抵抗泄露攻击的可撤销 IBE 机制

周彦伟[1),2),3)] 杨 波[1),2)] 夏 喆[4)] 来齐齐[1)] 张明武[2),3)] 穆 怡[5)]

[1)](陕西师范大学计算机科学学院 西安 710062)

[2)](密码科学技术国家重点实验室 北京 100878)

[3)](桂林电子科技大学广西可信软件重点实验室 广西 桂林 541004)

[4)](武汉理工大学计算机科学与技术学院 武汉 430070)

[5)](福建师范大学数学与信息学院福建省网络安全与密码技术重点实验室 福州 350117)

摘 要 隐私信息的泄露已成为密码系统当前的严重安全性隐患,因此抗泄露性已成为密码机制安全性的重要评价指标;并且连续的泄露攻击将被敌手在现实环境中执行,所以抵抗连续泄露攻击的密码机制具有更强的实用性.可撤销的身份基加密(Revocable Identity-Based Encryption,RIBE)机制由于能够快速实现用户私钥的撤销,具有广泛的实际应用前景;然而传统 RIBE 机制无法抵抗信息泄露对方案所造成的危害,针对上述不足,本文以身份基哈希证明系统(Identity-Based Hash Proof System,IB-HPS)为底层工具设计了选择明文攻击(Chosen-Plaintext Attack,CPA)安全的抗泄露 RIBE 机制的通用构造,并基于 IB-HPS 的安全属性,对通用构造的 CPA 安全性进行了形式化证明;为进一步增强安全性和抗泄露能力,在我们上述构造的基础上,通过非交互式零知识论证和可更新的身份基哈希证明系统分别构造了 CCA 安全和抗连续泄露攻击的 RIBE 机制,并基于底层工具的安全属性证明了相应构造的安全性.相较于传统的 RIBE 机制而言,本文 RIBE 机制的通用构造在秘密信息存在一定泄露的前提下,依然保持其所声称的安全性.由于过去的几年中底层基础工具的多个实例相继被构造,这表明我们抗泄露 RIBE 机制的通用构造方法具有较强的实用性.

关键词 可撤销 IBE 机制;有界泄露模型;连续泄露模型;身份基哈希证明系统

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2020.01535

Revocable Identity-Based Encryption Scheme with Leakage-Resilience

ZHOU Yan-Wei[1),2),3)] YANG Bo[1),2)] XIA Zhe[4)] LAI Qi-Qi[1)] ZHANG Ming-Wu[2),3)] MU Yi[5)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

[2)](*State Key Laboratory of Cryptology, Beijing* 100878)

[3)](*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)

[4)](*School of Computer Science and Technology, Wuhan University of Technology, Wuhan* 430070)

[5)](*Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University, Fuzhou* 350117)

Abstract In the traditional security model, it is assumed that only legitimate participants possess the internal secret states (e.g., the user's private key, random value, etc.), and these states are completely inaccessible to the adversary. However, in many real-world applications, these states could be leaked through various leakage attacks, such as side-channel attacks, cold boot attacks, etc. Therefore, if an adversary obtains some information of the internal secret

收稿日期:2019-11-07;在线发布日期:2020-01-20.本课题得到国家重点研发计划(2017YFB0802000)、国家自然科学基金(61802242,61772326,61802241)、"十三五"国家密码发展基金(MMJJ20180217)、广西可信软件重点实验室研究课题(KX202002)及中央高校基本科研业务费(GK202003079,GK202007033)资助.**周彦伟**,博士,高级工程师,硕士生导师,主要研究领域为密码学、匿名通信技术等.E-mail:zyw_snnu@foxmail.com.**杨 波**(通信作者),博士,教授,博士生导师,陕西省"百人计划"特聘教授,主要研究领域为信息安全、密码学等.E-mail:byang@snnu.edu.cn.**夏 喆**,博士,副教授,硕士生导师,主要研究领域为信息安全.**来齐齐**,博士,讲师,主要研究方向为信息安全、密码学等.**张明武**,博士,教授,博士生导师,主要研究领域为信息安全、密码学等.**穆 怡**,博士,教授,博士生导师,主要研究领域为信息安全、密码学等.

