



云环境下基于属性加密体制算法加速方案

吴国威, 樊宁, 汪来富, 王帅, 沈军, 金华敏

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 云计算为租户提供存储、计算和网络服务, 数据安全保护和租户间的数据共享与访问控制是其必不可少的能力。基于属性的加密体制是一种一对多的加密体制, 可以根据用户属性实现细粒度访问控制, 适用于云计算环境多租户数据共享。但现有的基于属性加密体制的算法效率较低, 难以在实际环境中应用。分析了基于属性的加密体制的两种类型及其应用场景, 提出一个基于属性加密体制算法的加速方案。通过实验表明, 提出的方案可提高基于属性加密体制的密钥生成算法、加密算法和解密算法的效率。

关键词: 云计算; 安全; 访问控制; 基于属性加密

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019145

Accelerated algorithm in attribute-based encryption over cloud environment

WU Guowei, FAN Ning, WANG Laifu, WANG Shuai, SHEN Jun, JIN Huamin

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: Cloud computing provides storage, computing and network services to tenants. Data security and data sharing and access control between tenants are indispensable functions. Attribute-based encryption (ABE) system is a one to many encryption system, which allows users to fine-grained access control on encrypted data according to users' attributes. This encryption system is very suitable for multi-tenant data sharing overcloud computing environment. However, the existing attribute-based encryption schemes is inefficient, which cannot be applied to practical applications. Two types of ABE and their application scenarios were analyzed, and an acceleration algorithms scheme in attribute encryption cryptosystem was proposed. The experiment can illustrate that the proposed scheme can improve the efficiency of key generation algorithm, encryption algorithm and decryption algorithm.

Key words: cloud computing, security, access control, attribute-based encryption

1 引言

随着云计算技术的迅猛发展, 越来越多的政企与公众客户选择将私有数据存储到云。而用户

数据隐私和安全问题成为很多客户使用第三方云服务的主要顾虑之一。为保证数据机密性, 租户可以采用传统对称加密算法将数据加密后再上传至云, 但租户将难以对数据共享进行细粒度的访



问控制。如果租户通过公钥加密算法将数据加密上传,在数据共享时,租户只能采用一对一的方式,将云中加密数据下载至本地,先用私钥解密,再用接收者公钥加密,然后分发。当共享对象过多时,租户需要将上述步骤执行多次,这将耗费大量的计算、带宽资源和时间成本。因此,如何同时实现用户数据的机密性和高效安全的数据共享成为云存储服务亟待解决的问题。

为此, Sahai 等人^[1]提出了基于属性加密(attribute-based encryption, ABE)的概念。这是一种一对多的公钥加密方式,将用户身份以一组属性描述,并通过密钥策略或密文策略来细粒度地控制用户的解密能力,非常适用于云计算环境多租户数据共享。目前业界将基于属性的加密体制分为两类:密钥策略基于属性加密体制和密文策略基于属性加密体制。在密钥策略基于属性加密体制中,每组密文对应一组属性,密钥对应一个访问策略;在密文策略基于属性加密体制中,每组密钥对应一组属性,密文对应一个访问策略。对于这两类基于属性的加密体制,只有当属性集合满足访问策略时,用户的私钥才能成功解密密文。

需要注意的是,在密钥策略基于属性加密体制中,属性是用来客观地描述加密数据本身的,而访问策略是针对数据本身属性的与或非门策略,数据访问控制的权限由属性权威中心分配,数据拥有者更多地,侧重于对数据的管理,并不能决定哪一类用户可以访问加密的数据。密文策略基于属性加密更贴近实际应用场景,属性被用来描述用户的身份信息,数据拥有者对数据具有完全的访问控制能力,可以制定相应的访问策略以决定哪一类用户可以访问加密数据。

相较于密钥策略基于属性加密体制,密文策略基于属性加密体制的应用领域更大,例如安全邮件列表、安全数据库、IP 地址多播和个人医疗数据专家诊断等。以个人医疗数据专家诊断为例,

