

# 改进的外包解密策略隐藏 CP-ABE 方案

刘文扬, 王志伟

(南京邮电大学 计算机学院, 江苏 南京 210003)

**摘要:** 为了有效解决属性基加密技术在智能电网领域应用中计算效率低以及访问策略隐藏等问题, 在 CP-ABE 方案的基础上, 提出了一种改进的 CP-ABE 方案。该方案具有外包解密计算功能和策略隐藏能力, 利用单向匿名密钥协商技术达到了模糊属性的目的, 以实现策略隐藏能力。在解密过程中, 对密钥进行转换, 将转换密钥和密文发送给计算代理, 实现解密计算的外包, 减轻了用户的计算代价, 提高了方案的解密计算效率。与原方案及其他同类方案相比, 所提出的方案在拥有同等安全级别的同时, 增加了策略隐藏功能, 同时显著提高了解密计算效率。安全性分析结果表明, 所提出的新方案能够抵抗共谋攻击, 保证数据的机密性; 性能分析表明, 所提出的方案在密文长度以及解密复杂性方面均有很大程度的改进。

**关键词:** 智能电网; 属性基加密; 策略隐藏; 外包解密

**中图分类号:** TP301

**文献标识码:** A

**文章编号:** 1673-629X(2017)07-0101-05

**doi:** 10.3969/j.issn.1673-629X.2017.07.024

## Improved CP-ABE Scheme with Outsourced Decryption and Hidden Policy

LIU Wen-yang, WANG Zhi-wei

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

**Abstract:** In order to tackle the problems of computational efficiency and hide access policy in smart grid for attribute-based encryption scheme, an improved CP-ABE scheme has been proposed based on CP-ABE, which has been endowed with the capabilities of outsourced decryption and policy hidden. It employs one-way anonymous key agreement to fuzzy attribute in order to realize hide access policy. In the process of decryption, a transformed key and the cipher text have been sent to a proxy to finish outsource of decryption computation, which could reduce the calculation cost on user's side and improve decryption efficiency. Compared with the original scheme and other similar schemes, the proposed scheme has increased the capability of policy hidden and improved the computational efficiency significantly while having the same security level. Security analysis indicates that it has resisted collusion attack and ensured data confidentiality. Performance analysis show that the length of cipher text and decryption efficiency has been improved.

**Key words:** smart grid; attribute-based encryption; hidden policy; outsourced decryption

## 0 引言

智能电网<sup>[1-2]</sup>是信息技术和能源技术的结合, 作为未来电网的发展方向, 近年来逐渐成为研究的热点。智能电网允许用户充分地参与信息交流, 但用户对电力的使用模式不仅披露了用户的使用情况, 还可能推断出具体活动的信息, 同时用户交流的敏感信息也面临被攻击利用的可能。因此智能电网中对用户的隐私保护日益引起人们的关注。

CP-ABE 是用于访问控制的一种新型密码学原

语, 在智能电网中有很好的应用前景。然而, 许多现有 ABE 方案都存在一个效率上的缺点, 就是解密的计算成本, 使用智能电表的用户通常具有有限的计算资源, 因此将繁琐的解密计算开销委托给一个具有高度计算能力的代理中心是一个有效的解决思路。而随之带来的另一个缺点是, 访问策略与密文相关联可能泄漏大量的用户敏感信息。计算代理中心是半可信的, 它会对访问策略像其他明文数据一样产生好奇, 而出于其自身利益的考虑, 它可能会出卖部分敏感的访问策略,

