文章编号:1671-4229(2022)04-0053-15

公钥广播加密研究综述

崔 岩[1],黄欣沂[2*],赖建昌[3],宁建廷[1]
(1. 福建师范大学 计算机与网络空间安全学院,福建 福州 350117;
2. 香港科技大学(广州),广东 广州 511400;3. 东南大学 网络空间安全学院,江苏 南京 211189)

摘 要:近年来,随着网络带宽的不断增加,大数据、云计算、外包计算等新兴应用得到飞速发展,同时也带来了更多的安全挑战,传统的点对点安全传输已无法满足错综复杂的网络环境,一对多安全传输变得极为重要。广播加密允许数据拥有者向一组选定的接收者安全分享数据,仅需运行一次加密算法并将密文发布到广播信道,监听此信道的授权用户均可解密获取明文,未授权用户即使合谋也无法正确解密,极大地减少了计算和通信开销。公钥广播加密相比于对称广播加密具有灵活性高、应用范围广等优点,近年来受到广泛关注。文章回顾了公钥广播加密的相关研究历史,从公钥广播加密的应用场景出发,重点介绍了公钥广播加密的系统模型和典型方案,包括标识广播加密、匿名广播加密、叛逆者追踪广播加密和可撤销广播加密,并阐述了各类公钥广播加密的原理和特征。最后,讨论了公钥广播加密的应用场景和未来的研究方向,旨在促进公钥广播加密的研究与发展。

关键词:广播加密;公钥密码;标识密码;匿名性;可追踪性;可撤销性
中图分类号:TP 309.7 **文献标志码**:A

A survey on public-key broadcast encryption

CUI Yan[1], *HUANG Xin-yi*[2*], *LAI Jian-chang*[3], *NING Jian-ting*[1]
(1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China;
2. The Hong Kong University of Science and Technology, Guangzhou 511400, China;
3. School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China)

Abstract: Recently, with the increasing of network bandwidth, emerging applications such as big data, cloud computing and outsourcing computing are growing rapidly. At the same time, it brings more security challenges. Traditional point-to-point secure transmission cannot satisfy the requirement of network, and one to many secure transmission has become extremely important. Broadcast encryption allows a data owner to securely share the same data with a group of selected users by running the encryption algorithm once and publishing the ciphertext to a public broadcast channel. All authorized users listening to the channel can decrypt the ciphertext successfully and unauthorized users cannot learn the plaintext even if they collude. Broadcast encryption greatly reduces computational and communication overheads. Compared with symmetric broadcast encryption, public key broadcast encryption has the advantage of flexibility and has received widespread attention in recent years. This paper examines public key broadcast encryption comprehensively. We begin with the application scenarios of public key broadcast encryption and focus on system models and typical schemes including identity-based

收稿日期:2022-09-30;**修回日期**:2022-10-09
基金项目:国家自然科学基金资助项目(62032005,U21A20466,61902191,61972094);福建省自然科学基金资助项目(2020J02016);福建省科协第二届青年人才托举工程资助项目
作者简介:崔岩(1997—),男,硕士研究生. E-mail:crocky829@gmail.com
*通信作者. E-mail:xyhuang81@gmail.com
引文格式:崔岩,黄欣沂,赖建昌,等. 公钥广播加密研究综述[J]. 广州大学学报(自然科学版),2022,21(4):53-67.

broadcast encryption, anonymous broadcast encryption, traitor tracing broadcast encryption, and revocable broadcast encryption. We also show how they work and the characteristics of various schemes. Finally, the application scenarios and future research directions are given, which aim to promote the research of public key broadcast encryption.

Key words: broadcast encryption; public key cryptography; identity-based cryptography; anonymity; traceability; revocability

广播加密的概念由 Fiat 等[1]提出,假设 Alice 想要向大量接收者发送相同的消息,若采用多次执行加密算法并将密文依次发送给接收者的方法,虽然可实现一对多加密,但加密和解密的计算代价高昂且通信代价随着接收者的数量增加而线性增加。随着付费直播、数字产品、在线会议的迅速发展,点对点的加密方式已经逐渐不能满足互联网环境的通信需求,亟需一对多或多对多的安全通信方式。

广播加密是一种支持在不安全的公开信道上实现多用户数据安全共享的加密技术,适用于一对多安全传输场景。广播加密的工作方式为:数据拥有者首先选取一组接收者,运行广播加密算法,将加密得到的密文发布到公开信道,监听该信道的所有用户均可获取密文,但只有授权用户可利用解密密钥正确解密,未授权用户不能从密文中获取任何明文信息。广播加密在付费电视、数字版权保护及区块链等领域广泛使用。

根据加密和解密过程中密钥的不同,广播加密可分为对称广播加密和公钥广播加密。在对称广播加密中,广播者只能是可信机构,该机构负责生成并分发已授权用户的解密密钥,因此,对称广播加密在实际应用中局限性较大,应用范围窄。公钥广播加密允许系统内任意用户作为数据拥有者,且数据拥有者可指定任意系统内一个用户集合作为数据接收者,只有集合内的用户可以解密。由于系统中任意用户均可作为发送者运行加密算法,更具一般性且灵活。因此,公钥广播加密具有更加广泛的应用,得到了专家学者的广泛关注和研究。

公钥广播加密为多用户数据安全共享的典型方法技术,其研究方向主要可概括为2个方向:

(1)根据广播加密的应用场景需求不同或功能不同,可分为标识广播加密、匿名广播加密、叛逆者追踪广播加密,以及可撤销广播加密等;

(2)从算法本身对广播加密方案进行优化,可分为2类:①对算法安全性的研究,例如选择密文攻击、自适应安全性等;②对算法效率的研究,包括加密和解密算法的时间复杂度、公共参数大小、私钥长度以及密文长度等。

评估广播加密方案的优劣通常从方案满足的安全属性、方案的计算和通信代价进行分析。一个健壮的广播加密系统应满足如下安全属性:

(1)权限控制:系统用户的添加或删除由可信中心执行,用户的解密权限由加密者(数据拥有者)决定。

(2)抗合谋攻击:任何数量的非授权接收者即使合谋都无法解密获取加密数据的内容。

(3)接收者无状态:在系统的整个生命周期内接收者无需改变自己的设置,解密操作只能按照系统初始设置进行。

Wong 等[2]于2000年基于逻辑层次树结构提出了组播密钥管理方案,该方案也称为有状态广播加密。在该系统中,接收者需利用接收到的组密钥解密广播密文。若组内成员发生变化,即有成员新加入系统或离开系统,为保证系统安全性,所有用户的组密钥必须更新;若利用该方案实现无状态广播加密,则通信代价和计算开销极高,且可信中心知道每个接收者的信息,无法实现匿名等功能,灵活性较差。因此,本文不考虑该类型的广播加密。

另一种广播加密称为静态广播加密[3],该机制需要在系统建立阶段确定接收者集合,每个用户的私钥生成都与其他所有授权接收者的公钥相关,应用场景较为有限,本文同样不考虑该类型的广播加密。

本文着重关注近年来公钥广播加密的研究进展,阐述了公钥广播加密的研究历史、形式化定义和典型构造,旨在推动广播加密的研究与发展。

1 基于PKI的广播加密

一对多加密传输最早由 Berkovits[4]提出,在文献[4]中,利用拉格朗日插值,可将任意秘密分享方案转换成秘密广播方案。随后 Fiat 等[1]在1993年提出"广播加密"的概念并给出了广播加密的形式化定义和安全模型,同时给出了对称广播加密方案的具体构造。

然而由于对称广播加密的局限性较大,近年来对广播加密的研究主要围绕公钥广播加密展开。公钥广播

加密(Public Key Broadcast Encryption, PKBE)的概念由 Naor 等[5]首次提出,传统公钥广播加密方案通常为基于证书的密码方案,为确保用户公钥的真实有效性,公钥基础设施(Public Key Infrastructure, PKI)应运而生。PKI 中通常包含一个证书认证机构(Certificate Authority, CA),负责为用户签发证书。文献[5]中的方案利用门限秘密共享技术,实现了有效叛逆者追踪,最多撤销 t 个用户的解密权限,满足 t - 抗合谋攻击的安全性。

1.1　公钥广播加密定义

公钥广播加密包括 3 个过程:

(1)Setup(λ,n):输入安全参数 λ,广播接收者人数 n,输出 n 个私钥 $k_1,k_2,\cdots,k_n$ 和一个公钥 PK。

(2)Encrypt (S,PK):以授权接收者集合 $S\in\{1,2,\cdots,n\}$ 和公钥 PK 为输入,输出二元组(Hdr,K),其中,Hdr 称为首部;K 为加密密钥,用于加密广播内容。已知广播消息为 M,利用会话密钥 K 加密消息 M 得到密文 C_M,则整个广播内容为(S,Hdr,C_M),其中,(S,Hdr)通常称为广播头,C_M 称为广播体。

(3)Decrypt (S,i,k_i,Hdr,PK):输入接收者集合 $S\in\{1,2,\cdots,n\}$,用户 i 和对应的私钥 k_i,首部 Hdr 和公钥 PK。若 $i\in S$,则算法可正确输出会话密钥 K,进而解密 C_M 得到消息 M,否则不能获取明文信息。

基于 PKI 的广播加密的正确性要求对任意的消息 M,(PK,($k_1,\cdots,k_n$))←Setup(λ,n),(Hdr,K)←Encrypt(S,PK)。若 $i\in S$,那么

$\Pr[\text{Decrypt}(S,i,k_i,Hdr,PK)=M]=1$。

1.2　公钥广播加密安全模型

在广播加密的安全模型中,根据敌手的攻击能力不同可将敌手分为自适应敌手和静态敌手。静态敌手要求在发起攻击之前给出要攻击的接收者集合。显然,自适应敌手具有更强的攻击能力,敌手无需在攻击前选取待攻击的接收者集合。因此,自适应敌手模型比静态敌手模型安全性更强。

