CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 44 卷第 6 期 2022 年 6 月
Vol. 44, No. 6, Jun. 2022

文章编号:1007-130X(2022)06-1003-10

智慧城市中隐私保护性广播加密算法*

牛淑芬[1],方丽芝[1],宋　蜜[1],王彩芬[2],杜小妮[3]

(1.西北师范大学计算机科学与工程学院,甘肃 兰州 730070;2.深圳技术大学大数据与互联网学院,广东 深圳 518118;
3.西北师范大学数学与统计学院,甘肃 兰州 730070)

摘　要:现代化城市公共部门和市民社交网络会产生大量的数据,这些海量数据的使用和处理主要依赖现代化信息通信技术和网络技术。为了保护用户隐私和数据安全,在数据传输过程中采用加密算法对数据进行加密,广播加密是多用户环境下最有效的方法。传统算法中,基于身份的广播加密密文可以广播到一组接收方,接收方的身份包含在密文中,当多个接收方解密密文时会泄露其他用户的身份信息。为了保护接收方用户之间的身份隐私,提出一种基于身份的隐私保护性广播加密算法,实现了接收方用户之间的匿名性。此外,考虑了如何从匿名广播的密文中撤销指定目标的接收者,根据数据访问控制策略决定用户的数据访问权限,为用户提供密文撤销操作,撤销过程不泄露明文和接收者的身份信息。在随机预言模型下,基于 BDH 困难性问题证明了该算法的安全性,并通过实际数据集的仿真实验验证了算法的有效性和可行性。

关键词:智慧城市;基于身份的加密;广播加密;用户撤销;隐私保护

中图分类号:TP309.7　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2022.06.007

Privacy-preserving broadcast encryption in smart city

NIU Shu-fen[1], FANG Li-zhi[1], SONG Mi[1], WANG Cai-fen[2], DU Xiao-ni[3]

(1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070;
2. College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118;
3. College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China)

Abstract: A large number of data are generated by the public city departments and citizen in modern city, and modern information and communication technology and network technology are adopted to use and process the massive data. To protect the privacy and data security of users, the encryption algorithm is used to encrypt the data in the process of data transmission. Broadcast encryption is the most effective method in multi-user environment. Traditionally, the ciphertext of identity-based broadcast encryption can be broadcasted to a group of receivers, and the identity of the receiver is contained in the ciphertext. When multiple receivers decrypt the ciphertext, the identity information of other users will be exposed. In order to protect the identity privacy between receivers, an identity-based privacy-preserving broadcast encryption algorithm is proposed, which realizes the anonymity between receivers. In addition, the algorithm focuses how to revoke some re-ceivers of the specified target from the ciphertext of anonymous broadcast and determines the user's data access authority according to the data access control policy, so as to provide users with the revocation of ciphertext. The revocation process does not reveal the plaintext and the identity information of the receivers. In the random oracle model, the security of the algorithm is proved based on the BDH difficulty problem, and the effectiveness and security of the

* **收稿日期**:2021-01-08;**修回日期**:2021-08-28
基金项目:国家自然科学基金(61562077,61662071,61662069,61772022);国家留学基金(201708625061);西北师范大学青年教师科研提升计划(NWNU-LKQN-14-7)
通信作者:方丽芝(1439902640@qq.com)
通信地址:730070 甘肃省兰州市西北师范大学计算机科学与工程学院
Address: College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, Gansu, P. R. China

algorithm are verified by the simulation experiment on the actual data set.

Key words: smart city; identity-based encryption; broadcast encryption; revocation; privacy-preserving

1 引言

随着我国城市人口的持续增长,城市化治理出现了一系列问题,政府部门有必要提供一些公共服务来提高市民的生活质量。有效的安全监控网络能够确保水电、交通、医疗和教育等数据的安全,政府可以通过公民参与式管理,推动可持续经济增长和高质量的生活。但是,传统的技术和管理方法很难有效解决这些问题。因此,利用新兴的信息通信技术来解决城市化管理问题是非常必要的。在这样的背景中,一些学者提出了智慧城市的概念[1-3]。文献[4]分析了物联网应用于智慧城市中智能家居、车联网、智能电网和公共基础设施场景下存在的不足。文献[5]利用智慧城市中的智能方法解决了互联网环境下车辆的管理控制。智慧城市中最核心的是用户数据,这些数据大部分是敏感的,例如社交账号和密码。敏感数据在传输的过程中必须要保证其安全性和隐私性。如何有效地保护数据的机密性,已经成为智慧城市中的一个重要问题。

Fiat 等[6]在 1993 年提出了广播加密技术,允许中心广播站点向任意一组接收方广播密文,同时最小化与密钥管理相关的传输。文献[6-12]运用广播加密技术在多个接收者的场景下保护了数据安全性和隐私性。Naor 等[13]在 2001 年提出一种应用于无状态接收者的"子集覆盖"框架,该框架基于对称密钥广播加密。Naor 等[14]在 2000 年提出了基于公钥的广播加密算法,采用门限秘密共享方法解决了基于对称密钥广播加密的安全问题,克服了只有可信中心才可以广播密文的缺点。广播加密技术允许一个数据拥有者将数据共享给包含多个用户的集合 S,只有集合 S 内的授权用户才可以访问共享数据。例如,智能电力系统将密钥分发给授权用户,用户通过密钥享受电力服务,反之,若用户没有收到密钥,则不能享受电力服务。

在智慧城市中,"智能"设备应该在一定范围内自动地处理数据访问控制,即根据数据访问控制策略决定用户是否具有访问控制权限。文献[15]提出一种支持用户撤销的属性认证密钥协商协议算法,该算法研究如何对用户进行直接撤销,将用户标识嵌入在私钥中并在通信消息密文中嵌入用户撤销列表,若用户被撤销,则无法认证。文献[16]在合数阶双线性群上提出了完全细粒度属性撤销模型,在密文中添加多个属性用户撤销列表来撤销任意数量的属性,但密文长度与用户数量线性相关,造成智能电网中大数量级的数据文件加密时间过长,不适用于智能电网云存储平台。文献[17]提出一种细粒度权限撤销的云存储模型,数据属主可以是属性分发机构,负责产生属性集合和加入属性撤销参数,但在加密之前要知道用户集合,不适合智能电网中大量的用户属性变化,可能造成用户信息泄露。Lai 等[18]在 2016 年提出了匿名身份的广播加密,发送方可有效地向大量接收者广播密文。文献[19]提出了可撤销身份的广播加密算法,重点突出在数据访问控制下允许第三方撤销用户身份。这 2 种算法保护了接收者之间的身份隐私,但传输量和计算量较大,会造成数据文件加密和解密时间过长。针对这些问题,本文从基于身份的广播加密生成密文中撤销指定目标集合的接收者,通过对已撤销用户的身份进行加密,未撤销的用户使用私钥对密文解密,保护了接收者之间的匿名性和隐私性。本文主要创新点包含以下 2 个方面:

(1) 使用广播加密技术实现对加密数据的有效共享,且保证了其加密和共享效率。利用拉格朗日插值实现用户身份的匿名和数据的完全隐私保护,任何接收者在解密时都无法获取其他用户的身份信息。

(2) 算法结合智慧城市中智能电网应用场景进行数据共享。针对用户权限可能会发生改变,用户离开系统会产生数据更新等问题,通过直接撤销实现对智能电网中用户身份的灵活管理。

在 Linux Ubuntu-10.10 操作系统下利用 PBC 和 C 语言进行编程,对本文算法和现有的部分广播加密算法进行对比实验。实验结果表明,本文算法的效率和性能优于其它算法。在随机预言模型下运用 BDH 困难问题证明了本文算法的安全性。

2 系统模型与安全模型

本节给出本文算法的系统模型和安全模型。图 1 为智慧城市的主要应用领域。

2.1 系统模型

智慧城市中基于身份的隐私保护性广播加密

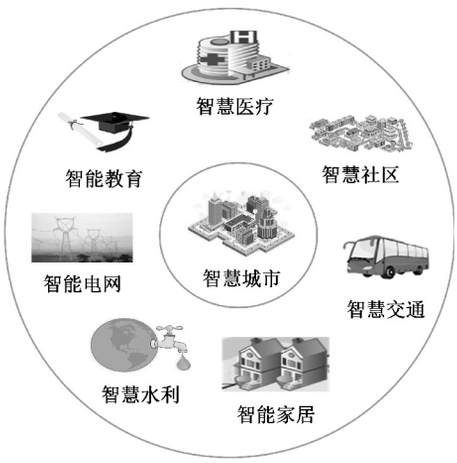

Figure 1 Application domains in a smart city

图 1 智慧城市应用领域

算法适用于一对多的密文传播场景。而智能电网则是智慧城市的应用领域之一,是电网技术发展的有利趋势。图 2 给出了智能电网的典型应用场景。数据属主智能供电系统将加密的数据文件广播给用户,存储在智能电表中。密钥生成中心生成用户私钥。接收到密钥的用户具有使用智能电力服务的权限,且可以访问加密数据。当用户要离开当前居住地或者使用其他电力系统需要撤销身份时,智能供电系统可以为用户提供管理身份权限的服务,通过智能方式撤销和更新用户信息,被撤销授权的用户无法再解密密文。

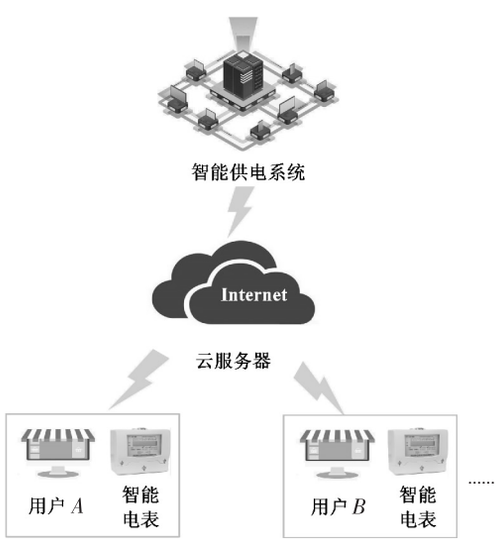

Figure 2 A typical application scenario in smart grid

图 2 智能电网应用场景

智能供电系统为确保客户及其数据隐私,智能电表与智能供电系统之间的数据会被加密。智能供电系统将加密的原始密文传输给云服务器,然后云服务器将原始密文转换为可以用未撤销用户私钥解密的密文。本文算法包括智能供电系统、密钥生成中心、云服务器、智能设备(智能电表)和数据用户 5 类实体。

2.2 安全模型

参照文献[20]中基于匿名身份的广播加密算法的思想,本文定义了 4 种安全模型:基于身份的选择明文攻击不可区分性 IND-ID-CPA(INDistinguishability under IDentity-based Chosen Plaintext Attack security)安全;基于匿名身份的选择明文攻击不可区分性 ANON-ID-CPA(ANONymous IDentity-based Chosen Plaintext Attack security)安全;基于可撤销身份的选择明文攻击不可区分性 IND-rID-CPA(INDistinguishability under revocable IDentity-based Chosen Plaintext Attack security)安全;选择性匿名可撤销身份的选择明文攻击性 ANON-rID-CPA(selective revocable ANONymous IDentity-based Chosen Plaintext Attack security)安全,以上 4 种安全模型通过概率多项式时间内的攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏定义。

游戏 1 IND-ID-CPA 安全。

在没有有效私钥的情形下,密文中消息与相同长度的随机字符串无法区分。该安全模型定义如下:

(1)系统建立:挑战者 $\mathcal{C}$ 建立算法,输入安全参数 λ,输出系统公钥 mpk 和主密钥 msk。

(2)阶段 1:攻击者 $\mathcal{A}$ 可对任何身份发起私钥询问。收到身份为 ID_i 的私钥询问时,挑战者 $\mathcal{C}$ 运行密钥生成算法得到私钥 d_{ID_i}。

(3)阶段 2:受制于上述挑战,攻击者 $\mathcal{A}$ 发起适应性私钥询问。

(4)挑战:对任何的 $ID_i \in S^*$,攻击者 $\mathcal{A}$ 没有发起私钥询问的限制下,输出不同长度的消息 M_0 和 M_1,以及挑战身份集合 $S^* = (ID_1, ID_2, \cdots, ID_n)$,挑战者 $\mathcal{C}$ 随机选取 $b \in \{0,1\}$,在 S^* 下为 M_b 生成挑战密文 CT^*,并将其返回给 $\mathcal{A}$。

(5)猜测:$\mathcal{A}$ 输出 $b' \in \{0,1\}$ 并赢得游戏。将这样的游戏称为 IND-ID-CPA 攻击者,攻击者获得明文 M 并赢得游戏的优势定义为 $Adv^{\mathcal{A},M}_{\text{IND-ID-CPA}}(\lambda) = |Pr[b = b'] - 1/2|$。

定义 1 如果对任何多项式时间内的 IND-ID-CPA 攻击者在游戏 1 中获胜的优势 $Adv^{\mathcal{A},M}_{\text{IND-ID-CPA}}(\lambda)$ 都是可忽略的,则称基于身份的隐私保护性广播加密算法是 IND-ID-CPA 安全的。

游戏 2 ANON-ID-CPA 安全。

系统建立、阶段 1 和阶段 2 与游戏 1 的一致，挑战和猜测步骤如下所示：

(1) 挑战：攻击者 $\mathcal{A}$ 对任意一个身份 $ID_i \in S_0 \triangle S_1 = (S_0 \backslash S_1) \cup (S_1 \backslash S_0)$ 输出 M^*、身份集合 $S_0 = (ID_{0,1}, \cdots, ID_{0,n})$ 和 $S_1 = (ID_{1,1}, \cdots, ID_{1,n})$。挑战者 $\mathcal{C}$ 随机选取 $b \in \{0,1\}$，在 S_b 下对消息 M^* 生成挑战密文 CT^*。

