数次的快速解密 ABE 方案(ABE scheme with Fast decryption, FABE)。文献[11-12]分别提出了支持与门限访问结构的 FABE 方案。文献[13]提出了一个支持门限访问结构的 FABE 方案。文献[14]提出了支持一般访问结构的 FABE 方案。文献[15]从经典 ABE 方案出发,将解密所需双线性配对次数减少到常数。

本文利用双线性群上的数学性质,提出一种具有扩展通配符的快速解密 ABE 方案(ABE scheme with Fast decryption and Generalized Wildcards, FGWABE),并将该方案安全性归约到判定性 q-BDHE(q-parallel Bilinear Diffie-Hellman Exponent)假设。该方案支持任意可以表达为线性秘密分享体制(Linear Secret Sharing Schemes, LSSS)的单调访问策略,解密时双线性配对为常数次。同时,与文献[10]相似, FGWABE 方案能够与完全子树构架[16]结合,方便解决叛徒追踪和撤销问题。

2　预备知识

2.1　双线性对

定义 1　G 和 G_T 为阶为素数 p 的群,g 为群 G 的生成元[17]。定义双线性配对 $e:G\times G\rightarrow G_T$:

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

(2)非退化性:$e(g,g)\neq 1$。

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

2.2　线性秘密共享

定义 2　令 $\Lambda:=\{P_1,P_2,\cdots,P_n\}$ 表示参与方的集合[18]。对于访问结构 $\Phi\subseteq 2^{\Lambda}$,如果任意 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。

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。令 $(\boldsymbol{A},\rho)$ 表示访问结构 Φ,对于任意秘密 $s\in Z_p$,当 $S\in\Phi$ 时,存在集合 $J:=\{j:\rho(j)\in S\}$,可计算常数 $\{\omega_j\in Z_p\}_{j\in J}$,使得 $\sum_{j\in J}\omega_j\lambda_j=s$;当 $S\notin\Phi$ 时,这样的常数是不存在的。

2.3　困难假设

判定性 q-BDHE 假设[19]:给定一个群生成算法 $\Im$,定义如下分布。

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

$g\xleftarrow{R}G$

$a,s\xleftarrow{R}Z_p$

$D:=(C,p,g,g^s,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}})$

$T_0=e(g,g)^{a^{q+1}s},T_1\xleftarrow{R}G$

攻击者的优势为:

$adv:=|\Pr[A(D,T_0)=1]-\Pr[A(D,T_1)=1]|$

3　模型定义

3.1　系统模型

定义 3　对于长度为 n 的位串,身份模式为 $P:=P_{ip}\|*\|P_{is}$,其中,P_{ip} 和 P_{is} 分别为长度为 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 $n-is$[10]。

给定用户的身份 id 和身份模式 P,如果 id 可表示为 $P_{ip}\|id_*\|P_{is}$,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。

参照文献[10]的 GWABE 方案,FGWABE 方案由 4 个算法组成:初始化(Setup),密钥生成(KeyGen),加密(Enc),解密(Dec)。

$Setup(\lambda)\rightarrow PK,MSK$:输入安全参数 λ,输出系统公钥 PK 和主密钥 MSK。

$KeyGen(id,(\boldsymbol{A},\rho),MSK)\rightarrow d_{id,(\boldsymbol{A},\rho)}$:输入用户的身份 id,访问结构 $(\boldsymbol{A},\rho)$ 和 MSK,输出用户私钥 $d_{id,(\boldsymbol{A},\rho)}$。

$Enc(M,S,P,PK)\rightarrow CT$:输入消息 M,属性集 S,身份模式 P 和 PK,输出密文 CT。

$Dec(d_{id,(\boldsymbol{A},\rho)},CT)\rightarrow M$:输入 $d_{id,(\boldsymbol{A},\rho)}$ 和用 S 和 P 加密的密文 CT,仅当 $id\in_* P$ 且 S 满足访问结构 $(\boldsymbol{A},\rho)$ 时,用户 $(id,(\boldsymbol{A},\rho))$ 才能解密密文,否则,解密失败。