广播加密最基本的要求是保证数据的机密性,即非授权用户不能获取任何明文信息。针对数据的机密性,下面给出自适应选择密文攻击下的不可区分性(Indistinguishability against Adaptive Chosen-Ciphertext Attacks, IND-CCA)[6],通过敌手和挑战者的交互游戏定义,安全模型定义如下:

(1)系统建立。挑战者C运行 Setup(n)算法得到 n 个私钥 $k_1,k_2,\cdots,k_n$ 和一个公钥 PK,秘密保存私钥,将公钥 PK 发送给敌手$\mathcal{A}$。

(2)询问阶段 1。敌手允许在该阶段自适应地发起如下询问:

a. 私钥询问:敌手可自适应地询问集合中第 u 个位置的私钥,挑战者将 k_u 发送给敌手;

b. 解密询问:敌手可针对密文发起解密询问,询问的格式为 (u, S, Hdr),挑战者运行算法 Decrypt(S,u,k_u,Hdr,PK),将解密结果 K 返回给敌手。

(3)挑战阶段。敌手输出挑战接收者集合 S^*,要求敌手没有发起过对 $u\in S^*$ 的私钥询问。挑战者运行加密算法 Encrypt(S^*,PK),输出二元组(Hdr^*,K)。接着挑战者随机选取 1 比特 $b\in\{0,1\}$,令 $K_b=K$,从密钥空间中选取随机密钥 $K'\in K$,令 $K_{1-b}=K'$,最后将(Hdr^*,K_0,K_1)发送给敌手。

(4)询问阶段 2。敌手可在该阶段继续发起私钥询问和解密询问,询问的限制是不能询问 $u\in S^*$ 的私钥,不能发起 $Hdr=Hdr^*$,$S=S^*$ 的解密询问。挑战者的回复方式与询问阶段 1 相同。

(5)猜测。敌手输出猜测值 $b'\in\{0,1\}$,若 $b=b'$,则敌手获胜。

定义敌手 A 获胜的优势 Adv_A^{PKBE} 为

$$\text{Adv}_A^{PKBE}(\lambda,n)=\left|\Pr[b=b']-\frac{1}{2}\right|。$$

定义 1(可忽略)　令 $|\mathbb{N}|$为自然数集合,对于任意 $d\in\mathbb{N}$,若存在 $\lambda_d\in\mathbb{N}$,使得对于任意 $\lambda>\lambda_d$,$\varepsilon(\lambda)\leqslant\lambda^{-d}$始终成立,那么函数 $\varepsilon:\mathbb{N}\to[0,1]$称为可忽略函数。

定义 2　如果对于任意的多项式时间(Probabilistic Polynomial Time, PPT)敌手,在上述游戏中获胜的优势是可忽略的,则称广播加密方案是 IND-CCA 安全的。

若在上述 IND-CCA 模型中,不允许敌手在询问阶段发起密钥询问,则相应的模型为 IND-CPA 模型。

广播加密与传统点对点的公钥加密在 IND-CCA 安全模型的不同点主要体现在:前者要求在系统建立阶段,挑战者需要将所有用户的公钥信息发送给敌手,敌手可在询问阶段自适应的发起密钥询问。在挑战阶段,敌手可根据已掌握的信息选取接收者集合进行攻击;后者在系统建立阶段只需要向敌手发送挑战用户的公钥信息即可。

1.3　公钥广播加密研究现状

在 2002 年,Dodis 等[7]对基于对称密钥的广播加密和公钥广播加密展开进一步研究,将对称广播加密中的子集差分法(Subset Difference, SD)拓展到公钥体制广播加密,给出一种对称广播加密向公钥广播加密的转化关系,提出具有定长公钥的公钥广播加密方案。

2005 年,Boneh 等[6]利用双线性对技术提出首个完

全抗合谋攻击(fully collusion resistant)的无状态公钥广播加密方案(简称BGW方案),文献[6]中给出了两种PKBE构造方案,第一个构造中具有定长的密文长度,公钥长度和解密代价均随着接收者线性增长,能够抵抗选择明文攻击(Chosen Plaintext Attack, CPA);第二个构造具有亚线性大小的密文长度和公钥长度。并利用相同的参数给出一种可抵抗选择密文攻击的方案。

Delerablée等[8]在2007年提出了动态广播加密的概念,在系统建立阶段用户总数不是固定的,系统参数的生成也无需用到接收者的公钥信息,新用户可随时加入广播系统,并获取之前公布的广播消息,且无需修改其他用户的私钥。该方案适用于付费电视等应用,当新用户想观看之前的直播回放时,即可利用自己的私钥解密。

Gentry等[9]在2009年提出具有抵抗自适应性选择明文攻击安全的广播加密方案,安全性基于判定性BDHE(Bilinear Diffie-Hellman Exponent)假设。文献[9]中引入半静态(semi-static)敌手模型的概念,在半静态模型中,敌手在系统建立阶段之前要提交一个集合S,在挑战阶段可以选取集合S的任意子集S'作为攻击目标。该模型比静态敌手模型具有更强的灵活性,在静态模型中敌手只能攻击集合S。

在2012年,Phan等[10]基于文献[6]的CPA方案,提出了一个定长密文的公钥广播加密方案,可抵抗静态选择密文敌手攻击,其公钥长度在BGW方案的基础上增加一个群元素。文献[10]还提出了一个具有撤销功能的广播加密方案,与第一个方案采用同样的参数,安全性基于较为普遍的BDH(Bilinear Diffie-Hellman)困难假设。

2018年,Gay等[11]在文献[6]的基础上做了进一步研究,指出文献[6]的两点局限性:①BGW方案不能抵抗自适应敌手,敌手可根据获取到的公共参数后选择容易发起攻击的用户;②BGW方案的安全性依赖参数化假设(parameterized assumptions),即q-type的安全性假设,其安全性较弱。文献[11]提出一种更安全高效的公钥广播加密方案,实现了固定大小的密文和用户私钥,且满足自适应安全性。

1.4 典型方案回顾

在文献[6]中提出的两个公钥广播加密方案,均具有完全抗合谋的安全特性。其中,第一个方案(简称BGW1)计算代价较低,而通信代价过高,当接收者数量为n时,系统公钥长度为$2n+1$,难以应用于大规模网络;第二个方案(简称BGW2)中牺牲了部分计算量,获得更短的公钥长度。

BGW2为公钥广播加密的典型构造,后续大量公钥广播加密的研究均基于该方案[10-11],因此,本小节给出该方案的具体构造,方案描述如下:

已知接收者集合为$\{u_1,u_2,\cdots,u_n\}$,将n个用户进行分组,首先确定每个分组的最大接收者数量为$B(B<n)$,将n个用户分为A组,每组可看作独立的广播分组,分组内共享公钥$\{g,g_1,\cdots,g_B,g_{B-2},\cdots,g_{2B}\}$。方案由以下3个多项式时间算法构成。

(1)Setup(λ,n):输入安全参数λ,系统接收者数量n,令$A=\lceil n/B\rceil$。G是阶为素数p的双线性群,随机选取生成元$g\in G$和一个随机数$\alpha\in\mathbb{Z}_p$。对于任意$i=1,2,\cdots,B,B+2,\cdots,2B$,计算$g_i=g^{\alpha^i}$。接着随机选取$A$个群元素$\gamma_1,\gamma_2,\cdots,\gamma_A\in\mathbb{Z}_p$,设$v_1=g^{\gamma_1},\cdots,v_A=g^{\gamma_A}\in G$,将系统公钥设置为

$$PK=(g,g_1,\cdots,g_B,g_{B+2},\cdots,g_{2B},v_1,\cdots,v_A)\in G^{2B+A}。$$

对于每个用户$i\in\{1,\cdots,n\}$的私钥k_i,计算过程如下:设$i=(a-1)B+b$,其中,$a=\lceil i/B\rceil(1\leqslant a\leqslant A)$,$b=i\bmod B(1\leqslant b\leqslant B)$,用户$i$的私钥$k_i=g_b^{\gamma_a}\in G$,即$k_i=v_a^{(\alpha^b)}$。最后将私钥通过安全信道分发给所有接收者。

(2)Encrypt(PK,S):对于任意$l=1,\cdots,A$,定义子集$\hat{S}_l$和S_l为

$$\hat{S}_l=S\cap\{(l-1)B+1,\cdots,lB\},$$

$$S_l=\{x-lB+B\mid x\in\hat{S}_l\}\subseteq\{1,\cdots,B\}。$$

接着,随机选取$t\in\mathbb{Z}_p$,设会话密钥为$K=e(g_{B+1},g)^t\in G$,其中,$e(g_{B+1},g)$可通过$e(g_n,g)$获得。最后,输出(Hdr,K),其中,$Hdr=(C_0,C_1,\cdots,C_A)\in G^{A+1}$,$C_0=g^t$,$C_1=\left(v_1\cdot\prod_{j\in S_1}g_{B+1-j}\right)^t,\cdots,C_A=\left(v_A\cdot\prod_{j\in S_A}g_{B+1-j}\right)^t$。

(3)Decrypt(S,i,k_i,Hdr,PK):输入接收者集合S、用户下标i、用户私钥k_i、密文首部Hdr和系统公钥PK,其中,$i=(a-1)B+b$,若用户为合法接收者,则可以通过利用获得的私钥k_i计算出

$$K=e(g_b,C_a)\Big/e\left(k_i\cdot\prod_{j\in S_a,j\neq b}g_{B+1-j+b},C_0\right)。$$