(2) 猜测：$\mathcal{A}$ 输出 $b' \in \{0,1\}$ 并赢得游戏。将这样的游戏称为 ANON-ID-CPA 攻击者，攻击者赢得游戏的优势定义为 $Adv^{\mathcal{A},M}_{\text{ANON-ID-CPA}}(\lambda) = |Pr[b=b']-1/2|$。

定义 2 如果对于任何多项式时间内的 ANON-ID-CPA 攻击者在游戏 2 中获胜的优势 $Adv^{\mathcal{A},M}_{\text{ANON-ID-CPA}}(\lambda)$ 都是可忽略的，则称基于身份的隐私保护性广播加密算法是 ANON-ID-CPA 安全的。

游戏 3 IND-rID-CPA 安全。

系统建立、阶段 1 和阶段 2 与游戏 1 的一致，挑战和猜测步骤如下所示：

(1) 挑战：对任何 $ID_i \in S^* \backslash R^*$，攻击者 $\mathcal{A}$ 没有发起私钥询问的限制下，输出消息 M_0 和 M_1、挑战身份集合 $S^* = (ID_1, ID_2, \cdots, ID_n)$ 和撤销身份集合 $R^* = \{ID_{l_1}, ID_{l_2}, \cdots, ID_{l_t}\}$。挑战者 $\mathcal{C}$ 在 S^* 和 R^* 下为消息 M_b 生成挑战密文 CT'^* 并将其返回给 $\mathcal{A}$。

(2) 猜测：$\mathcal{A}$ 输出 $b' \in \{0,1\}$ 赢得游戏。这样的游戏称为 IND-rID-CPA 攻击者，攻击者赢得游戏的优势定义为 $Adv^{\mathcal{A},M}_{\text{IND-rID-CPA}}(\lambda) = |Pr[b=b']-1/2|$。

定义 3 如果对于任何多项式时间内的 IND-rID-CPA 攻击者在游戏 3 中获胜的优势 $Adv^{\mathcal{A},M}_{\text{IND-rID-CPA}}(\lambda)$ 都是可忽略的，则称基于身份的隐私保护性广播加密算法是 IND-rID-CPA 安全的。

游戏 4 选择性 ANON-rID-CPA 安全。

系统建立和阶段 1 与游戏 1 的一致，其他步骤如下所示：

(1) 初始化：输出不同长度的撤销身份集合 $R_0 = (ID_{0,1}, \cdots, ID_{0,t})$ 和 $R_1 = (ID_{1,1}, \cdots, ID_{1,t})$。

(2) 挑战：输出消息 M^* 和广播身份集合 $S^* = (ID_1, ID_2, \cdots, ID_n)$。挑战者 $\mathcal{C}$ 随机选取 $b \in \{0,1\}$，在 S^* 和 R_b 下为消息 R_b 生成挑战密文 CT'^*。

(3) 猜测：$\mathcal{A}$ 输出 $b' \in \{0,1\}$ 赢得游戏。这样的游戏称为 ANON-rID-CPA 攻击者，攻击者赢得游戏的优势为 $Adv^{\mathcal{A},M}_{\text{ANON-rID-CPA}}(\lambda) = |Pr[b=b']-1/2|$。

定义 4 若对于任何多项式时间内的 ANON-rID-CPA 攻击者在游戏 4 中获胜的优势 $Adv^{\mathcal{A},M}_{\text{ANON-rID-CPA}}(\lambda)$ 都是可忽略的，则称基于身份的隐私保护性广播加密算法是 ANON-rID-CPA 安全的。

3 本文具体算法

智慧城市中基于身份的隐私保护性广播加密算法包括以下 5 个阶段：系统建立阶段、密钥生成阶段、加密阶段、撤销阶段和解密阶段。

(1) 系统建立阶段。该阶段由密钥生成中心执行，输入安全参数 λ，具体步骤如下所示：

①随机选取双线性映射群 $BG = (G, G_T, e, p)$，其中，$e: G \times G \rightarrow G_T$，$P \in G$ 是阶为 p 的生成元。选取 $s \in \mathbf{Z}_p$，计算公共参数 $P_{\text{pub}} = sP$。

②定义 3 个抗碰撞的哈希函数：

$H: \{0,1\}^* \rightarrow \mathbf{Z}_p$

$H_1: \{0,1\}^* \rightarrow G$

$H_2: G_T \times \{0,1\}^* \rightarrow G$

③输出系统公钥 mpk 和主密钥 msk：

$mpk = (BG, P, P_{\text{pub}}, H, H_1, H_2)$

$msk = s$

(2) 密钥生成阶段。该阶段由密钥生成中心执行。给定密钥对 (mpk, msk) 和身份 $ID \in \{0,1\}^*$，输出私钥 $d_{ID} = sH_1(ID)$。

(3) 加密阶段。该阶段由智能供电系统执行。选定一组特定的电力用户身份集合 $S = (ID_1, ID_2, \cdots, ID_n)$，公钥 mpk 和共享给用户的明文 $M \in G$，加密 M 得到密文 CT，存储在智能电表中。加密阶段模型如图 3 所示。

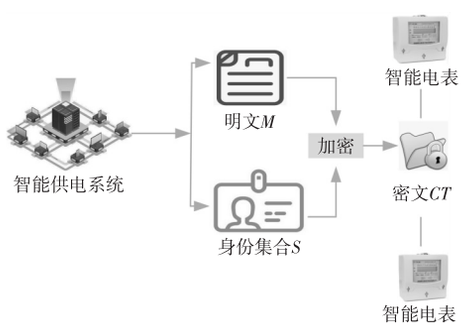

Figure 3 Data encrypt

图 3 数据加密

加密阶段的具体步骤如下所示:

①计算用户身份的哈希值 $x_i=H(ID_i)$,$i=1,2,\cdots,n$。构造多项式函数 $f_i(x)=\sum_{j=0}^{n-1}a_{i,j}x^j \bmod p$。

②随机选取 $r_1\in\mathbf{Z}_p$ 和 $k_1\in G$ 作为秘密值,计算 $A_i=k_1+H_2(e(H_1(ID_i),P_{\text{pub}})^{r_1},ID_i)$,$i\in[1,n]$。

③计算 $C_0=k_1+M$,$C_1=r_1P$。

④计算 $u_i=\sum_{j=1}^{n}a_{j,i-1}A_j$,$i=1,2,\cdots,n$。

⑤生成密文 $CT=(C_0,C_1,u_i)$,$i\in[1,n]$。

(4)撤销阶段。该阶段由云服务器执行。云服务器收到密文后根据撤销后的身份集合 S' 加密数据得到撤销后的密文 CT'。设用户 A 为撤销后的用户,其他用户可以收到 CT',而用户 A 则无法接收到。在此过程中,算法利用拉格朗日插值隐藏用户身份和数据信息,云服务器无法从密文中获取任何用户身份和数据信息。撤销阶段模型如图 4 所示。该阶段主要步骤如下所示:

①给定系统公钥 mpk、撤销身份集合 $R(|R|=t,t\leqslant n)$ 和密文 $CT=(R,C_0,C_1,u_i)$,$i\in[1,n]$。

②若撤销身份集合 $R=\varnothing$,则撤销后的密文满足 $CT'=CT$;否则,云服务器随机选择 $k_2\in G$ 作为秘密值。对任意的 $ID_i\in R$,计算 $C_0'=k_2+C_0$,构造函数 $g(x)=\prod_{i=1}^{t}(x-x_i)=\sum_{i=1}^{t}b_ix^{i-1} \bmod p$。

③云服务器对任意的 $i=1,2,\cdots,n$,计算 $T_i=g(x_i)^{-1}b_ik_2$,$b_i=0(i=t+1,t+2,\cdots,n-1)$,得到撤销后的密文 $CT'=(R,C_0',C_1,[u_i,T_i]_{i=1}^n)$。

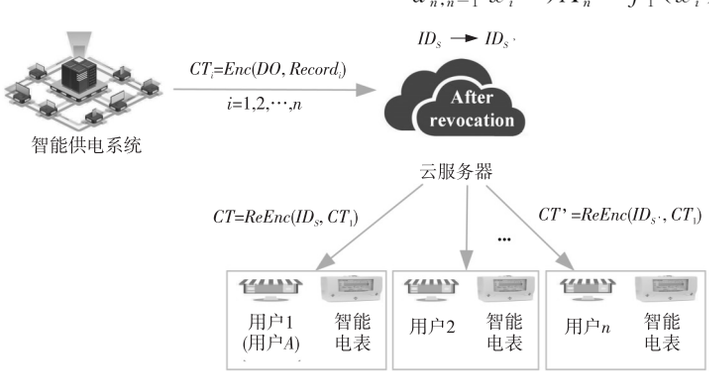

Figure 4 ID revoke

图 4 用户身份撤销

(5)解密阶段。给定撤销后的密文 $CT'=(R,C_0',C_1,[u_i,T_i]_{i=1}^n)$、身份 ID_i、用户私钥 d_{ID_i} 和系统公钥 mpk。云服务器利用撤销后的身份加密原始密文发送给用户,用户通过此阶段得到明文 M。解密阶段模型如图 5 所示。该阶段具体步骤如下所示:

①计算 $u=u_1+x_iu_2+x_i^2u_3+\cdots+x_i^{n-1}u_n$。

②用户使用自己的私钥 d_{ID_i} 计算:$k'_1=u-H_2(e(C_1,d_{ID_i}),ID_i)$,$k'_2=T_1+x_iT_2+x_i^2T_3+\cdots+x_i^{t-1}T_t$。

恢复消息 $M=C_0'-k_1'-k_2'$。若存在身份满足 $ID_i\in S$,$ID_i\notin R$,则 $k_1'=k_1$,$k_2'=k_2$。本阶段通过计算获得 k_1' 和 k_2',解密获得正确的明文。

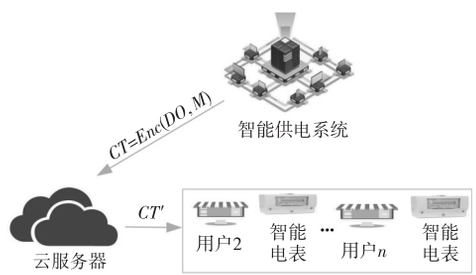

Figure 5 Data decrypt

图 5 数据解密

在本文构造的算法定义中,撤销编号 $t(t<n)$ 的大小取决于实际情况的应用。若 $t=0$,说明数据拥有者不允许服务器撤销任何用户的身份;若 $t=n$,意味着数据拥有者允许撤销身份集合中的任何身份。

本文算法的正确性验证如下所示:对于任何 $ID_i\in S$,获得 x_i 后,计算:$u=u_1+x_iu_2+x_i^2u_3+\cdots+x_i^{n-1}u_n=(a_{1,0}+a_{1,1}x_i+a_{1,2}x_i^2+\cdots+a_{1,n-1}x_i^{n-1})A_1+(a_{2,0}+a_{2,1}x_i+a_{2,2}x_i^2+\cdots+a_{2,n-1}x_i^{n-1})A_2+\cdots+(a_{n,0}+a_{n,1}x_i+a_{n,2}x_i^2\cdots+a_{n,n-1}x_i^{n-1})A_n=f_1(x_i)A_1+f_2(x_i)A_2+\cdots+$

$f_n(x_i)A_n=A_i$,然后计算 $k'_1=u-H_2(e(C_1,d_{ID_i}),ID_i)=k_1+H_2(e(sH_1(ID_i),P)^{r_1},ID_i)-H_2(e(P,sH_1(ID_i)^{r_1},ID_i))=k_1$,对于任何 $ID_i\in S$ 和 $ID_i\notin R$,都有 $g(x_i)\neq 0$,通过计算得到 $k'_2=T_1+x_iT_2+x_i^2T_3+\cdots+x_i^{t-1}T_t=g(x_i)^{-1}k_2g(x_i)=k_2$,通过恢复 k'_1 和 k'_2 得到明文消息 $C'_0-k'_1-k'_2=k'_2+C_0-k'_1-k'_2=k_1+M-k'_1=M$。

4 安全性证明

本节基于 BDH 困难问题证明了本文提出的算法在安全模型定义中达到的安全目标和随机预言模型下的安全性。

定理 1 定义 2 个抗碰撞的哈希函数 H 和 H_2,若 BDH 困难问题成立,本文提出的基于身份的隐私保护性广播加密算法是 IND-ID-CPA 安全的。$\mathcal{A}$ 以 ε 的优势攻击算法,模拟者 $\mathcal{B}$ 以 $\varepsilon'\geqslant\varepsilon\cdot(e\cdot n\cdot q_E\cdot q_{H_2})^{-1}$ 的优势解决 BDH 困难问题。其中,n 为广播身份的数量,q_E 是对私钥的询问数量,q_{H_2} 是对哈希函数 H_2 的询问数量。

证明 假设存在 IND-ID-CPA 的攻击者以不可忽略的优势 ε 对提出的算法进行攻击。利用攻击者 $\mathcal{A}$ 构建模拟者 $\mathcal{B}$,以 ε' 的优势解决 BDH 困难问题。由模拟者 $\mathcal{B}$ 输入 BDH 困难问题的随机实例 (P,aP,bP,cP),其目标是计算 $e(P,P)^{abc}$。在游戏 1 中,模拟者 $\mathcal{B}$ 与攻击者 $\mathcal{A}$ 的互动过程如下所示:

(1) 系统建立。模拟者 $\mathcal{B}$ 令 $P_{pub}=aP$ 并构建 $mpk=(P,P_{pub},H_1,H_2)$。

①H-询问:$\mathcal{B}$ 创建 $L(ID_i,C_i,t_i,h_i)$ 并初始化为空。若 $\mathcal{B}$ 询问的身份 ID_i 在 L 中,返回 $H(ID_i)=h_i$。$\mathcal{B}$ 选取 $t_i\in\mathbf{Z}_p^*$。用 $Pr[c_i=0]=\delta$ 选择 $c_i\in\{0,1\}$,若 $c_i=0$,计算 $h_i=t_ibP$,否则计算 $h_i=t_iP$,将 (ID_i,c_i,t_i,h_i) 添加到 L 中,用 h_i 响应 $\mathcal{A}$。

