

改进的隐藏访问结构的 CP-ABE 方案

翁岸祥 凌捷

(广东工业大学计算机学院 广州 510000)

摘要 隐藏访问结构的密文策略属性基加密(CP-ABE)算法能将访问结构隐式地嵌入密文中,用户即使多次尝试不同的属性组合,也无法得出访问结构,而避免了加密方的相关信息的泄露,但是同时也导致了计算复杂、访问效率低等问题。文中提出了一种改进方案,将双线性对的运算量减少了近一半,有效地提高了效率,并且证明了在 DBDH(判定双线性问题)假设下,该方案在标准模型下是选择明文安全的。

关键词 密文策略属性基加密,隐藏访问结构,访问控制,DBDH 假设

中图分类号 TP309 **文献标识码** A

Improved Scheme of CP-ABE with Hidden Access Structure

WENG An-xiang LING Jie

(School of Computers,Guangdong University of Technology,Guangzhou 510000,China)

Abstract In the scheme of CP-ABE with hiding access structure,the access structure is implicitly embedded in the ciphertext. The users can not get access structure although trying different attribute combinations,so that the information of encryptor will not be revealed. But this will lead to complicated calculations and low access efficiency. This article proposed an improved scheme,which improves the efficiency by reducing operation of bilinear pairings by nearly half. Besides, based on DBDH assumption, we proved the scheme selectively secure against chosen-plaintext attack under standard model.

Keywords Ciphertext-policy attribute-based encryption,Hidden access structure,Access control,DBDH assumption

1 引言

随着网络技术和分布式计算的发展,越来越多的人与企业为了降低成本而将大部分的数据保存到了云端。然而,储存在云端的数据遭遇严重的安全隐患,如果没有一个好的安全机制,这些数据将会完全暴露,并将造成重大损失。密文策略属性基加密(CP-ABE)作为一种细粒度的数据加密方式,被广泛地应用于云计算中,它解决了复杂信息系统中的细粒度访问控制和大规模用户动态扩展的问题,为开放的网络环境提供了比较理想的访问控制方案。

属性基加密(Attribute-Based Encryption, ABE),是由 Sahai 等人^[1]于 2005 年提出的一种新的公钥加密机制,实现了公钥密码体制一对多的加密。为了表示更灵活的访问控制策略,相关学者在之后又提出了密钥策略属性基加密(Key-Policy Attribute-Based Encryption, KP-ABE)^[2]和密文策略属性基加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)^[3]两类 ABE 加密机制。在密钥策略属性基加密机制中,密钥与访问结构相关,密文与属性集相关;而在密文策略属性基加密机制中,密钥与属性集相关,密文与访问结构相关^[4]。在密文策略属性基加密机制中,加密者使用访问结构和公钥加密消息,解密者根据自身的属性集预先从一个可信

的授权方获取解密密钥,如果解密者的属性不满足嵌入在密文中的访问结构,解密者则不能解密该密文。

然而,在传统的 CP-ABE 方案中,访问策略和加密的明文往往会被一起发送给解密者,而访问结构有可能包含着与明文相关的信息,一旦密文被截获,加密者的隐私将有被泄露的风险。为了解决该问题,出现了许多隐藏访问结构的密文策略属性基加密方案。文献[5]提出了隐藏访问结构的 CP-ABE 方案,该方案能对访问结构进行丰富的表达,但存在安全性不足的问题;文献[6]提出了选择安全的两个方案,将访问结构隐藏在加密的信息中,但这两个方案均只能实现部分访问结构的隐藏;文献[7]提出了一种隐藏访问结构的 CP-ABE 方案以支持文献[6]中的访问结构,并且证明了该方案是完全安全的;文献[8]利用合数阶群构造了一种基于访问树的策略隐藏方案,使用户可以指定灵活的访问控制策略而不必担心策略泄露的问题,但增加了访问结构的复杂性以及计算和存储开销;文献[9]利用非对称双线性的素数阶群实现了隐藏访问结构的 CP-ABE 方案,但增加了双线性对的计算开销;文献[10]提出了支持策略隐藏的加密云存储访问机制;文献[11]提出了基于访问树的隐藏访问机构的密文策略属性基加密方案,并将该方案运用到云计算中;文献[12]基于策略隐藏属性基加密提出了适用于云环境的访问控制方案;文献