正确性分析:对于合法接收者u_{ij},通过输入k_{ij},有如下等式成立:

$$\begin{aligned}K&=e(g_b,C_a)\Big/e\left(k_i\cdot\prod_{j\in S_a,j\neq b}g_{B+1-j+b},C_0\right)=\\&e(g_b,g_{B+1-b}^t)\cdot e\left(g_b,\left(v_a\cdot\prod_{j\in S_a,j\neq b}g_{B+1-j}\right)^t\right)\Big/\\&e\left(v_a^{(\alpha^b)}\cdot\prod_{j\in S_a,j\neq b}g_{B+1-j+b},g^t\right)=\\&e(g_b,g_{B+1-b}^t)\cdot e\left(g_b,\left(v_a\cdot\prod_{j\in S_a,j\neq b}g_{B+1-j}\right)^t\right)\Big/\end{aligned}$$

$e\left(v_a \cdot \prod_{j \in S_x, j \neq b} g_{B+1-j}^{(a^b)} g^t\right) =$
$e(g_{B+1}, g)^t$。

2　标识广播加密

在公钥密码体制的实际应用过程中,用户公钥为一串毫无意义的字符串,不便于记忆,对用户并不友好。为保证用户公钥的有效性,需通过证书绑定用户,而证书的引入增加了额外的存储和验证开销。标识密码体制[12]可有效解决公钥密码中加密存在的证书问题,消除了对证书的依赖,用户的公钥可由能够唯一标识用户身份信息的字符串组成,如邮箱地址、手机号码等,使用上述字符串具有便于用户记忆的优点。

随着双线性对实用且安全算法[13]的提出,标识广播加密(Identity-Based Broadcast Encryption, IBBE)也得到了广泛研究。IBBE 也称为基于身份的广播加密,系统中的密钥生成中心负责为新加入系统的用户生成并分发用户私钥。

标识广播加密是公钥广播加密的一种特例,用户的私钥由额外的可信第三方生成。标识广播加密工作流程如图 1 所示。

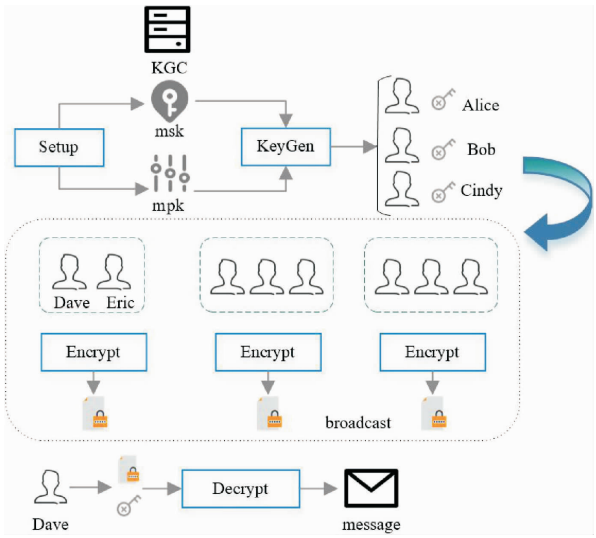

图 1　标识广播加密工作流程

Fig. 1　The workflow of identity-based broadcast encryption

由图 1 可知,密钥生成中心(Key Generator Center, KGC)首先运行 Setup 算法生成主密钥 msk 和主公钥 mpk,接着运行 KeyGen 算法生成用户私钥,系统中的任意用户均可选择任意接收者集合运行加密算法 Encrypt 并发布广播密文。在图 1 中,Alice 可向 Dave 和 Eric 发送加密消息,授权接收者 Dave 可利用自己的用户私钥解密广播密文进而获取数据。

2.1　标识广播加密定义

IBBE 方案由以下 4 个可在多项式时间内计算出的算法组成:

(1)Setup$(1^\lambda, m) \rightarrow (mpk, msk)$:输入安全参数 λ 和系统可容纳的最大接收者个数 m,KGC 运行 Setup 算法,输出系统主私钥 msk、系统主公钥 mpk。系统主私钥由 KGC 秘密保存,系统主公钥公开。

(2)KeyGen$(mpk, msk, ID) \rightarrow sk_{ID}$:输入系统主公钥 mpk,主私钥 msk,用户标识 ID,KGC 运行 KeyGen 算法生成用户私钥 sk_{ID}。

(3)Encrypt$(mpk, S, M) \rightarrow CT$:输入系统主公钥 mpk、接收者标识集合 $S = (ID_1, ID_2, \cdots, ID_n)$ 和待加密消息 M,其中,$n \leqslant m$,加密者运行加密算法 Encrypt,输出密文 CT 并通过公开信道广播。

(4)Decrypt$(mpk, S, CT, ID, sk_{ID}) \rightarrow (M/\perp)$:输入系统主公钥 mpk、接收者身份集合 S、密文 CT、接收者标识 ID 以及对应的私钥 sk_{ID},解密者运行解密算法 Decrypt,输出正确的明文数据 M 或者 $\perp$ 代表解密失败。

标识广播加密的正确性要求对任意的消息 M,$(mpk, msk) \leftarrow$Setup$(1^\lambda, m)$,$sk_{ID} \leftarrow$KeyGen(mpk, msk, ID),$CT \leftarrow$Encrypt(mpk, S, M)。若 $ID \in S$,那么

$$\Pr[\text{Decrypt}(mpk, S, CT, ID, sk_{ID}) = M] = 1。$$

2.2　安全模型

IBBE 的安全模型与 PKBE 的安全模型相似,主要区别体现在私钥询问阶段,敌手可发起对任意身份 ID 的私钥询问,但不能询问挑战标识 ID^* 的私钥,挑战者运行 KeyGen(mpk, msk, ID)算法并将产生的密钥发送给敌手[14]。

2.3　标识广播加密研究现状

Sakai 等[14]在 2007 年提出了标识广播加密,可利用任意字符串作为接收者的公钥,避免了对公钥基础设施的依赖。在通信代价方面,该方案优于 BGW 方案,其公钥大小与最大接收者数量有关,适用于潜在用户数量较多,而实际接收者数量比较少时且接收者不会经常发生变化的场景;在安全性方面,该方案满足完全抗合谋攻击,基于随机谕言模型证明了方案满足 CPA 安全。

同年,Delerablée[15]提出具有定长密文和私钥的 IBBE 方案,文献[15]利用多接收者密钥封装(multi-receiver Key Encapsulation Mechanism, mKEM)[16]机制,mKEM 是一种高效的多用户密钥协商技术,与多接收者公钥加密[17-18]不同,文献[17-18]为一个发送者向多个接收者发送不同的消息。文献[16,19]中将多接收者

密钥封装的概念扩展到标识多接收者密钥封装(multi-receiver Identity-based Key Encapsulation Mechanism, mID-KEM)。

Boneh 等[20]为构造标识广播加密提供了通用的构造方案,并使用分层标识加密技术构造了首个具有短密文的分层标识广播加密方案,密文由 3 个元素组成,私钥长度随系统的复杂性线性增长。

刘潇等[21]基于文献[15],通过在广播接收者集合中引入虚拟标识,构造了一个具有静态(selective)选择密文安全(Chosen Ciphertext Attack, CCA)的标识广播加密方案,与文献[15]相比,公钥长度增加一个群元素。在加密过程中,增加了与接收者集合相关群元素的哈希值计算过程,解密过程中也增加了对该哈希值的计算,可利用该部分的内部关联特性检验广播密文是否有效。

Kim 等[22]利用混合阶群下的对偶加密(dual system encryption)技术提出一个自适应(adaptive)选择密文安全的标识广播加密方案,该方案的系统公钥和用户私钥均随着最大接收者个数线性增长,密文长度为定长。

文献[23]把内积加密技术融合到广播加密系统中,提出内积型标识广播加密方案,解密结果不在是明文,而是与用户私钥和明文关联的内积值,可用于数理统计等应用场景。

赖建昌等[24]结合 SM9 商用标识密码的特点,提出了首个基于 SM9 的标识广播加密方案,在 SM9 标识加密算法的基础上,密文长度仅增加一个群元素,并采用与 SM9 标识加密算法相同的密钥生成算法。

Yao 等[25]也对内积型广播加密进行了深入研究,考虑到广播加密接收者的身份隐私,提出了具有匿名性质的基于证书的内积广播加密,同时证明了该方案在 IND-CCA 安全模型下是自适应安全的,密文长度随着接收者数量线性增长。Liu 等[26]针对云场景中重复数据的删除进行研究,利用广播加密技术提出了一种无需独立密钥管理服务器的客户端重复数据删除协议。

2.4 典型方案回顾

在 Delerablée[15]提出的方案中,系统公钥长度与系统可容纳最大接收者个数成线性关系,密文长度为固定长度。后续具有定长密文的 IBBE 方案大多采取该方案的构造技术,方案的具体描述如下:

(1)Setup(λ,m):输入系统安全参数 λ 和系统可容纳最大接收者个数 m,选取双线性群 $BP=(p,G_1,G_2,G_T,e(\cdot,\cdot))$,其中 $|p|=\lambda$。随机选取群 G_1,G_2 的生成元 $g\in G_1$,$h\in G_2$ 以及一个随机数 $\gamma\in\mathbb{Z}_p^*$,计算 $w=g^{\gamma}$,$v=e(g,h)$ 作为主私钥。接着选取哈希函数 $H:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$,系统公钥设为 $PK=(w,v,h,h^{\gamma},\cdots,h^{\gamma^m})$,系统私钥设为 $MSK=(g,\gamma)$;

(2)Extract(MSK,ID):已知系统私钥 $MSK=(g,\gamma)$,用户标识为 ID,KGC 计算用户私钥 $SK_{ID}=g^{\frac{1}{\gamma+H(ID)}}$。