②H_2-询问:$\mathcal{B}$ 创建 $L_3(Y_i,ID_i,\gamma_i)$ 并初始化为空。若 (Y_i,ID_i) 在列表 L_3 中,则返回 $H_2(Y_i,ID_i)=\gamma_i$。否则,选取 $H_2(Y_i,ID_i)=\gamma_i$,将 (Y_i,ID_i,γ_i) 添加到 L_3,使用 γ_i 响应 $\mathcal{A}$。

(2) 阶段 1。$\mathcal{B}$ 从 L 中获得 c_i 和 t_i。若 $c_i=0$,返回 $\perp$,$c_i=1$,则 $d_{ID_i}=sH_1(ID_i)=at_iP=t_iP_{pub}$。

(3) 挑战:对任意 $ID_i\in S^*$ 没有发起私钥询问,$\mathcal{A}$ 输出 M_0、M_1 和 $S^*=(ID_1,ID_2,\cdots,ID_n)$。模拟者 $\mathcal{B}$ 随机选取 $b\in\{0,1\}$ 并执行如下操作:

①选取 $ID_0\in S^*$ 和 $B_i^*\in G$,$i\in[0,n]$。

②选取 $r_1^*\in\mathbf{Z}_p$ 和 $C_0^*\in G$,计算 $C_1^*=r_1^*P$。

③从 L 中获取 $H(ID_i)$ 的值,计算 $x_i^*=H(ID_i)$,$A_i^*=k_1+H_2(e(H_1(ID_i),P_{pub})^{r_1^*},ID_i)$。构造函数 $f_i(x)=\sum_{j=0}^{n-1}a_{i,j}x^j$,$i\in[0,n]$,计算 $u_i^*=\sum_{j=1}^{n}a_{j,i}A_j^*$。定义挑战密文为 $CT^*=(C_0^*,C_1^*,r_1^*,u_i^*)$,$i\in[0,n]$。

(4) 猜测:当 $c_j=0$ 时,有 $H(ID_j)=t_jbP$ 和 $d_{ID_j}=t_jabP$,得到 $e(d_{ID_j},C_1^*)=e(P,P)^{t_jabr_1^*}$。定义 $W_i=(e(H(ID_i),P_{pub})^{r_1},ID_i)$,$ID_i\in S^*$,然后计算 $A_i^*=u+H_2(W_i)$。根据以上分析定义如下事件:

E_1:在私钥询问中模拟不会终止;E_2:挑战者身份的 H 值中至少有一个包含困难问题;E_3:攻击者 $\mathcal{A}$ 选择一个 $c_i=0$ 的标识区分挑战信息;E_4:模拟者 $\mathcal{B}$ 从 L_3 中准确地选择解决算法。因此,$Pr[E_r]=Pr[c_i=1,i=1,2,3,\cdots,q_E]=(1-\delta)^{q_E}$。攻击者得到 $Pr[E_3]=(1/n)Pr[c_i=0]+(1/n)\cdot Pr[c_i=1]=1/n$。已知困难问题的解决算法在 L_3 中,$Pr[E_4]\geqslant(q_{H_2})^{-1}$。因此 $\varepsilon'\geqslant Pr[E_1\wedge E_2\wedge E_3\wedge E_4]\cdot\varepsilon\geqslant(1-\delta)^{q_E}\cdot\delta\cdot\varepsilon\cdot(n\cdot q_{H_2})^{-1}$。函数 $(1-\delta)^{q_E}\cdot\delta$ 在 $\delta_{opt}=(q_E+1)^{-1}$ 时最大。由 δ_{opt} 得,$\varepsilon'\geqslant\varepsilon\cdot(e\cdot n\cdot q_E\cdot q_{H_2})^{-1}$。□

定理 2 定义哈希函数 H 和 H_2,若 BDH 困难问题成立,本文提出的基于身份的隐私保护性广播加密算法是 ANON-ID-CPA 安全的。若存在 ANON-ID-CPA 攻击者 $\mathcal{A}$ 以 ε 的优势攻击提出的算法,存在模拟者 $\mathcal{B}$ 以 $\varepsilon'\geqslant\varepsilon\cdot(e\cdot n\cdot q_E\cdot q_{H_2})^{-1}$ 的优势解决 BDH 困难问题,其中 q_{H_2} 是询问 H_2 的数量。

证明 H-询问,H_2-询问和阶段 1 与定理 1 中一致。游戏 2 中,$\mathcal{B}$ 与 $\mathcal{A}$ 的互动过程如下所示:

(1) 系统建立:$\mathcal{B}$ 构建 $mpk=(P,P_{pub},H_1)$。

H_2-询问:$\mathcal{B}$ 创建 $L_2(X_i,ID_i,\lambda_i)$,若 (X_i,ID_i) 询问在 L_2 中,则 $H_2(X_i,ID_i)=\lambda_i$;否则选取 $\lambda_i\in G$,将 (X_i,ID_i,λ_i) 添加到 L_1 中,用 λ_i 响应敌手 $\mathcal{A}$。

(2) 挑战:$\mathcal{A}$ 输出 M^*、$S_0=(ID_{0,1},\cdots,ID_{0,n})$ 和 $S_1=(ID_{1,1},\cdots,ID_{1,n})$。$\mathcal{B}$ 执行如下步骤:

①选择身份 $ID_i \in S_0 \triangle S_1$,$B_0^* \in G$,随机整数 $r_1^* \in \mathbf{Z}_p$ 和 $k_1^* \in G$,计算 $C_0^* = k_1^* + M^*$ 和 $C_1^* = r_1^* P$。

② $\mathcal{B}$ 从 L 中获得 c_i 和 t_i。若 $c_i = 1$,计算 $X_i = e(aP, cP)^{r_1^* t_i}$。若 (X_i, ID_i),$ID_i \in S_b \backslash S_{1-b}$ 在 L_2 中,获得 λ_i,设 $A_i^* = \lambda_i$;否则,选取 $A_i^* \in G$,将 (X_i, ID_i, A_i^*) 添加到 L_2 中,计算 $Y_i = e(aP, cP)^{t_i}$。获取 γ_i 并设 $\omega_i^* = \gamma_i$。否则,选取 $\omega_i^* \in G$,将 (Y_i, ID_i, ω_i^*) 添加到 L_3 中,计算 $A_i^* = k_1^* + \omega_i^*$。

(3) 猜测:$\mathcal{B}$ 从 L_2 中选取任意的 (X_i, ID_i, λ_i) 或从 L_3 中选取任意的 (Y_i, ID_i, γ_i)。若 $\mathcal{A}$ 选择 L_2,输出 $X_j^{(r_2^* t_j)^{-1}}$,若选择 L_3 则输出 $Y_j^{t_j^{-1}}$。由定理 1,存在 $\varepsilon \cdot (e \cdot n \cdot q_E \cdot q_{H_2})^{-1}$。 □