**收稿日期:** 2016-07-19

**修回日期:** 2016-10-26

**网络出版时间:** 2017-06-05

**基金项目:** 江苏省网络监控工程中心 2015 年开放课题 (KJR1505); 上海市信息安全综合管理技术研究重点实验室 2016 年开放课题 (AGK201603)

**作者简介:** 刘文扬 (1991-), 男, 硕士研究生, 研究方向为密码学与信息安全; 王志伟, 副教授, 研究方向为密码学与信息安全。

**网络出版地址:** <http://cnki.net/kcms/detail/61.1450.TP.20170605.1507.042.html>

这可能会造成严重的后果。

为解决计算效率的问题,Green 等<sup>[3]</sup>提出了带外包解密的 ABE 概念,将繁琐的计算开销交给代理处理。Lai 等<sup>[4]</sup>提出了改进的带可验证的外包解密的 ABE 概念,从而允许用户验证由代理处理的部分解密密文的正确性。文献[5-8]相继提出了一些基于外包解密的 ABE 方案。在策略隐藏方面,Bethencourt 等提出了第一个密文策略的属性基加密方案(Ciphertext Policy Attribute Based Encryption,CP-ABE)<sup>[9]</sup>,用户私有密钥与一个属性组相关联,并且叙述了密文相关的访问控制策略。如果用户属性满足解密密文所需要的访问控制策略,它有获得明确的文本信息的能力。Nishide 等<sup>[10]</sup>提出了两种实现策略隐藏的 CP-ABE 构造,通过多值属性之间的与逻辑来表示访问控制策略。Lai 等<sup>[11]</sup>基于子群判定性假设,在合数阶双线性群上提出了一种适应性选择密文攻击安全的策略隐藏 CP-ABE 方案。文献[12-13]中也提出了实现策略隐藏的 ABE 方案。CP-ABE 的访问结构可以分为“与”门、访问树和 LSSS 矩阵 3 类<sup>[14]</sup>,其中访问树和 LSSS 矩阵的结构较为复杂,但策略可表达性更强,访问树结构比 LSSS 矩阵更直观。

在 Ibraimi<sup>[15]</sup>方案的基础上,增加了一个 GenToken 算法,将用户私钥和拥有的属性进行变换,利用单向匿名密钥协商的思路,将属性值进行模糊操作达到隐藏策略的目的。同时在原方案中增加一个 Outsourced Decrypt 算法,将解密计算交由计算代理进行,计算代理返回一个部分解密密文给用户,用户只需运行轻量解密算法即可得到明文。

## 1 预备知识

### 1.1 访问结构

假设  $\{P_1, P_2, \dots, P_n\}$  是一个参与方集合。如果  $A \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$  是单调的,那么对于  $\forall B, C$ ,若  $B \in A$  且  $B \subseteq C$ ,则  $C \in A$ 。

访问结构  $A$  是  $\{P_1, P_2, \dots, P_n\}$  的非空子集,即  $A \subseteq 2^{\{P_1, P_2, \dots, P_n\}} / \{\emptyset\}$ 。  $A$  中的集合称为授权集,否则称为非授权集。在 CP-ABE 中,采用属性替代参与方,访问结构  $A$  包含授权属性集。

在该方案中,访问树是一棵  $n$  叉树,其中叶子节点代表属性,内部节点代表  $\wedge$  和  $\vee$  的布尔操作。访问树即访问策略,指定了哪些属性的组合可以解密密文。

### 1.2 秘密共享方案

为了共享一个秘密值  $s$ ,对于某个整数  $p$ ,有  $0 \leq s \leq p-1$ 。首先生成  $t-1$  个随机数  $s_i$  ( $1 \leq s_i \leq p-1$ ,  $1 \leq i \leq t-1$ ) 且满足  $s_i = \sum_{i=1}^t s_i \bmod p$ 。  $s$  可由  $s = \sum_{i=1}^t s_i$  恢复。

恢复。分量  $s_i$  对于每个参与方  $P_i$  是分散的,对每个参与方  $P_i$  而言,这些分量是介于 0 和  $p-1$  中的随机数,因此单个参与方无法获得秘密值  $s$  的任何信息。

### 1.3 双线性对

设  $k$  为安全参数,  $p$  为  $k$  比特长的素数。令  $G_0$  为由  $P$  生成的循环加法群,阶为  $p$ ,  $G_T$  为具有相同阶  $p$  的循环乘法群,  $a, b$  是  $Z_p^*$  中的元素。0 为  $G_0$  的单位元,1 为  $G_T$  的单位元。假设  $G_0$  和  $G_T$  上的离散对数问题均不能在多项式时间内解决。双线性配对的映射  $e: G_0 \times G_0 \rightarrow G_T$  都具有下列属性:

(1) 双线性 (bilinearity): 对任意  $P, Q \in G_0$  和  $a, b \in Z_p^*$ ,  $e(aP, bQ) = e(P, Q)^{ab}$  成立。

(2) 非退化性 (non-degeneracy): 存在  $P, Q \in G_0$ , 使得  $e(P, Q) \neq 1$ 。当然,有  $e(0, Q) = e(Q, 0) = 1$ 。

