doi:10.3969/j.issn.1000-436x.2013.11.006

双向匿名的基于属性的密钥隔离签密

张兴兰，张振
(北京工业大学 计算机学院，北京 100124)

摘 要：为解决发送者和接收者都具有匿名性的基于属性签密方案中密钥泄露的问题，将密钥隔离机制引入到基于属性签密方案中，给出了基于属性密钥隔离签密的形式化定义和安全模型，构建了随机预言模型下安全的基于属性的密钥隔离签密方案。改进后的方案不仅没有失去原有的双向匿名性，而且满足前向安全性和后向安全性的要求，减轻了密钥泄露带来的危害。最后在安全模型的基础上，给出了双向匿名的基于属性的密钥隔离签密的机密性、认证性和匿名性的安全性证明。

关键词：基于属性签密；属性基；密钥隔离；密钥泄露；双向匿名
中图分类号：TP309 **文献标识码：**A **文章编号：**1000-436X(2013)11-0042-09

Attribute-based key-insulated signcryption with bidirectional anonymity

ZHANG Xing-lan, ZHANG Zhen
(College of Computer Science, Beijing University of Technology, Beijing 100124, China)

Abstract: To solve exposure of secret key in attribute-based signcryption with anonymity for both sender and receiver, key-insulation mechanism to attribute-based signcryption was untroduced. Given the formal definition and security notions, the scheme of attribute-based key-insulated signcryption was proposed, which is provably secure under the random oracle model. The improved scheme not only satisfies the requirement of bidirectional anonymity, but also achieves forward security and afterward security, consequently reduced the hazard of key exposure. Finally, confidentiality, authentication and anonymity in attribute-based key-insulated signcryption scheme were proved based on given security notions.
Key words: attribute-based signcryption; attribute based; key insulated; key exposure; bidirectional anonymity

1 引言

为了改善基于生物信息的身份加密系统的容错性，SAHAI 和 WATERS [1]在 2005 年欧洲密码年会上发表了《Fuzzy Identity Based Encryption》一文，首次提出了基于属性加密(ABE, attribute-based encryption)的概念。基于属性加密方案[1]通过引入门限方案思想[2]将基于身份加密方案[3,4]中表示用户身份的唯一标识符泛化为表示用户身份的属性集合，属性集合由一个或多个属性组成，可表示一个或多个用户组成的用户组。基于属性加密[1]将基于身份加密[3,4]中加密者与解密者之间的一对一通信扩展为一对多保密通信。另外，属性集合还可以与访问结构相结合，实现密文策略[5]和密钥策略[6]的属性加密。不久，MAJI 等[7]提出了基于属性的签名方案，并支持访问结构与属性的结合。LI 等[8]为解决签名者的匿名性，提出了基于属性的环签名。GAGNE 等[9]结合基于属性加密和基于属性签名首次提出了(t, n)门限的基于属性加密方案，该方案不仅提供了消息的保密性，也提供了消息的认证性，而且签密的效率高于传统的“先签名后加密”的效率，但该方案没有提供默认属性集合，因此签密者和加密者的签密的属性个数是固定的，不适用于属性个数小于 t 的情况。EMURA 方案[10]描述了正在

收稿日期：2013-06-17；修回日期：2013-09-28
基金项目：国家自然科学基金资助项目(61272044)
Foundation Item: The National Natural Science Foundation of China(61272044)

进行基于属性签密的研究工作，但并没有提出具体的动态的基于属性签密方案。LIU 方案[11]提出了矢量空间的属性基签密方案，但不具有匿名性。WANG 方案[12]提出了基于属性的密文策略的断言签密，但并没有给出所提方案的安全性证明。WEI 方案[13]含有(t- 1)默认属性的属性集合，用户可使用 k(k<t)个属性，加上(t- k)默认属性进行签密，而且该方案具有双向匿名性，文献[13]最后给出了方案一的机密性、不可伪造性和匿名性的证明。由于基于属性加密机制的模糊身份优点，吸引了大量的人员研究[5~13]。

为解决前向安全的密码体制[14]只能保证在密钥泄漏发生之前的安全性不能保证之后的安全性的问题，DODIS 和 KATZ 等[15]提出了密钥隔离的概念，它既能保证前向安全性，又能保证后向安全性。其主要思想是：将整个生命周期内，划分成若干时间片，用户私钥由临时私钥和协助器密钥两部分构成，临时私钥存储在用户设备中，而协助器密钥存储在协助器中，用户设备通过与协助器的交互来定期更新临时私钥。协助器密钥只负责时间片开始时临时私钥的更新，而不参与密文的解密操作，所以某些时间片的临时私钥泄漏，不会对其他时间片的临时私钥的安全性构成威胁。

2　相关研究

密钥隔离公钥加密概念首先由 DODIS 和 KATZ 等[15]提出，BELLARE 等[16]针对其只满足(t, N)密钥隔离的安全性，而且对时间片段数目有限制的缺点提出了一个新的密钥隔离方案[16]，该方案满足强密钥隔离和完备密钥隔离安全性，并且支持随机密钥更新和无限制的时间片段数目。HANAOKA 等[17]针对 BELLARE 方案[16]的单一协助器的不足提出了并行密钥隔离的概念并构造了并行密钥隔离的公钥加密方案[17]。HANAOKA 等[18]后来又将密钥隔离机制引入到基于身份的加密系统中，WENG 等人[19,20]针对多个协助器提出了标准模型下安全的基于身份的门限密钥隔离加密方案[19]和并行密钥隔离加密方案[20]。CHEN 等[21,22]将密钥隔离机制引入到基于属性加密系统中，提出了密文策略的基于属性的并行密钥隔离加密方案[21]和门限结构的基于属性的密钥隔离加密方案[22]，陈剑洪[23]提出了签名者匿名的基于属性的密钥隔离签名方案，并在标准模型下给出了所提方案的安全性证明。

3　预备知识

3.1　双线性映射

设 p 是一个大素数，G、G_T 是 2 个阶为 p 的循环乘法群，G 到 G_T 的双线性映射 $e: G\times G? G_T$ 满足以下性质。

1) 双线性:对于 $\forall g, h\in G, \forall a, b\in \mathbb{Z}_p^*$，均有 $e(g^a, h^b)=e(g, h)^{ab}$ 成立。

2) 非退化性:存在 $g, h\in G$，满足 $e(g, h)?1$。

3) 可计算性:对于所有的 $g, h\in G$，存在一个有效的算法计算 $e(g, h)$。

3.2　困难问题假设

定义 1　判定双线性 Diffie-Hellman (DBDH) 问题及假设：给定 2 个四元组(g^a, g^b, g^c, g^{abc})和(g^a, g^b, g^c, g^z)，其中，$a, b, c, z\in \mathbb{Z}_p^*$是随机的。设 k 为安全参数，概率多项式时间内攻击算法 B 解决 DBDH 问题的优势 $Adv_B^{DBDH}(k)$ 的定义为

$$Adv_B^{DBDH}(k) = |Pr[B(g^a, g^b, g^c, g^{abc}) = 1] - Pr[B(g^a, g^b, g^c, g^z) = 1]|$$