本文受广东省科技计划项目(2014B090908010, 2015B090906016, 2016B090918039, 2016B010107002),广州市重大科技专项(201604010048)资助。

翁岸祥(1991—),男,硕士生,主要研究方向为信息安全,E-mail:wenganxiang@163.com;凌捷(1964—),男,博士,教授,CCF 会员,主要研究方向为网络与信息安全。

[13]将多值与门表达的访问结构转化为树,但是密钥和密文过长,这样会增加双线性对运算的数量。

本文提出了一种隐藏访问结构的 CP-ABE 改进方案,其利用访问树将访问结构嵌入密文中,利用多值与门来表达访问结构,访问结构中的每个属性可以取多个值,增加了系统的灵活性,并且通过降低双线性对的运算数量提高了加密和解密的效率。

2 预备知识

2.1 访问结构

设二维矩阵 $U = \{U_1, U_2, \dots, U_n\}$ 表示一个给定的属性集合,其中 $U_i = \{u_{i,1}, u_{i,2}, \dots, u_{i,m}\} (m \geq 1)$ 。用户的属性集合表示为 $S = \{S_1, S_2, \dots, S_n\}$,其中 $S_i = \{att_{i,1}, att_{i,2}, \dots, att_{i,m}\}$ 。访问结构为 $A = \{A_1, A_2, \dots, A_n\}$,其中 $A_i \subseteq U_i$ 。对 $\forall i \in [1, n]$,都有 $S_i \subseteq A_i$,称用户的属性集满足访问结构。

本文利用多值与门来表示访问结构,将访问结构转化为一棵访问树,中间节点用“ $\wedge$ ”和“ $\vee$ ”表示,叶子节点表示属性,每一个中间节点下的所有叶子节点构成一个属性,其中“ $\wedge$ ”下的每一个叶子节点构成一个属性,“ $\vee$ ”下的所有叶子节点构成一个属性;而用户的身份则用特定的属性集合表示。图 1 所示的一棵访问树^[13]表示访问结构 $A = [\text{属性 } 1, \text{属性 } 2, \text{属性 } 3, \text{属性 } 4] = [\{v_{1,2}\}, \{v_{2,1}, v_{2,4}\}, \{v_{3,1}\}, \{v_{4,2}, v_{4,3}, v_{4,4}\}]$,属性集 $S = \{v_{1,2}, v_{2,1}, v_{3,1}, v_{4,2}\}$ 或属性集 $S = \{v_{1,2}, v_{2,4}, v_{3,1}, v_{4,3}\}$ 都满足访问结构 A 。

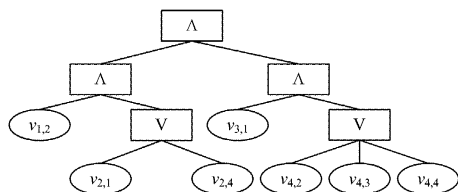


图 1 访问树

2.2 双线性对

映射 $e: G_1 \times G_1 \rightarrow G_2$ 若满足下列特征,则是双线性对: 1) 双线性: 对 $\forall a, b \in Z_q, \forall f, h \in G_1$, 都有 $e(f^a, h^b) = e(f, h)^{ab}$, 则称映射 $e: G_1 \times G_1 \rightarrow G_2$ 是双线性的; 2) 非退化性: $\exists f \in G_1$, 使 $e(f, f) \neq 1$; 3) 可计算性: $\forall f, h \in G_1$, 存在一个有效的算法来计算 $e(f, h)$ 。注意: $e(*, *)$ 是对称操作, 即 $e(f^a, h^b) = e(f, h)^{ab} = e(h^b, f^a)$ 。

2.3 DBDH 假设

随机选择 $a, b, c, z \in Z_p^*$, p 是群 G 的阶, g 是 G 的生成元。DBDH 假设即为不存在一个多项式时间的概率算法能够以不可忽略的优势区分元组 $[g^a, g^b, g^c, e(g, g)^{abc}]$ 和元组 $[g^a, g^b, g^c, e(g, g)^z]$ 。

