1-2018

Online/Offline traceable attribute-based encryption [in Chinese]

Kai ZHANG

Jianfeng MA

Junwei ZHANG

Zuobin YING

Tao ZHANG

See next page for additional authors

Citation

ZHANG, Kai; MA, Jianfeng; ZHANG, Junwei; YING, Zuobin; ZHANG, Tao; and LIU, Ximeng. Online/Offline traceable attribute-based encryption [in Chinese]. (2018). *Journal of Computer Research and Development (计算机研究与发展)*. 55, (1), 216-224.

Available at: https://ink.library.smu.edu.sg/sis_research/4821

计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20160799
55(1):216-224,2018

在线/离线的可追责属性加密方案

张 凯[1] 马建峰[2] 张俊伟[2] 应作斌[3] 张 涛[2] 刘西蒙[4]
[1](西安电子科技大学通信工程学院 西安 710071)
[2](西安电子科技大学计算机学院 西安 710071)
[3](安徽大学计算机科学与技术学院 合肥 230601)
[4](新加坡管理大学信息系统学院 新加坡 178902)
(629zhangkai@163.com)

Online/Offline Traceable Attribute-Based Encryption

Zhang Kai[1], Ma Jianfeng[2], Zhang Junwei[2], Ying Zuobin[3], Zhang Tao[2], and Liu Ximeng[4]
[1](*School of Telecommunications Engineering, Xidian University, Xi'an* 710071)
[2](*School of Computer Science and Technology, Xidian University, Xi'an* 710071)
[3](*School of Computer Science and Technology, Anhui University, Hefei* 230601)
[4](*School of Information Systems, Singapore Management University, Singapore* 178902)

Abstract Attribute-based encryption (ABE), as a public key encryption, can be utilized for fine-grained access control. However, there are two main drawbacks that limit the applications of attribute-based encryption. First, as different users may have the same decryption privileges in ciphertext-policy attribute-based encryption,it is difficult to catch the users who sell their secret keys for financial benefit. Second, the number of resource-consuming exponentiation operations required to encrypt a message in ciphertext-policy attribute-based encryption grows with the complexity of the access policy, which presents a significant challenge for the users who encrypt data on mobile devices. Towards this end, after proposing the security model for online/offline traceable attribute-based encryption, we present an online/offline traceable ciphertext-policy attribute-based encryption scheme in prime order bilinear groups, and further prove that it is selectively secure in the standard model. If a malicious user leaks his/her secret key to others for benefit, he/she will be caught by a tracing algorithm in our proposed scheme. Extensive efficiency analysis results indicate that the proposed scheme moves the majority cost of an encryption into the offline encryption phase and is suitable for user encryption on mobile devices. In addition, the proposed scheme supports large universe of attributes, which makes it more flexible for practical applications.

Key words attribute-based encryption (ABE); traceability; online/offline; large universe; standard model

收稿日期:2016-11-04;**修回日期**:2017-02-21

基金项目:国家"八六三"高技术研究发展计划基金项目(2015AA016007);中央高校基本科研业务费专项资金项目(BDZ011402);国家自然科学基金项目(U1405255,61472310)
This work was supported by the National High Technology Research and Development Program of China (863 Program) (2015AA016007), the Fundamental Research Funds for the Central Universities (BDZ011402), and the National Natural Science Foundation of China (U1405255, 61472310).

通信作者:马建峰(jfma@mail.xidian.edu.cn)

摘　要　作为一种公钥加密,属性加密能够实现细粒度的访问控制.然而,由于在密文策略属性加密中多个用户可能会拥有相同的解密权限,所以抓获那些出售自己私钥的用户是困难的.其次,在密文策略的属性加密中,加密一个消息所要用到的指数运算是随着访问策略复杂性的增长而增长的,由此带来的计算开销对使用移动设备进行加密的用户造成了重大挑战.针对上述问题,给出了在线/离线可追责属性加密的安全模型,然后在素数阶双线性群下构造了一个在线/离线的可追责密文策略属性加密方案,并在标准模型下证明了方案是选择性安全的.当一个恶意用户泄露的自己私钥给别人时,该方案能够通过一个追责算法将其抓获.效率分析表明该方案加密的主要开销是在离线阶段,更适用于移动设备进行加密.此外,所提方案支持大属性域,在实际应用中更加灵活.

关键词　属性加密;可追责;在线/离线;大属性域;标准模型

中图法分类号　TP309

随着云计算技术的快速发展,人们越来越多地将数据存储在云服务器上以减少本地的存储和管理开销.然而,使用云存储服务在给人们带来了极大便捷的同时,也对数据的安全性造成了威胁.远端云服务器可能会查看甚至出售用户的敏感数据以获取商业利益.因此,利用加密技术来保护用户的敏感数据是非常必要的.传统的公钥加密技术能够保证用户将自己的数据秘密分享给一个指定的用户.然而,在许多情形下,用户希望所有满足指定访问策略的用户都能够访问数据,从而实现细粒度的访问控制.例如,病人希望自己的医疗数据能被 A 医院的所有内科医生访问.

为了解决上述问题,Sahai 和 Waters[1] 在 2005 年提出了属性加密(attribute-based encryption, ABE)的概念.在 ABE 方案中,用户的解密能力依赖于自身的属性.因此,ABE 在保护数据机密性的同时,可以实现数据的细粒度访问控制.在密文策略属性加密[2](ciphertext-policy ABE, CP-ABE)中,用户的私钥对应于自身属性,密文对应于一个访问策略,当且仅当用户的属性满足访问策略时,用户才能够成功解密.虽然现有的 ABE 方案[2-6] 支持细粒度访问控制,但效率过低和私钥泄露仍是阻碍其实际应用的 2 个关键问题.

近年来,ABE 中的私钥泄露问题[7-11] 越来越受到研究者们的重视.在 CP-ABE 方案中,多个用户可能拥有相同的属性,从而有相同的解密能力.若一个恶意用户出售自己的私钥,则难以通过这个私钥找出该用户.例如一个病人想利用 ABE 来分享自己的医疗信息给 A 医院的内科医生,而张三和李四都是 A 医院的内科医生.如果张三和李四中某人泄露了私钥,则难以判断是谁泄露的私钥.另一方面,ABE 虽然实现了细粒度访问控制,但效率要比传统加密低得多.例如在 CP-ABE 方案中,用户的加密时间是和访问策略的复杂性成线性关系的.因此,使用 CP-ABE 加密会给用户造成巨大的时间开销和能源开销,尤其是会对使用移动设备进行操作的用户造成巨大挑战.