假设:对任意概率多项式时间内的攻击算法 B, $Adv_B^{DBDH}(k)$ 是可以忽略的。

定义 2　计算 Diffie-Hellman (CDH) 问题及假设: 给定输入(g, g^a, g^b)，计算输出 g^{ab}，其中，$a, b\in \mathbb{Z}_p^*$, $g, g^a, g^b\in G$。设 k 为安全参数，概率多项式时间内攻击算法 B 成功解决 CDH 的优势 $Adv_B^{CDH}(k)$ 的定义为

$$Adv_B^{CDH}(k) = Pr[B(g, g^a, g^b) = g^{ab}],\ a, b\in \mathbb{Z}_p^*$$

CDH 假定: 对任意概率多项式时间内的攻击算法 B， $Adv_B^{CDH}(k)$ 是可以忽略的。

4　方案的形式化定义及安全模型

4.1　语法定义

双向匿名的基于属性的密钥隔离签密由以下 6 个算法构成。

1) $Setup(k, d)$? (cp, msk)　该算法由密钥生成中心执行，输入安全参数 k，门限值 d，输出系统公开参数 cp 和系统主密钥 msk。

2) $Extract(cp, msk, ?)$? $(TK_?, _0, HK_?)$ 该算法由密钥生成中心执行，输入系统公开参数 cp，系统主密钥 msk，用户的属性集合 $?$，该算法输出用户属性集合 $?$ 对应的临时私钥 $TK_{?,0}$ 和协助器密钥 $HK_?$。

3) $HelperUpdate(cp, t', t, ?, HK_?)$? $UI_{w,t',t}$ 该算法由协助器执行，输入公开参数 cp，时间片 t'和 t，用户属性集合 $?$ 及协助器密钥 $HK_?$，输出属性集合为 $?$ 的用户的临时私钥由时间片段 t'更新到 t 所需的更新信息$UI_{w,t',t}$。

4) $UserUpdate(cp, t', t, ?, UI_{w,t',t}, TK_{w,t'})$? $TK_{w,t}$ 该算法由用户执行，输入公开参数 cp，用户属性集合 $?$，协助器产生的更新信息$UI_{w,t',t}$，t'时间片的用户密钥$TK_{w,t'}$，输出 t 时间片的用户密钥$TK_{w,t}$。

5) $Signcrypt(cp, t, m, TK_{w_S,t}, ?_S', ?_R)$? (t, s) 该算法由签密者执行，输入公开参数 cp，时间片 t，需要签密的明文 m，签密者的私钥$TK_{?_S,t}$，签密者使用的拥有属性 $?_S$的子集 $?_S'$进行签密，即 $?_S' \subseteq ?_S$，接收者属性集合为 $?_R$，输出签密密文(t,s)。

6) $Unsigncrypt(cp,(t,s), TK_{w_R,t})$该算法由接收者执行，输入公开参数 cp，对消息 m 的签密密文(t,s)和接收者的 t 时间片的用户私钥$TK_{w_R,t}$，若签密密文合法，则成功解密出明文 m，否则输出$\perp$。

4.2 安全模型

定义 3 机密性。在基于属性的密钥隔离签密方案中，如果不存在多项式时间的攻击算法 A 以不可忽略的优势赢得以下游戏，则称该方案在适应性选择密文攻击下具有不可区分性(IND-KI-ABSC-CCA)。

初始化阶段：攻击算法 A 选择挑战的接收者的属性集合 $?_R$，挑战者 C 运行算法 $Setup(k,d)$? (cp, msk)，并将 cp 发送给 A，而秘密保存主密钥 msk。

询问阶段 A 能够执行以下多次询问。

散列值查询：A 向 C 查询它选择的任意字符串的散列值，C 控制着散列预言，返回对应的散列值。

私钥提取查询：如果属性集合 $?_u$ 满足 $?_R \not\subset ?_u$，C 运行算法 $Extract(cp,msk,?_u)$? $(TK_{?_u,0}, HK_{?_u})$并将生成的临时私钥 $TK_{?_u,0}$ 和协助器密钥 $HK_{?_u}$，发送给 A；否则，C 拒绝回应。

临时私钥查询：A 向 C 发送属性 $?_u$ 和时间片 t，C 运行算法 $UserUpdate(cp, t', t, ?_u, UI_{w_u,t',t}, TK_{w_u,t'})$? $TK_{w_u,t}$ 得到并发送给 A 临时私钥$TK_{w_u,t}$。

签密查询：A 询问$(m, ?', ?_j)$对应的签密密文，其中，m 为消息，$?'$为签名属性，$?_j$ 为接收者的属性，C 运行算法 $Extract(cp,msk,?')$,$UserUpdate(cp, t', t, ?', UI_{w',t',t}, TK_{w',t'})$，得到临时私钥 $TK_{?',t}$，运行签密算法(t,s)=$Signcrypt(cp, t, m, TK_{w',t}, ?', ?_j)$，并将$(t,s)$发送给 A。

解签密查询：从 A 得到签密密文(t,s)，C 运行算法 $Extract(cp, msk, ?_j)$，$UserUpdate(cp, t', t, ?_j, UI_{w_j,t',t}, TK_{w_j,t'})$得到临时私钥 $TK?_{j,t}$，运行解签密算法 $Unsigncrypt(cp,(t,s), TK_{w_j,t})$，若成功，返回 m 给 A，否则返回$\perp$。

挑战阶段：攻击者 A 向 C 发送 2 个长度相等的明文 M_0 和 M_1，挑战者 C 随机选择 $b \in \{0,1\}$，并在时间片 t 使用签名属性 $?'$和接收者属性 $?_R$ 对 M_b 签密(t,s)，发送给敌手 A。

询问阶段二：重复询问阶段，但不能对挑战的密文进行解签密查询。

猜测阶段：最后 A 输出 b 的一个猜测值 b'。如果 $b=b'$，A 赢得游戏。A 赢得游戏的优势定义为

$$Adv^{\text{IND-KI-ABSC-CCA}}(A) = |Pr[b'=b] - 1/2|$$

定义 4 不可伪造性。在基于属性的密钥隔离签密方案中，如果不存在多项式时间的伪造算法 A 以不可忽略的优势赢得以下游戏，则称该方案在适应性选择明文攻击下具有不可伪造性(EU-KI-ABSC-CMA)。

初始化阶段：A 选择挑战的签名属性集合 $?_S$，且$|?_S|<d$，其他与 4.2 节中的初始化阶段类似。

查询阶段：与 4.2 节中的查询阶段类似。

伪造阶段：攻击者 A 输出消息 m 以及时间片 t，签名属性为 $?_S$ 和接收者属性 $?_R$ 的签密密文(t,s)。如果(t,s)是针对$(m, ?_S, ?_R)$的 t 时间片的合法签密密文，并且$(m, ?_S, ?_R)$没有被查询，说攻击者 A 赢得该游戏，定义攻击者 A 的优势为

$$Adv^{\text{EUF-KI-ABSC-CMA}}(A) = |Pr[Unsigncrypt(cp,w_S,TK_{w_R,t},(t,s)) = m]|$$

定义 5 签密者匿名性。签密者匿名性要求在随机模型下不存在多项式时间攻击算法 A 以不可忽略的优势赢得以下游戏。

初始化阶段：A 选择挑战的签密属性集合 $?_S$，且$|?_S|<d$，C 选择 2 个属性集合 $?_{S_1}$ 和 $?_{S_2}$ 且 $?_S \not\subset ?_{S_1} \cap ?_{S_2}$.挑战者 C 运行 $Setup$ 算法，得到主密钥 x 和系统公开参数 cp，并发送 x 和 cp 发送给攻击者 A。在拥有主密钥的情况下，A 能够为自己产生私钥和签密密文。

挑战阶段：A 输出消息 m^*，接收者属性集合 $?_R$，签密属性集合 $?_S$，挑战者 C 从$\{1, 2\}$中选取 b，

计算签密结果s^*，并发送给攻击者 A。

猜测阶段：攻击者 A 试图从属性 $?_1^*$和 $?_2^*$的签名中猜测 b 的值为 b'，如果 $b'=b$，A 赢得游戏，优势定义为 $Adv^{\text{SA-ABKISC-CCA-SA}}(\text{A})=|Pr[b=b']-1/2|$。