(3)Encrypt(S,PK):已知接收者标识集合为 $S=\{ID_1,ID_2,\cdots,ID_n\}$ $(n\leqslant m)$,加密者选取随机数 $k\in\mathbb{Z}_p^*$,计算 $C_1=w^{-k}$,$C_2=h^{k\cdot\prod_{i=1}^{n}(\gamma+H(ID_i))}$,$K=v^k$。$K$ 为用来加密明文的会话密钥,(C_1,C_2) 为封装密文,最后输出密文首部 $Hdr=(C_1,C_2)$。

(4)Decrypt(S,ID_i,SK_{ID_i},Hdr,PK):输入由广播信道获取的密文首部 $Hdr=(C_1,C_2)$,接收者标识集合 S,用户自身的标识 ID_i 和标识对应的私钥 SK_{ID_i} 以及公钥 PK。首先计算

$$K=(e(C_1,h^{p_{i,n}(\gamma)})\cdot e(SK_{ID_i},C_2))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_j)}},$$

其中,

$$p_{i,n}=\frac{1}{\gamma}\cdot\Big(\prod_{j=1,j\neq i}^{n}(\gamma+H(ID_k))-\prod_{j=1,j\neq i}^{n}H(ID_j)\Big).$$

方案的正确性分析如下:

若 $ID_i\in S$,则

$$\begin{aligned}T&=(e(C_1,h^{p_{i,n}(\gamma)})\cdot e(SK_{ID_i},C_2))=\\&e(g^{-k\cdot\gamma},h^{p_{i,n}(\gamma)})\cdot e(g^{\frac{1}{\gamma+H(ID_i)}},h^{k\cdot\prod_{j=1}^{n}(\gamma+H(ID_j))})=\\&e(g,h)^{-k\cdot(\prod_{j=1,j\neq i}^{n}(\gamma+H(ID_j))-\prod_{j=1,j\neq i}^{n}H(ID_j))}\cdot\\&e(g,h)^{k\cdot\prod_{j=1,j\neq i}^{n}(\gamma+H(ID_j))}=\\&e(g,h)^{k\cdot\prod_{j=1,j\neq i}^{n}H(ID_j)}=\\&K^{\prod_{j=1,j\neq i}^{n}H(ID_j)},\end{aligned}$$

因此,$T^{\frac{1}{\prod_{j=1,j\neq i}^{n}H(ID_j)}}=K$。

3 匿名广播加密

由广播加密的定义可知,在解密过程中,每个用户需要输入密文 CT,接收者集合 S,自己的私钥 sk_{ID} 和主公钥 mpk,所有接收者信息也作为广播密文的一部分传输,这种设置将造成严重的隐私泄露问题。假设在付费电视中使用的是上述不提供匿名性的广播加密,授权用户集合为某个频道所有付费用户的集合,那么用户必须知道所有购买该频道的用户才能解密,该做法侵犯了消费者隐私,在实际部署中极为不便。

然而在当今互联网环境,保护用户的隐私至关重要,密码学几个重要研究领域都依赖匿名性,例如数字签名中的群签名和匿名凭证。在很多广播场景中,授权用户的身份信息和广播消息本身同样是敏感内容。理想情况下,广播加密方案应确保密文不会泄露任何接收

者集合的任何信息,进而保护接收者的隐私。

3.1　匿名广播加密定义

匿名广播加密的形式化定义与 IBBE 类似,区别在于匿名广播加密在解密阶段无需输入接收者集合。

3.2　匿名广播加密安全模型

匿名广播加密不仅需要保证消息的机密性,还要保证接收者的匿名性。接收者的匿名性由选择密文攻击下的用户集合不可区分性(Anonymous indistinguishability under Chosen-Ciphertext Attacks, ANON-CCA)[27] 来定义,该交互游戏确保敌手无法区分由两个不同接收者集合生成的密文。

(1)系统建立阶段

已知安全参数 λ 和系统可容纳的最大接收者个数 m,挑战者运行 Setup$(1^{\lambda},m)$算法,输出主公钥 mpk 及主私钥 msk,将 mpk 发送给$\mathcal{A}$。

(2)询问阶段 1

敌手允许在该阶段自适应地发起如下询问:

a. 私钥询问:输入标识 ID,挑战者运行算法 KeyGen$(mpk,msk,ID)\rightarrow sk_{ID}$,将结果发送给敌手;

b. 解密询问:输入标识 ID 和密文 CT,挑战者运行解密算法 Decrypt$(mpk,S,CT,ID,sk_{ID})\rightarrow M$,将解密得到的消息 M 返回给敌手。

(3)挑战阶段

当$\mathcal{A}$决定询问阶段 1 结束,敌手将挑战消息 M^* 和 2 个不同的标识集合 S_0,S_1 发送给挑战者。要求 $|S_0|=|S_1|$且 A 没有发起过对标识 $ID\in S_0\triangle S_1$ 的私钥询问,其中,$S_0\triangle S_1$ 表示$(S_0\cup S_1)-(S_0\cap S_1)$。挑战者随机选取比特 $c\in\{0,1\}$,运行 Encrypt(mpk,S_c,M^*)算法,输出密文 CT^*,将 CT^* 发送给敌手。

(4)询问阶段 2

$\mathcal{A}$允许在该阶段继续进行私钥生成询问和解密询问,挑战者回复询问的方式与询问阶段 1 相同。询问限制如下:

a. $\mathcal{A}$不能发起对标识 $ID\in S_0\triangle S_1$ 的私钥询问;

b. $\mathcal{A}$不能发起对(ID,CT^*)的解密询问。

(5) 猜测阶段

最后,$\mathcal{A}$输出 1 比特对 c 的猜测值 $c'\in\{0,1\}$,若 $c=c'$,则定义为敌手获胜。

定义敌手$\mathcal{A}$获胜的优势 Adv_A^{ANON} 为

$$\mathrm{Adv}_A^{ANON}(1^{\lambda},m)=\left|\Pr[c=c']-\frac{1}{2}\right|。$$

定义 3　如果对于任意的 PPT 敌手,在上述游戏中获胜的优势是可忽略的,则称广播加密方案是 ANON-CCA 安全的。

3.3　相关工作

在以往对广播加密的研究中,大多围绕提高广播加密系统的抗合谋能力和减少广播密文长度展开,Barth 等[28]提出私有广播加密的概念,首次解决了用户隐私泄露的问题。并提出一个私有广播加密方案的通用构造,方案满足静态敌手模型下的匿名性和 IND-CCA 安全,能够保证在不泄露接收者身份信息的情况下正确解密。

文献[29]利用子集覆盖(subset-cover)技术提出具有亚线性密文长度的匿名标识广播加密方案,并给出了外部匿名性的形式化定义。对于接收者集合 S 外的用户来说是匿名的,但对于 S 内的用户不满足匿名性。

Libert 等[30]指出文献[29]中的匿名性较弱,不能满足完全匿名性,然而完全匿名性在实际应用中是必要的。文献[30]给出了匿名广播加密的形式化定义,并提出两个具有 CCA 安全的匿名广播加密的一般构造。然而,方案的匿名性由多个对称加密的密文构成,通信代价和解密计算开销较大。

文献[31]提出可在不需要解密的情况下匿名撤销 IBBE 系统中部分接收者的解密权限,该方案满足完全匿名性,只有数据发送方知道接收者的身份信息,并且撤销过程不会泄露明文和接收者身份的任何信息。

基于证书(certificate-based)的匿名广播加密概念在文献[32]中给出,文献[32]同时给出了相应的形式化定义和安全模型,并提出一个自适应 CCA 安全的基于证书的匿名广播加密方案。基于证书的密码机制解决了传统公钥密码体制中的证书管理问题,无需建立安全信道,同时也避免了标识密码体制中的密钥托管问题。

3.4　典型方案回顾

文献[27]提出了在选择密文攻击下可同时满足机密性和完全匿名性的 AIBBE 方案,且公共参数和私钥大小与接收者数量无关,方案通信代价较小,具有代表性。该方案描述如下:

符号定义为$[x]_{\ell}$表示比特串 x 的前ℓ位,$[x]^{\ell}$表示比特串 x 的后ℓ位。$x\|y$ 表示将比特串 x 和 y 连接。

(1)Setup(1^{λ}):以安全参数 λ 为输入,首先生成双线性群(p,G,G_T,e),其中,p 是长度为 λ 的素数,G,G_T 为两个 p 阶循环群,e 为双线性映射 $e:G\times G\rightarrow G_T$。随机选取生成元 $g,u,v,w\in G$,选取一个随机数 $\alpha\in\mathbb{Z}_p$作为主密钥,计算 $g_1=g^{\alpha}$。接着选取 4 个哈希函数:$H_1:\{0,1\}^*\rightarrow G$,$H_2:G_T\rightarrow\mathbb{Z}_p$,$H_3:\mathbb{Z}_p\times G\rightarrow\{0,1\}^l$,$H_4:G\times\{0,1\}^l\times\mathbb{Z}_p^t\rightarrow\mathbb{Z}_p$。公共参数设为

$paras=(p,G,G_T,e,g,g_1,u,v,w,H_1,H_2,H_3,H_4)$，私钥 $msk=\alpha$。

(2) Extract(msk,ID)：输入主私钥 msk 和身份信息 $ID\in\{0,1\}^*$，首先计算 $Q_{ID}=H_1(ID)$，计算并输出用户私钥 $sk_{ID}=Q_{ID}^{\alpha}$。

(3) Encrypt($params,S,m$)：输入系统公开参数 $params$，接收者身份信息集合 $S=\{ID_1,ID_2,\cdots,ID_t\}$ 和代价密广播消息 $m\in\{0,1\}^l$，执行以下步骤：