3.2　安全模型

参照文献[1,10],定义如下 FGWABE 方案的安全模型。

定义 4　FGWABE 方案在选择模型下是安全的,如果对于下述的游戏,敌手 A 在概率多项式时间内的攻击优势是可忽略的。

前提　敌手 A 声明挑战密文的属性集合 S^*。

初始化　仿真者 B 向敌手发布系统公钥。

询问 1　敌手 A 询问用户私钥,仿真者 B 生成并向敌手 A 发送私钥。敌手 A 可重复询问。

挑战　敌手 A 提交明文 M_0,M_1 和身份模式 P,仿真者 B 随机选择 $b\in\{0,1\}$,计算并向敌手 A 发送 $CT=Enc(M_b,S,P,PK)$。

询问 2 与询问 1 相同。

猜测 敌手 A 输出猜测值 b'。

若 $b'=b$ 且敌手 A 未询问 $id\in{}_*P, S^*$ 满足访问结构$(\boldsymbol{A},\rho)$的用户$(id,(\boldsymbol{A},\rho))$的密钥,则称敌手 A 获胜。敌手 A 在上述游戏中获胜的优势为 $adv:=|\Pr[b'=b]-1/2|$。

4 FGWABE 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 $n:=\mathrm{lb}|\mathcal{N}|$。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。

$Setup(\lambda)\rightarrow PK, MSK$:可信授权机构根据 λ 生成(p,G,G_T,e),随机选择 $a\in Z_p$;对于每个属性 $i\in W$,随机选择 $h_i\in Z_p$,令 $H_i=g^{h_i}$,对于每个 $x\in[0,n]$,选择随机数 $u_x\in Z_p$,令 $U_x=g^{u_x}$,输出系统公钥:

$$PK:=\{p,g,e(g,g)^a,\{H_i\}_{i=1}^{w},\{U_x\}_{x=0}^{n}\}$$

主密钥为:

$$MSK:=\{a\}$$

$KeyGen(id,(\boldsymbol{A},\rho),MSK)\rightarrow d_{id,(A,\rho)}$:$\boldsymbol{A}$ 为 l 行 n 列的矩阵,令 $\Gamma=\{d:\exists x\in[1,l],\rho(x)=d\}$,即 Γ 为 $\boldsymbol{A}$ 的所有行对应属性的集合,随机选择以 a 为首元素的向量 $\boldsymbol{v}\in Z_p^n$,对于 $\boldsymbol{A}$ 的每一行 A_j,随机选择 r_j,$r_j'\in Z_p$,令 $F(id)=U_0\prod_{j\in S(id)}U_j$,计算:

$$K_j:=g^{A_j\cdot v}H_{\rho(j)}^{r_j}F(id)r_j'$$

$$D_j:=g^{r_j},R_j:=g^{r_j'}$$

$$Q_{j,d}:=H_d^{r_j}\ \forall d\in\Gamma/\rho(j)$$

$Enc(M,S,P,PK)\rightarrow CT$:算法输入消息 $M\in G_T$,属性集合 $S\in W$,身份模式 $P:=P_{ip}\|*\|P_{is}$和系统公钥 PK,随机选择 $s\in Z_p$,计算如下密文 CT。

$$C_0:=Me(g,g)^{as},C_1:=g^s$$

$$C_i:=H_i^s\ \forall i\in S$$

$$C_3:=(C_{3,ip,is},C_{3,x}),C_{3,ip,is}=F(P_{ip}\|0\ \cdots 0\|P_{is})^s$$

$$C_{3,x}:=U_x^s\ \forall x\in[ip+1,n-is]$$

其中,位串 $P_{ip}\|0\ \cdots 0\|P_{is}$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。