states, the cryptographic schemes may fail to achieve their claimed security. Thus, leakage of private information has become a serious security risk of the cryptography schemes, so the leakage resilience has become an important evaluation index of the security of the cryptography schemes; And the continuous leakage attack will be executed by the adversary in the real environment, so the cryptography schemes with continuous leakage resilience has stronger practicability. That is, in order to further increase the practicability, many researchers have begun to pay attention to the design of continuous leakage resilient cryptography scheme. Very recently, several concrete constructions were proposed to capture the (continuous) leakage-resilience requirement, such as the (continuous) leakage-resilient public-key encryption, the (continuous) leakage resilient identity-based encryption, the (continuous) leakage-resilient authenticated key exchange, the (continuous) leakage resilient certificate-based encryption, etc. A revocable identity-based encryption (RIBE) scheme can be widely used in the real world because it can quickly revoke the user's identity key. However, the previous RIBE schemes cannot keep their claimed security if an adversary can obtain a certain amount of leakage on the private information. In other words, no RIBE scheme against (continuous) leakage attack has been proposed in the past few years. Therefore, in this paper, to solve the above problem, a generic construction of chosen-plaintext attacks (CPA) secure leakage-resilient RIBE scheme is created from the identity-based hash proof system (IB-HPS), and the security of created scheme can be proved based on the corresponding security of IB-HPS. To further improve the security and the practicability of RIBE scheme, the chosen-ciphertext attacks (CCA) secure RIBE scheme with leakage resilience can be created from the non-interactive zero-knowledge argument, and a continuous leakage-resilient RIBE scheme can be obtained by using an updatable identity-based hash proof system (U-IB-HPS) as an underlying basic tool, in which, an additional key update algorithm can push some new randomness into the private key of user, and the leakage of the previous private key does not affect the security of the updated private key. Similarly, the security of proposed continuous leakage-resilient RIBE scheme can be proved from the corresponding security of the underlying U-IB-HPS. Compared with the previous traditional RIBE scheme, our generic construction can keep its claimed security even if the adversary can obtain some leakage from the private information. Specially, to further show the difference of technology, a new generic construction of CCA secure RIBE scheme with leakage resilience is created from the one-time lossy filter and IB-HPS. Our proposed generic construction method is a practical leakage resilient RIBE scheme because some instantiations of the underlying basic tools had created in the past few years.

Keywords　revocable identity-based encryption; bounded leakage model; continuous leakage model; identity-based Hash proof system

1　引　言

传统密码学机制的安全性均假设秘密信息对潜在的任意敌手而言是完全保密的，即密码机制是以黑盒形式运行的，敌手仅能观察到密码机制运行前的输入和运行结束后的输出，无法获知运行过程的任何信息. 然而，由于边信道、冷启动等物理攻击方式的存在，使得敌手能够获得密码机制运行过程中秘密信息的部分泄露内容，导致传统安全模型下的密码机制在现实环境中已不再满足其所声称的安全性.

1.1　密码机制的抗泄露性研究

近年来，为了缩短实际应用与理论研究之间的差距，越来越多的密码学研究者开始关注密码机制抗泄露性的研究. 根据敌手执行泄露攻击的能力，将泄露模型分为有界泄露模型和连续泄露模型两种：(1) 有界泄露模型中，关于秘密信息的泄露量不能

超过系统设定的泄露参数;(2)连续泄露模型中,密码机制的生命周期通过执行相应的操作(如密钥更新等)被划分成了多个时间周期,在每一个时间周期内敌手能够获得关于秘密钥的任意泄露信息,并且同一秘密值的泄露量不能超过系统设定的泄露参数,但是在整个生命周期内不限制泄露的总量.由于真实环境中敌手能够执行持续的泄露攻击,因此连续泄露模型更加接近现实环境的应用需求.为增强密码机制的实用性,应在连续泄露模型下对相应密码机制的抗泄露性进行研究.

下文中,我们将详细介绍当前密码机制抗泄露性的研究现状.