(3) 可计算性 (computability): 对于所有的  $P, Q \in G_0$ , 可以通过确定的算法计算  $e(P, Q)$ 。

双线性映射可以通过有限域上的超奇异椭圆曲线或超奇异超椭圆曲线中的 Weil 配对或 Tate 配对进行推导<sup>[16]</sup>。

### 1.4 DBDH 假设

给定两个阶为  $p$  的循环加法群  $G_0$  和  $G_T$ 、一个双线性映射  $e: G_0 \times G_0 \rightarrow G_T$  和一个群  $G_0$  的生成元  $P$ , 判定双线性 Diffie-Hellman (Decisional Bilinear Diffie-Hellman, DBDH) 问题是给定  $(P, aP, bP, cP)$  和  $z \in G_T$ , 判断  $z = e(P, P)^{abc}$  是否成立。其中,  $a, b, c \in Z_p^*$  是未知的整数。

## 2 方案设计

在智能电网中,数据和访问策略可能包含隐私信息,数据所有者或收件人的信息。J. Hur<sup>[17]</sup>提出了适用于智能电网的策略隐藏的 ABE 加密方案,在数据分享的过程中,同时保护了电网节点的数据和访问策略,从而达到了保护数据和策略的目的。借鉴其策略隐藏思路,在 Ibraimi 方案的基础上,增加了两个 Hash 函数以及一个 GenToken 算法,改进了加密算法使之可以实现策略隐藏。增加了一个云中的计算代理,辅助进行外包解密计算,用户只需运行轻量解密算法即可恢复明文信息。

改进方案如下:

1) Setup( $\lambda$ ): 输入安全参数  $\lambda$ , 然后算法按如下方式运行:

(1) 生成群  $G_0$ , 其生成元为  $g$ , 素数阶为  $p$  双线性群。定义双线性映射  $e: G_0 \times G_0 \rightarrow G_T$ 。定义两个抗碰

撞 Hash 函数  $H_0: \{0, 1\}^* \rightarrow G_0$  和  $H_1: G_T \rightarrow \{0, 1\}^{\log p}$ 。

(2) 生成属性集  $\Omega = \{a_1, a_2, \dots, a_n\}$ , 随机选择  $\alpha$ ,  $\beta, t_1, t_2, \dots, t_n \in Z_p^*$ 。

(3) 计算  $h = g^\beta, y = e(g, g)^\alpha, T_j = g^{t_j} (1 \leq j \leq n)$ 。  
主公钥为  $\text{MPK} = \langle h, y, T_j \rangle$ , 私主钥为  $\text{MSK} = \langle \beta, g^\alpha, t_j \rangle$ 。

2) KeyGen: 输入用户属性集  $\omega$ , MSK。

(1) 随机选择  $r \in Z_p^*$ , 计算  $d_0 = g^{\frac{a-r}{\beta}}$ 。

(2) 对于每个满足  $\omega$  的属性  $a_j$ , 计算  $d_j = g^{r_{j-1}}, d'_j = H(a_j)^\beta$ 。

输出用户私钥  $\text{sk}_\omega = (d_0, \forall a_i \in \omega: d_i, d'_i)$ 。

3) Encrypt: 输入明文  $M$ , 访问策略树  $\gamma$ , MPK。

选择访问树的叶子节点集合  $Y$ 。发送者选择随机

值  $a \in Z_p^*$ , 对于  $y \in Y$ , 计算  $S_a = e(h^a, H(a_y))$ , 然后用  $H_1(S_a)$  替换分配给叶子节点  $y$  的属性  $a_y$ , 达到模糊属性的目的<sup>[17]</sup>。

给定访问树  $\gamma$  下的消息  $M \in G_1$ , 构造密文:

(1) 第一层加密。

选择随机数  $s \in Z_p^*$ , 计算  $C_0 = h^s, C_1 = M \cdot y^s =$

$$M \cdot e \wedge (g, g) \propto \circ$$

(2) 第二层加密。

将访问树根节点  $\gamma$  的值设置为  $s$ , 标记全部子节点为未访问, 标记根节点为已访问。对于每个未访问非叶子节点进行如下递归操作:

如果节点关系为 and, 并且其子节点标记为未访问, 则前  $t-1$  个子节点取随机值  $s_i (1 \leq s_i \leq p-1)$ , 设置最后一个子节点的值为  $s_t = s - \sum_{i=1}^{t-1} s_i$ , 并标记该节点已访问。