定义 6　解密者匿名性。解密者匿名性要求在随机模型下不存在多项式时间攻击算法 A 以不可忽略的优势赢得以下游戏。

初始化阶段：A 选择挑战的解密者属性集合 $?_R$，且$|?_R|<d$，C 选择 2 个属性集合 $?_{R_1}$和 $?_{R_2}$且 $?_R \not\subset ?_{R_1} \cap ?_{R_2}$。挑战者 C 运行 *Setup* 算法，得到主密钥 x 和系统公开参数 cp，并发送 x 和 cp 发送给攻击者 A。在拥有主密钥的情况下，A 能够为自己产生私钥和签密密文。

挑战阶段：A 输出消息 m 对应的签密密文s^*，接收者属性集合 $?_R$，签密属性集合 $?_S$，挑战者 C 从$\{1,2\}$中选取 b，使用自己生成的密钥$TK_{wb,t}$ 解密 s^*，将解密结果 m'发送给攻击者 A。

猜测阶段：A 检查 m'，如果 $m'=m$，返回猜测结果 b'，否则返回_，如果 $b'=b$，A 赢得游戏，定义 A 赢得游戏优势定义为 $Adv^{\text{RA-ABKISC-CCA-SA}}(\text{A})=|Pr[b=b']-1/2|$。

5　方案设计

Setup(k,d)：k 为安全参数，d 为门限值，为简化起见，设属性全域为 $\mathbb{Z}_p^*$，其中，p 为大素数，该算法的执行过程如下。

选取 2 个阶为素数 p 的循环乘法群 G 和 G_T(由安全参数 k 决定)，g 为 G 的生成元，$(d-1)$个默认的属性集合为 $O=\{O_1, O_2,\cdots, O_{d-1}\}$，$x$ 为从 $\mathbb{Z}_p^*$中随机选择的正整数，$g_1=g^x$, g_2、h_1 为从 G 中随机选择的正整数。定义散列函数 H_1: $\mathbb{Z}_p^*$? G, H_2: $M\times G^{d+1}$? G, H_3: $\{0,1\}^*$? $\{0,1\}^{128}$。设 e 为一个双线性映射 e: $G\times G$? G_T，$Z=e(g_1,g_2)$。选取一个伪随机函数 F: 给定一个 k bit 的输入参数 x 和一个 k bit 原始参数 s，函数 F 将输出一个 k bit 长的伪随机字符串 $F_S(x)$。选取对称加密算法 $En(\cdot)$和对应的解密算法 $De(\cdot)$。选取一个函数 $H_?$:$\mathbb{Z}_p^*$? G 且 $H_?(x)=g_1^x h_1$。系统公开参数 $cp=(\mathbb{Z}_p^*, G, G_T, g, g_1, g_2, (En, De), Z, H_1, H_2, H_3, H_?, F, O), msk=x$。

Extract$(cp, msk, ?)$：$?$ 为用户拥有的属性集合，msk 为主密钥，cp 为公开参数。协助器密钥 $HK_?$ 为从$\{0,1\}^k$ 中选取的随机正整数，选取$(d-1)$次多项式 $q(x)$且 $q(0)=x, k_{?,0}=F_{HK_w}(0)$, $\hat{w}=w\cup W$，对于每一个属性 $i\in\hat{w}$，从 $\mathbb{Z}_p^*$中选取随机整数 r_i，$d_{i,0}^{(1)}=g_2^{q(i)}\cdot H_1(i)^{r_i}\cdot H_w(0)^{k_{w,0}}$, $d_{w,0}^{(2)}=g^{k_{w,0}}$, $d_{i,0}^{(3)}=g^{r_i}$，初始密钥为 $TK_{w,0}=(\{d_{i,0}^{(1)}, d_{i,0}^{(3)}\}_{i\in\hat{w}}, d_{w,0}^{(2)})$，协助器密钥为 $HK_?$。

HelperUpdate$(cp, t', t, ?, HK_?)$：cp 为公开参数，将用户更新密钥所需要的更新信息由时间片 t'更新为当前时间片 t, $k_{w,t'}=F_{HK_w}(t')$, $k_{w,t}=F_{HK_w}(t)$，协助器密钥为

$$UI_{w,t',t}=(UI_{w,t',t}^{(1)}, UI_{w,t',t}^{(2)})=\left(\frac{H_w(t)^{k_{w,t}}}{H_w(t')^{k_{w,t'}}}, g^{k_{w,t}}\right)$$

UserUpdate$(cp, t', t, ?, UI_{w,t',t}, TK_{w,t'})$：$cp$ 为公开参数，$?$ 为用户属性集合，$UI_{w,t',t}$ 为协助器产生的更新信息，$TK_{w,t'}$ 为 t'时间片的用户密钥，该算法将用户的 t'时间片的临时密钥更新为 t 时间片的临时密钥，为

$$TK_{w,t}=(\{d_{i,t'}^{(1)}UI_{w,t',t}^{(1)}, d_i^{(3)}\}_{i\in\hat{w}}, UI_{w,t',t}^{(2)})$$

$$=(\{g_2^{q(i)}H_1(i)^{r_i}H_w(t)^{k_{w,t}}, g^{r_i}\}_{i\in\hat{w}}, g^{k_{w,t}})$$

Signcrypt$(cp, m, TK_{w_s,t}, ?_S', ?_R)$：该输入公开参数 cp，需要签密的明文 m，签密者的私钥$TK_{w_s,t}$，时间片 t，签密者使用所拥有属性 $?_S$ 的子集 $?_S'$进行签密，即 $?_S'\subseteq ?_S$，接收者属性集合为 $?_R$ 设 $?_S'=\{i_1,i_2,\cdots,i_l\}$，$1\le l\le d$，从 O 中选取默认属性集合的子集$O_S=\{i_{l+1}, i_{l+2},\cdots,i_d\}\subseteq O$。同样地，设 $?_R=\{j_1, j_2,\cdots, j_n\}$，$1\le n\le d$，从 O 中选取默认属性集合的子集 $O_R=\{j_{n+1}, j_{n+2}, \cdots, j_d\}\subseteq O$。从 $\mathbb{Z}_p^*$选择随机数整数 $k_t, u, s, u_1, u_2, \cdots, u_d, s_1, s_2, \cdots, s_d$，随机选择$(d-1)$次多项式 $L(\cdot)$且 $L(0)=0$，$T=g^u$，$k'=Z^{u+s}$，$sk=H_3(k')$对于每个 $1\le v\le d$, $E_v=H_1(j_v)^u$, $h=H_2(m, T, E_1, E_2, \cdots, E_d)$，$s_{v,t}^{(1)}=d_{i_v,t}^{(1)s}H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t}$, $s_{v,t}^{(2)}=(d_{i_v,t}^{(3)})^s g^{s_v}$, $s_{v,t}^{(3)}=g^{u_v}$, $s_{w,t}^{(4)}=H_?(t)^u$, $s_{w,t}^{(5)}=(d_{w,t}^{(2)})^s g^{k_t}$。使用对称加密算法得到的密文为 $E=En_{Sk}(m)$，算法最后输出签密结果为$(t, s)=(t, (T, E, h, ?_S', O_S, ?_R, O_R, (E_v, s_{v,t}^{(1)}, s_{v,t}^{(2)}, s_{v,t}^{(3)})_{1\le v\le d}, s_{w,t}^{(4)}, s_{w,t}^{(5)})$。

Unsigncrypt$(cp,(t,s), TKw_R, t)$：cp 为系统公开参数，(t,s)为对消息 m 的 t 时间片的签密，s 可分解为$(T, E, h, ?_S', O_S, ?_R, O_R, (E_v, s_{v,t}^{(1)}, s_{v,t}^{(2)}, s_{v,t}^{(3)})_{1\le v\le d}, s_{w,t}^{(4)}, s_{w,t}^{(5)})$，设 $Y=?_S'\cup O_S$，$S=?_R\cup O_R$，拥有属性 $?_R$ 的用户可解密签密。该算法计算

$$k'=\prod_{v=1}^{d}\left(\frac{e(d_{j_v,t}^{(1)},T)}{e(d_{j_v,t}^{(3)},E_v)e(s_{w,t}^{(4)},d_{w,t}^{(2)})}\right)^{\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e(s_{v,t}^{(1)},g)}{e(s_{v,t}^{(2)},H_1(i_v)e(s_{v,t}^{(3)},h)e(H_w(t),s_{w,t}^{(5)}))}\right)^{\Delta i_v,Y(0)}$$

