基于可撤销外包属性加密的二维码加密

高 丹 凌 捷 陈家辉
(广东工业大学计算机学院 广州 510006)

摘 要 二维码技术应用广泛,性能优越,但传统的二维码技术的安全性较低,仅适合单一权限对单一信息的扫码获取,不能实现不同权限用户扫码获取不同信息的功能。密文策略属性加密(CP-ABE)作为一种细粒度的数据加密方式,可在保证数据安全的同时实现对用户的访问控制,实现一对多模式的信息传输获取。结合二维码和密文策略属性加密技术的特点和优点,提出一种基于可撤销外包属性加密的二维码加密方案,对基于权限划分的信息块进行二次加密后外包给服务器进行相应的解密和权限匹配,再把初次解密的密文返回给用户,用户通过扫码获得私钥后进行二次解密得到明文,二维码的生成可随随机密钥的不同而变化。通过方案的安全性分析,证明了该方案具有前向安全、后向安全和在双线性 q-BDHE 假设下的选择明文攻击安全(IND-CPA);通过设计的实验,验证了方案在保障二维码信息安全的同时,可实现二维码的一对多的信息有选择获取,具有用户端计算开销低、属性可撤销、二维码生成随机的优点。

关键词 二维码,属性加密,外包,可撤销
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/jsjkx.181102187

Two-dimensional Code Encryption Based on Revocable Outsourced Attribute Encryption

GAO Dan LING Jie CHEN Jia-hui
(School of Computers, Guangdong University of Technology, Guangzhou 510006, China)

Abstract The two-dimensional code technology has a wide range of applications and superior performance, but the traditional two-dimensional code technology has low security and is only suitable for single-privilege scanning of a single information, and cannot implement different functions for users to scan different codes. As a fine-grained data encryption method, ciphertext policy attribute-based encryption (CP-ABE) can realize user access control while ensuring data security, and realize information transmission in one-to-many mode. Combining the characteristics and advantages of two-dimensional code and ciphertext policy attribute-based encryption technology, a two-dimensional code encryption scheme based on revocable outsourcing attribute encryption was proposed. The information block based on the rights division is secondarily encrypted, and then outsourced to the server for corresponding decryption and permission matching. Then the first decrypts ciphertext is returned to the user, and the user obtains the private key by scanning the code and decrypts it twice to get the plaintext. The generation of the two-dimensional code can vary with the different random keys. Through the analysis of the security of the scheme, it is proved that the scheme has forward security, backward security and selective plaintext attack security (IND-CPA) under the bilinear q-BDHE assumption. Through the design experiments, it is verified that the scheme can realize the one-to-many information of the two-dimensional code while ensuring the security of the two-dimensional code information. This scheme has the advantages of low computational overhead on the client side, reversible attributes, and random generation of two-dimensional codes.

Keywords Two-dimensional code, Attribute encryption, Outsourcing, Revocable

1 引言

二维码作为一种被广泛应用的信息获取载体,有着优越的性能特点。传统二维码中信息对任意用户透明,难以保障信息的安全,且不能根据用户属性有选择地传输获取的信息。

基于密文策略的属性加密(Ciphertext-policy Attribute-Based Encryption, CP-ABE),信息可定向传输获取,并通过访问结构 AS(Access Structure)控制用户访问权限。文献[1]提出了基于属性加密的二维码分级加密算法,运用分级加密和密文属性加密相结合的方式,将二维码信息分块进行加密处理,通过访问控制树计算用户的权限信息并进行权限匹配,从而实现对不同权限用户的访问控制。但该方案的用户计算开

到稿日期:2018-11-27 返修日期:2019-04-05 本文受广东省科技计划项目(2017B090906003),广州市重大科技专项(201604010063,201802010043,201807010058)资助。

高 丹(1993-),女,硕士生,主要研究方向为网络信息安全技术,E-mail:2051240381@qq.com;凌 捷(1964-),男,教授,主要研究方向为网络信息安全技术,E-mail:jling@gdut.edu.cn(通信作者);陈家辉(1986-),男,讲师,主要研究方向为密码学及应用。