针对上述问题,本文在素数阶群下构造了一个在线/离线的可追责 CP-ABE(online/offline traceable CP-ABE, OO-T-CP-ABE)方案.此外,我们在标准模型下证明了方案是选择性安全(selectively secure)和可追责的.方案的特点总结为 4 点:

1) 可追责.当恶意用户泄露或出售自己的私钥时,能够利用追责算法追踪到该用户的身份.

2) 在线/离线加密.加密的绝大部分运算是在离线阶段提前执行的,在线加密数据所带来的计算开销较小,因此适合于资源受限的移动设备使用.

3) 大属性域(large universe).整个系统的属性域并不需要在系统建立时固定,而且公钥长度并不随属性个数的增加而增加.这使得方案有较好的扩展性.

4) 丰富的访问策略.访问策略可以表示为任意单调访问结构,从而能够支持灵活的访问控制.

1　相关工作

Sahai 和 Waters[1] 在 2005 年首次提出了 ABE 的概念.随后,Goyal 等人[3] 将 ABE 划分为密钥策略 ABE (key-policy ABE, KP-ABE) 和 CP-ABE.此后,选择性安全的 CP-ABE 方案[2,4] 和自适应安全(adaptively secure)的 CP-ABE 方案[5-6] 也被陆续提出.2011 年,Lewko 和 Waters[12] 在合数阶群下构造了第 1 个支持大属性域的 CP-ABE 方案.相比于文献[1-6],文献[12]中的方案并不需要在系统建立

时确定属性域,而且公钥的长度与属性个数无关.之后,Rouselakis 和 Waters[13]在素数阶群下构造了一个更加高效的支持大属性域的 CP-ABE 方案.近年来,为了提高 ABE 方案的效率,可外包解密的 ABE[14]、在线/离线 ABE[15]和密文长度固定的 ABE[16]方案也被相继提出.然而,上述方案[14-16]并不能够对恶意用户进行追责,因此存在用户私钥泄露的风险.

文献[7-8]首先研究了 ABE 的追责问题.但是文献[7-8]中的访问策略只能表示为"与门和通配符(AND gates with wildcard)".针对此问题,Liu 等人提出了支持任意单调访问结构的白盒追责 ABE[9]和黑盒追责 ABE[10]方案.随后,Ning 等人[11]提出了一个支持大属性域的可追责 CP-ABE 方案.但已有的可追责 CP-ABE 方案[7-11]的在线加密开销过大,从而会严重影响用户在移动设备上的使用体验.与文献[7-11]相比,本文提出的 ABE 方案不仅支持恶意用户追责,而且支持在线/离线加密,从而大幅减少了用户的在线加密开销.

2 背景知识

2.1 访问结构

定义 1. 访问结构[17].设$\{P_1,P_2,\cdots,P_n\}$为所有参与者组成的集合.一个集合$A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$是单调的,当且仅当对任意$B,C$,如果$B\in A$,且$B\subseteq C$,则$C\in A$.一个(单调)访问结构(access structure)A是由$\{P_1,P_2,\cdots,P_n\}$的非空子集组成的(单调)集合,即$A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\backslash\{\varnothing\}$.包含在$A$中的集合称为授权集合,不包含在$A$中的集合称为非授权集合.

2.2 线性秘密共享

定义 2. 线性秘密共享[17].定义在参与者集合P上的一个秘密共享方案Π称为在$\mathbb{Z}_p$上是线性的,当满足 2 个条件:

1) 每个参与者关于$s\in\mathbb{Z}_p$的秘密分享值组成$\mathbb{Z}_p$上的一个向量.

2) 存在一个Π的分享生成矩阵$\boldsymbol{M}\in\mathbb{Z}_p^{l\times n}$和函数$\rho:[l]\to P$.对于$i\in[l]$,函数$\rho$将其映射到参与者$\rho(i)$.随机选择$y_2,y_3,\cdots,y_n\in\mathbb{Z}_p$,令列向量$\boldsymbol{y}=(s,y_2,y_3,\cdots,y_n)^{\mathrm{T}}$,则$\boldsymbol{My}$是秘密$s$关于$\Pi$的$l$个分享份额.其中分享份额$\lambda_i=(\boldsymbol{My})_i$属于参与者$\rho(i)$.

文献[17]指出任何一个线性秘密共享方案(linear secret sharing scheme, LSSS)都具有如下线性重构性质.如果Π是访问结构A的一个 LSSS,S是A中的一个授权集合,$I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$,则存在常数$\{\omega_i\in\mathbb{Z}_p\}$使得$\sum_{i\in I}\omega_i\lambda_i=s$.

2.3 双线性群和困难问题假设

本文将在素数阶双线性群(prime order bilinear groups)下构造方案,并基于素数阶双线性群中的 2 个困难问题假设来证明方案的安全性.

设G和G_{T}都是阶为素数p的循环群,g是G的生成元.双线性对$e:G\times G\to G_{\mathrm{T}}$是一个满足 2 个条件的映射:

1) 双线性.$\forall u,v\in G,e(u^a,v^b)=e(u,v)^{ab}$.

2) 非退化性.$e(g,g)\neq 1$.

如果双线性对$e:G\times G\to G_{\mathrm{T}}$和群中的运算都是可以有效计算的,则称$G$是一个素数阶双线性群.

定义 3. $q-1$ 假设[13].G是阶为素数p的双线性群,g是G的生成元.群G中的$q-1$难题定义如下:随机选取$a,s,b_1,b_2,\cdots,b_q\in\mathbb{Z}_p$,给定

$$D=(p,g,G,G_{\mathrm{T}},e,g,g^s,\{g^{a^i},g^{b_j},g^{sb_j},g^{a^ib_j},g^{a^ib_j^2}\}_{(i,j)\in[q,q]},\{g^{a^ib_j/b_{j'}^2}\}_{(i,j,j')\in[2q,q,q],j\neq j'},\{g^{a^i/b_j}\}_{(i,j)\in[2q,q],i\neq q+1},\{g^{sa^ib_j/b_{j'}},g^{sa^ib_j/b_{j'}^2}\}_{(i,j,j')\in[q,q,q],j\neq j'})$$

区分G_{T}中的随机元素R和$e(g,g)^{sa^{q+1}}$.