由于个人医疗数据涉及很多隐私敏感信息,因此病人利用密文策略基于属性加密体制加密医疗数据来保护自己的隐私,并制定访问控制策略使得只有满足相关资质并且是这类疾病的医疗专家才可以查看自己的医疗数据。

2 基于属性加密体制算法效率改进思路

2.1 现有算法效率分析

基于属性加密体制涉及 3 个主要算法:密钥生成算法、加密算法和解密算法。密钥生成算法和加密算法主要是涉及模指数和点乘运算,解密算法主要涉及双线性配对运算。针对两类不同基于属性加密体制,本文分析了其效率及计算开销。在密钥策略基于属性加密体制中,密钥生成算法计算开销随着访问策略的复杂度增加呈线性增加,加密算法计算开销随着属性个数的增加呈线性增加。在密文策略基于属性加密体制中,密钥生成算法计算开销随着属性个数增加呈线性增加,加密算法计算开销随着访问策略复杂度的增加呈线性增加。

2.2 改进技术与思路

针对基于属性加密体制的算法效率问题,目前采取的改进技术主要包括如下。

(1) 通过双线性配对聚合提高解密算法中的双线性配对运算效率,达到快速解密^[2]的目的。但不足之处在于,密钥大小随属性个数增加呈非线性增加。

(2) 将 online/offline 技术^[3]应用于基于属性加密体制的加密算法和密钥生成算法,分成两个阶段:第一个阶段即 offline,由空闲设备或第三方服务器完成算法大量的计算工作;第二个阶段即 online,当执行加密算法和密钥生成算法时,通过拼接 offline 阶段所生成的参数,只需要少量计算即可完成加密或者密钥生成。但由于在 offline 阶段,算法随机数是由不可信的第三方服务器选择的,第三方服务器可以轻易地解密密文,存在安

全隐患。

(3) 通过密钥盲化技术^[4]将解密运算外包给第三方服务器, 由第三方服务器完成部分配对运算, 数据使用者只需完成一个模指运算就可以解密, 恢复明文。但这种技术减少了基于属性加密体制的解密运算量, 并没有减少密钥生成和加密算法的运算量。

为了提高基于属性加密体制的算法效率, 本文提出了一个密文策略基于属性加密的算法加速方案, 对密钥生成算法、加密算法和解密算法进行同步加速, 将算法大部分的模指数、点乘运算和双线性配对运算由外包云服务提供商来完成, 属性权威中心、数据拥有者和数据使用者只需要做少量常数级别的运算就可以完成密钥生成、加密和解密。

3 基于属性加密体制的算法加速方案

在密文策略基于属性加密的算法加速方案中, 本文引入了3个不同云服务提供商的半可信云服务器, “半可信”是指这些云服务提供商如实

完成用户的操作指令, 但存在窥探用户机密信息的可能。3个半可信云服务提供商帮助属性权威中心、数据拥有者和数据使用者分别完成密钥生成、加密和解密中的大部分繁重的计算工作。针对属性权威中心、数据拥有者和数据使用者的职能, 如图1所示, 密文策略基于属性加密体制算法加速方案的工作流程如下。

(1) 当数据使用者需要申请密钥时, 将用户的属性集合发给密钥生成外包云服务提供商(key generation cloud service provider, KG-CSP), 由KG-CSP来生成与用户属性相关的部分密钥, 并发给属性权威中心。属性权威中心用自己的主密钥生成用户完整的密钥并发送给数据使用者。

(2) 当数据拥有者需要加密数据的时候, 数据拥有者将访问策略发给加密外包云服务提供商(encryption cloud service provider, E-CSP), 由E-CSP来完成生成与访问策略相关的部分密文并发给数据拥有者。数据拥有者将消息和部分密文加密生成最终的密文, 发送给存储云服务提供商(storage cloud service provider, S-CSP)。