1)选取随机数 $r,k,\tau\in\mathbb{Z}_p$；

2)计算 G 中群元素 $C_0=g^r$；

3)对任意 $ID_i\in S$，计算 $V_{ID_i}=H_2(e(Q_{ID_i},g_1))$；

4)计算多项式

$$f(x)=\prod_{i=1}^{t}(x-V_{ID_i})+k=\sum_{j=0}^{t-1}a_jx^j+x^t \bmod p$$，其中 a_j 为 x^j 对应的系数；

5)计算

$$C_1=[H_3(k\|C_0)]_{l-l_1}\|([H_3(k\|C_0)]^{l_1})\oplus m,$$

$$h=H_4(C_0,C_2,a_0,a_1,\cdots,a_{t-1}),\ C_2=(u^hv^{\tau}w)^r,$$

输出密文 $CT=(\tau,C_0,C_1,C_2,a_0,a_1,\cdots,a_{t-1})$。

(4) Decrypt($params,sk_{ID},CT$))：输入系统公开参数 $params$，用户私钥 sk_{ID} 和广播密文 CT。用户首先计算 $h=H_4(C_0,C_2,a_0,a_1,\cdots,a_{t-1})$，接着检查等式 $e(C_0,u^hv^{\tau}w)=e(g,C_2)$ 是否成立，若不成立，输出 $\perp$ 表示解密失败；若成立，计算 $V_{ID_i}=H_2(e(sk_{ID},C_0))$，将结果带入多项式求得 $k=f(V_{ID})=\sum_{j=0}^{t-1}a_j(V_{ID})^j+V_{ID}^t \pmod p$，若

$$[C_1]_{l-l_1}\neq[H_3(k\|C_0)]_{l-l_1},$$

则解密失败，输出 $\perp$。否则可得到广播明文 $m=[C_1]^{l_1}\|([H_3(k\|C_0)]^{l_1})$。

由上述方案可知，用户在解密过程中无需输入接收者集合，有效保护了接收者的身份信息。方案的正确性分析如下：

若接收者获得的 C_0,C_2 未经篡改过，则如下等式成立：

$$\begin{aligned}e(g,C_2)&=e(g,(u^h,v^{\tau},w)^r)=\\&e(g^r,u^h,v^{\tau},w)=\\&e(C_0,u^h,v^{\tau},w),\end{aligned}$$

接收者接着可利用自己的私钥计算 V_{ID}：

$$\begin{aligned}V_{ID}&=H_2(e(sk_{ID},C_0))=\\&H_2(e(Q_{ID}^{\alpha},C_0))=\\&H_2(e(Q_{ID}^{\alpha},g^r))=\\&H_2(e(Q_{ID},g_1)^r),\end{aligned}$$

带入 $f(x)$ 可得到正确的 k，进而求得正确解密的广播明文。

4 叛逆者追踪广播加密

在一对一传输场景中，只存在一个授权方，若授权方知晓的某个秘密泄露出来，显而易见泄密者就是该授权方。当授权方有多个时，找出泄露秘密的授权方就变得比较复杂。随着网络服务的不断多样化，越来越多的数字产品都以广播的形式进行发放，例如电子图书、电子软件及音乐等。通常情况下，数据提供商会向每一个合法用户分发一个包含用户私钥的硬件或软件“解密盒”，这在付费电视和电子商务中更为常见。然而盗版问题是不可避免的，若某个恶意的订阅者将自己的“解密盒”拷贝给其他人，数据提供商并不能阻止该做法；另一种恶意用户是利用自己的私钥通过共谋生成非法的盗版产品，再进行转卖获取利润。这种行为既侵犯了作者的知识产权，又破坏了正常市场秩序。为减少数据提供商的经济损失，需尽快找出该恶意用户(叛逆者)。

4.1 叛逆者追踪广播加密定义

叛逆者追踪广播加密由以下4个多项式时间算法组成：

(1) KeyGen(λ,n)：密钥生成算法，又称为用户初始化算法，输入安全参数 λ 和接收者个数 n，算法输出公钥 e 和 n 个私钥 $d_1,d_2,\cdots,d_n$，其中任何的私钥都可以对广播密文解密。

(2) Encryption(e,S,M)：输入公钥 e，接收者集合 S 和待加密消息 M，加密算法输出广播密文 C 并发送给所有用户。

(3) Decryption(C,d_i)：输入广播密文 C 和私钥 d_i，输出解密后得到明文 M。

(4) Tracing(D)：输入一个盗版解密盒 D，若该解密盒在创建时使用到多个私钥 $d_1,d_2,\cdots,d_k$，则叛逆者追踪算法至少追踪到其中一个叛徒。

叛逆者追踪广播加密的正确性要求对任意的消息 M，$(e,(d_1,\cdots,d_n))\leftarrow$Setup($\lambda,n$)，$C\leftarrow$Encrypt($e,S,M$)。若 $i\in S$，那么

$$\Pr[\text{Decrypt}(S,i,d_i,Hdr,PK)=M]=1。$$

4.2 叛逆者追踪广播研究现状

叛逆者追踪技术由 Chor 等[33]在1994年的美密会上首次提出，主要用于对抗广播加密中合谋攻击和重放攻击。文献[33]为基于对称密钥的叛逆者可追踪的广播加密，采用的方法是为每个接收者提供不同的密钥，每一个密钥相当于一个水印，可追溯到特定解密盒的所

有者。但对于多个叛逆者合谋产生的解密盒,该方案无法实现有效追踪。随后,Naor 等[34]提出了门限叛逆者追踪方案,可有效降低存储代价与计算开销。随后,研究方向主要集中于基于公钥的叛逆者追踪,大量基于公钥的叛逆者追踪方案也相继被提出[35-42]。

Pfitzmann[35]在 1996 年首次提出了基于公钥的叛逆者追踪方案,指出在对称叛逆者追踪加密体制中存在不满足不可抵赖性的问题,这与对称的消息认证码类似,不提供不可抵赖性,也称为不可否认性。系统权威机构与订阅用户共享密钥,恶意的权威机构可能利用用户的密钥生成盗版解密盒,并且将诚实的用户控告为叛逆者。而非对称的叛逆者追踪方案可避免该问题。文献[35]中利用交互式的密钥分发协议实现叛逆者追踪广播加密方案。

Boneh 等[43]指出文献[34,36]中的方案仅能够实现概率性的叛逆者追踪,提出了改进版的公钥叛逆者追踪方案,能够实现确定性追踪且满足k-抗共谋攻击,即当发起共谋的恶意用户(叛逆者)个数不超过 k 时,至少可以有效识别出其中一个叛逆者,若个数超过 k,则不能有效追踪。该方案同样具有黑盒追踪性(无需打开解密盒)。

自此,公钥叛逆者追踪得到了积极的研究[5,43],但大多只能满足 k-抗共谋。Boneh 等[41]于 2006 年提出首个完全抗共谋的叛逆者追踪方案,可抵抗任意数量恶意用户发起的共谋攻击。然而该方案的计算代价和通信代价较高,公钥长度、私钥长度和密钥长度均为$\sqrt{N}$(N 为用户个数),追踪过程也需要耗费大量计算资源。

2008 年,Boneh 等[44]提出了定长密文的叛逆者追踪方案,密文仅由两个群元素组成,可满足t-抗共谋攻击。与文献[43]的 k-抗共谋攻击不同的是,t-抗共谋攻击中允许叛逆者数量 t 和接收者数量 n 相等。在文献[44]中 $t=n$ 时,满足完全抗共谋攻击,且不会增加密文大小。但该方案的私钥长度过大,私钥复杂度为 $O(t^2\log n)$。

文献[40-41]中的方案均利用复合阶(composite order)双线性群提出,然而复合阶双线性群存在针对模数因式分解的亚指数攻击。为保证安全性,必须使用阶数较大的复合阶群。Garg 等[45]指出利用复合阶双线性群效率较低,与素数阶双线性群相比,在相同的安全级别下,复合阶双线性群中的指数运算时间是素数阶双线性群中的 25 倍,在很多实际应用场景不便于使用。Garg 基于素数阶双线性群首次提出了完全抗共谋攻击的叛逆者追踪方案,与文献[43]相比,该方案的加解密效率有大幅提升,且密文长度更短。

4.3　典型方案回顾

文献[42]利用多项式插值技术提出一种具有撤销能力的公钥叛逆者追踪方案,方案满足黑盒追踪性。若出现盗版解密盒,可追踪并撤销门限值为 z 的用户私钥,而无需更新其他用户的私钥,并可以恢复已撤销用户私钥的解密权限。该方案还满足 k-弹性追踪,如果叛逆者的数量为 k 或更少,跟踪算法可以找到所有叛逆者。由于该方案代表性较强,此后众多叛逆者追踪且可撤销方案均是基于该方案的构造技巧,这里给出文献[42]的具体构造:

令 k 为最大叛逆者数量,z 为可撤销的叛逆者数量门限值,并设 $2k-1\leqslant z$。

(1)Syetem setup:选取阶为素数 q 的群 G_q,g 为 G_q 的生成元。数据提供商随机选取 z 阶多项式 $f(x)=\sum_{t=0}^{z}a_t x^t \bmod q$,作为数据提供商的私钥,将公钥设为 $e=(g,g^{a_0},g^{f(1)},\cdots,g^{f(z)})$,供订阅者验证其私钥。

(2)Registrastion:当订阅者 i 注册时,数据提供商向订阅者提供用于解密的私钥$(i,f(i))$。同时,订阅者i 可检查等式 $g^{a_0}=\prod_{t=0}^{z}g^{f(x_t)\lambda_t}$ 是否成立,验证接收到的密钥是否正确,其中,$\lambda_t=\prod_{0\leqslant j\neq t\leqslant z}\frac{x_j}{x_j-x_t}$ 为拉格朗日系数。对于上述等式的正确性分析可参考文献[42]。