$Dec(d_{id,(A,\rho)},CT)\rightarrow M$:输入使用身份模式 P 和属性集合 S 加密的密文 CT 时,如果 $id\in{}_*P$ 或 S 满足(A,ρ)不成立,则输出终止 $\perp$,否则,存在集合 $J\subseteq\{1,2,\cdots,l\}$,能够计算常数集合$\{\omega_j\}_{j\in J,\rho(j)\in S}$,使得$\sum_{j\in J}\omega_jA_j=(1,0,\cdots,0)$。令 $\Delta=\{x:\exists j\in J,\rho(j)=x\}$,即 Δ 为解密用到的属性集合,易知 $\Delta\subseteq S,\Delta\subseteq\Gamma$,定义函数$f(\Delta)=\sum_{i\in\Delta}h_i$。在解密前,对密钥进行预处理,对于任意 $j\in J$,计算:

$$\hat{K}_j=K_j\prod_{d\in\Delta/\rho(j)}Q_{j,d}=g^{A_j\cdot v}g^{f(\Delta)r_j}F(id)r_j'$$

对密文进行预处理,计算:

$$L=\prod_{i\in\Delta}C_i=g^{f(\Delta)s}$$

$$C_3':=C_{3,ip,is}\prod_{x\in S(id)\cap\{ip+1,\cdots,n-is\}}C_{3,x}=F(id)^s$$

在此基础上,计算:

$$X=\frac{e(C_1,\prod_{j\in J}\hat{K}^{\omega_{jj}})}{e(\prod_{j\in J}D_j^{\omega_j},L)e(C_3',R_j)},M=C_0/X$$

上述解密是正确的,因为:

$$\begin{aligned}X&=\frac{e(C_1,\prod_{j\in J}\hat{K}^{\omega_{jj}})}{e(\prod_{j\in J}D_j^{\omega_j},L)e(C_3',\prod_{j\in J}R_j^{\omega_j})}\\&=\frac{e(g^s,\prod_{j\in J}(g^{A_j\cdot v}g^{f(\Delta)r_j}F(id)r_j')^{w_j})}{e(\prod_{j\in J}g^{r_jw_j},g^{f(\Delta)s})e(F(id)^s,\prod_{j\in J}g^{r_j'w_j})}\\&=\frac{e(g^s,\prod_{j\in J}(g^{A_j\cdot v})^{w_j}\prod_{j\in J}g^{f(\Delta)r_jw_j}\prod_{j\in J}F(id)^{r_j'w_j})}{e(\prod_{j\in J}g^{r_jw_j},g^{f(\Delta)s})e(F(id)^s,\prod_{j\in J}g^{r_j'w_j})}\\&=e(g,g)^{as}\end{aligned}$$

5 安全性证明

定理 1 如果判定性 q-BDHE 假设成立,则 FGWABE 方案在选择模型下是安全的。

证明:如果存在一个敌手 A 以不可忽略的优势 ε 攻破 FGWABE 方案,就可以构造一个有效的仿真算法 B 以不可忽略的优势攻破判定性 q-BDHE 假设,那么根据反证法,可证明定理 1 成立。

假设一个挑战者 C 令 $q=w$,根据判定性 q-BDHE 假设,生成 $C,p,g,g^s,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}$,随机选择 $\mu\in\{0,1\}$,若 $\mu=0$,令 $T=e(g,g)^{a^{q+1}s}$,否则,令 T 为随机值,然后向仿真者 B 提供 $C,p,g,g^s,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}},T$。

前提 敌手 A 声明挑战密文的属性集合 S^*。

初始化 仿真者 B 随机选择 $a',z_1,z_2,\cdots,z_w\in Z_p$,令 $e(g,g)^a=e(g,g)^{a'}ve(g^a,g^{a^w})$,即令 $a=a'+a^{w+1}$。对于每个属性 $i\in W$,令:

$$H_i=\begin{cases}g^{z_i} & i\in S^*\\ g^{z_i}g^{a^i} & i\notin S^*\end{cases}$$