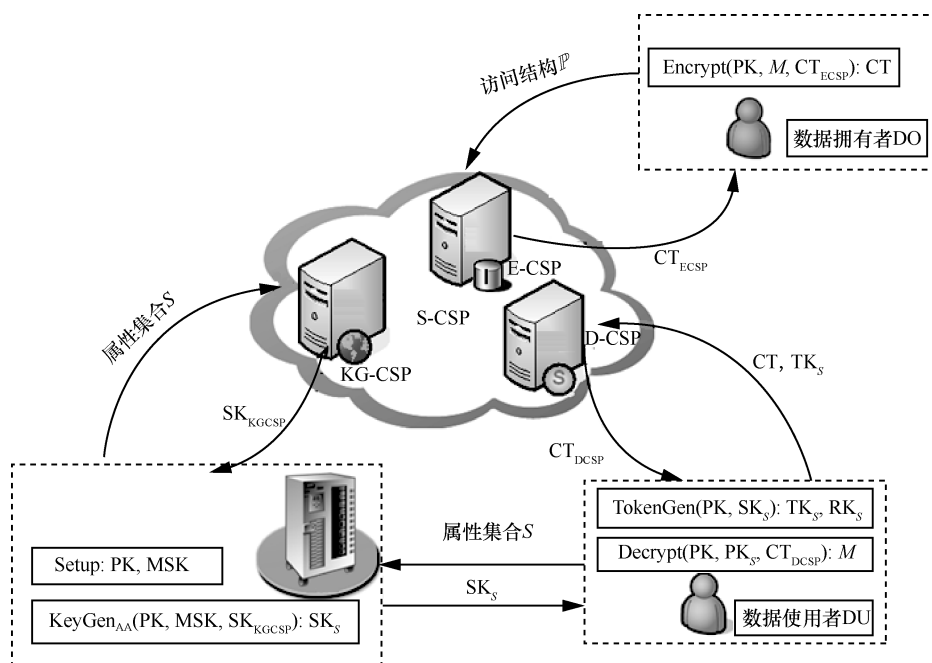


图1 密文策略基于属性加密体制算法加速方案工作流程



(3) 数据拥有者将自己的私钥生成代理密钥和赎回密钥, 把代理密钥发给解密外包云服务提供商 (decryption cloud service provider, D-CSP), 自己保留赎回密钥。D-CSP 通过解密算法解密得到部分解密密文并发给数据使用者。此时数据使用者只需赎回密钥完成解密恢复成明文。

本文所提出的密文策略基于属性加密的算法加速方案是基于 Waters^[5]的方案进行构造的。

3.1 系统建立算法

系统建立算法 $\text{Setup}(1^\lambda, U)$, 输入安全参数 λ 、描述属性域 $U = \{1, 2, \dots, |U|\}$ 根据安全参数生成双线性映射群 (p, G, G_T, e) 。其中, G 和 G_T 都是 p 阶的素数阶循环群。然后从群 G 中随机的选择元素 $g, h_1, \dots, h_{|U|}$, 从群 Z_p^* 中随机选择 α, β 。公开参数为 $\text{PK} = (p, G, G_T, e, g, g^\beta, e(g, g)^\alpha, h_1, \dots, h_{|U|})$, 主密钥为 $\text{MSK} = \alpha$ 。

3.2 密钥生成算法

(1) 部分密钥生成算法 $\text{KeyGen}_{\text{KGCS}}(\text{PK}, S)$ 输入公开参数 PK 和属性集合 S 。然后, 随机选择 $t \in Z_p^*$, 计算部分密钥 $\text{SK}_{\text{KGCS}} = (S, K', K'_0, K'_x)$:

$$K' = g^{t\beta}, K'_0 = g^t, K'_x = h'_x, \forall x \in S \quad (1)$$

(2) 密钥生成算法 $\text{KeyGen}_{\text{AA}}(\text{PK}, \text{MSK}, \text{SK}_{\text{KGCS}})$ 输入公开参数 PK 、主密钥 MSK 和部分密钥 SK_{KGCS} 。计算私钥 $\text{SK}_S = (S, K, K_0, K_x)$:

$$K = g^\alpha \cdot K', K_0 = K'_0, K_x = K'_x, \forall x \in S \quad (2)$$

可以从以上两个算法看出, 密钥生成外包云服务提供商 KG-CSP 完成了大部分密钥生成计算, 属性权威中心只需要利用自己的主密钥完成一次点乘运算即可生成最终密钥。