一个算法$\mathcal{A}$解决群G中的$q-1$难题的优势为ε,当:

$$|Pr[\mathcal{A}(D,e(g,g)^{sa^{q+1}})=0]-Pr[A(D,R)=0]|\geqslant\varepsilon.$$

若没有一个多项式时间算法能够以不可忽略的优势解决群中的$q-1$难题,则称群中的$q-1$假设成立.

定义 4. q'-SDH 假设[18].G是阶为素数p的循环群,g是G的生成元.群G中的q'-SDH 难题定义如下:随机选取$x\in\mathbb{Z}_p^*$,给定$(g,g^x,g^{x^2},\cdots,g^{x^{q'}})$,计算$(c,g^{\frac{1}{x+c}})$,其中$c\in\mathbb{Z}_p^*$.

一个算法$\mathcal{A}$解决群G中的q'-SDH 难题的优势为ε,当:

$$Pr[\mathcal{A}(g,g^x,g^{x^2},\cdots,g^{x^{q'}})=(c,g^{\frac{1}{x+c}})]\geqslant\varepsilon.$$

若没有一个多项式时间算法能够以不可忽略的优势解决群中的q'-SDH 难题,则称群中的q'-SDH 假设成立.

3 在线/离线可追责 ABE 的定义和安全模型

本文方案是在密钥封装机制(key encapsulation

mechanism, KEM)下定义的,即基于属性的加密是用来加密会话密钥的,而该会话密钥能够作为对称加密的密钥来加密任意长度的消息.

3.1　定　义

一个在线/离线的可追责密文策略属性密钥封装机制(online/offline traceable CP-AB-KEM, OO-T-CP-AB-KEM)包括 6 个算法:

1) $Setup(\lambda,U)$. 该算法输入安全参数 λ 和属性域 U,输出公钥 PK 和主密钥 MSK. 此外,该算法初始化一个追责列表 $T=\varnothing$.

2) $KeyGen(MSK,PK,id,S)$. 该算法输入主密钥 MSK、公钥 PK、用户的身份 id 和一个属性集合 $S\subseteq U$,输出一个对应于 (id,S) 的用户私钥 $SK_{id,S}$,并将 id 加入列表 T 中.

3) $Offline.Encrypt(PK)$. 该算法输入公钥 PK,输出一个间接密文 IT.

4) $Online.Encrypt(PK,IT,(\boldsymbol{M},\rho))$. 该算法输入公钥 PK、间接密文 IT 和一个访问策略 $(\boldsymbol{M},\rho)$,输出一个会话密钥 key 和一个密文 CT.

5) $Decrypt(SK_{id,S},PK,CT)$. 该算法输入公钥 PK、对应于属性集 S 的私钥 $SK_{id,S}$、对应于访问策略 $(\boldsymbol{M},\rho)$ 的密文 CT. 如果属性集 S 不满足访问策略 $(\boldsymbol{M},\rho)$,直接输出 $\perp$ 表示解密失败;否则,输出一个会话密钥 key.

6) $Trace(PK,T,SK)$. 该算法输入公钥 PK、追责列表 T、私钥 SK. 该算法首先检查 SK 是否为一个合理的私钥以确定是否有必要进行追责. 如果 SK 是一个合理的私钥,则输出 SK 对应的身份 id;否则,输出符号 Λ 表示 SK 不是一个合理的私钥.

3.2　选择性安全模型

本节通过一个敌手和挑战者之间的游戏给出 OO-T-CP-AB-KEM 的安全模型. 具体游戏描述如下:

1) 初始化. 敌手声明并发送自己要攻击的访问策略 $(\boldsymbol{M}^*,\rho^*)$ 给挑战者.

2) 系统建立. 挑战者运行 $Setup(\lambda,U)\rightarrow(PK,MSK)$,并将公钥 PK 发给敌手.

3) 询问阶段 1. 敌手向挑战者询问对应于属性集 $(id_1,S_1),(id_2,S_2),\cdots,(id_{q_1},S_{q_1})$ 的私钥. 对于所有 $i\in[q_1]$,挑战者运行 $KeyGen(MSK,PK,id_i,S_i)\rightarrow SK_{id_i,S_i}$,并将 SK_{id_i,S_i} 发送给敌手. 这里要求对任何 $i\in[q_1]$,S_i 都不满足访问策略 $(\boldsymbol{M}^*,\rho^*)$.

4) 挑战. 挑战者运行 $Online.Encrypt(PK,Offline.Encrypt(PK),(\boldsymbol{M}^*,\rho^*))\rightarrow(key^*,CT^*)$ 算法,并随机选择 $b\in\{0,1\}$. 如果 $b=0$,则将 (key^*,CT^*) 发送给敌手;如果 $b=1$,则在会话密钥空间中选择一个随机值 R,并将 (R,CT^*) 发送给敌手.

5) 询问阶段 2. 这一阶段和询问阶段 1 相同. 敌手继续向挑战者询问对应于属性集 $(id_{q_1+1},S_{q_1+1}),(id_{q_1+2},S_{q_1+2}),\cdots,(id_{q_s},S_{q_s})$ 的私钥. 同样地,对于所有 $i\in[q_s]$,要求 S_i 不能满足访问策略 $(\boldsymbol{M}^*,\rho^*)$.

6) 猜测. 敌手输出对于 b 的猜测结果 $b'\in\{0,1\}$.

敌手在上述游戏中获胜的优势被定义为 $|Pr[b=b']-1/2|$.

定义 5. 如果任何多项式时间敌手在上述游戏中获胜的优势都是可忽略的,则称一个 OO-T-CP-AB-KEM 方案是选择性安全的.

3.3　可追责性安全模型

本节通过一个敌手和挑战者之间的游戏给出 OO-T-CP-AB-KEM 中可追责性的定义. 具体追责游戏描述如下:

1) 系统建立. 挑战者运行 $Setup(\lambda,U)\rightarrow(PK,MSK)$,并将公钥 PK 发送给敌手.

2) 询问阶段. 敌手向挑战者询问对应于属性集 $(id_1,S_1),(id_2,S_2),\cdots,(id_{q_s},S_{q_s})$ 的私钥. 对于所有 $i\in[q_s]$,挑战者运行 $KeyGen(MSK,PK,id_i,S_i)\rightarrow SK_{id_i,S_i}$,并将 SK_{id_i,S_i} 发送给敌手.

3) 私钥伪造. 敌手输出一个私钥 SK^*.

敌手在上述游戏中获胜的优势被定义为 $Pr[Trace(PK,T,SK^*)\notin\{\Lambda,id_1,id_2,\cdots,id_{q_s}\}]$.