定理 3 定义 2 个抗碰撞的哈希函数 H 和 H_2,若 BDH 困难问题成立,提出的基于身份的隐私保护性广播加密算法是 IND-rID-CPA 安全的。若有一个 IND-rID-CPA 的攻击者 $\mathcal{A}$ 以 ε 的优势攻破算法,则 $\mathcal{B}$ 以 $\varepsilon' \geqslant \varepsilon \cdot (e \cdot n \cdot q_E \cdot q_{H_2})^{-1}$ 的优势解决 BDH 困难问题。

证明 H-询问与阶段 1 与定理 1 中的一致,H_2-询问与定理 2 中的一致。在游戏 3 中,模拟者 $\mathcal{B}$ 与攻击者 $\mathcal{A}$ 的互动过程如下所示:

(1) 系统建立:构建 $mpk = (P, P_{\text{pub}}, H_1, H_2)$。

(2) 挑战:$\mathcal{A}$ 对任意 $ID_i \in S^* \backslash R^*$ 没有发起私钥询问,输出 M_0、M_1、集合 $S^* = (ID_1, \cdots, ID_n)$ 和 $R^* = (ID_{l_1}, \cdots, ID_{l_t})$。$\mathcal{B}$ 执行以下操作:

①对任意身份 $ID_0 \notin S^* \cup R^*$,随机选取 $A_0^*, k_1^*, k_2^* \in G$ 和 $r_1^* \in \mathbf{Z}_p$,然后计算 $C_1^* = r_1^* P$ 和 $C_0'^* = C_0^* + k_2^* = k_1^* + M_b + k_2^*$。

②从 L 中获取元组 (c_i, t_i, h_i)。若 $c_i = 1$,计算 $X_i = e(aP, cP)^{t_i}$。若 (X_i, ID_i),$ID_i \in S^* \cap R^*$ 存在于 L_2 中,返回 λ_i。否则选取 $\lambda_i \in G$,定义 $A_i^* = \lambda_i$,在 L_2 中添加 (X_i, ID_i, λ_i)。

③计算 $x_i^* = H_1(ID_i)$,$ID_i \in R^*$,构造多项式函数 $g(x) = \prod_{i=1}^{t}(x - x_i^*) = \sum_{i=1}^{t} b_i x^{i-1} b \bmod p$。然后计算 $T_i^* = g(x_i)^{-1} b_i k_2^*$。定义撤销后的密文为 $CT'^* = (R, C_0'^*, C_1^*, [u_i^*, T_i^*]_{i=1}^n)$。

(3) 猜测:$\mathcal{B}$ 从 L_2 中选取 (X_j, ID_j, λ_j) 得到 t_j,输出 $X_j^{t_j^{-1}}$。若以大于 1/2 的概率输出正确的 b' 或 $\perp$,只考虑 $\mathcal{A}$ 选择 $ID_i (H(ID_i) = t_i bP)$ 的情况,则利用困难问题的输入来询问 H_2 攻击该算法。正如定理 1 所示,存在 $\varepsilon' \geqslant \varepsilon \cdot (e \cdot n \cdot q_E \cdot q_{H_2})^{-1}$。 □

定理 4 定义 2 个抗碰撞的哈希函数 H 和 H_1,若 BDH 困难问题成立,提出的基于身份的隐私保护性广播加密算法是选择性 ANON-rID-CPA 安全的。若存在选择性 ANON-rID-CPA 攻击者 $\mathcal{A}$ 以 ε 的优势攻击该算法,则存在一个模拟者 $\mathcal{B}$ 以 $\varepsilon' \geqslant \varepsilon \cdot (t \cdot q_{H_1})^{-1}$ 的优势解决 BDH 困难问题。其中 q_{H_1} 是 H_1 询问的数量。

证明 在游戏 4 中,模拟者 $\mathcal{B}$ 与攻击者 $\mathcal{A}$ 的互动过程如下所示:

(1) 初始化:攻击者 $\mathcal{A}$ 输出不同的目标撤销集合 $R_0 = (ID_{0,1}, \cdots, ID_{0,t})$ 和 $R_1 = (ID_{1,1}, \cdots, ID_{1,t})$。

(2) 系统建立:构建 $mpk = (P, P_{\text{pub}}, H_2)$。随机选取 $b \in \{0,1\}$ 和身份 $ID^* \in R_b \backslash R_{1-b}$。

①H-询问:$\mathcal{B}$ 创建 L 并初始化为空。若 ID_i 询问已存在于 L 中,返回 $H(ID_i) = h_i$,否则选取 $k_i \in \mathbf{Z}_p$。如果 $ID_i = ID^*$,令 $h_i = k_i bP$。否则,$h_i = k_i P$。

② H_1-询问:若 (T_i, ID_i) 出现在 $L_1(T_i, ID_i, \eta_i)$ 中,则 $H_1(T_i, ID_i) = \eta_i$,将 (T_i, ID_i) 添加到 L_1 中,用 η_i 响应攻击者 $\mathcal{A}$。

(3) 阶段 1:$\mathcal{A}$ 发起私钥询问;$\mathcal{B}$ 从 L 中获得 k_i,计算 $d_{ID_i} = sH_1(ID_i) = ak_i P = k_i P_{\text{pub}}$。

(4) 挑战:$\mathcal{A}$ 输出 M^* 和 $S^* = (ID_1, \cdots, ID_n)$;$\mathcal{B}$ 执行以下步骤:

①选取身份 $ID_0 \notin S^* \cup R_0 \cup R_1$ 和 k_1^*,$k_2^* \in G$,计算 $C_0^* = k_1^* + k_2^* + M_b$ 和 $C_1^* = c^* P$。

②对每个 $ID_i \in S^*$ 和 ID_0 存在 $ID_i = ID^*$,选取 $x^* \in \mathbf{Z}_p$,令 $x_i^* = x^*$。否则,计算 $T_i = e(aP, cP)^{k_i}$。选取 $\eta_i \in \mathbf{Z}_p$,设 $x_i^* = \eta_i$,将新的元组添加到 L_1 中。

③从 L 中获取 (k_i, h_i),计算 $T_i = e(aP, cP)^{k_i}$,检查是否出现 (T_i, ID_i),$ID_i \in R_0 \cap R_1$。若存在,返回 η_i;否则随机选取 $\eta_i \in \mathbf{Z}_p$,设 $x_i^* = \eta_i$,将新的 (T_i, ID_i, η_i) 添加到 L_1 中。对 $ID^* \in R_b \backslash R_{1-b}$ 选取 $x_i^* \in \mathbf{Z}_p$,计算 $g(x) = \prod_{i=1}^{t}(x - x_i^*) = \sum_{i=1}^{t} b_i x^{i-1} \bmod p$。

④计算 $T_i^* = g(x_i)^{-1} b_i k_2^*$,$i = 1, 2, \cdots, t$,定义撤销后的密文为 $CT'^* = (R, C_0'^*, C_1^*, [u_i^*, T_i^*]_{i=1}^t)$。