3.3 加密算法

(1) 代理加密算法 $\text{Encrypt}_{\text{ECS}}(\text{PK}, \mathcal{P})$ 输入公开参数 PK 、消息 M 和一个 LSSS 访问结构 $\mathcal{P}$ 。访问结构 $\mathcal{P} = (A, \rho)$, A 是一个 $\ell \times n$ 的矩阵, 函数 ρ 把矩阵 A 的每一行映射到属性 $\rho(i)$ 。首先, 该算法均匀随机地选择 $s_1, v_2, \dots, v_k \in Z_p^{*k}$, 然后设置向

量 $v = (s_1, v_2, \dots, v_k)$, 其中 s 是要被分享的随机秘密。对于 i 从 1 到 ℓ_s , 计算 $\lambda_i = A_i \cdot v$, 其中 A_i 是 A 的第 i 行。最后, 随机选择 $r_1, \dots, r_{\ell_s} \in Z_p^{*\ell_s}$, 并计算密文 $\text{CT}_{\text{ECS}} = (\mathcal{P} = (A, \rho), C', C'_0, E', C'_i, D'_i)$:

$$\begin{aligned} C &= e(g, g)^{\alpha s_1}, C'_0 = g^{s_1}, \\ C'_i &= g^{\beta \lambda_i} h_{\rho(i)}^{-r_i}, D'_i = g^{r_i}, \forall i \in [\ell_s] \end{aligned} \quad (3)$$

(2) 加密算法 $\text{Encrypt}_{\text{DO}}(\text{PK}, M, \text{CT}_{\text{ECS}})$ 输入公开参数 PK 、消息 M 和部分加密的密文。首先, 该算法均匀随机的选择 s_2 , 计算密文 $\text{CT} = (\mathcal{P} = (A, \rho), C, C_0, E, C_i, D_i)$:

$$\begin{aligned} C &= M \cdot C' \cdot e(g, g)^{\alpha s_2} = \\ M \cdot e(g, g)^{\alpha s} \cdot C'_0 &= C'_0 \cdot g^{s_2} = g^s, \\ E &= g^{\beta s_2}, C_i = C'_i, D_i = D'_i, \forall i \in [\ell_s] \end{aligned} \quad (4)$$

可以从以上两个算法看出, E-CSP 完成了大部分密文生成计算, 数据拥有者只需要执行三个点乘运算和两个模指数运算即可生成最终密文。由于对加密消息部分的密文被随机数 s_2 重新随机化, 所以 E-CSP 无法通过辅助生成的部分密文获得消息。

3.4 解密算法

(1) 代理密钥生成算法 $\text{TokenGen}(\text{PK}, \text{SK}_S)$ 输入公开参数 PK 和私钥 $\text{SK}_S = (S, K, K_0, K_x)$ 。随机选择 $z \in Z_p^*$, 计算代理密钥 $\text{TK}_S = (S, \text{TK}, \text{TK}_0, \text{TK}_x)$:

$$\text{TK} = K^{1/z}, \text{TK}_0 = K_0^{1/z}, \text{TK}_x = K_x^{1/z}, \forall x \in S \quad (5)$$