对于每个用户标识 $x\in[0,n]$,选择随机数 $u_x\in Z_p$,计算 $U_x=g^{u_x}$,向敌手发布系统公钥:

$$PK:=\{p,g,e(g,g)^a,\{H_i\}_{i=1}^{w},\{U_x\}_{x=0}^{n}\}$$

询问 1 敌手 A 询问用户$(id,(\boldsymbol{A},\rho))$的私钥,仿真者 B 执行如下两步。

第 1 步 生成有效密钥。

令 $Y=\{y:y\in[1,l],\rho(y)\in S^*\}$,选择以 1 为首

元素且满足 $\lambda_j'=\boldsymbol{A}_j\cdot\boldsymbol{v}'=0\ \forall\rho(j)\in S^*$ 的向量 $\boldsymbol{v}'$,由于 S 不满足$(\boldsymbol{A},\rho)$,向量 $\boldsymbol{v}'$是存在的,令 $\boldsymbol{v}=a\boldsymbol{v}'$,有 $\lambda_j=\boldsymbol{A}_j\cdot v=\boldsymbol{A}_j\cdot(a\boldsymbol{v}')=0\ \forall\rho(j)\in S^*$。

对于 $i\in Y$,令 $r_j=0$,随机选择 $r_j'\in Z_p$,计算:

$$K_j:=F(id)r_j'=g^{\lambda_j}H_{\rho(j)}^{r_j}F(id)r_j'$$

$$D_j:=1_G=g^{r_j},R_j:=g^{r_j'}$$

$$Q_{j,d}:=1_G=T_d^{r_j}$$

对于 $i\notin Y$,令 $\lambda_j'=\boldsymbol{A}_j\cdot\boldsymbol{v}'$,$\lambda_j=\boldsymbol{A}_j\cdot\boldsymbol{v}=\boldsymbol{A}_j\cdot(a\boldsymbol{v}')=(a'+a^{w+1})\lambda_j'$,同时令 $R_j=g^{-\lambda_j'a^{(w+1)-\rho(j)}}$,即 $r_j:=-\lambda_j'a^{(w+1)-\rho(j)}$,随机选择 $r_j'\in Z_p$,计算:

$$\begin{aligned}K_j&:=g^{\lambda_j'a'}R_j^{z_{\rho(j)}}F(^id)r_j'\\&=g^{\lambda_j'a'}g^{\lambda_j'a^{w+1}}g^{-z_{\rho(j)}\lambda_j'a^{(w+1)-\rho(j)}}\\&\cdot(g^{a^{\rho(j)}})^{-\lambda_j'a^{w+1}a^{-\rho(j)}}F(id)^{r_j'}\\&=g^{\lambda_j}(g^{z_{\rho(j)}})^{r_j}(g^{a^{\rho(j)}})^{r_j}F(id)^{r_j'}\\&=g^{\lambda_j}H_{\rho(j)}^{r_j}F(id)^{r_j'}\end{aligned}$$

同时计算:

$$D_j:=g^{r_j}=g^{-\lambda_j'a^{(w+1)-\rho(j)}}$$

$$R_j:=g^{r_j'}$$

$$Q_{j,d}:=g^{-z_d\lambda_j'a^{(w+1)-\rho(j)}}=H_d^{r_j}\ \text{if}\ d\in S^*$$

$$\begin{aligned}Q_{j,d}&:=g^{-z_d\lambda_j'a^{(w+1)-\rho(j)}}g^{-\lambda_j'a^{(w+1)-\rho(j)+d}}\\&=H_d^{r_j}\ \text{if}\ d\notin S^*\end{aligned}$$

第 2 步　对生成的密钥进行随机化。

目前生成的密钥对于敌手来说不是随机的,因此需要进行随机化。生成以 0 为首元素的向量 $\boldsymbol{v}''$,则 $\lambda_j''=\boldsymbol{A}_j\cdot\boldsymbol{v}''$是对秘密 0 的拆分。

对于 $\boldsymbol{A}$ 的每一行,随机选择 $\gamma_j,\gamma_j'\in Z_p$,通过下计算实现密钥随机化。

$$K_j':=K_jg^{\lambda_j''}H_{\rho(j)}^{\gamma_j}F(^id)\gamma_j',D_j':=D_jg^{\gamma_j}$$

$$R_j':=R_jg^{\gamma_j'},Q_{j,d}:=Q_{j,d}H_d^{\gamma_j}$$

挑战　敌手 A 提交两条同样长度的明文 M_0,M_1,仿真者 B 随机选择一个条明文 M_b,计算如下密文 CT。

$$C_0:=M_be(g,g^s)^{a'}T,C_1:=g^s$$

$$C_{2,i}:=(g^s)z_i=H_i^s\ \forall i\in S$$

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

$$\begin{aligned}C_{3,ip,is}&:=(g^s)u_{0_{j\in S(P_{ip}\|0\cdots0\|P_{is})}}\prod(g^s)u_j\\&=F(P_{ip}\|0\ \cdots0\|P_{is})^s\end{aligned}$$