(5) 猜测:攻击者 $\mathcal{A}$ 输出猜测 $b' \in \{0,1\}$。若攻击者选择 ID^* 来区分撤销集合,$\mathcal{B}$ 成功地解决了 BDH 困难问题。在定理 4 的范围内,$\mathcal{A}$ 选择 ID^* 攻破算法的概率为 $(t-k)^{-1} \geqslant t^{-1}(k=|R_0 \cap R_1|)$,存在 $\varepsilon' \geqslant \varepsilon \cdot (tq_{H_1})^{-1}$。 □

5 效率及性能分析

5.1 功能特性比较

将本文提出的算法与近几年广播加密文献[8-10,12,20]中的算法进行功能性对比,对比结果如表 1 所示。

由表 1 可以看出,文献[10,20]算法与本文算法一致,皆为基于身份的加密;本文算法利用基于身份的广播加密,结合智慧城市中用户权限的变化,运用用户撤销的特性灵活管理用户身份,而其它对比算法无法达到用户撤销功能;本文算法还利用拉格朗日插值将用户身份信息嵌入密文中,实现了用户身份的匿名性,保护了接收者之间的身份隐私,文献[8,10]算法不具备保护用户身份隐私的功能。通过与表 1 中其它广播加密算法的对比表明,本文算法在功能特性上具有一定的优势。

5.2 理论分析与比较

本节从理论角度对比本文算法、文献[18,19]算法在计算量和通信量上的优劣。

(1) 计算量比较。

计算量对比结果如表 2 所示。在表 2 中,T_p 表示双线性配对运算时间,T_e 表示指数运算时间,T_m 表示乘法运算时间,T_h 表示哈希运算时间,T_{Inv} 表示乘法逆元运算时间。常用密码算法操作计算的时间顺序为 $T_p > T_e > T_m > T_h > T_{Inv}$,且 T_p 远大于其它时间。n 表示系统中用户身份的数量。

(2) 通信量比较。

通信量比较结果如表 3 所示。在表 3 中,分别用 $|G|$、$|G_T|$ 和 $|\mathbf{Z}_p|$ 表示 G、G_T 和 $\mathbf{Z}_p$ 中元素的长度。

由表 3 可以看出,在数据加密阶段,各个算法通信量由大到小依次为文献[19]算法、文献[18]算法和本文算法;在用户撤销阶段,各个算法通信量由大到小依次为文献[18]算法、文献[19]算法和本文算法;在解密阶段,各个算法通信量由大到小依次为文献[18]算法、文献[19]算法和本文算法。

5.3 数值实验与比较

数值模拟实验是在 Linux 操作系统下利用双线性对包(pairing-based cryptography library)[21]实现的,双线性对包参数类型为 Type-A。基于 C 语言进行编程,在 2.60 GHz CPU,8 GB RAM PC 机上运行。

实验对文献[18]算法、文献[19]算法和本文算

Table 1 Comparison of functional properties

表 1 功能特性比较

功能特性	文献[8]算法	文献[9]算法	文献[10]算法	文献[12]算法	文献[20]算法	本文算法
基于身份	×	×	√	×	√	√
广播加密	√	√	√	√	√	√
用户撤销	×	×	×	×	×	√
隐私保护	×	√	×	√	√	√

Table 2 Computation comparison

表 2 计算量比较

算法	数据加密	用户撤销	数据解密
本文算法	$2T_h+T_p+(n+1)T_m+T_e$	T_m+T_{Inv}	T_h+T_p
文献[18]算法	$3T_h+2T_p+2(n+1)T_m+2T_e$	T_h+T_m	$2T_h+2T_p$
文献[19]算法	$6T_h+2T_p+(2+n)T_m+3T_e$	$2T_h+T_p+T_m+T_e$	$3T_h+3T_p+T_{Inv}$

Table 3 Storage comparison

表 3 通信量比较

算法	数据加密	用户撤销	数据解密
本文算法	$(2+n)\|G_1\|+\|G_T\|+\|\mathbf{Z}_p\|$	$\|G_1\|+\|\mathbf{Z}_p\|$	$\|G_1\|+\|G_T\|+\|\mathbf{Z}_p\|$
文献[18]算法	$2(2+n)\|G_1\|+\|G_T\|+\|\mathbf{Z}_p\|$	$2\|G_1\|+(t+2)\|\mathbf{Z}_p\|$	$(2n+2)\|G_1\|+2\|G_T\|+\|\mathbf{Z}_p\|$
文献[19]算法	$10(n+1)\|G_1\|+3\|G_T\|+\|\mathbf{Z}_p\|$	$\|G_1\|+\|G_T\|+\|\mathbf{Z}_p\|$	$4\|G_1\|+3\|G_T\|+\|\mathbf{Z}_p\|$

法分别在数据加密算法、用户撤销算法和数据解密算法上的时间开销进行了对比分析。文献[18]算法、文献[19]算法和本文算法用户身份权限会发生变化,将用户身份的个数分别设置为10,20,30,40和50。实验采用50次运行结果的平均值作为实验结果,如图6所示。

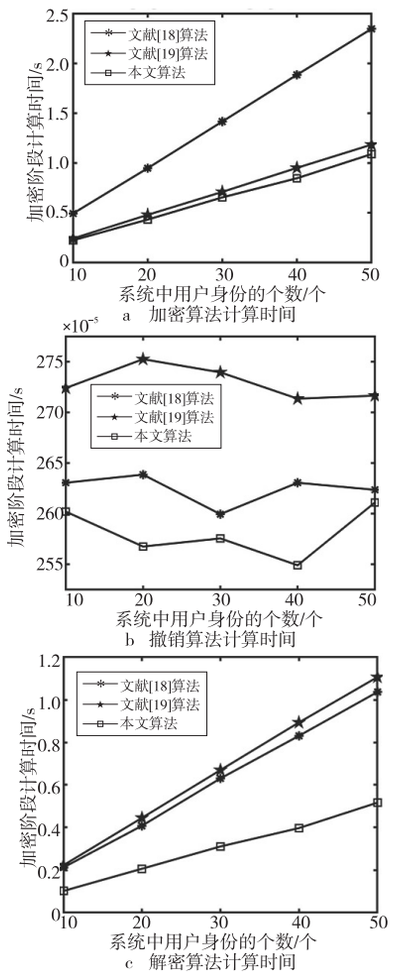

Figure 6 Relationships between time cost of algorithms and number of user identities

图6 计算时间与用户身份数量的关系

图6a表示各个算法数据加密算法的运行时间和系统中用户身份数量的关系。由表2可知,在数据加密阶段,文献[18]算法有2个配对运算,文献[19]算法有2个配对运算,本文算法有1个配对运算。由常用密码算法计算时间可知,配对运算时间远远大于其他运算时间,故本文算法加密时间小于文献[18]算法和文献[19]算法加密时间,运行效率更高。