和赎回密钥 $\text{RK}_S = z$ 。

(2) 代理解密算法 $\text{Decrypt}_{\text{DCSP}}(\text{PK}, \text{TK}_S, \text{CT})$ 算法输入公开参数 PK 、代理密钥 TK_S 以及密文 CT 。解密算法输入公开参数 PK 、代理密钥 $\text{TK}_S = (S, \text{TK}, \text{TK}_0, \text{TK}_x)$ 和密文 $\text{CT} = (\mathcal{P} = (A, \rho), C, C_0, E, C_i, D_i)$ 。假设属性集合 S 满足访问策略 $\mathcal{P}$ 时, 存在集合 $I_s \in \{1, 2, \dots, \ell_s\}$, 分别定义为 $I_s = \{i | \rho(i) \in S\}$, 存在一个集合 $\{\mu_i \in Z_p\}_{i \in I_s}$ 使得 $\{\lambda_i\}$ 是秘密 s 基于矩阵 A 的有效分享, 那么存在以下等式成立 $\sum_{i \in I_s} \mu_i \lambda_i = s$ 。该算法首先计算:

$$\begin{aligned}
 T_1 &= \frac{e(C_0, \text{TK})}{e(E, \text{TK}_0) \prod_{i \in I_s} (e(C_i, \text{TK}_0) e(\text{TK}_{\rho(i)}, D_i))^{\mu_i}} = \\
 &= \frac{e(g, g)^{\alpha s/z} e(g, g)^{\beta t s/z}}{e(g, g)^{\beta t s_2/z} \prod_{i \in I_s} e(g, g)^{\beta t \lambda_i \mu_i/z}} = \\
 &= \frac{e(g, g)^{\alpha s/z} e(g, g)^{\beta t s/z}}{e(g, g)^{\beta t s_2/z} e(g, g)^{\beta t s_1/z}} = \\
 &= e(g, g)^{\alpha s/z}
 \end{aligned} \quad (6)$$

然后, 输出部分解密密文 $\text{CT}_{\text{DCSP}} = (C, T_1)$ 。

(3) 解密算法 $\text{Decrypt}_{\text{DO}}(\text{PK}, \text{RK}_s, \text{CT}_{\text{DCSP}})$ 输入公开参数 PK 、赎回密钥 RK_s 以及部分解密密文 CT_{DCSP} 。计算 $C/T_1^z = M$ 。

可以从以上 3 个算法看出, D-CSP 完成了大部分密文解密计算, 数据使用者只需要一个点乘运算和一个模指数运算即可解密获得明文。数据使用者对密钥重新盲化, 使得解密外包云服务提供商无法知道密文对应的明文信息。

4 安全性与可行性

4.1 安全性

从方案的构造角度分析, 本文提出的密文策略基于属性加密体制算法加速方案的安全性分析如下。

(1) 密钥外包云服务器只负责生成与属性相关的部分密钥, 由于不知道主密钥, 无法获取完整的密钥。

(2) 数据拥有者在加密算法中选择了随机数, 采用了盲化技术产生最终的密文, 加密外包云服务器无法从密文中直接得到关于明文的有效信息。

(3) 解密阶段, 由于解密外包云服务器只得到经过盲化后的代理解密密钥, 只能获得部分解密密文, 无法直接解密得出明文。从密码学可证明安全理论分析, 本文提出的方案可以通过安全模型和形式化的证明, 归结到 DBDH 判定性困难问题。