1.1.1 PKE机制的抗泄露性

在公钥加密(Public Key Encryption,PKE)领域,Naor和Segev[1]联合哈希证明系统(Hash Proof System,HPS)和强随机性提取器(Strong Randomness Extractor,Ext)设计了抵抗有界泄露攻击PKE机制的通用构造.Alwen等人[2]提出了身份基哈希证明系统(Identity-Based Hash Proof System,IB-HPS)这一新的密码原语,并以IB-HPS作为底层工具构造了泄露放大的PKE机制.Liu等人在文献[1]的基础上提出了更加实用、高效的选择密文攻击(Chosen Ciphertext Attacks,CCA)安全的泄露容忍的PKE机制[3].Qin等人[4-5]基于HPS和一次性损耗滤波器(One-Time Lossy Filter,OT-LF)给出了具有抗泄露选择密文攻击(Leakage-resilient Chosen Ciphertext Attacks,LR-CCA)安全的PKE机制的通用构造.Li等人[6]对文献[1]中的方案进行了改进,提出了密钥长度更短的抗泄露攻击的PKE机制,并基于判定性Diffie-Hellman假设对提出方案的安全性进行了证明.文献[7]在文献[1]的基础上提出一个新的抗泄露PKE机制,该机制通过减少密钥的长度达到提高泄露率的目的.在辅助输入模型中,文献[8]基于OT-LF提出一个抗泄露攻击的CCA安全的PKE方案.

由于连续泄露模型中敌手能够进行持续的泄露攻击,使得其更加接近现实环境的实际应用需求,并且在FOCS2010中,Dodis等人[9]详细介绍了连续泄露模型中的敌手攻击能力的定义,同时给出了连续泄露模型与有界泄露模型间的转换联系.文献[10]在增强文献[8]中方案安全性的同时,提出一个抗持续辅助输入泄露的CCA安全的PKE方案.为进一步增强PKE机制的实用性,Zhou等人[11-12]采用矩阵运算和向量内积的方法设计了两个抗连续泄露攻击的PKE机制,并通过形式化证明对相应机制的CCA安全性进行了证明.Yang等人[13]提出了一个新的密码学原语,称为可更新的哈希证明系统(Updatable Hash Proof System,U-HPS),并基于该原语在Qin等人工作[4-5]的基础上,构造出抗连续泄露攻击的PKE机制的通用构造.综上所述,现有的抗(连续)泄露PKE机制的通用构造方式总结如表1所示.

表1 现有抗(连续)泄露PKE机制的通用构造方法

属性	CPA安全性	CCA安全性
抗有界泄露	HPS+Ext	HPS+Ext+OT-LF
抗连续泄露	U-HPS+Ext	U-HPS+Ext+OT-LF

1.1.2 IBE机制的抗泄露性

在传统身份基加密(Identity-based Encryption,IBE)机制的研究基础上,Li等人[14]设计了抗有界泄露攻击的IBE机制.文献[15]设计了一个抗密钥弹性泄漏的可委托层次模板加密方案,该方案是抗泄漏的层次身份加密方案和隐藏向量加密方案的一般扩展,可有效地抵抗密钥弹性泄漏,并达到自适应语义安全性.Zhang等人[16]设计了一个新颖的抗泄露的分层IBE机制,为接收者提供匿名性保护.Sun等人[17]受Liu等人工作[3]的启发,设计了泄露参数不受待加密消息长度限制的抗泄露IBE机制;此外,他们还在合数阶双线性群上设计了一个完全安全的具有通配符密钥衍生功能的抗泄露IBE机制[18].在EUROCRYPT 2010中,Alwen等人[2]基于IB-HPS和强随机性提取器提出了构造选择明文攻击(Chosen Plaintext Attacks,CPA)安全的抗泄露IBE机制的通用方法.Chow等人[19],Chen等人[20-21]分别给出了几种IB-HPS的具体实例.为提升实用性,Zhou等人[22-24]在连续泄露模型中基于不同的技术提出了三种抗连续泄露攻击的IBE机制,增强了IBE机制的抗泄露攻击的能力.由于不同应用环境的泄露需求各不相同,用一个不变的泄露界很难满足现实中不同环境的实际应用需求,为了实现根据应用环境的需求动态设置IBE机制泄露界的目标,文献[25]设计了泄露界可灵活变化的抗泄露IBE机制,其中可根据实际环境的泄露需求通过控制相应的初始化参数来控制IBE机制的泄露上界,切实做到了泄露界的按需设计目标;即该机制在保持公开参数不变的前提下,通过增加用户私钥的长度达到提升机制抗泄露攻击的能力.