(3)Encryption:输入待加密广播消息 M,数据提供商随机选取 z 个未使用过的二元份额组$(j_1,f(j_1))$,$(j_2,f(j_2))$,$\cdots$,$(j_z,f(j_z))$和一次性随机数 $r\in\mathbb{Z}_q$,接着计算联合授权分组

$$T=(sg^{ra_0},g^r,(j_1,g^{rf(j_1)}),(j_2,g^{rf(j_2)}),\cdots,(j_z,g^{rf(j_z)})),$$

其中,s 是加密广播数据的会话密钥。数据提供商将广播密文设为 $E(f(x),M)=(T,E'(s,M))$,其中,$E()$为分组加密算法,例如 DES 算法。

(4)Decryption:订阅者获取到广播密文$(T,E'(s,M))$,可利用密文中的 T 按照如下方式计算会话密钥 s,

$$s=\frac{sg^{a_0 r}}{(g^r)^{f(i)\lambda_z}\cdot\prod_{t=0}^{z-1}(g^{rf(x_t)})^{\lambda_t}},$$

其中,$x_0=j_1,x_1=j_2,\cdots,x_{z-1}=j_z,x_z=i,\lambda_t=\prod_{0\leqslant j\neq t\leqslant z}\frac{x_j}{x_j-x_t}$ 为拉格朗日系数。

(5) Traitor tracing:假设可能存在 m 个订阅者 $\{c_1, c_2, \cdots, c_m\}$ $(m \leqslant k)$,利用其份额构造了盗版解密盒,为确定这 m 个用户是否确定为叛逆者。数据提供商可按如下步骤操作:数据提供商随机选取 $z-m$ 个未使用的份额,如 $\{j_1, \cdots, j_{z-m}\}$,利用测试消息 M 构造测试密文 $E(f(x), M) = (T, E'(s, M))$,其中

$$T = (sg^{ra_0}, g^r, (c_1, g^{rf(c_1)}), (c_2, g^{rf(c_2)}), \cdots, (c_m, g^{rf(c_m)}), (j_1, g^{rf(j_1)}), (j_2, g^{rf(j_2)}) \cdots, (j_{z-m}, g^{rf(j_{z-m})})),$$

将 $(T, E'(s, M))$ 作为盗版解密盒的输入,若该解密盒无法正确解密输出测试消息 M,则 $\{c_1, c_2, \cdots, c_m\}$ 中存在叛逆者。接着,可缩小集合范围或对集合 $\{c_1, c_2, \cdots, c_m\}$ 的标识元素单独运行上述算法,以精确求得叛逆者集合。

5 可撤销广播加密

仅实现叛逆者追踪性质并不能完全满足应用的需求。一个健壮的广播加密系统需满足追踪并撤销功能,当出现非法解密设备时,应确保在第一时间追踪到该非法设备所使用密钥的来源并撤销密钥拥有者的解密能力,使撤销用户不再能够解密密文。

在将一个广播加密系统部署到付费电视等实际应用中时,可能存在如下问题:①用户的私钥可能泄露、丢失;②用户因退订服务退出广播加密系统等;③用户主动离开广播加密系统等。为保证数据机密性,广播加密系统需保证上述用户不再具有解密权限。用于解决该问题的广播加密称为接收者可撤销广播加密(Recipient Revocable Identity-Based Broadcast Encryption, RR-IBBE)。

5.1 可撤销广播加密定义

文献[46]给出的标识可撤销广播加密的定义与标识广播加密的定义类似,区别在于前者在加密阶段输入为撤销用户的标识集合,而后者在加密阶段输入为授权接收者用户的标识集合。

在 Susilo 等[47]提出的方案中,撤销方式同样为利用接收者标识集合撤销,该方案在加密阶段输入的集合为当前已授权用户的标识集合 S,撤销阶段输入撤销标识集合 R,则解密阶段只有 $S' = S - R$ 中的用户可正确解密。

5.2 可撤销广播加密的研究现状

Naor 等[48]利用子集-覆盖方法提供了一种经典的追踪可撤销的广播加密构造方法。子集-覆盖算法为每个不相交的划分集合分配一个长期密钥,并为每个子集加密短期密钥,用短期密钥加密需要广播的消息。文献[48]分别利用完全生成子树和子集差分给出了2种方案的构造。当加密者为一些授权用户集合 $S \subseteq \{1, 2, \cdots, N\}$ 提供广播密文时,若存在一个盗版者利用合谋用户 $T \subseteq \{1, 2, \cdots, N\}$ 的一组私钥构造了一个盗版解密盒 D,那么,跟踪算法可以与 D 进行交互,并识别追踪到盗版者拥有的一个活动密钥,即其中一个用户的密钥 $t \in S \cap T$。广播者将授权用户集合 S' 设置为 $S' \leftarrow S \backslash \{t\}$,再进行广播,其中,$S \backslash \{t\}$ 表示删除集合 S 中的 t 元素。如果盗版解密盒依旧可以解密,再次运行跟踪算法并得到另一个参与共谋的密钥 $t' \in S' \cap T$,将授权用户集合 S'' 设置为 $S'' \leftarrow S' \backslash \{t'\}$。按照此方法进行下去,直到盗版解密盒无法解密。

Boneh 等[40]提出了增强广播加密(Augmented Broadcast Encryption, ABE)的概念,并给出了可同时满足叛逆者追踪并撤销、完全抗合谋性、黑盒追踪性的方案构造,方案具有亚线性大小的密文和私钥,且可抵抗自适应选择明文攻击的敌手。

文献[45]提出了两个具有短密钥的可撤销广播加密方案,方案的密文开销均为 $O(r)$,其中,r 为被撤销的用户数量。公钥和私钥的大小为素数阶椭圆曲线群中的定长群元素,公钥的长度分别为5个和12个群元素,私钥长度分别为3个和5个群元素。与文献[5,7,9]中的方案不同,该方案允许用户创建一个可以撤销无限数量用户的广播密文。而在其他系统中,公共参数限制了系统中的可撤销用户数量,必须更新系统公共参数才能支持撤销更多用户。

谭作文等[49]在2005年提出一种完全式的公钥广播加密方案,与传统的公钥广播加密方案不同,在完全式广播加密方案中,由用户自己生成解密密钥,而传统公钥广播加密中用户的解密密钥由广播者分发。文献[49]还实现了叛逆者追踪和非法用户撤销的功能,该方案在 DDH 困难假设下可抵抗选择密文攻击。

文献[47]首次提出接收者可撤销的广播加密,在 RR-IBBE 中,数据提供商将生成的密文内容发送给受信任的第三方,即广播公司。广播公司会周期性的向订阅者广播内容,也可以从加密内容中撤销一组用户,而无需对其进行解密。在文献[47]提出的方案中,首先发送给广播公司长度为 $m+3$ 个群元素的广播密文,其中,m 为一次加密中最大撤销用户数量,广播公司执行撤销算法后生成长度为3个群元素的广播密文发送给订

阅者。

Lai 等[31]基于文件共享的应用场景提出了匿名标识可撤销广播加密方案,该方案适用于:数据拥有者将文件加密后存储于云服务器中共享,当一个用户集合 R 中的用户离开公司后,该服务器必须撤销 R 中用户的访问权限。撤销算法执行后,集合 R 中用户将不能再利用自己的私钥解密文件。文献[31]提出的方案具有恒定大小的公钥和私钥,撤销阶段的计算开销为 $O(r)$,其中,r 为撤销用户的数量。

Ge 等[50]从密钥更新的角度出发,实现了可撤销广播加密。文献[50]基于二叉树结构和素数阶双线性群的非对称配对,提出了可撤销 IBBE 的具体方案。在该方案中,KGC 定期发布一些更新密钥所需的元素,只有未撤销的用户才能更新其解密密钥,已撤销用户无法更新密钥。在标准模型中,选择明文攻击下,该方案被证明是半自适应安全的,且实现了固定长度的密文。

5.3　典型方案回顾

文献[46]的方案采用了新型的秘密分享技术,将秘密份额 s_i 和撤销用户标识 ID_i 一同嵌入到密文中,使得已撤销用户无法解密密文。该方案的构造技巧后来被广泛应用于属性基加密方案构造中[51-52]。该方案代表性较强,其方案构造具体描述如下:

(1)Setup:定义阶为素数 p 的双线性群 G,随机选取 G 中 2 个生成元 $g,h\in G$ 和$\mathbb{Z}$中两个随机数 $\alpha,b\in\mathbb{Z}_p$将公钥设为 $PK=(g,g^b,g^{b^2},h^b,e(g,g)^\alpha)$,系统私钥为 $MSK=(\alpha,b)$。

(2)KeyGen(MSK,ID):首先随机选取 $t\in\mathbb{Z}_p$,依次计算 $D_0=g^\alpha g^{b^2t}$,$D_1=(g^{b\cdot ID}h)^t$,$D_2=g^{-t}$,将私钥设为 $SK_{ID}=(D_0,D_1,D_2)$。