销较大，不能实现属性撤销，可扩展性不高，对相同密文和访问结构生成的二维码内容固定单一，不能更好地实现随机生成二维码，存在易遭攻击的安全隐患。

随着云计算的发展，外包被认为可以有效解决属性加密中用户计算开销大的问题。文献[2-5]提出了具体的外包方案，文献[6-9]解决了多权威的外包加密问题，但这些方案同样不能很好地实现属性撤销，可扩展性较低。文献[9]提出的用于分层属性的多权限 CP-ABE 方案，可以有效地压缩密文中的冗余信息。文献[10]提出一种可以解决属性撤销问题的可追溯外包 CP-ABE 方案，该方案采用配对外包技术，利用子集覆盖算法来解决撤销和追溯问题。同样地，文献[11-14]也对属性撤销进行了研究。文献[14]提出了 TFDAC-MACS 方案，可以为多权限云存储系统的撤销提供双因素数据加密控制，增加了系统的安全性。文献[15]提出了可撤销的多权限云存储系统 DAC-MACS 的基本数据访问控制方案和广泛的数据访问控制方案 EDAC-MACS，通过经过认证机构认证的属性颁发机构实现用户属性的准确撤销。2017 年，文献[16]提出了改进的 DAC-MACS 方案 NEDAC-MACS，在与文献[15]方案性能相同的情况下，保证了撤销安全。这些方案较好地实现了低计算开销和方案的可扩展性，但无法随机生成二维码。

本文基于文献[16]提出了一种可撤销外包属性加密的二维码加密方案，利用二次加密的方法先对明文信息加密，再把加密后的密文按照不同权限进行划分，然后把密文块基于属性二次加密，形成一个密文集，最后上传给服务器进行解密处理。用户通过扫描二维码可获得一个随机的私钥，再通过上传自己的属性信息，得到云端传回的进行了初次解密的符合用户权限的密文块，用私钥解密即可得到相应的明文信息。本文方案同时具有可撤销、可外包、二维码随机生成的特点，适用于对安全性要求较高的二维码应用场景。此外，二次加密部分运用外包方法，在保障系统安全的同时能减少用户的计算开销。实验结果表明，本文方案能在几乎不损失计算开销的情况下，有效实现可撤销、可扩展、二维码随机生成这 3 个目标。

2　预备知识

2.1　LSSS 矩阵

LSSS 矩阵适用于单调的 CP-ABE 访问结构，可以有效降低 CP-ABE 的计算开销。

访问结构：设一组属性集为 $A=\{A_1,A_2,\cdots,A_n\}$，访问结构为非空集合 $S=\{S_1,S_2,\cdots,S_n\}$，若 $A\neq\varnothing$ 且 $A\subseteq S$，则称集合 A 为授权集合，否则称其为未授权集合。

线性共享[17]：如果一个方案满足线性共享，则：1）存在一个 Z_p 使得集合中的每一个成员份额都可以形成一个向量；2）存在一个分享矩阵 $\boldsymbol{M}$ 使得每一个成员份额都依次被标记。

在 CP-ABE 中，访问结构限制了只有拥有授权集合的用户才可以访问信息。访问结构树由与门、或门及门限门构成，任何单调的线性访问方案都可以转换为相应的 LSSS 矩阵[18]。一个与门及门限门的线性访问结构树如图 1 所示。

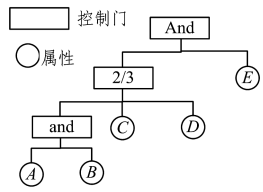

图 1　访问结构树

Fig. 1　Access structure tree

LSSS 矩阵中，每一行都可以通过 $\rho(x)$ 映射到一个属性[19]，如式(1)所示：

$$\begin{pmatrix}1&1&1&1\\1&1&1&2\\1&1&2&0\\1&1&3&0\\1&2&0&0\end{pmatrix}\begin{matrix}\rho(1)\to A\\\rho(2)\to B\\\rho(3)\to C\\\rho(4)\to D\\\rho(5)\to E\end{matrix}\tag{1}$$

2.2　双线性映射

设 G_1,G_2,G_3 为 p 阶循环群，其中 p 为素数；存在一个映射关系 $e:G_1\times G_2\to G_3$，若 e 为双线性对，则满足：

(1)双线性。任意的 $a,b\in Z_p$，都有 $e(G_1^a,G_2^b)=e(G_1,G_2)^{ab}$。

(2)非退化性。存在一个 G_1 和 G_2，使得 $e(G_1,G_2)\neq 1$。

(3)可计算性。存在一个有效的算法计算 $e(G_1,G_2)$。

2.3　DAC-MACS 方案

在 DAC-MACS 方案中，云存储系统具有 5 种类型的实体：全局证书颁发机构(CA)、用户(User)、云服务器(Server)、数据所有者(Owner)和 K 个属性颁发机构(AA_k)，具体步骤如下。