计算对称密钥 $sk=H_3(k')$，**解密密文** $De_{Sk}(E)=m$，**如果** $h=H_2(m, T, E_1, E_2, \cdots, E_d)$，**则接受签密，输出明文** m，**否则返回**-。

正确性证明如下。

$$k'=\prod_{v=1}^{d}\left(\frac{e(d_{j_v,t}^{(1)},T)}{e(d_{j_v,t}^{(3)},E_v)e(s_{w,t}^{(4)},d_{w,t}^{(2)})}\right)^{\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e(s_{v,t}^{(1)},g)}{e(s_{v,t}^{(2)},H_1(i_v)e(s_{v,t}^{(3)},h)e(H_w(t),s_{w,t}^{(5)}))}\right)^{\Delta i_v,Y(0)}$$

$$=\prod_{v=1}^{d}\left(\frac{e(g_2^{q(j_v)}H_1(j_v)^{r_{j_v}}H_w(t)^{k_{w,t}},g^u)}{e(g^{r_{j_v}},H_1(j_v)^u)e(H_w(t)^u,g^{k_{w,t}})}\right)^{\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e((d_{i_v,t}^{(1)})^s H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t},g)}{e((d_{i_v,t}^{(3)})^s g^{s_v},H_1(i_v))e(g^{u_v},h)e(H_w(t),g^{sk_{w,t}+k_t})}\right)^{\Delta i_v,Y(0)}$$

$$=\prod_{v=1}^{d}\left(\frac{e(g_2^{q(j_v)},g^u)e(H_1(j_v)^{r_{j_v}},g^u)e(H_w(t)^{k_{w,t}},g^u)}{e(g^{r_{i_v}},H_1(j_v)^u)e(H_w(t)^u,g^{k_{w,t}})}\right)^{\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e((g_2^{q(i_v)}H_1(i_v)^{r_{i_v}}H_w(t)^{k_{w,t}})^s H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t},g)}{e(g^{r_{i_v}s}g^{s_v},H_1(i_v))e(g^{u_v},h)e(H_w(t),g^{sk_{w,t}+k_t})}\right)^{\Delta i_v,Y(0)}$$

$$=\prod_{v=1}^{d}e(g_2^{q(j_v)},g^u)^{\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e(g_2^{q(i_v)s}H_1(i_v)^{r_{i_v}s}H_w(t)^{k_{w,t}s+k_t}H_1(i_v)^{s_v}g_2^{L(i_v)},g)e(h^{u_v},g)}{e(g^{r_{j_v}s}g^{s_v},H_1(i_v))e(g^{u_v},h)e(H_w(t),g^{sk_{w,t}+k_t})}\right)^{\Delta i_v,Y(0)}$$

$$=e(g_2,g^u)^{\sum_{v=1}^{d}q(j_v)\cdot\Delta j_v,S(0)}\prod_{v=1}^{d}\left(\frac{e(g_2^{q(i_v)\cdot s+L(i_v)}H_1(i_v)^{r_{i_v}s+s_v}H_w(t)^{k_{w,t}s+k_t},g)}{e(g^{r_{j_v}\cdot s+s_v},H_1(i_v))e(H_w(t),g^{sk_{w,t}+k_t})}\right)^{\Delta i_v,Y(0)}$$

$$=e(g_2,g^u)^x\prod_{v=1}^{d}\left(\frac{e(g_2^{q(i_v)\cdot s+L(i_v)},g)e(H_1(i_v)^{r_{i_v}s+s_v},g)e(H_w(t)^{k_{w,t}s+k_t},g)}{e(g^{r_{j_v}s+s_v},H_1(i_v))e(H_w(t),g^{sk_{w,t}+k_t})}\right)^{\Delta i_v,Y(0)}$$

$$=e(g_2,g^u)^x\prod_{v=1}^{d}e(g_2^{q(i_v)\cdot s+L(i_v)},g)^{\Delta i_v,Y(0)}=e(g_2,g^u)^x\prod_{v=1}^{d}e(g_2,g)^{\Delta i_v,Y(0)\cdot(q(i_v)\cdot s+L(i_v))}=e(g_2,g^u)^x e(g_2,g)^{\sum_{v=1}^{d}\Delta i_v,Y(0)(q(i_v)s+L(i_v))}$$

$$=e(g_2,g^u)^x e(g_2,g)^{q(0)s+L(0)}=e(g_2,g^u)^x e(g_2,g)^{xs}=e(g_2,g^x)^{(u+s)}=Z^{u+s}=k'$$

6 安全性证明

定理 1 机密性

如果存在 IND-KI-ABSC-CCA **攻击算法** A，**能够以** e **的优势赢得定义** 3 **的游戏，则存在挑战者** C **以** $e'=e/2$ **的优势解决** DBDH **难题。**

证明 设默认属性为 $O=\{O_1,O_2,\cdots,O_{d-1}\}$，$d$ **为系统参数中的门限值。假设攻击者** A **选择挑战的属性为** $?_R$ **和时间片参数** t^*，$?_R$ **对应的默认属性为** O_R。

初始化阶段：挑战者 C **运行** $Setup(k,d)$ (cp, msk)，**设置** $g_1=g^a$，$g_2=g^b$，**并发送公开参数给** A。**从** $\mathbb{Z}_p^*$ **选择随机数整数** ß，**定义** $h_1=g_1^{-t^*}g^{ß}\in G$ **函数** $H_?(x)=g_1^{x}h_1=g_1^{x-t^*}g^{ß}$。

模拟阶段。

随机预言：H_1 **模拟** A **查询他选择的属性集合中任意属性** i **对应的随机预言** H_1 **的散列值。如果** $i\in ?_R\cup O_R$，**挑战者** C **返回** $H_1(i)=g^{b_i}$，**其中，**$ß_i\in\mathbb{Z}_p^*$；**如果** $i\notin ?_R\cup O_R$ **挑战者** C **返回** $H_1(i)=g^{-b_i}g^{y_i}$，**其中，**$ß_i$，$y_i\in\mathbb{Z}_p^*$。

私钥生成模拟：A **查询属性** $?$ **且** $?_R\notin ?$，C **构造属性集合** G，G' **和** S，**并且** $G=(?\cap ?_R)\cup O_R$，$G\subseteq G'\subseteq S$，$|G'|=d-1$ **和** $S=G'\cup\{0\}$。C **计算** $k_{w,0}=F_{HKw}(0)$，**设定** $d_{w,0}^{(2)}=g_2^{\frac{-1}{0-t^*}}g^{k_{w,0}}$，**令** $k_{w,0}=k_{w,0}-\frac{b}{0-t^*}$ **则，**$d_{w,0}^{(2)}=g^{k_{w,0}}$，$g_2^{\frac{-b}{0-t^*}}H_w(0)^{k_{w,0}}=g^{ab}H_w(0)^{k_{w,0}}g^{-ab}g_2^{\frac{-b}{0-t^*}}=g_2^{a}H_w(0)^{k_{w,0}}g_1^{b}g_2^{\frac{-b}{0-t^*}}=g_2^{a}H_w(0)^{k_{w,0}}$。