2.4 方案步骤

隐藏访问结构的密文属性基加密方案的参与方有 3 个: 加密者、解密者和一个可信的授权中心 AC (Authorization Center)。加密者指定解密密文所需要满足的访问结构和负责加密明文, AC 负责生成系统公钥 PK 、系统主密钥 MK 和用户的私钥 SK 。一个完整的密文策略属性基加密方案包括 4 个算法: 初始化算法、密钥生成算法、加密算法和解密算法, 详细描述如下。

1) 初始化算法: 输入公共参数, 算法产生系统公钥 PK 和主密钥 MK 。

2) 密钥产生算法: 输入主密钥 MK 和用户属性集 S , 输出用户私钥 SK 。

3) 加密算法: 输入访问结构 A 、明文 M 和系统公钥 PK , 输出密文 CT 。

4) 解密算法: 输入密文 CT 、用户私钥 SK 、系统公钥 PK , 输出明文。

2.5 安全模型

本文方案可以达到选择明文攻击的密文不可区分性 (Indistinguishability of Ciphertext under Chosen-Message, IND-CMA), 其所基于的安全模型^[6]通过以下敌手 A 和挑战者 B 之间的交互游戏进行描述。

Step1 敌手 A 想挑战者 B 提交要挑战的访问结构 W_0 和 W_1 。挑战者 B 选择安全系数 k 后运行初始算法得到系统公钥 PK 和系统主密钥 MK 。挑战者 B 保留 MK 并把 PK 发送给 A 。

Step2 A 对 B 进行属性列表 S 的询问, 但是 S 必须同时不满足敌手提供的 W_0 和 W_1 , B 才能运行私钥产生算法, 并将私钥 SK 发送给 A 。敌手 A 可以进行多项式次数的询问。

Step3 A 提交两个消息 M_0 和 M_1 , B 抛硬币随机选择 b ($b \in \{0, 1\}$), 用 W_b 加密 M_b 。挑战者 B 运行加密算法并将密文返回给敌手 A 。

Step4 重复 Step2 和 Step3, 但是敌手 A 发起的询问必须限制在 S 不满足 W_0 和 W_1 内。

Step5 敌手 A 输出对 b 的猜测 b' ($b' \in \{0, 1\}$), 若 $b' = b$, 则敌手 A 赢得游戏, 否则 A 失败。

设敌手 A 获得攻击游戏胜利的优势为 $Adv_A = |\Pr[b' = b] - \frac{1}{2}|$ 。

在多项式时间内, 若不存在以不可忽略的优势赢得上述游戏的多项式时间敌手, 则称该隐藏访问机构的密文策略属性基加密方案是 IND-CMA 安全的^[10]。

3 方案描述

3.1 背景介绍

假设这样一个情景: 某个文件只能允许经理或经理以上级别的员工查看, 则文件加密者可以用访问结构 $A = [\text{经理} \vee \text{经理以上级别员工}]$ 和公钥来加密这个文件。Peter 是该公司的一名销售人员, 他的属性集表示为 $S = (\text{销售人员})$; Ann 是该公司的一名经理, 她的属性集表示为 $S = (\text{经理})$ 。Peter 和 Ann 经授权方认证后分别获得与其属性相对应的私钥。显而易见, Peter 的私钥不满足嵌入在该加密文件中的访问结构, Ann 的私钥满足嵌入在该加密文件中的访问结构, 因此 Peter 无法解密该文件, Ann 可以解密该加密文件。

3.2 方案步骤

令 $U = \{U_1, U_2, \dots, U_n\}$ 表示一个可能的属性取值集合。用户的属性集为 $S = \{S_1, S_2, \dots, S_n\}$, 其中 $\{S_i = \{att_{i,1}, att_{i,2}, \dots, att_{i,m}\} (m \geq 1)$ 。访问结构为 $A = \{A_1, A_2, \dots, A_n\}$, 且 $A_i \subseteq U_i$ 。

(1) 初始化算法 $\text{Setup}(k)$

该算法首先输入一个安全系数 k , 然后:

1) 产生一个双线性群 G 和映射 $G \times G \rightarrow G_T$, 其中 G 是一个 N 阶乘法循环群, $N = pqr$, p, q 和 r 为 3 个互不相同的素数。

2) 系统随机选取 $\alpha \in Z_N^*$, $t_{i,j} \in Z_N^* (1 \leq j \leq m)$ 。计算:

$X = g(g \text{ 是 } G_T \text{ 的生成元})$

$$Y=e(g,g)^a$$

$$T_{i,j}=g^{-t_{i,j}}$$

得出系统公钥 $PK=\{e,X,Y,T_{i,j}\}$, 主密钥 $MK=\{\alpha,t_{i,j}\}$ 。

(2) 密钥产生算法

1) 输入系统主密钥 MK 和用户的属性集 S ;

2) 随机选择 $r \in Z_N^*$, 计算:

$$D_0=g^{a-r}$$

$$D_{i,j}=g^{rt_{i,j}}$$

(3) 加密算法

1) 输入访问结构 A 、系统公钥 PK 和明文 M 。

2) 加密者将使用多值与门表达的访问结构 A 按规则转

化为对应的访问树 τ 。计算 $s=\sum_{i=1}^n s_i$ 。令 s 为访问树 τ 的根节点, 根节点被标记为已读状态, 其他节点被标记为未读状态。

如果当前节点的值为 $\wedge$ 且它的所有孩子节点都是未读状态, 那么就为所有的孩子节点 i 选择一个值 $s_i \in Z_N^*$, 并把这些节点都标记为已读状态。

如果当前节点的值为 $\vee$ 且它的所有孩子节点都是未读状态, 那么随机选择一个值 $s' \in Z_N^*$, 将 s' 赋给所有孩子节点的 s_i 。计算:

$$s=\sum_{i=1}^n s_i$$

$$C_0=X^s$$

$$C_1=M \cdot Y^s=M \cdot e(g,g)^{as}$$

$$C_{i,j}=T_{i,j}^{s_i}$$

3) 输出密文: $CT=\{C_0, C_1, C_{i,j}\}$ 。

(4) 解密算法

1) 输入系统公钥 PK 、用户私钥 SK 、隐藏了访问结构 A 的密文 CT 。

$$2) \text{ 计算 } M=\frac{C_1}{e(C_0, D_0) \prod_{i,j} e(C_{i,j}, D_{i,j})}。$$

3.3 安全性证明

下面证明本文方案在 DBDH 假设下满足密文的不可区分性。

若敌手 A 能以不可忽略的优势 ϵ 来攻破本文方案, 那么存在一个算法 Ψ 能以相同的优势 ϵ 来打破 DBDH 假设。具体过程描述如下:

挑战者给定 DBDH 的挑战元组 $[g, g^a, g^b, g^c, Z]$, 其中 Z 在 G_T 中的取值的概率与 $e(g, g)^{abc}$ 相同。

Step1 敌手 A 提供给挑战者 B 两个访问结构, 即 $W_0=[W_{0,1}, \dots, W_{0,n}]$ 和 $W_1=[W_{1,1}, \dots, W_{1,n}]$, B 抛硬币得到随机值 $b(b \in \{0,1\})$ 。对于 $\forall 1 \leq i \leq n, \forall 1 \leq j \leq m$, 随机选取 $t_{i,j} \in Z_N^*$, 当 $att_{i,j} \in W_{b,i}$ 时, 算法 Ψ 令 $T_{i,j}=g^{-t_{i,j}}$; 当 $att_{i,j} \notin W_{b,i}$ 时, 令 $T_{i,j}=g^{-bt_{i,j}}$ 。挑战者 B 把系统公钥 $PK=\{e,X,Y,T_{i,j}\}$ 发送给敌手 A , B 自己保留主密钥 MK 。

Step2 敌手 A 提供一个属性列表 $S=\{S_1, S_2, \dots, S_n\}$ 作为私钥询问的输入, 因为存在限制条件: 属性列表 S 不满足访问结构 W_0 和访问结构 W_1 , 所以必定存在一个 $j \in [1, \dots, n]$, $S_j \not\subseteq W_{b,j}$ 。

B 随机选择 $r \in Z_N^*$, 计算:

$$D_0=g^{a-r}$$

$$D_{i,j}=g^{rt_{i,j}}$$

B 将私钥 $SK=\{D_0, D_{i,j}\}$ 发送给 A 。

Step3 敌手 A 提交 2 个挑战消息 M_0 和 M_1 给挑战者

B 。对于 $\forall 1 \leq i \leq n, B$ 随机选择 $s_i, s=\sum_{i=1}^n s_i, C_0=X^s=g^s, C_1=M_0 \cdot e(g, g)^Z, C_{i,j}=T_{i,j}^{s_i}=g^{-t_{i,j}s_i}$ 。