(1)User 及 AA_k 注册：全局证书颁发机构(CA)对用户及属性颁发机构进行认证，颁发 uid 给用户，颁布 aid 给属性颁发机构。

(2)分发密钥 SK：AA_k 通过运行算法根据访问结构中的用户权限计算有效用户的密钥 SK，并将其发给用户。

(3)数据所有者对信息加密以获得密文 CT：所有者定义一个有效的访问结构，然后对信息基于访问结构属性加密，并把数据 CT 上传外包给服务器。

(4)User 解密：User 上传 SK 及其全局公钥 GPK 到 Server，以获得由 Server 计算出的解密令牌 TK 以及密文 CT，用户使用 TK 及全局密钥 GSK 来解密获得的信息。由于缺少全局密钥，CA、AA 和云服务器都无法解密密文以得到明文信息。

(5)属性撤销：当有属性进行撤销改变时，AA_k 运行算法计算更新密钥 CUK 并向 Server 提交更新密钥，Server 收到密钥后运行算法更新与撤销的属性相关的密文，同时用户更新相关属性 SK。只有与撤销属性相关的 CT 和 SK 才需要更新，其余的不变。

经证明，以上方案可保障前向、后向安全和 IND-CPA 安全。

3　本文方案设计

3.1　应用场景

患者在医院就诊时通常需要经历多个阶段的诊疗，如检

查、手术、住院、复诊等，需要多个医生的医治。假设患者 a 由于病情原因转移到了医院 Q，医院 Q 需要把患者 a 的信息移交给多个不同职位的医生以便诊治。医生 B 是主任医生，需要管理患者的所有基本信息；医生 C 是主治医生，需要患者的所有病例信息；医生 D 是住院医生，只需要患者近期的身体状况信息。为了保护患者的隐私，需要一个简单的扫描二维码的方式，在保证信息安全的同时，将不同类型的信息传送给不同职位的医生。

基于二维码应用的广泛性和多样性，本文提出了一种二维码外包属性加密方案，使得用户只需扫描一个随机二维码即可获得符合权限控制的信息，不同属性的用户获取信息的权限不同。

3.2 方法步骤

设 $A=\{A_1,A_2,\cdots,A_i\}(i\geqslant 1)$ 为用户的属性集，$U=\{U_1,U_2,\cdots,U_j\}(j\geqslant 1)$ 为所有可能取值的属性集，访问结构 $S=\{S_1,S_2,\cdots,S_n\}(n\geqslant 1)$。本文方案有 6 种类型的实体：全局证书颁发机构(CA)、用户(User)、云服务器(Server)、加密机构(EM)、K 个属性颁发机构(AA_k)以及密钥分发机构(PM)，如图 2 所示。

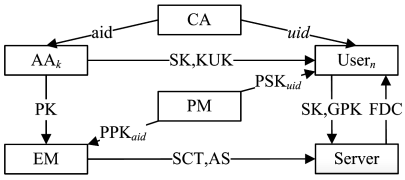

图 2 系统架构图

Fig. 2 System architecture diagram

具体步骤如下：

(1)注册

全局证书颁发机构(CA)对用户及属性颁发机构进行认证，并向用户颁发随机数 uid，向属性颁发机构颁发随机数 aid。

全局私钥：$GSK_{uid}=u_{uid}$，$GSK'_{uid}=u'_{uid}$。

用户全局公钥：$GPK_{uid}=g^{u_{uid}}$，$GPK'_{uid}=g^{u'_{uid}}$。

(2)AA_k 分发密钥 SK

AA_k 通过算法根据访问结构对用户权限进行计算，并向用户分发密钥 SK。

属性集密钥：$SK_{aid}=(\alpha_{aid},\beta_{aid},\gamma_{aid})$。

(3)PM 分发密钥并形成二维码

PM 通过运算向加密机构分发随机公钥 PK，同时通过计算形成二维码向用户分发私钥 PSK。二维码随着随机密钥的不同而变化。

加密公钥：$PPK_{aid}=(N,e)$。

用户私钥：$PSK_{uid}=(N,d)$。

(4)加密机构 EM 对信息 M 进行分段处理并上传二次加密密文 SCT 到服务器

1)基于用户权限分段处理信息 M，形成分段信息集 $M=\{M_1,M_2,\cdots,M_i\}$，如图 3 所示。

子块信息M_1	子块信息M_2	子块信息M_3	子块信息M_4	子块信息M_5

图 3 信息分块

Fig. 3 Information blocking

2)运用 PM 分发的密钥 PK 对信息 M 加密，生成初次加密密文 FCT，$FCT=\{FCT_1,FCT_2,\cdots,FCT_n\}$；密文 $FCT\equiv n^e/(\mathrm{mod}\ N)$。