由于抗连续泄露攻击的IBE机制具有更强的实用性,在PKE机制中,基于更新操作提出了抗连

续泄露攻击的版本.自然地,为了设计抗连续泄露的IBE机制,基于现有IB-HPS的定义,文献[26]提出可更新的身份基哈希证明系统(Updatable Identity-Based Hash Proof System,U-IB-HPS)的新密码学原语,并基于该技术设计了IBE机制、基于身份的混合加密机制和基于身份的密钥协商协议等密码机制抗泄露版本的通用构造.综上所述,现有的抗(连续)泄露IBE机制的通用构造方式总结如表2所示.

表2　现有抗(连续)泄露IBE机制的通用构造方法

属性	CPA安全性	CCA安全性
抗有界泄露	IB-HPS+Ext	IB-HPS+Ext+OT-LF
抗连续泄露	U-IB-HPS+Ext	U-IB-HPS+Ext+OT-LF

特别地,HPS、U-HPS、IB-HPS和U-IB-HPS间的关系如图1所示.

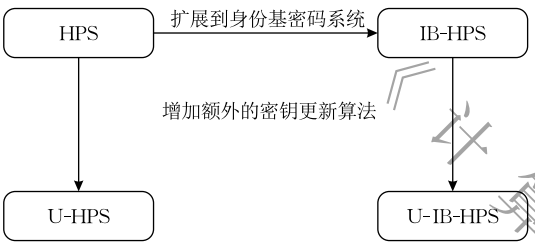

图1　HPS、U-HPS、IB-HPS和U-IB-HPS间的关系

除对PKE和IBE机制的抗泄露性研究之外,密码研究人员还对基于属性的密码机制[27-29]、无证书密码机制[30-33]、基于证书的密码机制[34-36]、签名机制[37-38]、密钥协商协议[39-40]和秘密共享[41-42]等密码原语的抗泄露性进行了大量的研究.可见密码机制抗泄露性的研究是当前密码学领域的一个热点问题.

1.2　可撤销的IBE机制

在公钥加密环境中,为了消除传统公钥基础设施(Public Key Infrastructure,PKI)中证书的管理问题,Shamir提出了基于身份的密码学[43],其中用户的任何公开信息可作为公开钥使用,而相应的秘密钥由私钥生成中心(Private Key Generator,PKG)负责生成.在真实的应用中,PKG需要撤销部分用户的私钥,然而此时PKG只能重新建立系统生成新的主密钥,并且对所有的未撤销用户生成新的秘密钥,该操作一定程度上降低了IBE机制的工作效率,并且限制了IBE机制在实际应用系统中的大规模部署,因此,需要具有撤销功能的IBE机制来灵活处理用户身份的撤销问题.针对上述实际应用需求,可撤销的身份基加密机制(Revocable Identity-Based Encryption,RIBE)被提出[44],即RIBE是传统IBE机制的扩展,增加了用户的身份撤销功能,PKG在不进行系统重建的前提下快捷地实现对用户的身份撤销.