Step4 重复 Step2 和 Step3, 继续私钥询问。

Step5 如果 $Z=e(g, g)^{abc}$, A 就能准确地猜中 b 的值, 即 $b'=b$; 否则 A 只能做一个随机的猜测。因此, B 能够以优势 ϵ 解决 DBDH 问题。

4 效率分析

为了说明本方案的优势, 从参数长度和加解密时间两个方面将本方案和文献[6, 12]作对比。

令 $|G|, |G_T|$ 和 $|Z_N^*|$ 分别代表 G, G_T 和 Z_N^* 中元素的位数; G 和 G_T 分别为群 G 和 G_T 上计算所用的时间, C_e 表示双线性对所需要的时间。

令 n 为系统属性的总数; n_i 表示属性 i 的取值个数, $L=\sum_{i=1}^n n_i$ 表示所有可能属性取值的总数。

实验结果如表 1、表 2 所列。

表 1 参数长度比较/bit

方案	PK	MK	SK	CT
文献[6]	$(2L+1) G + G_T $	$(2L+1) Z_N^* $	$3(n+1) G $	$2(L+1) G + G_T $
文献[13]	$(L+1) G + G_T $	$L Z_N^* + G_T $	$(2n+1) G $	$(2n+1) G + G_T $
本文方案	$(L+1) G + G_T $	$L Z_N^* + G_T $	$(n+1) G $	$(n+1) G + G_T $

表 2 时间开销

方案	加密时间	解密时间
文献[6]	$(2L+1)G+2G_T$	$(3n+1)c_e+(3n+1)G_T$
文献[13]	$(2n+1)G+G_T$	$(2n+1)c_e+3G_T$
本文方案	$(n+1)G+G_T$	$(n+1)c_e+3G_T$

如表 1 所列, 本文方案虽然与文献[13]的系统公钥长度和主密钥长度一样, 但是比文献[6]的短, 并且其用户私钥和密文的长度均比文献[6, 13]短, 在数据访问人数比数据加密者多的情况下, 私钥长度关系着授权中心的效率, 而密文长度则关系着通信代价。

从表 2 可知, 本方案的加密时间和解密时间均比文献[6, 13]的更短, 因为双线性运算代价减少了近一半, 所以方案的效率得以提高。

结束语 本文提出了一个隐藏访问结构的密文策略属性基加密改进方案, 在保证密文保密性的同时, 通过降低双线性对运算的数目提高了加解密的效率。最后, 证明了在 DBDH 假设下该方案能够抵抗选择明文攻击, 实现了密文的不可区分性。

参考文献

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005: 457-473.
- [2] GOYAL V, PANDEY O, SAHAI A, WATERS B. 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 Press, 2006: 89-98.
- [3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy

- attribute-based encryption[C]//Proc. of the 2007 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2007:321-334.
- [4] 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.
- [5] KAPADIA A, TSANG P P, SMITH S W. Attribute-based publishing with hidden credentials and hidden policies[C]//Proceedings USA of 14th Annual Network & Distributed System Security Symposium (NDSS 2007). San Diego, California, USA: NDSS, 2007:179-192.
- [6] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]//6th International Conference on Applied Cryptography and Network Security. Berlin: Springer Berlin Heidelberg, 2008:111-129.
- [7] LAI J, DENG R H, LI Y. Fully secure ciphertext-policy hiding

CP-ABE[M]//Information Security Practice and Experience. Berlin Heidelberg: Springer, 2011:24-39.

- [8] 宋衍,韩臻,刘凤梅,等. 基于访问树的策略隐藏属性加密方案[J]. 通信学报,2015,36(9):119-126.
- [9] 解理,任艳丽. 隐藏访问结构的高效基于属性加密方案[J]. 西安电子科技大学学报(自然科学版),2015,42(3):97-102.
- [10] 雷蕾,蔡权伟,荆继武,等. 支持策略隐藏的加密云存储访问控制机制[J]. 软件学报,2016,27(6):1432-1450.
- [11] XU R, WANG Y, LANG B A Tree-Based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computing[C]//2013 International Conference on Advanced Cloud and Big Data(CBD). Piscataway: IEEE, 2013:51-57.
- [12] 杜瑞颖,沈剑,陈晶,等. 基于策略隐藏属性加密的云访问控制方案[J]. 武汉大学学报(理学版),2016,62(3):242-248.
- [13] 汪海萍,赵晶晶. 隐藏访问结构的密文策略的属性基加密方案[J]. 计算机科学,2016,43(2):175-178,198.