有以下 2 **种情况。**

如果 $i\in G'$，C **计算** $d_{i,0}^{(1)}=g_2^{t_i}H_1(i)^{r_i}g_2^{\frac{-b}{0-t^*}}H_w(0)^{k_{w,0}}=g_2^{t_i}H_1(i)^{r_i}g_2^{a}H_w(0)^{k_{w,0}}$，$d_{i,0}^{(3)}=g^{r_i}$，**其中，**$t_i$ **和** r_i **为从** $\mathbb{Z}p^*$ **随机选择的整数，并且选择**$(d-1)$**次多项式**

$q(\bullet)$且有 $d-1$ 个点满足 $q(i)=t_i$，$q(0)=a$。

如果 $i\notin G'$，C 计算 $d_{i,0}^{(1)}=g_2^{\frac{D_0,S(i)y_i}{b_i}+\sum_{j\in G'}D_j,S(i)q(j)}\cdot(g_1^{-b_i}g^{y_i})^{r_i'}g_2^{\frac{-b}{0-t^*}}H_w(0)^{k_{w,0}}$　$d_{i,0}^{(3)}=g_2^{\frac{D_0,S(0)}{b_i}}g^{r_i'}$，其中，$y_i$ 和 r_i' 为从 $\mathbb{Z}p^*$ 随机选择的整数，设 $r_i=\frac{D_0,S(i)b}{b_i}+r_i'$，得 $d_{i,0}^{(1)}=g_2^{q(i)}H_1(i)^{r_i}g_2^{a}H_w(0)^{k_{w,0}}$，$d_{i,0}^{(3)}=g^{r_i}$。

临时私钥查询：C 从 $\mathbb{Z}p^*$ 选取随机数 $k_{?,t}$，由于攻击者 A 不知道相应种子 $HK_?$ 的值，从 A 的角度 $k_{?,t}$ 与真实环境不可区分。临时私钥模拟与私钥生成查询类似，仅将时间片有 0 变为 t 即可。

签密模拟：A 询问$(m, ?_S, ?_R)$对应的签密密文，其中 m 为消息，$?_S$ 为签名属性，$?_R$ 为接收者的属性，C 运行算法 $Extract(cp, msk, ?)$, $UserUpdate(cp, t', t, ?_S, UI_{w_S,t',t}, TK_{w_S,t'})$，得到临时私钥 $TK_{w_S,t}$，运行签密算法 $Signcrypt(cp, t, m, ?', TK_{w_S,t}, ?_R)$，并将$(t,s\ )$发送给 A。

解签密查询：从 A 得到签密密文$(t,s\ )$，C 运行算法 $Extract(cp, msk, ?_R)$，$UserUpdate(cp, t', t, ?_R, UI_{w_R,t',t}, TK_{w_R,t'})$得到临时私钥 $TK?_{R,t}$，运行解签密算法 $Unsigncrypt(cp, (t,s\ ), TK?_{R,t})$，若成功，返回 m 给 A，否则返回 $-$。

挑战阶段：攻击者 A 向 C 发送 2 个长度相等的明文 M_0 和 M_1，挑战者 C 抛取一个随机选择 $b\in\{0,1\}$，并在时间片 t 使用签名属性 $?_S$ 和接收者属性 $?_R$ 对 M_b 签密，得到$(t,\ s^*) = (t, (T, E, h, ?_S, O_S, ?_R, O_R, (E_v,\ s_{v,t}^{(1)},\ s_{v,t}^{(2)},\ s_{v,t}^{(3)})_{1\le v\le d}, s_{w,t}^{(4)}, s_{w,t}^{(5)})$。

在签密密文中 $T=C=g^c$，$k'=YZ^s$，$sk=H_3(k')$，$E=En_{Sk}(m_b)$，$E_V=C^{ßi}=(g^{ßi})^c$。如果 $m=0$，则 $Y=e(g,g)^{abc}$，设 $u=c$，则有 $Z^u=e(g,g)^{abc}$，签密密文是对 m_b 合法密文。如果 $m=1$，则 $Y=e(g,\ g)^y$，y 是从 $\mathbb{Z}p^*$ 随机选择的整数，从攻击者 A 的角度，E 是一个随机字符串，A 不能得到任何与 m_b 有关的信息。

询问阶段二：重复询问阶段。

猜测阶段：A 猜测 b 的值为 b'。如果 $b'=b$，C 输出 $m=0$，表示(A, B, C, Y)是一个合法的 BDH 元组，否则如果 $b'?b$，则挑战者输出 $m=1$，表示(A, B, C, Y)是一个非法的 BDH 元组。

由以上讨论可得，当 $m=1$ 时，A 不能得到任何与 m_b 有关的信息。因此 $Pr[b=b'|m=1]=1/2$，另外当 $b'?b$，C 返回 $m=1$，因此 $Pr[m'=m|m=1]=1/2$。

当 $m=0$ 时，A 得到一个合法的 m_b 签密，由 4.2 节定义 3 可知，A 以 e 的优势猜测到 b，因此 $Pr[b=b'|m=0]=1/2+e$，在 $b=b'$情况下，C 输出 $m=0$，因此 $Pr[m=m'|m=1]=1/2+e$。

有以上可知，C 以 e 的优势正确猜到 $m=m'$，即解决 DBDH 难题，可得。

$Pr[m=m'|m=1]/2+Pr[m=m'|m=0]/2-1/2=(1/2+e)/2+(1/2)/2-1/2=e/2$。

定理 2　不可伪造性

假设存在一个伪造者 A 以 e 的优势赢得 EU-KI-ABSC-CMA 游戏。A 可查询初始私钥 q_k 次，查询临时私钥 q_t 次，查询签密 q_S 次，查询 H_1 随机预言 q_{H_1} 次，查询 H_2 共 q_{H_2} 次，则存在挑战者 C 以 $e'=e/(eq_SC_{d-1}^{d-k_s})$ 优势解决 CDH 难题，其中，d 为门限值，k_S 为签密时用到的属性数，e 为自然常数。

证明　假设攻击者算法 A 能有以不可忽略的的优势 e 伪造签密密文，则挑战者 C 能够以不可忽略的优势解决 CDH 问题。假设 A 选择挑战的属性集合为 $?$，$|?_S|=k_S\le d$。

初始化阶段：挑战者 C 运行 $Setup(k,d\ )$，设置 $g_1=g^a=A$，$g_2=g^b=B$，并发送公开参数给 A。秘密保存 msk。定义 $H_?(x)=g_1^xh_1=g_1^{x-t^*}g^ß$，$ß\in\mathbb{Z}_p^*$。

模拟阶段。

随机预言模拟：假设 A 查询散列函数 H_1 和 H_2 的最大次数分别为 q_{H_1} 和 q_{H_2}。假设 A 将从 C 得到函数 H_1、H_2 的散列值存入到 L_1 和 L_2 列表中，如果 L_1 和 L_2 中对应的散列值已存在，则直接从 L_1 或 L_2 中取出，否则将查询的结果存入到 L_1 或 L_2 中。C 选择随机数 $d\in[1,q_{H_2}]$，属性集合 $O_S\subseteq O$ 且$|O_S|=d-k_S$。

1) H_1 的模拟查询与保密性中的模拟类似，其中接收者属性集合 $?_R$ 更改为签密者属性集合 $?_S$。

2) H_2 模拟查询：如果 $i?d$(假设 $Pr[i?d]=q_S/(q_S+1)$)，从 $\mathbb{Z}p^*$ 选择 2 个随机数 a_i、$ß_i$，返回给 A 的值为 $H_2(m_i,*,\cdots,*)=g_1^{ai}g^{ßi}$；如果 $i=d(Pr[i=d]=1/(q_S+1))$，从 $\mathbb{Z}p^*$ 选择随机数 $ß_i$，返回给 A 的值为 $H_2(m_i,*,\cdots,*)=g^{ßi}$。