3)构造基于用户属性的访问结构 AS(见图 1)，对初次加密密文 FCT 基于属性二次加密，形成最终的密文 $SCT=\{SCT_1,SCT_2,\cdots,SCT_n\}$。

$$SCT=(C=k\cdot(\prod_{aid_k\in I_A})PK_{aid_k}),C'=g^s,C''=G^{hs}$$

$$\forall 1\leqslant i\leqslant l,\rho(i)\in S_{aid_k}$$

$$C_i=g^{\alpha\lambda_i}\cdot(PK_{1,\rho(i)})^{-r_i},C_i'=g^{r_i}$$

$$D_i=g^{\frac{r_i}{\beta_{aid_k}}},D_i'=(PK_{2,\rho(i)})^{r_i}$$

4)将访问结构和二次加密密文集 SCK 上传给服务器。

(5)用户解密

1)用户上传属性集密钥 SK、全局密钥 GPK 给服务器。

2)服务器通过全局密钥、用户属性密钥和访问机构对密文 SCT 基于属性初次解密，生成初次解密密文集 FDC(First Decryption of Ciphertext)，并根据用户权限的不同仅返还符合用户权限的初次解密密文，不返还其余信息。

$$FDC=\{FDC_1,FDC_2,\cdots,FDC_k\}(n\geqslant 0)$$

其中，FDC 可以为空，$FDC\subseteq FCT$。

3)用户通过扫描二维码得到私钥 PSK，通过 PSK 对 FDC 进行二次解密，得到信息集 m，$m=\{m_1,m_2,\cdots,m_k\}(k>0)$。其中，$m\subseteq M$；$FCT^d\equiv n(\mathrm{mod}\ N)$，通过 n 可还原信息 m。

(6)属性撤销

假设需要撤销属性 x_{aid}，则 AA_k 通过运算更新密钥 CUK 并向 Server 提交更新密钥 K，Server 收到更新密钥 K 后运行算法更新与撤销的属性相关的密文，同时用户更新相关属性 SK。更新密钥：$\widetilde{K}_{\widetilde{x}_{aid'}}=(K_{\widetilde{x}_{aid'}})^{CUK_{1,\widetilde{x}_{aid'}}}$。

这样在运用外包减少用户计算开销的同时，也能保证数据的前向、后向安全。

4 实验与安全性分析

4.1 安全目标

本方案的安全性建立在 q-BDHE 假设之上，在标准模型下可达到 IND-CPA 安全和前向、后向安全。

本文方案类似于文献[16]，权限只能被静态破坏，攻击者查询的密钥不能用于询问解密密文，并假设：1)CA 是完全可信的，它不会与任何用户勾结；2)每个 AA 都是可信的，但可能被攻击者攻击破坏；3)服务器是半可信的，它会正确执行每个属性权威分配的任务，也会试图获取并破解加密信息；4)每个用户都可能相互串通，在未授权的情况下访问数据。同时，本方案中的所有有效属性权威都将生成一些随机常量应用于每个用户的属性密钥颁发中，因此当 q-BDHE 假设成立时，恶意攻击者或串谋用户会被蒙蔽，将很难发起被动或主动攻击，极大地保证了二维码在一对多有选择的信息传输获取过程中的安全。前向和后向安全是本方案在属性撤销时保证系统安全的基本条件；IND-CPA 安全可证明本方案能有效避免因为用户串谋或属性颁发机构被攻击而导致的信息泄漏。

q-BDHE 假设：设存在一个阶为素数 p 的群 G，g 是 G 上的生成元，双线性映射 $e:G\times G\rightarrow G_r$，给定 $2q+1$ 元组 $(g,h,$

$g^{a},\cdots,g^{a^{2q}})\in G$（其中 $a\in Z_p^*$ 未知），一个随机元素 $T\in G_T$，判断等式 $T=e(g,h)^{a^{q+1}}$ 是否成立。如果攻击者的优势在多项式时间内可忽略，则称 q-BDHE 假设成立。