定义 6. 如果任何多项式时间敌手在上述游戏中获胜的优势都是可忽略的,则称一个 OO-T-CP-AB-KEM 方案是可追责的.

4　支持在线/离线加密的可追责 CP-ABE 方案

本节将在 KEM 情形下构造一个支持追责和在线/离线加密的 CP-ABE 方案,并且在标准模型下证明方案是选择安全和可追责的. 最后,我们给出了本文方案和相关方案的性能对比.

4.1　方案构造

此处假定 LSSS 访问策略中的矩阵最多有 P 行,后面将指出如何去除这个限制条件. 具体的 OO-T-CP-AB-KEM 方案构造如下:

1) $Setup(\lambda,U)$. 该算法首先选择一个阶为素数 p 的双线性群 G. $e:G\times G\rightarrow G_T$ 是一个定义在 G 上的双线性对;然后随机选择 $g,h,u,v,w\in G$ 和 $\alpha,a\in\mathbb{Z}_p$,输出公钥 $PK=(G,p,g,h,u,v,w,e(g,$

$g)^{a}, g^{a})$和主密钥 $MSK=(\alpha,a)$;最后建立一个空的追责列表 T.

2) $KeyGen(MSK,PK,id,S=\{A_1,A_2,\cdots,A_k\}\subseteq\mathbb{Z}_p)$. 该算法随机选择 $r,r_1,r_2,\cdots,r_k\in\mathbb{Z}_p$和 $c\in\mathbb{Z}_p^*\setminus\{-a\}$,如果 c 已经存在于列表 T 中,则重新选择随机元 c;然后计算 $K_0=g^{\frac{a}{a+c}}w^r$, $K_0'=c$, $K_1=g^r$, $K_1'=g^{ar}$,并对所有 $i\in[k]$计算 $K_{i,2}=g^{r_i}$, $K_{i,3}=(u^{A_i}h)^{r_i}v^{-(a+c)r}$;最后输出用户的私钥 $SK_{id,S}=(S,K_0,K_0',K_1,K_1',\{K_{i,2},K_{i,3}\}_{i\in[k]})$,并将数组$(c,id)$加入到追责列表 T 中.

3) $Offline.Encrypt(PK)$. 该算法选择随机数 $s\in\mathbb{Z}_p$,计算 $key=e(g,g)^{as}$, $C_0=g^s$, $C_0'=g^{as}$;然后对所有的 $j\in[P]$,随机选择 $\lambda_j',x_j,t_j\in\mathbb{Z}_p$,并计算 $C_{j,1}=w^{\lambda_j'}v^{t_j}$, $C_{j,2}=(u^{x_j}h)^{-t_j}$, $C_{j,3}=g^{t_j}$;最后输出间接密文 $IT=(key,s,C_0,C_0',\{\lambda_j',t_j,x_j,C_{j,1},C_{j,2},C_{j,3}\}_{j\in[P]})$.

4) $Online.Encrypt(PK,IT,(\boldsymbol{M},\rho))$. 该算法输入公钥 PK、间接密文 IT 和 LSSS 访问策略$(\boldsymbol{M},\rho)$. 其中 $\boldsymbol{M}$ 是一个 $l\times n$ 矩阵,且 $l\leqslant P$, $\rho:[l]\to\mathbb{Z}_p$ 将矩阵的每一行 $\boldsymbol{M}_j$ 映射到属性 $\rho(j)$. 首先随机选择 $y_2,\cdots,y_n\in\mathbb{Z}_p$,令向量 $\boldsymbol{y}=(s,y_2,\cdots,y_n)^{\mathrm{T}}$;然后对所有的 $j\in[l]$,计算 $\lambda_j=(\boldsymbol{My})_j$, $C_{j,4}=\lambda_j-\lambda_j'$, $C_{j,5}=t_j(x_j-\rho(j))$;最终得到会话密钥 $key=e(g,g)^{as}$和密文 $CT=((\boldsymbol{M},\rho),C_0,C_0',\{C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5}\}_{j\in[l]})$.

5) $Decrypt(SK_{id,S},PK,CT)$. KEM 情形下的解密算法用来恢复会话密钥 key. 该算法输入对应于访问策略$(\boldsymbol{M},\rho)$的密文 $CT=((\boldsymbol{M},\rho),C_0,C_0',\{C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5}\}_{j\in[l]})$和对应于属性集 S 的私钥 $SK_{id,S}=(S,K_0,K_0',K_1,K_1',\{K_{i,2},K_{i,3}\}_{i\in[k]})$. 如果属性集 S 不满足访问策略$(\boldsymbol{M},\rho)$,直接输出$\perp$表示解密失败;否则,令 $I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,l\}$,并计算常数$\{\omega_i\in\mathbb{Z}_p\}$满足 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\cdots,0)$. 然后计算得到:

$$key=\frac{e(K_0,C_0^{K_0'}C_0')}{e(w^{\sum_{i\in I}(C_{i,4}\omega_i)}\prod_{i\in I}C_{i,1}^{\omega_i},K_1^{K_0'}K_1')\prod_{i\in I}(e(C_{i,2}u^{c_{i,5}},K_{j,2})e(C_{i,3},K_{j,3}))^{\omega_i}},$$

其中 j 是属性 $\rho(i)$在集合 $S=\{A_1,A_2,\cdots,A_k\}$中的索引,即 $\rho(i)=A_j$.

6) $Trace(PK,T,SK)$. 该算法输入公钥 PK、追责列表 T 和私钥 SK. 该算法首先检查 SK 是否为一个合理的私钥. 如果 SK 的形式为 $SK=(S,K_0,K_0',K_1,K_1',\{K_{i,2},K_{i,3}\}_{i\in[k]})$且通过下面的私钥检查,则表明 SK 是一个合理的私钥,其中 k 表示属性集中包含属性的个数. 然后在追责列表 T 中查找 K_0',并输出对应的身份 id. 否则;输出符号 Λ 表示 SK 不是一个合理的私钥. 具体的私钥检查条件如下:

$$S=\{A_1,A_2,\cdots,A_k\}\subseteq\mathbb{Z}_p,\tag{1}$$

$$K_0'\in\mathbb{Z}_p^*,K_0,K_1,K_1',K_{i,2},K_{i,3}\in G;\tag{1}$$

$$e(K_1,g^a)=e(K_1',g);\tag{2}$$

$$e(K_0,g^ag^{K_0'})=e(g,g)^ae(w,K_1^{K_0'}K_1');\tag{3}$$

存在 $i\in[k]$使得:

$$e(K_{i,3},g)e(v,K_1^{K_0'}K_1')=e(K_{i,2},u^{A_i}h).\tag{4}$$

正确性. 如果属性集 S 满足访问策略$(\boldsymbol{M},\rho)$,则有 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\cdots,0)$,所以:

$$\sum_{i\in I}\omega_i\lambda_i=\sum_{i\in I}\omega_i(\boldsymbol{My})_i=\boldsymbol{y}\times\sum_{i\in I}(\omega_i\boldsymbol{M}_i)=\boldsymbol{y}\cdot(1,0,\cdots,0)=s.$$