Boneh和Franklin在随机谕言机模型中通过拼接身份信息和时间戳的方法提出了第一个RIBE机制[44],即将 $id\|T$ 作为用户的公开信息(其中 id 是身份信息,T 是时间戳),然而该机制的效率较低,所有未撤销的用户都需要建立安全链路接收PKG为其生成的更新私密钥.Boldyreva等人[45]给出了RIBE机制的形式化定义,并基于Sahai和Waters提出的模糊身份的IBE机制[46]构造了一个选择身份安全的RIBE机制.该工作之后,完全安全的RIBE机制[47-48]、可撤销的分层IBE机制[49]、可撤销存储的属性基加密机制[50-51]等密码方案相继被提出.由于上述构造[47-51],均采用了文献[45]中所使用的完全子树这一基本技术,导致更新私密钥的长度较长;为了改进该问题,文献[52]基于子集差分提出一个新的RIBE构造技术;文献[53]提出了私密钥和更新私密钥更短的可撤销的分层RIBE机制.

然而,我们发现当前关于RIBE机制的工作主要集中在具体构造的研究,未曾有工作关注RIBE机制的抗泄露能力;因此本文将聚焦该问题,研究RIBE机制的抗泄露性,提出抵抗泄露攻击的RIBE机制,进一步增强RIBE机制的实用性.

1.3　我们的思路

受基于IB-HPS(U-IB-HPS)设计抗(连续)泄露IBE机制通用构造思路的启发,本文将研究抗(连续)泄露RIBE机制的通用构造.

RIBE机制的用户私钥 $sk_{(id,T_i)}=(k_{id},k_{T_i})$ 包含两部分:一部分是身份组件 k_{id},另一部分是时间组件 k_{T_i}.由于IB-HPS可视为是一个基于身份的密钥封装机制,因此我们抗泄露RIBE机制的通用构造中利用两个IB-HPS分别完成 k_{id} 和 k_{T_i} 的生成,其中 k_{T_i} 相对应的身份信息 id' 由用户的真实身份 id 和时间戳 T_i 通过映射生成,即 $id'=\mathcal{H}(id,T_i)$,其中 $\mathcal{H}(\cdot)$ 是身份映射函数;时间戳 T_i 使用方便PKG执行用户私钥信息的撤销操作,通过对时间组件 k_{T_i} 的更新实现对IBE机制中用户私钥 $sk_{(id,T_i)}$ 的撤销,即PKG无需重建系统,只需通过更新系统时刻将过去的私钥撤销.

IB-HPS确保输出的封装秘钥具有足够的平均最小熵,通过平均情况的强随机性提取器可将封装秘钥转换成对于任意敌手而言是完全均匀随机的对称秘钥,然后使用对称密钥对消息进行隐藏,其中随

机性提取器实现了用户秘钥的弹性泄漏容忍.特别地,用户私钥的时间组件和身份组件分别对应一个封装秘钥,两个封装秘钥的随机性是我们构造实现抗泄露性质的基础.

使用CPA安全的抗泄露RIBE机制结合非交互式零知识(Non-Interactive Zero-Knowledge,NIZK)论证的模式设计CCA安全的抗泄露RIBE机制,其中使用NIZK论证将密文中的各元素进行绑定,为密文提供防扩展的性质,并且抗泄露攻击的能力由底层的CPA安全的抗泄露RIBE机制提供.此外,本文使用NIZK构造RIBE的方法,可扩展到PKE和IBE机制中,将表1和表2中相应的OT-LF变成NIZK可得到构造CCA安全的PKE和IBE机制的新方法.

1.4 我们的工作

本文系统地介绍了IB-HPS和NIZK论证的概念及安全属性,并基于上述技术提出了抵抗泄露攻击的RIBE机制的通用构造.我们的贡献主要分为三个方面,详细叙述如下:

(1)在回顾RIBE机制形式化定义的基础上,定义了抗泄露攻击的RIBE机制的CPA和CCA安全模型.

(2)基于IB-HPS提出两种抗泄露RIBE机制的通用构造,其中第二种构造具有CCA安全性;基于底层IB-HPS和NIZK的安全属性对相应构造的CPA安全性和CCA安全性分别进行了形式化证明.

(3)为了进一步提高RIBE机制的实用性,增强其抗泄露攻击的能力,在U-IB-HPS的基础上,设计了抵抗连续泄露攻击的RIBE机制的通用构造,通过附加的密钥更新算法定期向用户的私密钥中注入新的随机性,消除先前秘密钥的泄露信息对系统安全性的影响,使得敌手已捕获的泄露信息对新的私密钥不起作用,因此敌手需要重新收集关于新私密钥的泄露,进而实现了抗连续泄露攻击的能力.