(上接第 356 页)

在内核层、本地层和应用层分别设计了破坏 PSL 安全策略的恶意软件,内核层恶意软件的表现形式为 Rootkit,本地层恶意软件的表现形式为本地可执行程序,应用层恶意软件为 apk 应用程序。由于智能移动终端的安全性研究是新兴的研究领域,目前尚无对恶意软件检测效能进行评价的权威数据集,因此自行设计了测试数据集,数据集的分布如表 1 所列。

表 1 3 个层次上被测软件的数据集分布

	总被测软件数	恶意软件数	正常软件数
内核层	100	20	80
本地层	100	20	80
应用层	100	20	80

为了评价 MacDroid 模型对 3 个层次上恶意软件的检测和防范效果,使用漏报率(False Negative Rate, FNR)、误报率(False Positive Rate, FPR)和检测率(Detection Rate, DR) 3 个参数来定量评价。3 个参数的计算方法如下:

$$FNR = \frac{\text{漏检恶意软件数量}}{\text{被测软件总数量}}$$

$$FPR = \frac{\text{误报恶意软件数量}}{\text{被测软件总数量}}$$

$$DR = \frac{\text{检测出的恶意软件数量}}{\text{恶意软件总数量}}$$

不同层的恶意软件检测测试属于模型的功能完备性测试,与具体硬件设备的配置和性能无关,因此只在 Google Nexus5 手机上进行测试。测试结果统计如表 2 所列。

表 2 3 个层次上层恶意软件漏报率、误报率和检测率统计表

	漏报数	漏报率/%	误报数	误报率/%	检测数	检测率/%
内核层	4	4	5	5	16	80
本地层	5	5	7	7	15	75
应用层	7	7	10	10	13	65

分析上面的测试结果可知,MacDroid 模型对 3 个不同层次的恶意软件检测的漏报率和误报率都较低,检测率较高。对 3 个层次之间进行比较可以发现,模型对内核层恶意软件的检测效果更好,原因在于:对于越底层的软件,在内核中获得的其主客体 and 动作行为的特征越准确,与 PSL 安全策略的匹配也越精确,因此其更容易被 PSL 安全策略控制。

结束语 本文主要从智能移动终端内核层安全防护角度深入分析和讨论了终端内核层安全防护的必要性,提出了一种可验证的轻量级内核层访问控制模型,并对模型进行了形式化描述,最后通过实验验证了模型在 3 种典型智能移动终端上的可用性和不足。

参考文献

- [1] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure Attribute-Based Systems[J]. Journal of Computer Security, 2010, 18(5):799-837.
- [2] ION I, DRAGOVIC B, CRISPO B. Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices[C]//Proc. of the Annual Computer Security Applications Conference, 2007:233-242.
- [3] ZHANG X W, ACHIÇMEZ O, SEIFER J. A Trusted Mobile Phone Reference Architecture via Secure Kernel[C]//Proc. of the ACM workshop on Scalable Trusted Computing, 2007:7-14.
- [4] ENCK, WILLIAM ONGTANG, et al. On Lightweight Phone Application Certification[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009:235-245.
- [5] KIRKPATRICK M S, BERTINO E. Enforcing Spatial Constraints for Mobile RBAC Systems[C]//Proc. of the 15th ACM Symposium on Access Control Models and Technologies, 2010:99-108.
- [6] NAUMAN M, KHAN S, ZHANG X W, et al. Beyond Kernel-Level Integrity Measurement Enabling Remote Attestation for the Android Platform[C]//International Conference on Trust and Trustworthy Computing, 2010:1-15.
- [7] NSA[OL]. <http://selinuxproject.org/page/SEAndroid>.
- [8] 黄琳雅. 基于内核的 Android 文件访问控制研究[D]. 北京:北京邮电大学, 2012.
- [9] 易筱茂. 面向 Android 操作系统的强制访问控制研究[D]. 北京:中国科学院大学, 2015.
- [10] 卿斯汉. Android 安全的研究现状与展望[J]. 电信科学, 2016(10):1-8.