(3)Encrypt(PK,M,S):随机选取 $s\in\mathbb{Z}_p$,令 $r=|S|$,即撤销用户数量。随机选取 r 个随机数 $s_1,\cdots,s_r$ 使得 $s=s_1+\cdots+s_r$。令 ID_i 表示撤销集合 S 中的第 i 个身份。接着计算 $C'=e(g,g)^{\alpha s}M$,$C_0=g^s$。对于任意 $i=1,2,\cdots,r$,计算

$$C_{i,1}=g^{b\cdot s_i},C_{i,2}=(g^{b^2\cdot ID_i}\cdot h^b)^{s_i},$$

密文为 $CT=(C',C_0,(C_{1,1},C_{1,2}),\cdots,(C_{r,1},C_{r,2}))$。

(4)Decrypt(S,CT,ID,SK_{ID}):输入撤销用户身份集合 S、密文 CT、用户的身份 ID 和用户私钥 SK_{ID},若用户身份在撤销集合内,则解密算法终止解密。否则,解密算法计算

$$W=\frac{e(C_0,D_0)}{e\left(D_1,\prod_{i=1}^{r}C_{i,1}^{\frac{1}{ID-ID_i}}\right)\cdot e\left(D_2,\prod_{i=1}^{r}C_{i,2}^{\frac{1}{ID-ID_i}}\right)},$$

最后计算 $M=\dfrac{C'}{e(g,g)^{\alpha s}}$可获得明文。

正确性分析:

$$\begin{aligned}W&=e(C_0,D_0)\Big/e\left(D_1,\prod_{i=1}^{r}C_{i,1}^{\frac{1}{ID-ID_i}}\right)\cdot e\left(D_2,\prod_{i=1}^{r}C_{i,2}^{\frac{1}{ID-ID_i}}\right)=\\&e(g^s,g^\alpha g^{b^2t})\Big/\prod_{i=1}^{r}e(g^{ID\cdot bt}\cdot h^t,g^{\frac{b\cdot s_i}{ID-ID_i}})\cdot e(g^{-t},(g^{b^2ID_i}\cdot h^b)^{\frac{s_i}{ID-ID_i}})=\\&e(g^s,g^\alpha)\cdot e(g^s,g^{b^2t})\Big/\prod_{i=1}^{r}(e(g^{ID\cdot bt}\cdot h^t,g^{b\cdot s_i})\cdot e(g^{-t},(g^{b^2\cdot ID_i}\cdot h^b)^{s_i}))^{\frac{1}{ID-ID_i}}=\\&e(g^s,g^\alpha)\cdot e(g^s,g^{b^2t})\Big/\prod_{i=1}^{r}((e(g^{b\cdot t},g^{b\cdot s_i}))^{ID}\cdot(e(h,g^{b\cdot s_i}))^t\cdot e(g,h^{b\cdot s_i})^{-t}\cdot(e(g^t,g^{b^2s_i})^{ID_i})^{\frac{1}{ID-ID_i}}=\\&e(g^s,g^\alpha)\cdot e(g^s,g^{b^2t})\Big/\prod_{i=1}^{r}((e(g^t,g^{b^2\cdot s_i}))^{ID}\cdot(e(g^t,g^{b^2s_i})^{ID_i})^{\frac{1}{ID-ID_i}}=\\&e(g^s,g^\alpha)\cdot e(g^s,g^{b^2t})\Big/e(g,g)^{b^2t\sum_{i=1}^{r}s_i}=\\&e(g^s,g^\alpha)。\end{aligned}$$

6　公钥广播加密的应用研究

广播加密可提供一对多场景下数据安全共享的功能,适用于互联网以及物联网中众多场景,如:

(1)车载自组织网络的安全通信

车载自组织网络(Vehicular Ad Hoc Networks, VANETs)也称车联网,通过车载智能设备可实现云端服务通讯与本地总线通讯,以及通过手机应用对车辆进行远程控制,目前已经成为通信领域和无线传感网领域的一个研究热点。VANETs 中的信息传播离不开车辆和基础设施的交互。在 VANETs 中,可信机构(Trust Authority, TA)通常需要与多台车辆建立安全连接,并发挥重要作用。然而,当 TA 向多台车辆发送相同的消息时,会产生较多的冗余信息,因为 TA 需要与每台车辆协商并向每个车辆发送不同的密文。目前,VANETs 采用的大多为点对点的通信方式,通信效率较低。因此,广播加密是 VANETs 通信中的重要研究方向。文献[53]针对车联网场景,提出了一种身份基广播加密方案,适用于

车辆到基础设施间的通信。

(2)云存储的访问控制

云存储的访问控制是公钥广播加密另一个重要的研究方向。随着社交媒体的不断发展,众多基于云存储的社交网络应用被广泛使用,如抖音、微信和微博等。用户使用这些应用会产生大量数据。具体而言,通过社交网络应用,用户可获取网络热点新闻,也可以建立朋友群组,以分享个人观点或个人内容,如照片、视频、文件等。社交应用通常会产生大量的敏感数据。一方面,个人终端设备的计算能力和存储空间通常是有限的,使用一段时间后不得不将一些敏感数据删掉;另一方面,对于大多数维持这些应用运行的中小企业来说,随着用户规模的快速增长,企业也无力承担相应的计算和存储成本。因此,云计算和云存储服务应运而生,使得计算资源和存储资源像水、电一样利用。企业用户可以向云计算厂商租用计算资源和存储资源,既可以将大部分计算任务外包给云计算服务器,也可以将大量数据存储于云存储服务器。

近年来,企业和个人用户越来越依赖云存储服务,云存储服务技术发展也逐渐成熟,既有商业级的云存储服务,如亚马逊 S3、Egnyte、和 Tresorit 等,也有消费级的云存储服务,如 Google Drive、iCloud、微软 OneDrive、Dropbox 等。然而,对于云存储服务,需要解决隐私保护问题,即如何确保存储在云中的照片和视频等用户个人数据只能由数据所有者授权的用户访问,而所有未经授权的用户,包括云存储提供商本身,都不能访问或恢复原始的个人数据。因此,针对上述应用场景,提出一种高效安全、低带宽需求的公钥广播加密方案是十分有意义且可行的。文献[54]针对云存储文件共享场景进行了研究,提出了功能广播加密(Functional Broadcast Encryption, FBE)的概念,这是带访问控制的公钥加密的一种表现形式,用于云数据的访问控制。文献[55]也对广播加密在云存储的应用进行了研究,提出了自适应安全的基于证书的广播加密。

(3)在物联网的应用

物联网目前与人们的工作和生活息息相关,海量物联网设备纷纷接入到互联网中,从智能手表到安全门锁,物联网技术已经成为人们生活中不可缺少的一部分。然而,物联网安全并没有得到足够重视,安全事件频发,全球近 20% 的企业和相关机构在过去 3 年遭遇物联网攻击。例如在 2021 年,美国的 15 万个摄像头被入侵造成个人隐私泄露,以及利用摄像头组成僵尸网络发起的分布式拒绝服务攻击(Distributed Denial-Of-Service, DDOS)攻击等。因此,物联网的安全问题亟待解决。随着物联网的大规模部署,为确保整个网络的安全,需及时进行设备更新以修复高危安全漏洞。文献[56]提出一种适用于物联网中组密钥管理的多变量广播加密方案,可有效减少功耗,并提高物联网数据传输的安全性。一种利用区块链技术提供软件更新的机制在文献[57]中得到研究,一旦更新作为有效区块的一部分添加到区块链中,那么该区块就不可删除,可抵抗阻止物联网设备更新的恶意实体发起的攻击,确保了更新的可用性。同时,还可抵抗针对中心化结构的拒绝服务攻击。对于区块链基础设施向物联网设备共享升级文件、网络配置文件等通信环节,均可采用广播加密技术实现。

(4)基于格密码的广播加密

目前,大多数公钥加密方案的设计通常基于数学困难问题,随着量子技术的飞速发展,现有公钥密码算法在量子计算下将不再安全,量子计算机的出现可能会威胁到基于数学困难问题的密码体制。目前,实用化的密码体制仍是基于数学困难问题的公钥密码。格密码作为抗量子密码算法,是公认的后量子密码领域中最热门的研究方向之一。近年来,学者们已经逐步开始研究抗量子广播加密,提出了一些优秀的基于格的广播加密方案[58-60],基于格密码的广播加密研究也将成为未来较为重要的研究方向之一。

7 结论与展望

近年来,随着无线传感网、智能终端、云计算等新兴应用的快速发展,网络形态逐步呈现出层次化、服务化等特点。面向服务的计算通常采用资源共享的工作方式,该工作方式的特点为多个用户请求同一个数据。企业或个人的数据上云首要解决的问题就是数据安全与隐私保护。广播加密为一对多场景下数据安全且高效的共享提供了解决方案,在物联网、云存储的访问控制等应用中得到广泛使用。

本文介绍了公钥广播加密的概念、定义以及安全模型,针对不同应用场景的安全需求,详细论述了公钥广播加密、标识广播加密、匿名广播加密、叛逆者追踪广播加密以及可撤销广播加密的原理、特征及研究成果。

虽然目前已经存在大量公钥广播加密研究的文献,但大多围绕国外算法展开,基于国产密码的广播加密算法及其衍生的功能型算法较少。因此,设计安全高效的

具有不同功能的国产公钥广播加密算法可作为未来的研究方向之一。此外,目前基于格的广播加密研究较少,也将成为未来的研究热点。

参考文献:

[1] Fiat A, Naor M. Broadcast encryption[C]//Advances in Cryptology-CRYPTO'93, 13th Annual International Cryptology Conference. Berlin: Springer, 1993: 480-491.

[2] Wong C K, Gouda M G, Lam S S. Secure group communications using key graphs[J]. IEEE/ACM Transactions on Networkings, 2000, 8(1): 16-30.

[3] Zhang L Y, Wu Q, Mu Y. Anonymous identity-based broadcast encryption with adaptive security[C]//Cyberspace Safety and Security-5th International Symposium, CSS 2013. Berlin: Springer, 2013: 258-271.

[4] Berkovits S. How to broadcast a secret[C]//Advances in Cryptology-EUROCRYPT'91, Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer, 1991: 535-541.

[5] Naor M, Pinkas B. Efficient trace and revoke schemes[C]//Financial Cryptography, 4th International Conference. Berlin: Springer, 2000: 1-20.