IND-CPA 安全模型可通过攻击者和挑战者的交互来描述（设 S_A 表示所有属性权威的集合）：

（1）系统建立，生成公私钥对。攻击者指定一组被攻击的属性权威 $S_A'\subset S_A$。对于 S_A 中未经破坏的属性权威，挑战者仅将公钥发送给攻击者；对于 S_A 中的被攻击的属性权威，挑战者将公钥和对应的密钥发送给攻击者。

（2）攻击者向挑战者询问在属性权威集合 S_A-S_A' 中与 (uid,S_{uid}) 相应的解密密钥 SK_{uid} 和更新密钥。

（3）攻击者选择两个相等长度的明文 M_1 和 M_2，并提供一个访问结构 S。挑战者随机选取 $b\in\{1,2\}$，并在访问结构 S 下对明文 M_b 加密，然后将密文 SCK 发送给攻击者。

（4）攻击者可重复步骤（2）中的密钥询问，但攻击者不能询问更新密钥。

（5）最后，挑战者猜测 b 的值 b'。若 $b'=b$，则攻击者在该游戏中获胜，其优势定义为 $\Pr[b'=b]-1/2$。如果攻击者的优势在多项式时间内可忽略，则称方案是 IND-CPA 安全的。

4.2　安全性分析

本文方案外包了大量属性解密的计算和用户权限匹配的计算过程，直接由服务器传回基于用户属性相关的初次解密密文 FDC，用户开销得以减少。由于进行了二次加密，使得二维码内容随着密钥的不同而改变，大大提高了系统的安全性。与此同时，进行属性撤销时，本文方案可满足前向安全、后向安全和 IND-CPA 安全。

（1）前向安全。当系统实行了属性撤销时，都会更新相关密文，以保证用户的密钥与对应的属性相关联。并且，每次改变都会更新相关的密文，使得合法的符合访问策略的用户都可以解密以前发布过的密文，以保证前向安全。

（2）后向安全。当发生属性撤销时，由于每个属性都有一个 AA 相关，AA 会直接生成新的属性密钥，更改相关密文和用户属性。而更新密钥与用户的全局标识 uid 关联，因此被撤销的属性及用户无法使用其他的属性或用户密钥来伪装相应权限的合法用户。每个 AA 都有自己的 aid 标识，当系统被非法用户攻击破坏后，由于相应的 aid 值，不能更新自己的密钥，因此保证了系统的后向安全。

（3）IND-CPA 安全。将本文方案规约到 NEDAC-MACS 方案（详情参考文献[16]）中，在 q-BDHE 假设下选择明文攻击安全（IND-CPA）。

攻击者和挑战者之间的游戏证明：

（1）挑战者随机选择一个安全系数 k 对系统进行初始化并运行算法得到公钥 PK、PPK，以及私钥 SK、PSK，将公钥 PK、PPK 发给攻击者，自己保留私钥 SK、PSK。

（2）攻击者可以进行多项式次数的询问。

（3）加密：

1）攻击者将长度相等的两个明文 M_1 和 M_2 发给挑战者，并指定一个访问结构。

2）挑战者随机选择一个明文 M_b 进行二次加密。

$$FCT=M_b^e/N$$

$$SCK=(M_b^e/N)T\prod_{k\in I_A}e(g^s,g^{a_k'}),C'=g^s,C''=g^{s/\beta_k}$$

其中，$b\in\{1,2\}$。

3）挑战者将二次加密密文 SCK 发送给攻击者。

（4）重复步骤（2），但攻击者不能查询更新密钥。

（5）挑战者猜测 b 的值，并给出 b'。若 $b'=b$，则攻击者获胜，$u=1$；反之，$u=0$，攻击者失败。

本文方案在进行属性加密之前进行了 RSA 加密（需要时可更换为国产密码 SM2 算法），对比与 NEDAC-MACS 方案中的加密结果：

$$C=M_bT\prod_{k\in I_A}e(g^s,g^{a_k'}),C'=g^s,C''=g^{s/\beta_k}$$

由此可知，C 和 SCK 是多项式时间不可区分的。当 $b'=b$ 时，本方案中攻击者在该游戏中的优势 $\Pr[b=b'\mid u=1]=1/2+\text{advanced}$；当 $b'\neq b$ 时，本方案中攻击者在该游戏中无优势，$\Pr[b=b'\mid u=0]=1/2$。因此挑战者获胜的概率为 advanced/2，本方案是 IND-CPA 安全的。