如果节点关系为 or, 则将其子节点值全部设置为 s, 并标记该节点已访问。

(3) 对于每个叶子节点属性  $a_{j,i} \in \gamma$ , 即  $\forall y \in Y$ , 计算  $C_y = T_j^a$  ( $i$  表示属性在访问策略树中的索引), 如图 1 所示。

输出密文信息  $CT = \langle \gamma, C_0, C_1, \forall y \in Y: C_y \rangle$ , 发送的密文消息为  $C_i = \langle g^a, CT \rangle$ 。

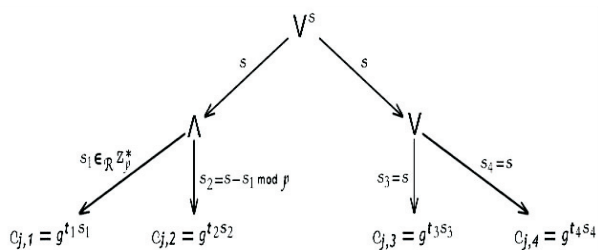


图 1 策略树

4) GenToken: 输入密文  $C$ , 和用户私钥  $sk_u$ 。

计算  $S_j = e^{\wedge}(g^a, d_j^*), H_1(S_j)$ , 如果  $\omega$  不满足  $\gamma$ , 返回  $\perp$ , 否则选择一个随机值  $\tau \in Z_p^*$ , 构造令牌:  $TK_\omega = \langle (d_0)^\tau, (d_i)^\tau, \forall j \in \omega: I_j = H_1(S_j) \rangle$ 。

5) Outsourced Decrypt: 输入密文  $C_t$  和令牌  $TK_\omega$ , 返回一个部分解密密文  $C'_t$ 。

$$\begin{aligned} & e^{\wedge}(C_0, (d_0)^\tau) \cdot \prod e^{\wedge}(C_j, (d_j)^\tau) = \\ & e^{\wedge}(h^s, g^{\frac{\alpha-r}{\beta}})^\tau \cdot \prod e^{\wedge}(T_j^{s_i}, g^{rt_j^{i-1}})^\tau = \\ & e^{\wedge}(g^s, g^{\alpha-r})^\tau \cdot \prod e^{\wedge}(g^{t_j^{s_i}}, g^{rt_j^{i-1}})^\tau = \\ & e^{\wedge}(g, g)^{s\alpha r} \end{aligned}$$

将部分解密密文  $C'_t = \langle C_\tau = e(g, g)^{\text{sat}}, C_0 \rangle$  返回给用户。

6) Light Decrypt: 输入密文  $C_i$  和部分解密密文  $C'_i$ 。

若  $C_0 \neq h^s$ , 输出 failure, 否则计算  $M' = \frac{C_1}{C_0^{-\tau}} =$

$$\frac{M \cdot e(g, g)^{\alpha s}}{e(g, g)^{s\alpha}} = M \circ$$

### 3 方案分析

### 3.1 安全性分析

1) 抗共谋攻击。

为抵抗共谋攻击,KeyGen 算法为每个用户生成一个不同的随机值  $r$ ,由于私钥的随机化,每个不同用户的私钥无法合并。而且在 GenToken 算法中,每个用户都会选取一个随机值  $\tau$  来生成令牌。在解密时,敌手必须知道如何恢复  $e^{\wedge}(g, g)^{\text{secret}}$ ,这意味着敌手必须知道隐藏在其后的随机值。

### 2) 数据机密性。

(1) 根据秘密共享方案的性质,若用户的属性集不满足密文的访问策略,就无法恢复出秘密值  $s$ , 因而无法解密。

(2)外包解密代理是半可信的,但它没有相应的私钥,因此无法解密得到明文。

(3) 计算代理拥有转换密钥—令牌, 可以对密文进行预解密, 但预解密的结果被随机数  $\tau$  随机化, 因此代理得不到任何与明文相关的信息。

### 3) 策略隱藏。

采用单向匿名密钥协商的方式,将属性信息进行模糊处理,实现访问策略的隐藏(其处理过程在第2部分有具体呈现)。

### 3.2 效率分析

在 Intel Edison<sup>[18]</sup> 开发芯片上进行了实验。Edison 开发芯片是 Intel 公司推出的物联网智能硬件产品,内

置 Yocto Linux 操作系统,可以通过 Eclipse 来编写 C++ 程序再导入 Edison 运行,用它可以模拟智能电网用户计算资源有限的环境。

测试了密钥生成、加密、解密等主要算法随属性个数增加在运行时间上的变化,并将该方案与 Lai<sup>[4]</sup>的外

包解密方案进行密文规模以及外包解密和轻量解密运算时间上的对比。将算法在 Edison 开发芯片和一台 Windows 操作系统的笔记本电脑上进行测试,分别与 Lai<sup>[4]</sup>方案中的 ARM 与 Intel 环境下的解密计算运算时间进行对比。其结果如图 2~4 所示。