2 基础知识

本节将介绍最小熵、平均最小熵、随机性提取器和非交互零知识论证等基础知识.

2.1 相关符号

用κ表示安全参数;$a\leftarrow_R A$表示从集合A中均匀随机的选取元素a;$\mathrm{negl}(\kappa)$表示在安全参数κ上是计算可忽略的;$x\leftarrow\mathcal{A}(y)$表示算法$\mathcal{A}$在输入$y$的作用下输出相应的计算结果$x$.

2.2 统计距离和最小熵

我们首先介绍统计距离的概念.令X与Y是有限域Ω上的任意两个随机变量,那么上述变量间的统计距离可表示为

$$\mathrm{SD}(X,Y)=\frac{1}{2}\sum_{w\in\Omega}|\Pr[X=w]-\Pr[Y=w]|.$$

定义1. 随机变量X的最小熵可表示为

$$H_\infty(X)=-\log(Max_x\Pr[X=x]).$$

特别地,$H_\infty(X)$表示无任何信息协助的前提下任意敌手猜测变量X的最大概率,即变量X的最小熵$H_\infty(X)$体现了X的不可预测性.

定义2. 当变量B已知时,变量A的平均最小熵可表示为

$$\widetilde{H}_\infty(A|B)=-\log(E_{b\leftarrow B}[2^{-H_\infty(A|B=b)}]),$$

其中E表示数学期望运算.平均最小熵$\widetilde{H}_\infty(A|B)$表示在变量$B$已知的前提下,变量$A$的不可预测性;也就是说,任意敌手在变量$B$的协助下猜测变量$A$的概率.

定理1. 对于任意的随机变量A,B和C,若B的取值最多有2^l个,则有

$$\widetilde{H}_\infty(A|(B,C))\geq\widetilde{H}_\infty(A|C)-l.$$

2.3 随机性提取

定义3. 令随机变量A和B满足条件$X\in\{0,1\}^{l_n}$和$\widetilde{H}_\infty(X|Y)\geq k$,对于任意的$R\in\{0,1\}^{l_t}$和$Z\in\{0,1\}^{l_m}$,若有

$$\mathrm{SD}((\mathrm{Ext}(X,R),R,Y),(Z,R,Y))\leq\varepsilon$$

成立,则称函数$\mathrm{Ext}:\{0,1\}^{l_n}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$是平均情况的$(k,\varepsilon)$-强随机性提取器,其中$R\in\{0,1\}^{l_t}$是可公开的提取器种子.

引理1(剩余哈希引理). 令通用哈希函数集合为$H_I=\{H_i:X\rightarrow Y\}_{i\in I}$.那么对于$A\leftarrow_R X,B\leftarrow_R Y$和$C$,则有

$$\mathrm{SD}((H_i(A),i),(B,i))\leq\frac{1}{2}\sqrt{2^{-H_\infty(A)}|Y|}\text{和}$$

$$\mathrm{SD}((H_i(A),i,C),(B,i,C))\leq\frac{1}{2}\sqrt{2^{-\widetilde{H}_\infty(A|C)}|Y|}.$$

引理2(广义剩余哈希引理). 令A和B是满足关系$A\leftarrow_R\{0,1\}^{l_n}$和$\widetilde{H}(A|B)\geq k$的两个变量随机变量.$H_I=\{H_i:\{0,1\}^{l_n}\rightarrow\{0,1\}^{l_m}\}_{i\in I}$是从集合$\{0,1\}^{l_n}$到集合$\{0,1\}^{l_m}$的通用哈希函数集合.那么对于任意的随机变量$i\leftarrow_R I$和$C\leftarrow_R\{0,1\}^{l_m}$,当$l_m$满足条件$l_m\leq k-2(\log 1/\varepsilon)$时,有关系

$$\mathrm{SD}((H_i(A),i,B),(C,i,B))\leq\varepsilon$$

成立，其中 $2(\log 1/\varepsilon)=\omega(\log\kappa)$.