4.3　实验环境与实验过程

本文设计的实验环境如下：硬件设备为 Dell 笔记本；操作系统为 64 位 Windows 8.1 专业版；内存为 4 GB；操作平台为 Visual Studio 2013，C++语言环境；资源文件为 MIRACL C++库。

本文方案经过了 50 次实验，得到的结果比较稳定。实验过程如下：

假设存在随机信息集 $M=\{M_1,M_2,M_3,M_4,M_5\}$。分别输入由 5 组不同信息块组合的明文集合 M，使明文 M 如表 1 所列。

表 1　输入明文 M

Table 1　Enter Plaintext M

序号	信息
M_1	429
M_2	55
M_3	28
M_4	186
M_5	422

对信息进行两次加密，使得高权限用户可以获得低权限的信息，但低权限用户不能获得高权限的信息。

第一次加密：使用 RSA（或者 SM2）加密算法。加密公钥 $Key(e,n)=(17,10\,961)$，并得到一个初次加密的密文集合 $FCT=\{FCT_1,FCT_2,FCT_3,FCT_4,FCT_5\}$，如表 2 所列。

表 2　初次加密密文 FCT

Table 2　First encryption ciphertext FCT

序号	信息
FTC_1	10497
FTC_2	10033
FTC_3	6471
FTC_4	186
FTC_5	5883

第二次加密：构建一个访问结构树，如图 1 所示，采用 LSSS 矩阵降低计算开销，然后加密机构对 FCT 进行第二次加密，得到一个二次加密的属性加密密文集 $SCT=\{SCT_1,SCT_2,SCT_3,SCT_4,SCT_5\}$，属性加密部分类似文献[16]的方案。

加密机构将经过二次加密的密文集 SCT 上传给服务器，服务器根据用户上传的属性密钥进行初次解密，并返还基于用户属性初次解密的信息集 $FDC=\{FDC_1,FDC_2,\cdots,FDC_k\}(n\geqslant 0)$。如表 3 所列，假设用户可能的属性集 $SK=\{A,B,C,D,E\}$，通过图 1 的访问结构控制，不同的用户属性权限返回不同的初次解密密文集 FDC。

表 3 初次解密结果 FDC

Table 3 First decryption result FDC

权限	用户属性	初次解密信息
1	A,B	10497 10033
2	A,B,C 或 A,B,D 或 C,D	10497 10033 6471 186
3	A,B,C,E 或 A,B,D,E 或 C,D,E	10497 10033 6471 186 5883

用户通过扫码得到密钥并对返回的密文 FDC 进行解密，得到最终的信息 $m=\{m_1,m_2,\cdots,m_k\}$，如表 4 所列，用户密钥 $Key(d,n)=(1265,10961)$。

表 4 最终结果 m

Table 4 Final result m

权限	最终解密信息
1	429 55
2	429 55 28 186
3	429 55 28 186 422

4.4 实验结果分析

本文方案支持多项功能，包括多权威属性加密、部分解密、随机生成不同内容的二维码。本文方案与文献[1]和文献[16]的功能比较结果如表 5 所列。

表 5 功能比较

Table 5 Functional comparison

实验方案	是否适用于二维码	二维码是否随机	是否支持外包	是否支持多权威	是否支持部分解密
文献[1]	是	否	否	否	是
文献[16]	否	—	是	是	否
本文方案	是	是	是	是	是

下面分析本文方案、文献[1]和文献[16]各方面的性能。

存在一段长为 n 的随机明文 M，分别采用文献[1]、文献[16]和本文方案的方法进行实验分析，记录各方案模拟实验的初始化时间、密钥分发时间、加密时间、总解密时间和用户解密时间。

1)各方案系统初始化时间的折线对比如图 4 所示。在初始化阶段，各个方案的性能都相对稳定，且文献[16]的方案和本文方案在初始化阶段都比文献[1]的方案更耗时。

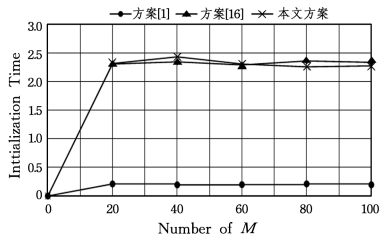

图 4 本文方案与文献[1]和文献[16]的方案的初始化时间

Fig. 4 Initialization time of the proposed scheme and the schemes in ref. [1] and ref. [16]