因此有:

$$e(w^{\sum_{i\in I}(C_{i,4}\omega_i)}\prod_{i\in I}C_{i,1}^{\omega_i},K_1^{K_0'}K_1')\prod_{i\in I}(e(C_{i,2}u^{c_{i,5}},K_{j,2})e(C_{i,3},K_{j,3}))^{\omega_i}=$$

$$\prod_{i\in I}e(w^{C_{i,4}\omega_i}C_{i,1}^{\omega_i},K_1^{K_0'}K_1')\prod_{i\in I}(e(C_{i,2}u^{c_{i,5}},K_{j,2})e(C_{i,3},K_{j,3}))^{\omega_i}=$$

$$\prod_{i\in I}(e(w^{C_{i,4}}C_{i,1},K_1^{K_0'}K_1')e(C_{i,2}u^{c_{i,5}},K_{j,2})e(C_{i,3},K_{j,3}))^{\omega_i}=$$

$$\prod_{i\in I}(e(w^{\lambda_i-\lambda_i'}w^{\lambda_i'}v^{t_i},g^{cr}g^{ar})e((u^{r_i}h)^{-t_i}u^{t_i(x_i-\rho(i))},g^{r_j})e(g^{t_i},(u^{A_j}h)^{r_j}v^{-(a+c)r}))^{\omega_i}=$$

$$\prod_{i\in I}(e(w^{\lambda_i},g)^{(a+c)r}e(v^{t_i},g)^{(a+c)r}e(u^{-t_i\rho(i)}h,g)^{-t_ir_j}e(g,u^{\rho(i)}h)^{t_ir_j}e(g,v)^{-(a+c)rt_i})^{\omega_i}=$$

$$\prod_{i\in I}(e(w^{\lambda_i},g)^{(a+c)r})^{\omega_i}=\prod_{i\in I}e(w,g)^{(a+c)r\lambda_i\omega_i}=e(w,g)^{(a+c)r\sum_{i\in I}\omega_i\lambda_i}=e(w,g)^{(a+c)rs}.$$

又因为 $e(K_0,C_0^{K_0'}C_0')=e(g^{\frac{a}{a+c}}w^r,g^{cs}g^{as})=e(g,g)^{as}e(w,g)^{(a+c)sr}$,所以有:

$$key=\frac{e(K_0,C_0^{K_0'}C_0')}{e(w^{\sum_{i\in I}(C_{i,4}\times\omega_i)}\prod_{i\in I}C_{i,1}^{\omega_i},K_1^{K_0'}K_1')\prod_{i\in I}(e(C_{i,2}u^{c_{i,5}},K_{j,2})e(C_{i,3},K_{j,3}))^{\omega_i}}=e(g,g)^{as}.$$

4.2　选择性安全证明

本节将证明本文方案在 $q-1$ 假设下是选择性安全的. 首先证明如下引理.

引理 1. 如果 HW (Hohenberger-Waters) 方案[15]是选择性安全的,则本文的 OO-T-CP-AB-KEM 方案是选择性安全的.

证明. 为了证明这个引理,我们将指出:在选择性安全模型下,如果有一个多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破 OO-T-CP-AB-KEM 方案,则能利用敌手 $\mathcal{A}$ 构造一个模拟者 $\mathcal{B}$ 以同样的优势 ε 攻破 HW 方案. $\mathcal{C}$ 是 HW 方案中与模拟者 $\mathcal{B}$ 交互的挑战者.

1) 初始化. 敌手 $\mathcal{A}$ 首先发送自己要攻击的访问策略 $(\boldsymbol{M}^*,\rho^*)$ 给模拟者 $\mathcal{B}$,$\mathcal{B}$ 将 $(\boldsymbol{M}^*,\rho^*)$ 发送给挑战者 $\mathcal{C}$. 其中 $\boldsymbol{M}^*$ 是一个 $l\times n$ 矩阵,$\rho^*:l\to\mathbb{Z}_p$ 将矩阵的每一行 $\boldsymbol{M}_j^*$ 映射到属性 $\rho^*(j)$.

2) 系统建立. 挑战者 $\mathcal{C}$ 将 HW 方案的公钥 $\overline{PK}=(G,p,g,h,u,v,w,e(g,g)^{\alpha})$ 发送给模拟者 $\mathcal{B}$. $\mathcal{B}$ 随机选择 $a\in\mathbb{Z}_p^*$,建立一个追责列表 $T=\varnothing$,并将公钥 $PK=(G,p,g,h,u,v,w,e(g,g)^{\alpha},g^{a})$ 发送给敌手 $\mathcal{A}$.

3) 询问阶段 1. 在这一阶段,模拟者 $\mathcal{B}$ 回答敌手 $\mathcal{A}$ 的私钥询问. 当 $\mathcal{A}$ 发送 (id,S) 给 $\mathcal{B}$ 并询问 OO-T-CP-AB-KEM 方案中对应的私钥时,$\mathcal{B}$ 将属性集 S 发送给挑战者 $\mathcal{C}$ 并询问 HW 方案中对应的私钥. $\mathcal{C}$ 将 HW 方案中的私钥 $SK=(S,\overline{K_0}=g^{\alpha}w^{\bar{r}},\overline{K_1}=g^{\bar{r}},\{\overline{K_{i,2}}=g^{r_i},\overline{K_{i,3}}=(u^{A_i}h)^{r_i}v^{-\bar{r}}\}_{i\in[k]})$ 发送给 $\mathcal{B}$. $\mathcal{B}$ 随机选择 $c\in\mathbb{Z}_p^*\setminus\{-a\}$,并取 $\bar{r}/(a+c)=r$,然后计算:

$$K_0=(\overline{K_0})^{\frac{1}{a+c}}=g^{\frac{\alpha}{a+c}}w^{\frac{\bar{r}}{a+c}}=g^{\frac{\alpha}{a+c}}w^{r},K_0'=c,K_1=(\overline{K_1})^{\frac{1}{a+c}}=g^{\frac{\bar{r}}{a+c}}=g^{r},K_1'=(K_1)^{a}=g^{ar},$$

$$K_{i,2}=\overline{K_{i,2}}=g^{r_i},K_{i,3}=\overline{K_{i,3}}=(u^{A_i}h)^{r_i}v^{-\bar{r}}=(u^{A_i}h)^{r_i}v^{-(a+c)r}.$$

$\mathcal{B}$ 将私钥 $SK_{id,S}=(S,K_0,K_0',K_1,K_1',\{K_{i,2},K_{i,3}\}_{i\in[k]})$ 发送给 $\mathcal{A}$,并将数组 (c,id) 加入到追责列表 T 中.