$$C_{3,x}:=(g^s)u_x=U_x^s\ \forall x\in[ip+1,n-is]$$

询问 2　与询问 1 相同。

猜测　敌手发布 b'。如果 $b'=b$,则仿真者 B 输出 $\mu'=0$;否则输出 $\mu'=1$。

当 $\mu=0$ 时,挑战密文是一条合法的密文,在这种情况下,敌手 A 能够以不可忽略的优势 $\varepsilon=\Pr[b=b']-1/2$ 攻破 FGWABE 方案。易知 $\Pr[b=b']=\Pr[\mu=\mu'|\mu=0]$,因此当 $\mu=0$ 时,仿真者 B 的优势为 $\Pr[\mu=\mu'|\mu=0]=\Pr[b=b']=\varepsilon+1/2$。

当 $\mu=1$ 时,挑战密文中 C_0 为随机值,不包含 M_b 的任何信息。在这种情况下,敌手 A 不具有任何优势。易知 $\Pr[\mu=\mu'|\mu=1]=\Pr[b\neq b']=1/2$。

最终,仿真者 B 攻破判定性 q-BDHE 假设的优势为:

$$\begin{aligned}&\frac{1}{2}\Pr[\mu=\mu'|\mu=0]\\&\quad+\frac{1}{2}\Pr[\mu=\mu'|\mu=1]-\frac{1}{2}\\&=\frac{1}{2}\left(\varepsilon+\frac{1}{2}\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}\end{aligned}$$

至此,定理 1 得证。

6　性能分析

由于解密是 ABE 方案应用中的高频行为,因此解密开销是 ABE 方案计算开销的最主要部分。令 I 表示解密时所用的属性集合。FGWABE 方案解密时需完成 $e(C_1,\prod_{j\in J}\hat{K}\omega_{jj})$,$e(\prod_{j\in J}D_j^{\omega_j},L)$ 和 $e(C_3',R_j)$ 共 3 次双线性配对。表 1 是 FGWABE 方案与文献[8,10]方案解密时双线性配对次数和支持访问策略的比较关系。

表 1　性能比较

方案	解密时双线性配对次数	访问策略
文献[8]方案	$3\|I\|$	门限访问策略
文献[10]方案	$3\|I\|$	LSSS 访问策略
FGWABE 方案	3	LSSS 访问策略

如表 1 所示,不考虑文献[10]方案构建在合数阶上,在双线性配对效率更低的情况下,FGWABE 方案解密时双线性配对为常数次,在参数解密属性数量为 1 时,与文献[8,10]方案相同,随着参数解密属性数量增加,性能优势逐步变大。

7　结束语

针对现有 GWABE 方案解密计算开销随参与属性的数量线性增长的状况,本文设计一种具有扩展通配符的快速解密 ABE 方案(FGWABE),同时在选择模型下证明了该方案的安全性。由于 FGWABE 对密钥进行了扩充,每个 H_i均被多次使用,而经典的基于对偶系统加密[20]的 ABE 方案自适应安全证明过程依赖一个统计意义假设,而该假设只有在密钥中 H_i不重复出现才能成立。因此,设计新的证明方法,构建自适应安全的 FGWABE 方案是下一步的研究方向。

参考文献

[1] Sahai A, Waters B. Fuzzy Iidentity-based Encryption[C]//Proceedings of Advances in Cryptology-EUROCRYPT'05. Berlin, Germany: Springer-Verlag, 2005:457-473.

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA:ACM Press,2006:89-98.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption[C]//Proceedings of 2007 IEEE Symposium on Security and Privacy. Washington D.C., USA:IEEE Computer Society,2007:321-334.

[4] 邓宇乔. 基于动态属性的加密方案[J]. 计算机工程, 2014,40(4):136-140.