密钥生成查询：与定理 1 中的密钥生成查询类似。

临时密钥查询：与定理 1 中的临时密钥查询类似。

签密查询：攻击者 A 最多进行 q_S 次签密查询。如果 $?_S\not\subset?$，C 运行 $Extract()$得到私钥 $TK_{?,0}$ 或运行 $UserUpdate()$得到私钥 $TK_{?,t}$，并计算合法的密文发送给 A，如果 $?_S\subset?$，A 构造属性集合 $O_S\subseteq O$ 且$|O_S|=d-|?_S|$，$O_R\subseteq O$ 且$|O_R|=d-|?_R|$。如果 $H_2(m_i,*,\cdots,*)=g^{ßi}$，C 模拟终止；如果 $H_2(m_i,*,\cdots,*)?g^{ßi}$，C 进行如

下模拟。

假设 $?_S \cup O_S=\{i_1,i_2,\cdots,i_d\}$ 和 $?_R \cup O_R=\{j_1, j_2,\cdots, j_d\}, t_1, t_2,\cdots, t_{d-1}$ 为 $d-1$ 个从 $\mathbb{Z}p^*$ 中选择的随机整数且 $q(i_v)=t_v(1\leq v\leq d-1)$，与另外从 $\mathbb{Z}p^*$ 中选择的随机整数 k_t、u、s。C 计算 $T=g^u$，$k'=Z^{u+s}$，$sk=H_3(k')$，$En_{Sk}(m)$，$E_v=H_1(j_v)^u$，$h=H_2(m,T,E_1,\cdots,E_d)$。对于前 $d-1$ 个点，选择随机整数 $s_v\in \mathbb{Z}p^*$。计算

$$s_{v,t}^{(1)}=g_2^{sq(i_v)}H_1(i_v)^{r_v}H_w(t)^{s\cdot k_{w,t}}h^{s_v},\ s_{v,t}^{(2)}=g^{r_v},\ s_{v,t}^{(3)}=g^{s_v},\ s_{w,t}^{(4)}=H_?(t)^u,\ s_{w,t}^{(5)}=g^{sk_{w,t}+k_t}$$

对于第 d 个点，随机选择 s_d'，$r_d\in \mathbb{Z}p$，计算

$$s_{d,t}^{(1)}=g_2^{s\sum_{v=1}^{d-1}D_{v,S(i_d)}q(i_v)+\frac{D0,S(i_d)b_d}{a_d}}g_1^{s_d'a_d}g^{s_d'b_d}H_1(i_d)^{r_d}\cdot H_w(t)^{sk_{w,t}}H_w(t)^{k_t},\ s_{d,t}^{(2)}=g^{r_d},\ s_{d,t}^{(3)}=g_2^{-s\frac{D0,S(i_d)}{a_d}}g^{s_d'},\ s_{d,t}^{(4)}=H_?(t)^u,\ s_{d,t}^{(5)}=g^{sk_{w,t}+k_t}$$

设 $s_d=-sD_{0,S(i_d)}/a_d+s_d'$，则上述密文为

$$s_{d,t}^{(1)}=g_2^{sq(i_d)}H_1(i_d)^{r_d}H_w(t)^{sk_{w,t}}h^{s_d}H_w(t)^{k_t},\ s_{d,t}^{(2)}=g^{r_d},\ s_{d,t}^{(3)}=g^{s_d}$$

因此得到的密文是合法的，C 能够赢得模拟的概率为 $(q_S/(q_S+1))^{q_S}=(1-q_S/(q_S+1))^{(q_S+1)}(q_S+1)/q_S\geq(q_S+1)/(eq_S)$。

解签密算法模拟：从 A 得到 (t^*,s^*)，$?_S$，$?_R$ 后，C 运行 $Extract(cp, msk, ?_S)$ 来计算私钥 $TK_{?,0}$ 或更新私钥得到 $TK_{?,t}$，然后运行解签密算法，返回 m 或 $-$ 给 A。

伪造阶段：A 输出消息 m^* 和 $(t^*,s^*)=(t^*,(T, E, h, ?_S^*, O_S^*, ?_R, O_R, (E_v, s_{v,t}^{(1)}*, s_{v,t}^{(2)}*, s_{v,t}^{(3)}*)_{1\leq v\leq d}, s_{w,t}^{(4)}*, s_{w,t}^{(5)}*)$。如果 $H_2(m^*,*,\cdots,*)?g^{\beta i}$。或者 $O_S^*?O_S$，C 终止游戏；否者验证

$$k'=\prod_{v=1}^{d}\left(\frac{e(d_{j_v,t}^{(1)},T)}{e(d_{j_v,t}^{(3)},E_v)e(s_{w,t}^{(4)}*,d_{w,t}^{(2)})}\right)^{Dj_v,S(0)}\prod_{v=1}^{d}\left(\frac{e(s_{v,t}^{(1)}*,g)}{e(s_{v,t}^{(2)}*,H_1(i_v))e(s_{v,t}^{(3)}*,h)e(H_w(t),s_{w,t}^{(5)}*)}\right)^{D_v,Y(0)}$$

$=Z^{u+s}$。

对于 $i\in ?_R\cup O_S, H_1(i)=g^{b_i}$ 且 $H_2(m^*,T,E_1,\cdots,E_d)=g^{b_d}$

$$\prod_{v=1}^{d}\left(\frac{e(s_v^{(1)}*,g)}{e(s_v^{(2)}*,H_1(i_v))e(s_v^{(3)}*,h)e(H_w(t^*),s_{w,t}^{(5)}*)}\right)^{D_v,Y(0)}=e(g^{abs},g)$$

因此，C 可计算出

$$\prod_{v=1}^{d}\left(\frac{s_v^{(1)}*,}{(s_v^{(1)})^{b_{i_v}}*(s_v^{(2)}*)^{b_d}(s_{w,t}^{(5)}*)^b}\right)^{D_v,Y(0)}=g^{abs}$$

计算 $(g^{abs})^{s^{-1}}=g^{ab}$。为赢得游戏，必须满足 $H_2(m^*, T, E_1, \cdots, E_d)=g^{b_d}$ 和 $O_S'=O_S$, $H_?(t^*)=g^{\beta}$。当从 $d-1$ 个属性中选取 $d-k$ 的属性时，以 $1/C_{d-1}^{d-k}$ 的概率得到想要的属性，因此 C 赢得游戏的概率为

$$e'\sim 1/((q_S+1)C_{d-1}^{d-k})1/e(q_S+1)/q_Se=e/(eq_SC_{d-1}^{d-k})$$

因此是不可忽略的。

定理 3 签密者匿名性

证明 首先，密钥生成中心运行 Setup 算法，得到系统公开参数 cp 和主密钥 x，并将 cp 和 x 发送给攻击者 A，攻击者 A 选择挑战的属性集合为 $?_S^*=\{i_1,i_2,\cdots,i_l\}$ 且 $l\leq d$。C 给出 2 个属性集合 $?_{S_0}^*$ 和 $?_{S_1}^*$。定义 $?_S^*=?_{S_0}^*\cap ?_{S_1}^*$，设置 $w_{Sb}^*=?_{Sb}^*\cup O$，其中，$b\in\{0,1\}$。A 生成

$$TK_{w_{sb}*,t}=(\{^{(b)}d_{i,t}^{(1)},{}^{(b)}d_{i,t}^{(3)}\}_{i\in\hat{w}_{sb}*},{}^{(b)}d_{w,t}^{(2)})=(\{g_2^{q_b(i)}H_1(i)^{r_i}H_w(t)^{k_{w_{sb}*,t}},g^{r_i}\}_{i\in\hat{w}_{sb}*},g^{k_{w_{sb}*,t}})$$