[6] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys[C]//Advances in Cryptology-CRYPTO 2005: 25th Annual International Cryptology Conference. Berlin: Springer, 2005: 258-275.

[7] Dodis Y, Fazio N. Public key broadcast encryption for stateless receivers[C]//Security and Privacy in Digital Rights Management. Berlin: Springer, 2002: 61-80.

[8] Delerablée C, Paillier P, Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys[C]//Pairing-Based Cryptography-Pairing 2007, First International Conference. Berlin: Springer, 2007: 39-59.

[9] Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts)[C]//Advances in Cryptology-EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin:Springer, 2009: 171-188.

[10] Phan D H, Pointcheval D, Shahandashti S F, et al. Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts[C]//Information Security and Privacy-17th Australasian Conference, ACISP 2012. Berlin: Springer, 2012: 308-321.

[11] Gay R, Kowalczyk L, Wee H. Tight adaptively secure broadcast encryption with short ciphertexts and keys[C]//Security and Cryptography for Networks-11th International Conference, SCN 2018. Berlin: Springer, 2018: 123-139.

[12] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology, Proceedings of CRYPTO'84. Berlin: Springer, 1984: 47-53.

[13] Boneh D, Franklin M K. Identity-based encryption from the weil pairing[C]//Advances in Cryptology-CRYPTO 2001, 21st Annual International Cryptology Conference. Berlin: Springer, 2001: 213-229.

[14] Sakai R, Furukawa J. Identity-based broadcast encryption[J]. IACR Cryptol. ePrint Arch., 2007: 217.

[15] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys[C]//ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer,2007: 200-215.

[16] Barbosa M, Farshim P. Efficient identity-based key encapsulation to multiple parties[C]//Cryptography and Coding, 10th IMA International Conference. Berlin: Springer, 2005: 428-441.

[17] Bellare M, Boldyreva A, Staddon J. Randomness re-use in multi-recipient encryption schemeas[C]//Public Key Cryptography-PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer, 2003: 85-99.

[18] Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: Security proofs and improvements[C]//Advances in Cryptology-EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 2000: 259-274.

[19] Baek J, Safavi-Naini R, Susilo W. Efficient multi-receiver identity-based encryption and its application to broadcast encryp-

tion[C]//Public Key Cryptography-PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer, 2005 380-397.

[20] Boneh D, Hamburg M. Generalized identity based and broadcast encryption schemes[C]//Advances in Cryptology-ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2008: 455-470.

[21] 刘潇,刘魏然,伍前红,等. 选择密文安全的基于身份的广播加密方案[J]. 密码学报, 2015, 2(1): 66-67.

[22] Kim J, Susilo W, Au M H, et al. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 679-693.

[23] Lai J C, Mu Y, Guo F C, et al. Identity-based broadcast encryption for inner products[J]. The Computer Journal, 2018, 61(8): 1240-1251.

[24] 赖建昌,黄欣沂,何德彪. 一种基于SM9的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897-907.

[25] Yao S, Zhang D. Anonymous certificate-based inner product broadcast encryption[J]. Security and Communication Networks, 2021,doi:10.1155/2021/6639835.

[26] Liu L, Zhang Y Q, Li X J. KeyD: Secure key-deduplication with identity-based broadcast encryption[J]. IEEE Transcations on Cloud Computing, 2021, 9(2):670-681.

[27] He K, Weng J, Liu J N, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security[C]//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. New York: ACM, 2016: 247-255.

[28] Barth A, Boneh D, Waters B. Privacy in encrypted content distribution using private broadcast encryption[C]//Financial Cryptography and Data Security, 10th International Conference, FC 2006. Berlin: Springer, 2006: 52-64.

[29] Fazio N, Perera IM. Outsider-anonymous broadcast encryption with sublinear ciphertexts[C]//Public Key Cryptography-PKC 2012-15th International Conference on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2012: 225-242.

[30] Libert B, Paterson K G, Quaglia E A. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model[C]//Public Key Cryptography-PKC 2012-15th International Conference on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2012: 206-224.

[31] Lai J C, Mu Y, Guo F C, et al. Anonymous identity-based broadcast encryption with revocation for file sharing[C]//Information Security and Privacy-21st Australasian Conference, ACISP 2016. Berlin: Springer, 2016: 223-239.

[32] Li J G, Chen L Q, Lu Y, et al. Anonymous certificate-based broadcast encryption with constant decryption cost[J]. Information Science, 2018, 454/455: 110-127.

[33] Chor B, Fiat A, Naor M. Tracing traitors[C]//Advances in Cryptology-CRYPTO'94, 14th Annual International Cryptology Conference. Berlin: Springer, 1994: 257-270.

[34] Naor M, Pinkas B. Threshold traitor tracing[C]//Annual International Cryptology Conference. Berlin: Springer, 1998: 502-517.

[35] Pfitzmann B. Trials of traced traitors[C]//Information Hiding, First International Workshop. Berlin: Springer, 1996: 49-64.

[36] Kurosawa K, Desmedt Y. Optimum traitor tracing and asymmetric schemes[C]//Advances in Cryptology-EUROCRYPT'98, International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1998: 145-157.

[37] Watanabe Y, Hanaoka G, Imai H. Efficient asymmetric public-key traitor tracing without trusted agents[C]//Topics in Cryptology-CT-RSA 2001, the Cryptographer's Track at RSA Conference 2001. Berlin: Springer, 2001: 392-407.

[38] Tô V D, Safavi-Naini R, Zhang F. New traitor tracing schemes using bilinear map[C]//Proceedings of the 2003 ACM Workshop on Digital Rights Management 2003. New York: ACM, 2003: 67-76.

[39] Matsushita T, Imai H. A public-key black-box traitor tracing scheme with sublinear ciphertext size against self-defensive pirates[C]//Advances in Cryptology-ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2004: 260-275.

[40] Boneh D, Sahai A, Waters B. Fully collusion resistant traitor tracing with short ciphertexts and private keys[C]//Advances in Cryptology-EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic

Techniques. Berlin: Springer, 2006: 573-592.

[41] Boneh D, Waters B. A fully collusion resistant broadcast, trace, and revoke system[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 211-220.

[42] Tzeng W G, Tzeng Z J. A public-key traitor tracing scheme with revocation using dynamic shares[C]//Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2001: 207-224.

[43] Boneh D, Franklin M K. An efficient public key traitor tracing scheme[C]//Advances in Cryptology-CRYPTO'99, 19th Annual International Cryptology Conference. Berlin: Springer, 1999: 338-353.

[44] Boneh D, Naor M. Traitor tracing with constant size ciphertext[C]//Proceedings of the 2008 ACM Conference on Computer and Communications Security. New York: ACM, 2008: 501-510.

[45] Garg S, Kumarasubramanian A, Sahai A, et al. Building efficient fully collusion-resilient traitor tracing and revocation schemes[C]//Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010. New York: ACM, 2010: 121-130.

[46] Lewko A B, Sahai A, Waters B. Revocation systems with very small private keys[C]//31st IEEE Symposium on Security and Privacy, S&P 2010. Piscataway: IEEE, 2010: 273-285.

[47] Susilo W, Chen R M, Guo F C, et al. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext[C]//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2016. New York: ACM, 2016: 201-210.

[48] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers[C]//Advances in Cryptology-CRYPTO 2001, 21st Annual International Cryptology Conference. Berlin: Springer, 2001: 41-62.

[49] 谭作文,刘卓军,肖红光. 一个安全公钥广播加密方案(英文)[J]. 软件学报, 2005(7): 1333-1343.

[50] Ge A J, Wei P W. Identity-based broadcast encryption with efficient revocation[C]//PKC 2019-22nd IACR International Conference on Practice and Theory of Public-Key Cryptography. Berlin: Springer, 2019: 405-435.

[51] Hur J. Improving security and efficiency in attribute-based data sharing[J]. IEEE Transactions on Knowledge and Data Engineering, 2011, 25(10): 2271-2282.

[52] Attrapadung N, Herranz J, Laguillaumie F, et al. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical Computer Science, 2012, 422: 15-38.

[53] Zhong H, Zhang S, Cui J, et al. Broadcast encryption scheme for V2I communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 2749-2760.

[54] Wang H, Zhang Y, Chen K, et al. Functional broadcast encryption with applications to data sharing for cloud storage[J]. Information Science, 2019,502: 109-124.

[55] Chen L Q, Li J G, Lu Y, et al. Adaptively secure certificate-based broadcast encryption and its application to cloud storage service[J]. Information Science, 2020,538: 273-289.

[56] Kumar M S, Purosothaman T. Multivariate broadcast encryption with group key algorithm for secured IoT[J]. International Journal of Computer System Science & Engineering, 2023, 45(1): 925-938.

[57] Boudguiga A, Bouzerna N, Granboulan L, et al. Towards better availability and accountability for IoT updates by means of a blockchain[C]//IEEE European Symposium on Security and Privacy. Piscataway: IEEE, 2017: 50-58.

[58] Wee H. Optimal broadcast encryption and CP-ABE from evasive lattice assumptions[C]//Advances in Cryptology-EUROCRYPT'22-41st Annual International Conference on the theory and Applications of Cryptographic Techniques. Berlin: Springer, 2022: 217-241.

[59] Agrawal S, Yamada S. Optimal broadcast encryption from pairings and LWE[C]//Advances in Cryptology-EUROCRYPT'20-39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2020: 13-43.

[60] Agrawal S, Wichs D, Yamada S. Optimal broadcast encryption from LWE and pairings in the standard model[C]//Theory of Cryptography-18th International Conference, TCC'20. Berlin: Springer, 2020: 149-178.

【责任编辑: 卓祯雨】