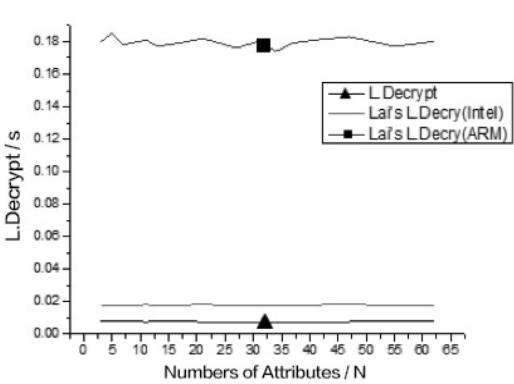


图 2 轻量解密运算时间比较

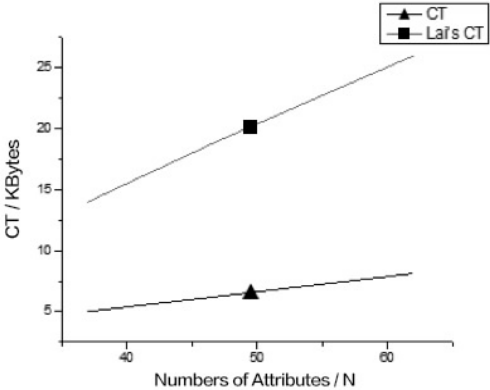


图 3 密文规模比较

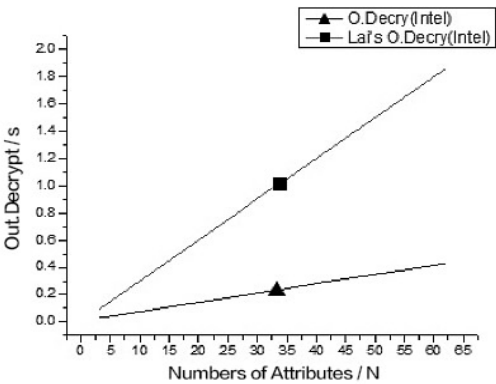
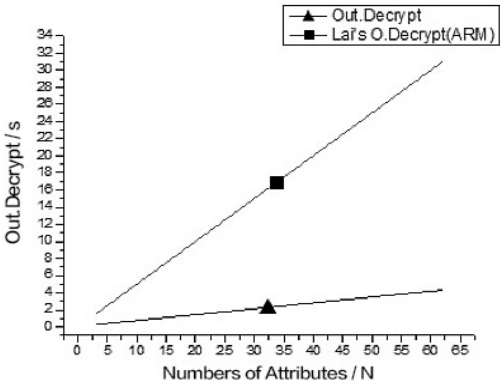


图 4 Edison 环境与笔记本电脑环境下的外包解密时间比较

通过对比可知,该方案较 Lai<sup>[4]</sup>方案在密文规模上更小,在算法运算效率上有显著提高。同时,将该方案与原方案<sup>[15]</sup>、Green<sup>[3]</sup>的 CP-ABE 方案以及 Lai<sup>[4]</sup>方案做了参数长度、算法计算量以及安全性三方面的比较

和分析,结果如表 1 和表 2 所示。其中,  $|G_0|$  表示群  $G_0$  上幂运算的复杂度,  $|G_T|$  表示群  $G_T$  上幂运算的复杂度,  $P$  表示配对运算的复杂度,  $|\omega|$  表示属性集大小,  $|\tau|$  表示访问策略属性的个数。

表 1 参数长度及方案安全性比较

方案	令牌长度	密文长度	Security	策略隐藏
Ibraimi <sup>[15]</sup>	/	$(1 +  \tau )G_0 + G_T$	CPA	×
Green's CP-ABE <sup>[3]</sup>	$(2 +  \omega )G_0$	$(1 + 2 \tau )G_0 + G_T$	CPA	×
Lai <sup>[4]</sup>	$(2 +  \omega )G_0$	$(4 + 6 \tau )G_0 + 2G_T$	CPA	×
文中方案	$(2 +  \tau )G_0$	$(1 +  \tau )G_0 + G_T$	CPA	✓