其中，$q_b(\cdot)$ 是 $(d-1)$ 次多项式，满足 $q_b(0)=x$。

其次，攻击者 A 向挑战者 C 提供明文消息 m 和解密者属性集合 $?_R=\{j_1, j_2, \cdots, j_n\}$ 且 $n\leq d$，C 随机从 $\{0,1\}$ 中选择 b，选择 2 个默认属性集合的子集 $O_S=\{i_{l+1},i_{l+2},\cdots,i_d\}\subseteq O$, $O_R=\{j_{n+1}, j_{n+2},\cdots, j_d\}\subseteq O$，使用 $TK_{w_{sb}*,t}$ 对消息 m* 进行签密，得到签密结果 (t, s^*)，其中 $s^*=(T, E, h, ?_S', O_S, ?_R, O_R, (E_v, s_{v,t}^{(1)}*, s_{v,t}^{(2)}*, s_{v,t}^{(3)}*)_{1\leq v\leq d}, s_{w,t}^{(4)}*, s_{w,t}^{(5)}*)$，其中 $T=g^u$, $E_v=H_1(j_v)^u$, $h=H_2(m, T, E_1, E_2, \cdots, E_d)$, $s_{v,t}^{(1)}*={}^{(b)}d_{i_v,t*}^{(1)\,s}H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t}$, $s_{v,t}^{(2)}*=(^{(b)}d_{i_v,t*}^{(3)})^s g^{s_v}$, $s_{v,t}^{(3)}*=g^{u_v}$, $s_{w,t}^{(4)}*=H_w(t)^{u_v}$, $s_{w,t}^{(5)}*=(^{(b)}d_{w,t}^{(2)})^s g^{k_t}$, k_t, u, s, u_v, s_v 为从 $\mathbb{Z}p^*$ 中选择的随机整数，$L(\cdot)$ 为 $d-1$ 次多项式且 $L(0)=0$。

证明 (t, s^*) 能够由 $TK_{w_{s_0}*,t}$ 和 $TK_{w_{s_1}*,t}$ 分别单独产生。假设 (t, s^*) 由 $TK_{w_{s_0}*,t}$ 产生，证明 s^* 同样可由 $TK_{w_{s_1}*,t*}$ 产生。证明如下。

$$s_{v,t}^{(1)}*={}^{(0)}d_{i_v,t}^{(1)\,s}H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t}={}^{(1)}d_{i_v,t}^{(1)\,s}\frac{{}^{(0)}d_{i_v,t}^{(1)\,s}}{{}^{(1)}d_{i_v,t}^{(1)\,s}}H_1(i_v)^{s_v}g_2^{L(i_v)}h^{u_v}H_w(t)^{k_t}$$

$= {}^{(1)}d_{i_v,t}^{(1)\,s}(g_2^{q_0(i_v)-q_1(i_v)}H_1(i_v)^{r_{i_v}^{(0)}-r_{i_v}^{(1)}}H_w(t)^{k_{w_{S0}*,t}^{(0)}-k_{w_{S1}*,t}^{(1)}})^s \cdot H_1(i_v)^{s_v} g_2^{L(i_v)} h^{u_v} H_w(t)^{k_t}$

$s_{v,t}^{(2)}* = ({}^{(0)}d_{i_v,t}^{(3)})^s g^{s_v} = ({}^{(1)}d_{i_v,t}^{(3)})^s \frac{({}^{(0)}d_{i_v,t}^{(3)})^s}{({}^{(1)}d_{i_v,t}^{(3)})^s} g^{s_v}$

$= ({}^{(1)}d_{i_v,t}^{(3)})^s (g^{r_{i_v}^{(0)}-r_{i_v}^{(1)}})^s g^{s_v}$，$s_{v,t}^{(3)}* = g^{u_v}$，$s_{w,t}^{(4)}* = H_?(t)^u$，

$s_{w,t}^{(5)}* = ({}^{(1)}d_{w,t}^{(2)})^s \frac{({}^{(0)}d_{w,t}^{(2)})^s}{({}^{(1)}d_{w,t}^{(2)})^s} g^{k_t} = ({}^{(1)}d_{w,t}^{(2)})^s g^{sk_{w_{S_1}*,t}-sk_{w_{S_0}*,t}+k_t}$

定义多项式 $\overline{q}(x) = q_0(x) - q_1(x)$，**显然** $\overline{q}(0) = 0$，**因此**

$s_{v,t}^{(1)}* = {}^{(1)}d_{i_v,t}^{(1)\,s} g_2^{s\overline{q}(i_v)+L(i_v)} H_1(i_v)^{s(r_{iv}^{(0)}-r_{iv}^{(1)})+s_v}$

$H_w(t)^{s(k_{w_{S0}*,t}-k_{w_{S1}*,t})+k_t}\ h^{u_v}\ s_{v,t}^{(2)}*$

$= ({}^{(1)}d_{i_v,t}^{(3)})^s (g^{r_i^{(0)}-r_i^{(1)}})^s g^{s_v} = ({}^{(1)}d_{i_v,t}^{(3)})^s g^{(r_i^{(0)}-r_i^{(1)})s+s_v}$

定义多项式 $q''(x)=L(x)+s\,\overline{q}(x)$ **(显然** $q''(0)=0$**)，设** $r_i''=s_v+s(r_{iv}^{(0)}-r_{iv}^{(1)})$，$k_t' = s(k_{w_{S_1}*,t} - k_{w_{S_0}*,t}) + k_t$，**得到**

$s_{v,t}^{(1)}* = {}^{(1)}d_{i_v,t}^{(1)\,s} g_2^{q''(i_v)} H_1(i_v)^{r_{i_v}''} h^{u_v} H_w(t)^{k_t'}$，$s_{v,t}^{(2)}*$

$= ({}^{(1)}d_{i_v,t}^{(3)})^s g^{r_{i_v}''}$，$s_{wt}^{(5)}* = ({}^{(1)}d_{w,t}^{(2)})^s g^{k_t'}$

因此 $s^*=(T, E, h, ?_S', O_S, ?_R, O_R, (E_v, s_{v,t}^{(1)}*, s_{v,t}^{(2)}*, s_{v,t}^{(3)}*)_{1\le v\le d}, s_{w,t}^{(4)}*, s_{w,t}^{(5)}*)$。**能够成为** $TK_{w_{S_1}*,t*}$ **的合法签密密文。**

同理，由 $TK_{w_{S_1}*,t*}$ **生成的签密密文也可由** $TK_{w_{S_0}*,t*}$ **生成。**

由以上可知，攻击者 A **的成功的概率为** 1/2，**他的优势为** $\mathrm{Adv}^{\mathrm{SA\text{-}ABKISC\text{-}CCA\text{-}SA}}(\mathrm{A}) = |Pr[b=b'] - 1/2| = 0$。

定理 4　解密者匿名性

证明　首先由密钥生成中心运行 setup **算法，得到公开参数** cp **和** msk，**并发送给攻击者** A，A **选取挑战属性集合** $?_R^*$，**设** $?_R^*=\{j_1, j_2, \cdots, j_n\}$，$n \le d$，**挑战者** C **给出属性集合** $?_{R_0}^*$，$?_{R_1}^*$ **且** $?_R^* = ?_{R_0}^* \cap ?_{R_1}^*$，$b \in \{0, 1\}$，A **生成** $?_{R_0}^*$，$?_{R1}^*$ **且对应的临时私钥** $TK_{w_{R_0}*,t}$、$TK_{w_{R_1}*,t}$。A **给出** $?_S^*$、$?_R^*$ **对应的签密密文** s^*，**设** $?_S^*=\{i_1, i_2, \cdots, i_l\}$ **且** $l \le d$，**选择** 2 **个默认属性集合的子集** $O_S=\{i_{l+1}, i_{l+2}, \cdots, i_d\} \subseteq O$，$O_R=\{j_{n+1}, j_{n+2}, \cdots, j_d\} \subseteq O$，C **随机从**{0,1}**中选择** b，**然后以** $?_{Rb}^*$ **对应临时私钥** $TK_{w_{Rb}*,t}$ **进行解密，并将解密结果** m' **发送给** A。