图6b表示各个算法用户撤销算法的运行时间和系统中用户身份数量的关系。由表2可知,在用户撤销阶段,文献[18]算法没有配对运算,文献[19]算法有1个配对运算,本文算法没有配对运算,故本文算法在用户撤销阶段的计算量小于文献[18]算法和文献[19]算法。本文算法在用户撤销算法的计算量比文献[18]算法计算量少 $T_h - T_{Inv}$,比文献[19]算法计算量少 $2T_h + T_p + T_e - T_{Inv}$。

图6c表示各个算法数据解密算法的运行时间和系统中用户身份数量的关系。由表2可知,在数据解密阶段,文献[18]算法有2个配对运算,文献[19]算法有3个配对运算,本文算法有1个配对运算,故本文算法在数据解密阶段的计算量小于文献[18]算法和文献[19]算法的。总之,本文算法在运行效率和通信效率上均具有较明显的优势,提高了系统的性能。

6 结束语

本文提出一个隐私保护性广播加密算法,利用广播加密技术为多个数据用户执行授权,完成加密数据的有效广播。并在智能电网中通过用户撤销对用户身份灵活管理,实现接收者之间的匿名性。给出了详细的正确性证明、安全性证明和性能分析。数值实验结果表明,本文提出的算法具有较高的效率。在未来的工作中考虑将其应用于基于生物特征的广播代理重加密场景中,以获得更实用的价值。

参考文献:

[1] Khan Z, Kiani S L. A cloud-based architecture for citizen services in smart cities[C]//Proc of the 2012 IEEE/ACM 5th International Conference on Utility and Cloud Computing, 2012:315-320.

[2] Clohessy T, Acton T, Morgan L, et al. Smart city as a service (SCaaS): A future roadmap for E-government smart city cloud computing initiatives[C]//Proc of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014:836-841.

[3] Monzon A. Smart cities concept and challenges: Bases for the assessment of smart city projects[C]//Proc of 2015 International Conference on Smart Cities and Green ICT Systems, 2015:17-31.

[4] Zhang Yu-qing, Zhou Wei, Peng An-ni. Survey of internet of things security[J]. Journal of Research and Development, 2017, 54(10):2130-2143. (in Chinese)

[5] Xu Zhi-wei, Zeng Chen, Chao Lu, et al. Zone-oriented architecture: An architectural style for smart web of everything [J]. Journal of Research and Development, 2019, 56(1):90-102. (in Chinese)

[6] Fiat A, Naor M. Broadcast encryption[C]//Proc of the 13th Annual International Cryptology Conference, 1993:480-491.

[7] Canard S,Phan D H,Trinh V C,et al. Attribute-based broadcast encryption scheme for lightweight devices[J]. IET Information Security,2017,12(1):52-59.

[8] Sun M,Ge C,Fang L,et al. A proxy broadcast re-encryption for cloud data sharing[J]. Multimedia Tools and Applications, 2018,77(9):10455-10469.

[9] Zhang J,Mao J. Anonymous multi-receiver broadcast encryption scheme with strong security[J]. International Journal of Embedded Systems,2017,9(2):177-187.

[10] Zhang L, Hu Y, Wu Q, et al. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups[J]. Mathematical and Computer Modelling,2012,55(1):12-18.

[11] Reid B. Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city [J]. Computing Reviews,2018,59(3):186-186.

[12] Zhang M,Yang B,Chen Z,et al. Efficient and adaptively secure broadcast encryption systems[J]. Security and Communication Networks,2013,6(8):1044-1052.

[13] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers[C]//Proc of Annual International Cryptology Conference,2001:41-62.

[14] Naor M,Pinkas B. Efficient trace and revoke schemes[C]// Proc of the 4th International Conference on Financial Cryptography,2000:1-20.

[15] Li Qiang,Feng Deng-guo,Zhang Li-wu. Attribute-based authenticated key agreement protocol supporting revocation [J]. Journal of Communications, 2014, 35(5): 33-43. (in Chinese)

[16] Wang Peng-pian, Feng Deng-guo, Zhang Li-wu. CP-ABE scheme supporting fully fine-grained attribute revocation [J]. Journal of Software, 2012, 23(10): 2805-2816. (in Chinese)

[17] Zhang Bing-hong,Zhang Chuan-rong,Jiao He-ping,et al. Secure model of cloud storage supporting attribute revocation [J]. Computer Science,2015,42(7):210-215. (in Chinese)

[18] Lai J,Mu Y,Guo F,et al. Anonymous identity-based broadcast encryption with revocation for file sharing[C]//Proc of Australasian Conference on Information Security and Privacy,2016:223-239.

[19] Lai J C,Mu Y,Guo F C,et al. Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city[J]. Personal and Ubiquitous Computing, 2017,21(5):855-868.

[20] Zhang L Y, Wu Q, Mu Y. Anonymous identity-based broadcast encryption with adaptive security[C]//Proc of International Symposium on Cyberspace Safety and Security, 2013:258-271.

[21] The pairing-based cryptography library[EB/OL]. [2020-11-12]. http://crypto.stanford.edu/pbc/.

附中文参考文献:

[4] 张玉清,周威,彭安妮. 物联网安全综述[J]. 计算机研究与发展,2017,54(10):2130-2143.

[5] 徐志伟,曾琛,朝鲁,等. 面向控域的体系结构:一种智能万物互联的体系结构风格[J]. 计算机研究与发展,2019,56(1):90-102.

[15] 李强,冯登国,张立武. 支持用户撤销的属性认证密钥协商协议[J]. 通信学报,2014,35(5):33-43.

[16] 王鹏翩,冯登国,张立武. 一种支持完全细粒度属性撤销的CP-ABE方案[J]. 软件学报,2012,23(10):2805-2816.

[17] 张柄虹,张串绒,焦和平,等. 一种属性可撤销的安全云存储模型[J]. 计算机科学,2015,42(7):210-215.

作者简介:

牛淑芬(1976-),女,甘肃兰州人,博士,副教授,研究方向为云计算、大数据网络的隐私保护和区块链。**E-mail**:sfniu76@nwnu.edu.cn

NIU Shu-fen,born in 1976,PhD,associate professor,her research interest includes cloud computing,privacy protection for big data networks, and blockchain.

方丽芝(1993-),女,甘肃张掖人,硕士生,研究方向为密码学。**E-mail**:1439902640@qq.com

FANG Li-zhi,born in 1993,MS candidate,her research interest includes cryptography.

宋蜜(1996-),女,河南南阳人,硕士生,研究方向为密码学。**E-mail**:1744391811@qq.com

SONG Mi, born in 1996, MS candidate,her research interest includes cryptography.

王彩芬(1963-),女,河北安国人,博士,教授,研究方向为密码学和信息安全。**E-mail**:wangcf@nwnu.edu.cn

WANG Cai-fen, born in 1963, PhD, professor, her research interests include cryptography, and information security.

杜小妮(1972-),女,甘肃庆阳人,博士,教授,研究方向为对称密码和编码理论。**E-mail**:ymldxn@126.com

DU Xiao-ni,born in 1972,PhD,professor,her research interests include symmetric cryptography, and coding theory.