综上所述, 本文提出的密文策略基于属性加

密体制算法加速方案是安全的。

4.2 可行性

本文所提出的密文策略基于属性加密体制算法加速方案, 在实验中进行实现。实验环境为 Charm 密码学 Python 库, 并分别在基于 ARM 架构的 Android 手机端和 Linux 系统的 Intel 电脑端运行本文方案, 其中 Android 手机具有 2 GB 内存, 为 Android 4.2 版本, Intel 电脑是采用 Linux Kernel 3.13.0 内核版本, Intel 双核 CPU。通过与参考文献[5]中的方案进行比较, 从图 2(a)、图 2(c)、图 2(e) 可以发现, 参考文献[5]中的属性权威中心、数据拥有者和数据使用者的计算开销都随着属性个数的增加而增加。从图 2(b)、图 2(d)、图 2(f) 可以发现, 本文提出的密文策略基于属性加密体制算法加速方案的 3 个角色所涉及的运算都是常数级别的, 与属性个数或者访问策略复杂度无关。属性权威中心只需要一个点乘运算, 数据拥有者只需要 3 个点乘运算和两个模指数运算, 数据使用者只需要一个点乘和一个模指数运算。从实验结果图可以看出, 采用参考文献[5]中的方案完成对 100 个属性的密钥生成算法在 Intel 和 ARM 平台分别需要 0.13 s 和 1.2 s, 而采用本文方案则需要 0.025 ms 和 0.325 ms; 采用参考文献[5]的方案完成对包含 100 个属性的访问策略的加密算法在 Intel 和 ARM 平台分别需要 1.0 s 和 12.5 s, 并完成对相应的密文解密算法分别需要 1.5 s 和 18 s。采用本文方案, 由于加密和解密大部分运算都交由第三方云服务器完成, 数据拥有者本地 Intel 和 ARM 平台分别只需要 5 ms 和 50 ms 完成加密运算, 数据使用者在 Intel 和 ARM 平台分别只需要完成需要 0.025 ms 和 0.325 ms 完成解密运算。因此, 可以得出该方案对密钥生成、加密和解密的效率提升明显, 可以在计算能力受限且能耗要求低的物联网设备等实际场景得到广泛应用。