表 2 算法计算量比较

方案	KeyGen	Out Decrypt	Light Decrypt
Ibraimi <sup>[15]</sup>	$(1 +  \omega ) G_0 $	/	$(1 +  \omega )P$
Green's CP-ABE <sup>[3]</sup>	$(3 +  \omega ) G_0 $	$(2 +  \tau )P + 2I G_0 $	$ G_T $
Lai <sup>[4]</sup>	$(3 +  \omega ) G_0 $	$(2 + 4 \tau )P + 2 \tau  G_T $	$2 G_T $
文中方案	$(1 + 2 \omega ) G_0 $	$(1 +  \omega )P$	$ G_T $



通过比较可知,该方案在参数长度、计算量、效率以及安全性上都具有一定的优势,特别是在密文长度上。而且与原方案相比,将复杂的解密计算外包给计算代理,用户只需进行轻量级解密,效率更高。与此同时,与上述其他方案相比,该方案在保证同等安全级别的基础上实现了策略隐藏,但也存在一些不足之处,如用户私钥还比较长,而且没有考虑到属性的增加与撤销问题,这将是以后致力解决的问题。

4 结束语

为解决属性基加密在智能电网应用中存在的计算效率低的问题以及实现策略隐藏,在 Ibraimi 方案的基础上进行改进,通过解密计算外包解决计算效率问题,通过模糊属性的方法实现策略隐藏,大大减轻了智能电网用户的解密复杂度,同时保证了数据机密性以及抗共谋攻击。与已有方案相比,新方案明显减少了密文长度和外包解密过程的复杂度,且没有降低方案的安全性。

参考文献:

[1] 曹军威,万宇鑫,涂国煜,等. 智能电网信息系统体系结构研究[J]. 计算机学报,2013,36(1):143-167.

[2] 谢远鹏,文 红. 应用于智能电网中的基于层次属性加密访问控制方法[J]. 智能电网,2015,5(3):93-99.

[3] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts[C]//USENIX conference on security. [s. l.]:USENIX,2011:34.

[4] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(8):1343-1354.

[5] Qin B, Deng R H, Liu S, et al. Attribute-based encryption with efficient verifiable outsourced decryption [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7):1384-1393.

[6] Liu H, Wang X, Zhang P. Verifying outsourced decryption of

CP-ABE with signature[C]//4th international conference on mechatronics, materials, chemistry and computer engineering. [s. l.]:[s. n.],2015.

[7] 马 华,白翠翠,李 宾,等. 支持属性撤销和解密外包的属性基加密方案[J]. 西安电子科技大学学报:自然科学版,2015,42(6):6-10.

[8] 丁晓红,秦敬源,王 新. 一种属性基加密方案的外包解密方法[J]. 计算机科学,2016,43(S1):357-360.

[9] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//IEEE symposium on security and privacy. [s. l.]:IEEE,2007:321-334.

[10] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [C]//International conference on applied cryptography and network security. New York, NY, USA:IEEE,2008:111-129.

[11] Lai J, Deng R H, Li Y. Fully secure ciphertext-policy hiding CP-ABE[C]//International conference on information security practice and experience. [s. l.]:[s. n.],2011:24-39.

[12] 陈 勤,马丹丹,张金漫,等. 隐藏访问策略的属性基加密机制[J]. 计算机应用,2011,31(11):2969-2972.

[13] Li X, Gu D, Ren Y, et al. Efficient ciphertext-policy attribute based encryption with hidden policy [C]//International conference on internet and distributed computing systems. [s. l.]:[s. n.],2012:146-159.

[14] 苏金树,曹 丹,王小峰,等. 属性基加密机制[J]. 软件学报,2011,22(6):1299-1315.

[15] Luan I, Tang Q, Hartel P, et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes [C]//International conference on information security practice and experience. Xi'an, China:[s. n.],2009:1-12.

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

[17] Hur J. Attribute-based secure data sharing with hidden policies in smart grid[J]. IEEE Transactions on Parallel and Distributed Systems,2013,24(11):2171-2180.

[18] 陈士凯,程 晨,臧海波. Intel Edison 智能硬件开发指南:基于 Yocto Project[M]. 北京:人民邮电出版社,2015.