2)各方案密钥分发时间的折线对比如图 5 所示。在此阶段，本文方案与文献[16]的方案花费的时间基本相同，且都比文献[1]的方案多。

图 4、图 5 所示结果的原因在于本文方案与文献[16]的方案均实现了属性撤销机制，保障了方案的可扩展性。

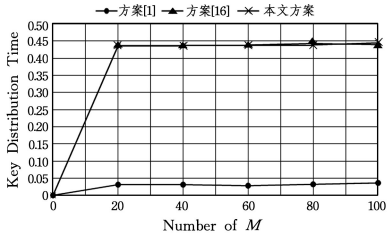

图 5 本文方案与文献[1]和文献[16]的方案的密钥分发时间

Fig. 5 Key distribution time of the probposed scheme and the schemes in ref. [1] and ref. [16]

3)各方案加密时间的折线对比如图 6 所示。在加密时间上，本文方案的加密时间比其他两个方案长，且加密时间随着信息长度的增加呈现增长趋势。这是因为本文方案进行了两次加密，包括 RSA(或 SM2)加密和属性加密，而其他两个方案都只进行了属性加密。值得注意的是，本文方案能实现最佳的二维码随机性，此外该加密实际是可外包的。

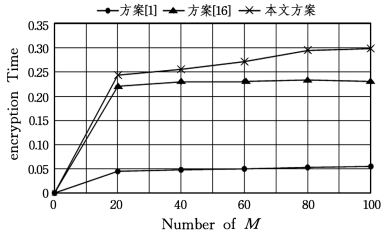

图 6 本文方案与文献[1]和文献[16]的方案加密时间

Fig. 6 Encryption time of the proposed scheme and the schemes in ref. [1] and ref. [16]

4)各方案总解密时间的折线对比如图 7 所示。在本文方案和文献[16]的方案中，总解密时间等于服务器解密工作时间和用户解密时间的总和。本文方案比文献[16]的方案的总解密时间长但相差不大。同时，两个方案都比文献[1]慢。这是由于外包方案比非外包方案多了与服务器交互的步骤，增加了总解密时间。

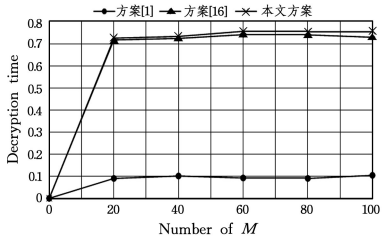

图 7 本文方案与文献[1]和文献[16]的方案的总解密时间

Fig. 7 Total decryption time of the proposed scheme and the schemes in ref. [1] and ref. [16]

5)各方案用户实际解密时间的折线对比如图 8 所示。在本文方案中，用户的实际解密时间短于文献[1]和文献[16]中的方案的解密时间。这是因为与文献[1]相比，本文方案外包了大量的计算；与文献[16]相比，本文方案通过二次加密，外包了用户属性解密和权限匹配的计算。

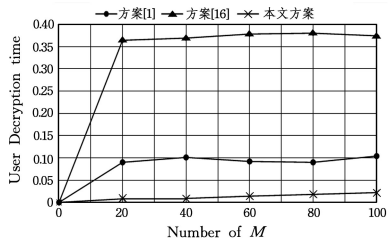

图 8　本文方案与文献[1]和文献[16]的方案的用户解密时间

Fig. 8　User decryption time isof the proposed scheme and the schemes in ref. [1] and ref. [16]

综上，在初始化和密钥分发阶段，本文方案与文献[16]的方案运行所需时间相差不大，但都比文献[1]慢。这是因为在外包方案中多出了对 AA 机构和用户的认证等外包步骤。从加密时间和总解密时间上来说，本文方案所需时间大于文献[1]、文献[16]的方案。这是因为本文方案进行了二次加密，在解密时也需要进行二次解密。在用户解密阶段，本文方案比方案[1]和方案[16]所需的时间短。这是因为本文方案通过二次加密直接返回通过权限匹配后的初次解密密文，省去了用户的匹配权限时间和属性解密时间，从而减少了用户的计算开销。因此，从用户角度看，本文方案的计算开销是最低的。