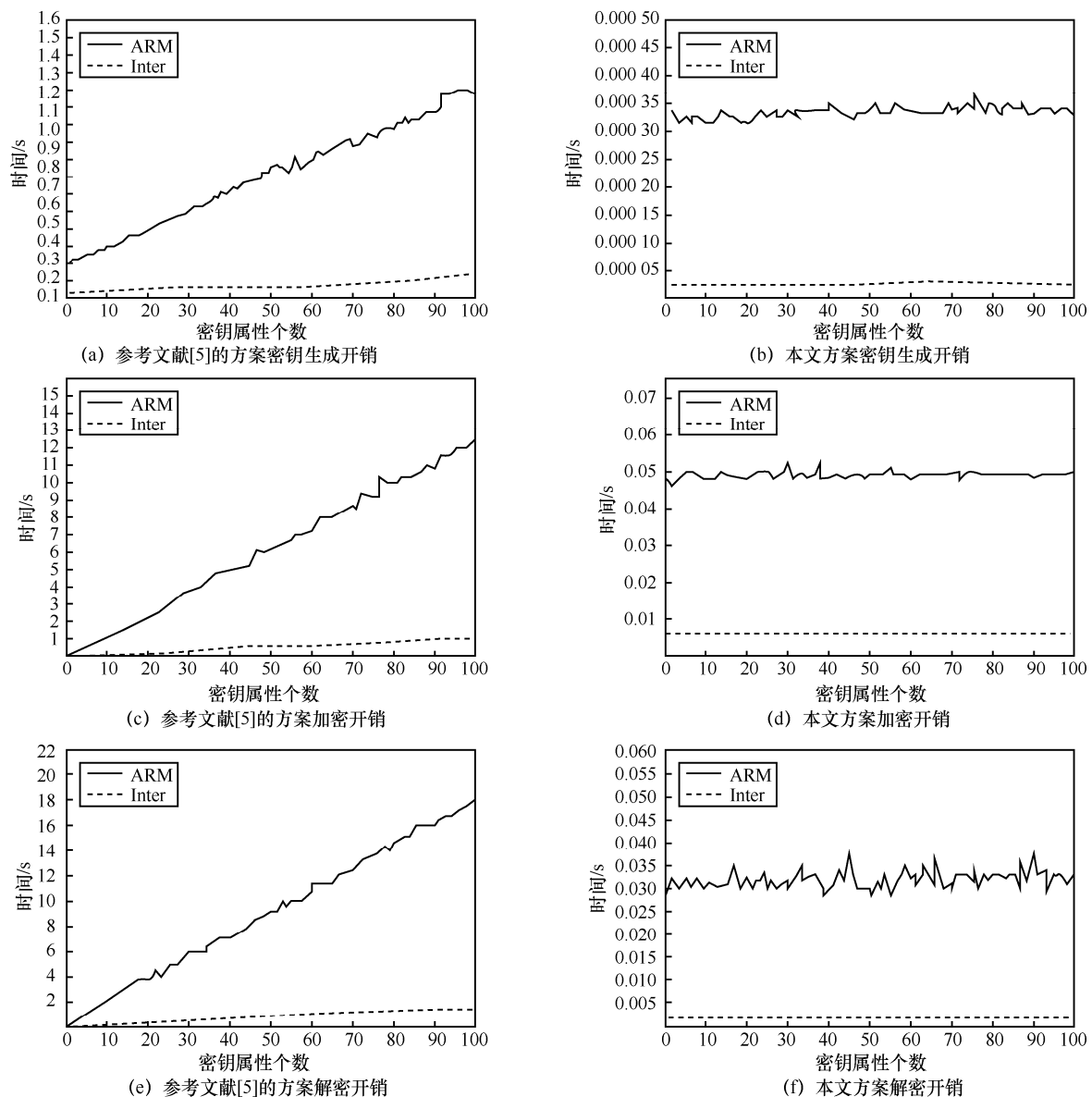


图2 本文方案与参考文献[5]的方案对比

5 结束语

随着云计算技术和云存储服务的普及,用户隐私和数据安全性变得越来越重要^[6-7]。基于属性加密体制具有一对多公钥加密方式以及对数据的细粒度访问控制等优点,适用于云环境下的数据共享访问控制。本文针对目前基于属性加密体制算法效率不高的问题,提出了一种基于属性加密体制算法加速方案,并通过实验验证,可以有效

提升基于属性加密体制的密钥生成算法、加密算法和解密算法的效率,满足云环境下实际应用需求。在移动互联网及未来的物联网时代,基于属性加密体制算法加速方案能够让终端设备减少大量的计算开销和能耗,具有广泛的应用前景。

参考文献:

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 22-26, 2005, Aarhus,

- Denmark. Heidelberg: Springer, 2005: 457-473.
- [2] HOHENBERGER S, WATERS B. Attribute-based encryption with fast decryption[M]//Public-Key Cryptography-PKC 2013. Heidelberg: Springer, 2013: 162-179.
- [3] HOHENBERGER S, WATERS B. Online/offline attribute-based encryption[C]//International Workshop on Public Key Cryptography, Mar 26-28, 2014, Buenos Aires, Argentina. Heidelberg: Springer, 2014: 293-310.
- [4] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//Usenix Conference on Security, Aug8-12, 2011, San Francisco, USA. Berkeley: USENIX Association, 2011:34.
- [5] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography, March 6-9, 2011, Taormina, Italy. Heidelberg: Springer, 2011: 53-70.
- [6] 李子姝, 谢人超, 孙礼, 等. 移动边缘计算综述[J]. 电信科学, 2018, 34(1): 87-101.
LI Z S, XIE R C, SUN L, et al. A survey of mobile edge computing[J]. Telecommunications Science, 2018, 34(1): 87-101.
- [7] 朱友康, 乐光学, 杨晓慧, 等. 移动边缘迁移研究综述[J]. 电信科学, 2019, 35 (4): 74-94.
ZHU Y K, LE G X, YANG X H, et al. A survey on edge computing offloading[J]. Telecommunications Science, 2019, 35(4): 74-94.

[作者简介]



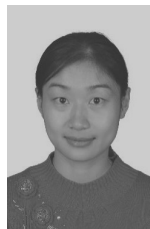
吴国威(1991-), 男, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为云计算安全、密码学与信息安全。



樊宁(1983-), 女, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为网络安全、SDN 安全及 NFV 安全解决方案。



汪来富(1976-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为云计算安全、大数据安全、物联网安全。



王帅(1979-), 女, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为大数据安全、云计算安全、网络与信息安全体系及攻防技术。



沈军(1976-), 女, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为 SDN 领域、大数据安全、云计算安全及移动互联网安全。

金华敏(1972-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为网络与信息安全、云计算安全。