4) 挑战. 挑战者 $\mathcal{C}$ 运行 HW 方案的加密算法得到会话密钥 $\overline{key}=e(g,g)^{\alpha s}$ 和密文 $\overline{CT}=((\boldsymbol{M}^*,\rho^*),\overline{C_0}=g^{s},\{\overline{C_{j,1}}=w^{\lambda_j'}v^{t_j},\overline{C_{j,2}}=(u^{x_j}h)^{-t_j},\overline{C_{j,3}}=g^{t_j},\overline{C_{j,4}}=\lambda_j-\lambda_j',\overline{C_{j,5}}=t_j(x_j-\rho(j))\}_{j\in[l]})$. $\mathcal{C}$ 随机选择 $b\in\{0,1\}$,如果 $b=0$,则令 $\overline{key}_b=e(g,g)^{\alpha s}$;如果 $b=1$,则在会话密钥空间中选择一个随机值 R,并令 $\overline{key}_b=R$. 然后 $\mathcal{C}$ 将 $(\overline{key}_b,\overline{CT})$ 发送给 $\mathcal{B}$. $\mathcal{B}$ 计算 $C_0'=(\overline{C_0})^{s}=g^{as}$,并令挑战密文为

$$CT^*=((\boldsymbol{M}^*,\rho^*),C_0=g^{s},C_0'=g^{as},$$
$$\{C_{j,1}=w^{\lambda_j'}v^{t_j},C_{j,2}=(u^{x_j}h)^{-t_j},C_{j,3}=g^{t_j},$$
$$C_{j,4}=\lambda_j-\lambda_j',C_{j,5}=t_j(x_j-\rho(j))\}_{j\in[l]}).$$

最后 $\mathcal{B}$ 将 $(key^*=\overline{key}_b,CT^*)$ 发送给敌手 $\mathcal{A}$.

5) 询问阶段 2. 这一阶段和询问阶段 1 相同.

6) 猜测. 敌手 $\mathcal{A}$ 发送给 $\mathcal{B}$ 对于 b 测猜结果 b'. 最后,$\mathcal{B}$ 输出 b'.

由于上述分布对于敌手 $\mathcal{A}$ 来说是完美的,因此,如果 $\mathcal{A}$ 能够以优势 ε 攻破我们的 OO-T-CP-AB-KEM 方案,则模拟者 $\mathcal{B}$ 能以同样的优势 ε 攻破 HW 方案. 证毕.

此外,下述 2 个引理已在文献[13,15]中被证明.

引理 2[15]. 如果 RW(Rouselakis-Waters)方案[13]是选择性安全的,则 HW 方案[15]也是选择性安全的.

引理 3[13]. 如果 $q-1$ 假设成立,且挑战矩阵 $\boldsymbol{M}^*$ 的大小 $l\times n$ 满足 $l,n\leqslant q$,则 RW 方案是选择性安全的.

定理 1. 如果 $q-1$ 假设成立,且挑战矩阵 $\boldsymbol{M}^*$ 的大小 $l\times n$ 满足 $l,n\leqslant q$,则本文的 OO-T-CP-AB-KEM 方案是选择性安全的.

证明. 由引理 1、引理 2 和引理 3 可以直接得出. 证毕.

4.3　可追责性安全证明

本节将证明本文方案在 q'-SDH 假设下是可追责的. 首先证明如下引理.

引理 4. 假设 BB(Boneh-Boyen)签名方案[18]在弱选择消息攻击下是存在性不可伪造的,则本文的 OO-T-CP-AB-KEM 方案是可追责的.

证明. 假设对于本文的 OO-T-CP-AB-KEM 方案,存在一个多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 赢得 3.3 中的追责游戏,则能构造出一个模拟者 $\mathcal{B}$ 在弱选择消息攻击下,以同样的优势 ε 伪造一个 BB 签名. $\mathcal{C}$ 是 BB 签名方案中与模拟者 $\mathcal{B}$ 交互的挑战者.

1) 系统建立. 挑战者 $\mathcal{C}$ 将 BB 签名方案中的公钥 $\overline{PK}=\{p,G,g,g^{a}\}$ 发送给模拟者 $\mathcal{B}$. $\mathcal{B}$ 随机选择 $h,u\in G$ 和 $\alpha,\beta,\gamma\in\mathbb{Z}_p$,将公钥 $PK=(G,p,g,h,u,v=g^{\beta},w=g^{\lambda},e(g,g)^{\alpha},g^{a})$ 发送给敌手 $\mathcal{A}$,并建立追责列表 $T=\varnothing$.

2) 询问阶段.在这一阶段,敌手 $\mathcal{A}$ 进行 q 次私钥询问,模拟者 $\mathcal{B}$ 回答 $\mathcal{A}$ 的私钥询问.当 $\mathcal{A}$ 进行第 $j(j\leqslant q)$ 次私钥询问时,$\mathcal{A}$ 发送 $(id_j, S_j=\{A_1, A_2,\cdots,A_K\}\subseteq\mathbb{Z}_p)$ 给 $\mathcal{B}$ 并询问 OO-T-CP-AB-KEM 方案中对应的私钥.$\mathcal{B}$ 首先随机选择 $c_j\in\mathbb{Z}_p^*$,如果 c_j 已经在列表 T 中,则重新选择 $c_j\in\mathbb{Z}_p^*$,然后向 $\mathcal{C}$ 询问 c_j 的 BB 签名.$\mathcal{C}$ 返回给 $\mathcal{B}$ 签名 $(c_j,\sigma_j=g^{\frac{1}{c_j+a}})$.$\mathcal{B}$ 随机选择 $r, r_1, r_2,\cdots, r_k\in\mathbb{Z}_p$,然后计算:

$$K_{0,j}=\sigma_j^a w^r=g^{\frac{a}{a+c_j}}w^r,$$

$$K'_{0,j}=c_j,$$

$$K_{1,j}=g^r,$$

$$K'_{1,j}=(g^a)^r=g^{ar},$$

$$K_{i,2,j}=g^{r_i},$$

$$K_{i,3,j}=(u^{A_i}h)^{r_i}(g^a g^{c_j})^{-\beta r}=$$

$$(u^{A_i}h)^{r_i}(g^\beta)^{-(a+c_j)r}=(u^{A_i}h)^{r_i}(v)^{-(a+c_j)r}.$$

对于 $c_j=-a$ 这种极小概率发生的情形,$\mathcal{C}$ 返回给 $\mathcal{B}$ 的签名为 $(c_j,1)$,这时 $\mathcal{B}$ 需要重新选择 $c_j\in\mathbb{Z}_p^*$,并重复上述过程.最后将私钥 $SK_{id_j,S_j}=(S_j, K_{0,j}, K'_{0,j}, K_{1,j}, K'_{1,j}, \{K_{i,2,j}, K_{i,3,j}\}_{i\in[k]})$ 发送给 $\mathcal{A}$,并将数组 (c, id) 加入到追责列表 T 中.

3) 私钥伪造.敌手 $\mathcal{A}$ 输出一个私钥 SK^* 给 $\mathcal{B}$.

假设敌手 $\mathcal{A}$ 在上述游戏中获胜,则 $Trace(PK, T, SK^*)\notin\{\Lambda, id_1, id_2,\cdots, id_q\}$.因此 $SK^*=(S, K_0, K'_0, K_1, K'_1, \{K_{i,2}, K_{i,3}\}_{i\in[k]})$ 通过私钥合理性检查,且 $K'_0\notin\{c_1, c_2,\cdots, c_q\}$.所以有:

$$S=\{A_1, A_2,\cdots, A_k\}\subseteq\mathbb{Z}_p,$$

$$K'_0\in\mathbb{Z}_p^*, K_0, K_1, K'_1, K_{i,2}, K_{i,3}\in G; \quad (5)$$

$$e(K_1, g^a)=e(K'_1, g); \quad (6)$$

$$e(K_0, g^a g^{K'_0})=e(g,g)^a e(w, K_1^{K'_0}K'_1). \quad (7)$$

假设 $K_1=g^t$,其中 t 是 $\mathbb{Z}_p$ 中的未知元.由式(6)可得 $K'_1=K_1^a=g^{at}$.因此由式(7)可得

$$e(K_0, g^{(a+K'_0)})=e(g,g)^a e(w, g^{(a+K'_0)t})=$$

$$e(g^{(a+K'_0)}, g^{\frac{a}{a+K_0}}w^t),$$

所以 $K_0=g^{\frac{a}{a+K_0}}w^t$.模拟者 $\mathcal{B}$ 计算:

$$\left(\frac{K_0}{K_1^\gamma}\right)^{a^{-1}}=\left(\frac{K_0}{g^{\gamma t}}\right)^{a^{-1}}=\left(\frac{K_0}{w^t}\right)^{a^{-1}}=(g^{\frac{a}{a+K_0}})^{a^{-1}}=g^{\frac{1}{a+K_0}}.$$

由于 $K'_0\in\mathbb{Z}_p^*$,所以 $(K'_0, g^{\frac{1}{a+K_0}})$ 是一个有效的 BB 签名.又因 $K'_0\notin\{c_1, c_2,\cdots, c_q\}$,所以模拟者 $\mathcal{B}$ 在弱选择消息攻击下,以优势 ε 对 BB 签名方案进行了存在性伪造. 证毕.

此外,由文献[18],我们有以下引理.

引理 5[18]. 如果 q'-SDH 假设成立,且进行私钥询问的次数 $q_s\leqslant q'$,则在弱选择消息攻击下 BB 签名方案[18]是存在性不可伪造的.

定理 2. 如果 q'-SDH 假设成立,且进行私钥询问的次数 $q_s\leqslant q'$,则本文的 OO-T-CP-AB-KEM 方案是可追责的.

证明. 由引理 4 和引理 5 可以直接得出. 证毕.

4.4 移除对访问策略的限制

在 4.1 节中,LSSS 访问策略中的矩阵行数不能超过 P,这将会限制方案的实际应用.在现实生活中我们会使用不同大小的访问策略,如果访问策略对应的矩阵行数大于 P,则不能够完成在线加密操作;如果访问策略对应的矩阵行数小于 P,就会造成在离线阶段产生和存储的一些中间密文不能被利用,从而造成不必要的计算和存储开销.为了移除这个限制条件,这里我们利用文献[15]中的“池化(pooling)”技术来对加密阶段做出改进.首先将间接密文 IT 分为 2 部分:主要模块 $IT_{\text{main}}=(key=e(g,g)^{\alpha s}, s, C_0=g^s, C'_0=g^{\alpha s})$ 和属性模块 $IT_{\text{att},j}=(\lambda'_j, t_j, x_j, C_{j,1}, C_{j,2}, C_{j,3})$.其中 $C_{j,1}=w^{\lambda'_j}v^{t_j}$,$C_{j,2}=(u^{x_j}h)^{-t_j}$,$C_{j,3}=g^{t_j}$.然后在离线阶段分别独立产生大量 IT_{main} 和 $IT_{\text{att},j}$.在线加密过程中,当访问策略对应的矩阵 $\boldsymbol{M}$ 是一个 $l\times n$ 矩阵时,只要输入 1 个主模块和 l 个属性模块,并执行 4.1 节中的在线加密算法就能够生成一个有效的密文 CT 和会话密钥 $key=e(g,g)^{\alpha s}$.由于任意的主要模块 IT_{main} 可以和任意的属性模块 $IT_{\text{att},j}$ 结合,所以剩下的主要模块 IT_{main} 和属性模块 $IT_{\text{att},j}$ 可以用到以后密文的产生,因此不会造成资源浪费.由于这里的改进并没有影响最终密文 CT 的结构和分布,所以改进后方案与 4.1 节中方案的安全性分析是一样的.