结束语　本文提出了一种二维码外包属性加密的方案，通过二次加密的方式，对信息块进行二次加密后外包给服务器进行相应的解密和权限匹配，再把初次解密的密文返回给用户，用户通过扫码获得私钥后进行二次解密得到明文。该方案与文献[1]和文献[16]的方案比较，同样能保障前向安全、后向安全和 IND-CPA 安全，但弥补了文献[1]中不能随机生成二维码的缺陷，提高了二维码的抗分析攻击能力，并减少了用户端的计算时间开销。本文方案具有用户计算开销低、可扩展性好、二维码随机生成等优点，提高了二维码的安全性。

参 考 文 献

[1] YANG K，YUAN H D，GUO Y B. Two-dimensional code hierarchical encryption algorithm based on attribute encryption[J]. Computer Engineering，2018，44(6)：136-140. (in Chinese)
杨康，袁海东，郭渊博. 基于属性加密的二维码分级加密算法[J]. 计算机工程，2018，44(6)：136-140.

[2] LAI J，DENG R H，GUAN C，et al. Attribute-Based Encryption With Verifiable Outsourced Decryption[J]. IEEE Transactions on Information Forensics and Security，2013，8(8)：1343-1354.

[3] GREEN M，HOHENBERGER S，WATERS B. Outsourcing the Decryption of ABE Ciphertexts[C]// Usenix Conference on Security. San Francisco，CA，2011：34-34.

[4] MAO X，LAI J，MEI Q，et al. Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption[J]. IEEE Transactions on Dependable & Secure Computing，2016，13(5)：533-546.

[5] LI J，WANG Y，ZHANG Y，et al. Full Verifiability for Outsourced Decryption in Attribute Based Encryption[J]. IEEE Transactions on Services Computing，2017，5(99)：1-1.

[6] LI W，XUE K，XUE Y，et al. TMACS：A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage[J]. IEEE Transactions on Parallel and Distributed Systems，2015，27(5)：1484-1496.

[7] WU X，JIANG R，BHARGAVA B. On the Security of Data Access Control for Multiauthority Cloud Storage Systems[J]. IEEE Transactions on Services Computing，2015，10(2)：258-272.

[8] WANG Y，LI F，XIONG J，et al. Achieving Lightweight and Secure Access Control in Multi-authority Cloud[C]// Trustcom/BigDataSE/ispa. IEEE，2015：459-466.

[9] ZHANG Z Y，LI C，GUPTA B B，et al. Efficient Compressed Ciphertext Length Scheme Using Multi-Authority CP-ABE for Hierarchical Attributes[J]. IEEE Access，2018，6(1)：38273-38284.

[10] ZHANG R，HUI L，YIU S，et al. A Traceable Outsourcing CP-ABE Scheme with Attribute Revocation[C]// 2017 IEEE Trustcom/BigDataSE/ICESS. IEEE，2017：363-370.

[11] LIU Z，WONG D S. Practical Ciphertext-Policy Attribute-Based Encryption：Traitor Tracing，Revocation，and Large Universe[C]// International Conference on Applied Cryptography and Network Security. Springer，Cham，2015：127-146.

[12] 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.

[13] ZHANG P，CHEN Z，LIANG K，et al. A Cloud-Based Access Control Scheme with User Revocation and Attribute Update[M]// Information Security and Privacy. Springer International Publishing，2016.

[14] LI X，TANG S，XU L，et al. Two-Factor Data Access Control With Efficient Revocation for Multi-Authority Cloud Storage Systems[J]. IEEE Access，2017，5(99)：393-405.

[15] YANG K，JIA X. Expressive，Efficient，and Revocable Data Access Control for Multi-Authority Cloud Storage[J]. IEEE Transactions on Parallel and Distributed Systems，2014，25(7)：1735-1744.

[16] WU X，JIANG R，BHARGAVA B. On the Security of Data Access Control for Multiauthority Cloud Storage Systems[J]. IEEE Transactions on Services Computing，2017，10(2)：258-272.

[17] LEWKO A，WATERS B. Decentralizing Attribute-Based Encryption[C]// Advances in Cryptology-eurocrypt-International Conference on the Theory and Applications of Cryptographic Techniques. 2011：568-588.

[18] BEIMEL A. Secure Schemes for Secret Sharing and Key Distribution[D]. Israel：Israel Institute of Technology，1996.

[19] DING S，LI C，LI H. A Novel Efficient Pairing-free CP-ABE Based on Elliptic Curve Cryptography for IoT[J]. IEEE Access，2018，6(99)：27336-27345.