首先用 $TK_{w_{R_0}*,t}$ **进行解密，解密过程如下**

$$\prod_{v=1}^{d}\left(\frac{e({}^{(0)}d_{j_v,t}^{(1)}, T)}{e({}^{(0)}d_{j_v,t}^{(3)}, E_v)e(s_{w,t}^{(4)}, {}^{(0)}d_{w,t}^{(2)})}\right)^{Dj_v,S(0)} \cdot$$

$$\prod_{v=1}^{d}\left(\frac{e(s_{v,t}^{(1)}, g)}{e(s_{v,t}^{(2)}, H_1(i_v))e(s_{v,t}^{(3)}, h)e(H_w(t), s_{w,t}^{(5)}))}\right)^{Di_v,Y(0)}$$

$= e(g_2, g^u)^x e(g_2, g)^{xs} Z^{u+s} = k'$

计算对称密钥 $sk=H_3(k')$，**解密密文** $De_{Sk}(E)=m$，**如果** $h=H_2(m, T, E_1, E_2, \cdots, E_d)$，**则接受签密，输出明文** m，**否则返回**_。

同样的方法，s^***也可由** $TK_{w_{R1}*,t}$ **解密。**

由以上可知，攻击者 A **的成功的概率为** 1/2，**他的优势为** $Adv^{\mathrm{RA\text{-}ABKISC\text{-}CCA\text{-}SA}}(\mathrm{A}) = |Pr[b=b'] - 1/2| = 0$。

7　结束语

给出 WEI **方案一**[13]**与改进后的方案的比较，如表** 1 **所示。其中** Exp **表示模指数运算，**Enc **和** Dec **为对称加密算法，**Hash **为散列运算，**$H_?$ **为函数** $H_?$ **运算，其中有些可以提前计算的，如** $d_{i_v,t*}^{(1)\,s}$ **和** $a^c b^d$ **简化记为一次模指数运算。**

本文研究了将密钥隔离机制[17]**引入到匿名的基于属性签密方案**[13]**，给出了双向匿名的基于属性密钥隔离签密的形式化定义和安全模型，实现了随机预言模型下可证安全的基于属性的密钥隔离签密方案。改进后的方案虽然增加了额外的运算代价，但改进后的方案既满足前向安全性又满足后向安全性要求，增强了抗密钥泄露的能力，而且改进后的方案同样具有双向匿名性。最后，本文在随机模型下给出了改进后签密方案的机密性、不可伪造性和匿名性的证明。由于匿名的基于属性签密的一对多保密通信的特性，即通信对象为具有某些属性值组合的用户集合且忽略集合中用户的数量，而且比先加密后签名具有更高的效率，因此该案在定向广播、密钥管理、电子商务、隐**

表 1　　效率分析

方案	密文长度	签密运算	解密运算
WEI **方案一**[13]	$(4d+2)\|G\|+\|m\|+2d\|p\|$	$(6d+2)$Exp$+(2d+2)$Hash$+1$Enc	$5d$ Pairing$+(d+2)$Hash$+2$Exp$+1$Dec
本文方案	$(4d+4)\|G\|+\|m\|+2d\|p\|$	$(6d+4)$Exp$+(2d+2)$Hash$+1$Enc$+2H_?$	$(5d+2)$Pairing$+(d+2)$Hash$+2$Exp$+1$Dec

私保护等领域有广阔的应用前景。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity based encryption[A]. Advances in Cryptology (EUROCRYPT 2005)[C]. Berlin, Springer-Verlag, 2005. 457-473.

[2] SHAMIR A. How to share a secret[J]. Communications of he ACM, 1979, 22(11):612-613.

[3] SHAMIR A. Identity based crypto systems and signature mes[A]. Advances in Cryptology (CRYPTO 1984)[C]. Berlin, Springer-Verlag, 1984.47-53.

[4] DAN B, XAVIER B. Efficient selective-id secure identity based encryption without random oracles[A]. Proceedings of the International Conference on Advances in Cryptology(EUROCRYPT 2004)[C]. Berlin, Springer-Verlag, 2004.223-238.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. Berkeley, CA, 2007.321-334.

[6] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine grained access control of encrypted data[EB/OL]. http://eprint.iacr.org/2006/309.

[7] MAJI H, PRABHAKARAN M, ROSULEK M. Attribute based signatures: achieving attribute privacy and collusion-resistance[EB/OL]. http://eprint. iacr. org/2008/328.

[8] LI J, KIM K. Attribute-based ring signatures[EB/OL]. http://eprint.iacr.org/2008/349.

[9] GAGNÉ M, NARAYAN S, SAFAVI-NAINI R. Threshold attribute based signcryption[A]. 7th International Conference on Security and Cryptography for Networks[C]. Amalfi, Italy, 2010.154-171.

[10] EMURA K, MIYAJI A, RAHMAN M. Toward dynamic attribute-based signcryption (poster)[A]. 16th Australasian Conference on Information Security and Privacy[C]. Melbourne, 2011.439-443.

[11] LIU J, WANG J, ZHANG Y. Attribute-based signcryption scheme on vector space[J]. Acta Electronica Sinica, 2013, 41(4):776-780.

[12] WANG C, HUANG J. Attribute-based signcryption with ciphertext policy and claim-predicate mechanism[A]. 7th International Conference on Computational Intelligence and Security, CIS[C]. China, 2011.905-909.

[13] WEI B D, OU H Y. Signcryption schemes with anonymity[J]. International Journal of Advancements in Computing Technology(IJACT), 2011, 3(8):127-137.

[14] GUNTHER C G. An identity-based key-exchange protocol, advances[A]. Workshop on the Theory and Application of Cryptographic Techniques[C] . Houthalen Belgium, Springer-Verlag, 1990.29-37.

[15] DODIS Y, KATZ J, XU S. Key-insulated public-key crypto systems[A]. Advances in Cryptology(EUROCRYPT 2002)[C]. London, Springer-Verlag, 2002.65-82.

[16] BELLARE M, PALACIO A. Protecting against key exposure: strongly key-insulated encryption with optimal threshold[J]. Applicable Algebra in Engineering, Communication and Computing archive, 2006, 16(6): 379-396.

[17] HANAOKA G, HANAOKA Y, IMAI H. Parallel key-insulated public key encryption[A]. Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography[C]. New York, 2006. 24-26.

[18] HANAOKA Y, HANAOKA G. Identity based hierarchical strongly key insulated encryption and its application[A]. Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security(EUROCRYPT 2005)[C]. Heidelberg, Springer-Verlag, 2005. 495-514.

[19] WENG J, LIU S. Identity based threshold key insulated encryption without random oracles[A]. Proceedings of the Cryptographers' Track at the RSA Conference[C]. San Francisco, 2008.203-220.

[20] WENG J, LIU S. Identity based parallel key insulated e yption without random oracles: security notions and construction[A]. Proceedings of the 7th International Conference on Cryptology[C]. Kolkata, India, Springer-Verlag, 2006.409-423.

[21] CHEN J H, CHEN K F. Ciphertext policy attribute-based parallel key-insulated encryption[J]. Journal of Software, 2012, 23(10): 2795-2804.

[22] CHEN J H, YU L. Attribute-based key-insulated encryption[J]. Journal of Information Science and Engineering, 2011, 27(2):437-449.

[23] **陈剑洪. 若干密钥隔离密码体制的研究**[D].**上海:上海交通大学**, 2011.
CHEN J H. Study on Several Key-Insulated Cryptographic Schemes[D]. Shanghai: Shanghai Jiaotong University, 2011.

作者简介：

张兴兰（1970-），女，山西兴县人，博士后，北京工业大学副教授，主要研究方向为密码学与信息安全。

张振（1989-），男，河南周口人，北京工业大学硕士生，主要研究方向为身份加密、属性加密。