[5] Hinek J, Jiang S, Safavi R, et al. Attribute-based Encryption with Key Cloning Protection[J]. Bulletin of the Korean Mathematical Society,2008(4):803-819.

[6] Yu Shucheng, Ren Kui, Lou Wenjing, et al. Defending Against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems[C]//Proceedings of Conference on Security and Privacy in Communication Networks. Berlin, Germany:Springer-Verlag,2009:311-329.

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

[8] Wang Yongtao, Chen Kefei, Chen Jianhong. Attribute-based Traitor Tracing[J]. Journal of Information Science and Engineering,2011,27(1):181-195.

[9] 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. New York, USA: ACM Press, 2007:195-203.

[10] 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.

[11] Emura K, Miyaji A, Nomura A, et al. A Ciphertext-policy Attribute-based Encryption Scheme with Constant Ciphertext Length[C]//Proceedings of Conference on Information Security Practice and Experience. Berlin, Germany:Springer-Verlag,2009:13-23.

[12] Chen Cheng, Zhang Zhenfeng, Feng Dengguo. Efficient Ciphertext Policy Attribute-based Encryption with Constant-size Ciphertext and Constant Computation-cost[C]//Proceedings of Conference on Provable Security. Berlin, Germany: Springer-Verlag, 2011: 84-101.

[13] Herranz J, Laguillaumie F, Rùfols C. Constant Size Ciphertexts in Threshold Attribute-based Encryption[C]//Proceedings of PKC'10. Berlin, Germany: Springer-Verlag,2010:19-34.

[14] Attrapadung N, Libert B, de Panafieu E. Expressive Key-policy Attribute-based Encryption with Constant-size Ciphertexts[C]//Proceedings of PKC'11. Berlin, Germany:Springer-Verlag,2011:90-108.

[15] Hohenberger S, Waters B. Attribute-based Encryption with Fast Decryption[C]//Proceedings of Public-key Cryptography-PKC'13. Berlin, Germany: Springer-Verlag,2013:162-179.

[16] Naor D, Naor M, Lotspiech J. Revocation and Tracing Schemes for Stateless Receivers[C]//Proceedings of Advances in Cryptology-Crypto'01. Berlin, Germany: Springer-Verlag,2001:41-62.

[17] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proceedings of Advances in Cryptology-Crypto'01. Berlin, Germany: Springer-Verlag,2001:213-229.

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

[19] Dan B, Xavier B, Eujin G. Hierarchical Identity Based Encryption with Constant Size Ciphertext[C]//Proceedings of Advances in Cryptology-Eurocrypt'05. Berlin, Germany:Springer-Verlag,2005:440-456.

[20] Waters B. Dual System Encryption: Realizing Fully Secure IBE and HIBE Under Simple Assumptions[C]//Proceedings of Advances in Cryptology-Crypto'09. Berlin, Germany:Springer-Verlag,2009:619-636.

编辑 索书志

(上接第 95 页)

[18] 李天华, 邹艳丽, 唐贤健, 等. 加权无标度网络的免疫策略研究[J]. 计算机工程,2010,36(22):158-160.

[19] 苏义鑫, 廉 城. 基于加权 BBV 网络的手机短信息传播研究[J]. 系统仿真学报,2013,25(2):322-326.

[20] 汪小帆, 李 翔, 陈关荣. 网络科学导论[M]. 北京: 高等教育出版社,2012.

[21] Yan Gang, Zhou Tao, Wang Jie, et al. Epidemic Spread in Weighted Scale-free Networks[J]. Chinese Physics Letters,2005,22(2):510-513.

[22] Newman M E J. The Structure of Scientific Collabora-tion Networks[J]. Proceedings of National Academy of Sciences of the United States of America,2001,98(2):404-409.

[23] Newman M E J. Finding Community Structure in Networks Using the Eigenvectors of Matrices[J]. Physical Review E,2006,74(3).

[24] Batagelj V, Mrvar A. Pajek Datasets[EB/OL]. [2015-08-15]. http://vlado.fmf.uni-lj.si/pub/networks/data/>.

编辑 索书志