4.5 方案对比

表 1 给出了本文方案与相关方案的性能对比.其中,l 表示 LSSS 访问策略中矩阵的总行数,E_{T} 表示群 G_{T} 中的指数运算,E_{G} 和 M_{G} 分别表示群 G 中的指数和乘法运算.相比群 G 和 G_{T} 中的运算,$\mathbb{Z}_p$ 中的运算开销很小,因此表 1 中忽略了 $\mathbb{Z}_p$ 中的运算开销.

从表 1 中可以看出,文献[15]中方案的在线加密开销很小,但是并不支持对恶意用户追责,存在恶意用户出售私钥的风险.文献[9,11]和本文方案都支持用户追责和 LSSS 访问策略,因此在实现灵活访问控制的同时,可以追踪泄露私钥的用户身份.然而,文献[9]并不支持大属性域,即系统的属性域需要在系统建立之初确定.如果后面新加入的属性超出了属性域,则需要重新建立系统,这导致文献[9]

中方案的可扩展性较差. 文献[11]尽管支持大属性域,但方案的加密过程全部需要用户在线完成,这会使得在线加密的时间和能源开销较大,不适用于移动设备进行加密. 相比于文献[9,11],本文方案的加密开销几乎全部在离线阶段,这样使用移动设备的用户可以在能源充足时进行离线加密操作,当需要加密具体数据时,只需要消耗较少能源就能够快速完成在线加密.

Table 1　Comparison with Other Related Schemes

表 1　与相关方案的对比

Scheme	Traceability	Large Universe	Access Policy	Computation Cost in Offline Encryption	Computation Cost in Online Encryption
Ref[15]	No	Yes	LSSS	$1E_T+(5l+1)E_G+2lM_G$	0
Ref[9]	Yes	No	LSSS	0	$1E_T+(3l+2)E_G+lM_G$
Ref[11]	Yes	Yes	LSSS	0	$1E_T+(5l+2)E_G+2lM_G$
Our Scheme	Yes	Yes	LSSS	$1E_T+(5l+2)E_G+2lM_G$	0

5　结束语

本文在素数阶双线性群下构造了一个支持在线/离线加密的可追责 CP-ABE 方案,并且在标准模型下证明了方案是选择性安全和可追责的. 在本文方案中,如果一个恶意用户泄露自己的私钥,则可以通过追责算法确定恶意用户的身份. 本文方案不仅支持任意的单调访问结构,而且绝大部分的加密操作是在离线阶段完成的,更适用于资源受限的移动设备. 此外,本文方案是支持大属性域的,因此在实际应用中具有较好的扩展性.

参　考　文　献

[1] Sahai A, Waters B. Fuzzy identity-based encryption [G] //LNCS 3494: Proc of EUROCRYPT'05. Berlin: Springer, 2005: 457-473

[2] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2007: 321-334

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[4] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [G] //LNCS 6571: Proc of PKC'11. Berlin: Springer, 2011: 53-70

[5] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [G] //LNCS 6110: Proc of EUROCRYPT'10. Berlin: Springer, 2010: 62-91

[6] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [G] //LNCS 6223: Proc of CRYPTO'10. Berlin: Springer, 2010: 191-208

[7] Hinek M J, Jiang Shaoquan, Safavi-Naini R, et al. Attribute-based encryption with key cloning protection [EB/OL]. International Association for Cryptologic Research (IACR), (2008-11-12) [2017-01-08]. http://eprint.iacr.org/2008/478

[8] Li Jin, Ren Kui, Kim K. A2BE: Accountable attribute-based encryption for abuse free access control [EB/OL]. International Association for Cryptologic Research (IACR), (2009-04-14) [2017-01-08]. http://eprint.iacr.org/2009/118

[9] Liu Zhen, Cao Zhenfu, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Trans on Information Forensics and Security, 2013, 8(1): 76-88

[10] Liu Zhen, Cao Zhenfu, Wong D S. Traceable CP-ABE: How to trace decryption devices found in the wild [J]. IEEE Trans on Information Forensics and Security, 2015, 10(1): 55-68

[11] Ning Jianting, Dong Xiaolei, Cao Zhenfu, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes [J]. IEEE Trans on Information Forensics and Security, 2015, 10(6): 1274-1288

[12] Lewko A, Waters B. Unbounded HIBE and attribute-based encryption [G] //LNCS 6632: Proc of EUROCRYPT'11. Berlin: Springer, 2011: 547-567

[13] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption [C] //Proc of the 20th ACM Conf on Computer and Communications Security. New York: ACM, 2013: 463-474

[14] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C] //Proc of USENIX the Security Symp. Berkeley, CA: USENIX Association, 2011: 523-538

[15] Hohenberger S, Waters B. Online/offline attribute-based encryption [G] //LNCS 8383: Proc of PKC'14. Berlin: Springer, 2014: 293-310

[16] Xiao Siyu, Ge Aijun, Ma Chuangui. Decentralized attribute-based encryption scheme with constant-size ciphertexts [J]. Journal of Computer Research and Development, 2016, 53(10): 2207-2215 (in Chinese)
(肖思煜, 葛爱军, 马传贵. 去中心化且固定密文长度的基于属性加密方案[J]. 计算机研究与发展, 2016, 53(10): 2207-2215)

[17] Beimel A. Secure schemes for secret sharing and key distribution [D]. Haifa, Israel: Technion-Israel Institute of Technology, Faculty of Computer Science, 1996

[18] Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups [J]. Journal of Cryptology, 2008, 21(2): 149-177

Zhang Kai, born in 1987. PhD candidate in the School of Telecommunications Engineering, Xidian University. His main research interests include cryptography and information security.

Ma Jianfeng, born in 1963. PhD. Professor and PhD supervisor in the School of Computer Science and Technology, Xidian University. Fellow member of CCF. His main research interests include information security, coding theory, and cryptography.

Zhang Junwei, born in 1982. PhD. Associate professor in the School of Computer Science and Technology, Xidian University. Member of CCF. His main research interests include cryptography and information security (jwzhang@xidian.edu.cn).

Ying Zuobin, born in 1982. PhD. Lecturer in the School of Computer Science and Technology, Anhui University. His main research interests include information security and security in big data (yingzb82@163.com).

Zhang Tao, born in 1986. PhD. Lecturer in the School of Computer Science and Technology, Xidian University. His main research interests include trusted computing and social network (taozhang@xidian.edu.cn).

Liu Ximeng, born in 1988. PhD. Research fellow in the School of Information Systems, Singapore Management University. His main research interests include cloud security, applied cryptography and big data security (snbnix@gmail.com).