由引理 1 和引理 2 可知，通用哈希函数可视为平均情况的强随机性提取器.

2.4　非交互式零知识论证

在 ASIACRYPT 2010 中，Dodis 等人[54]详细介绍了 NIZK 论证的形式化定义和安全模型. 为方便本文方案的构造，我们将对上述内容进行简要回顾.

令 R 是下述语言 L_R 上关于二元组 (x,y) 的 NP 关系，其中

$$L_R=\{y\mid \exists x, s.t.\ (x,y)\in R\}.$$

关系 R 上的 NIZK 论证包含三个算法 Setup、Prove 和 Verify，具体语法可表述为：

(1) $(CRS,tk)\leftarrow\text{Setup}(1^\kappa)$. 初始化算法 Setup 以系统安全参数 κ 为输入，输出公共参考串 CRS 和相应的陷门密钥 tk.

(2) $\pi\leftarrow\text{Prove}_{CRS}(x,y)$. 对满足 $R(x,y)=1$ 的二元组 (x,y) 生成相应的论证 π.

(3) $1/0\leftarrow\text{Verify}_{CRS}(\pi,y)$. 若 π 是相对应于 y 的论证，则输出 1，否则输出 0.

当 CRS 能从上下文中获知时，为了简便，可将算法 Prove_{CRS} 和 Verify_{CRS} 中的下标 CRS 省略，直接写成 Prove 和 Verify.

NIZK 需满足下述三个安全性质：

(1) 正确性. 对于任意的 $(x,y)\in R$，可知

$$\pi\leftarrow\text{Prove}(x,y)\text{ 和 }\text{Verify}(\pi,y)=1,$$

其中 $(CRS,tk)\leftarrow\text{Setup}(1^\kappa)$.

(2) 可靠性. 对于 $(CRS,tk)\leftarrow\text{Setup}(1^\kappa)$ 和 $(y,\pi')\leftarrow\mathcal{A}(CRS)$，有

$$\Pr[y\notin L_R\wedge\text{Verify}(\pi',y)=1]\le\text{negl}(\kappa)$$

成立，其中 $\mathcal{A}$ 是一个概率多项式时间(Probabilistic Polynomial Time，PPT)敌手. 换句话讲，对于不属于语言 L_R 上的元素 y，任意敌手 $\mathcal{A}$ 输出有效论据的概率是可忽略的.

(3) 零知识性. 存在一个 PPT 模拟器 Sim，使得任意的 PPT 敌手 $\mathcal{A}$ 在下述游戏中获胜的优势是可忽略的，即有

$$\left|\Pr[\mathcal{A}\ wins]-\frac{1}{2}\right|\le\text{negl}(\kappa)$$

成立.

① 挑战者 $\mathcal{C}$ 输入安全参数 κ 运行初始化算法 $(CRS,tk)\leftarrow\text{Setup}(1^\kappa)$，并发送系统公开参数 (CRS,tk) 给敌手 $\mathcal{A}$.

② 敌手 $\mathcal{A}$ 选择 $(x,y)\in R$，并将其发送给挑战者 $\mathcal{C}$.

③ 挑战者 $\mathcal{C}$ 首先计算

$$\pi_1\leftarrow\text{Prove}(x,y)\text{ 和 }\pi_0\leftarrow\text{Sim}(y,tk).$$

然后发送挑战论证 π_v 给敌手 $\mathcal{A}$，其中 $v\leftarrow_R\{0,1\}$.

④ 敌手 $\mathcal{A}$ 输出对 v 的猜测 v'. 若 $v'=v$，则称敌手 $\mathcal{A}$ 在该游戏中获胜.

在上述游戏中，对于任意的 $y\in L_R$，模拟器 Sim 可在陷门密钥 tk 的作用下输出一个模拟论证. 即使敌手获知二元组 (x,y)(其中 x 是私有的证据，y 是公开的状态信息)，零知识性依然保证了模拟论证与算法 Prove 生成的真实论证是不可区分的.

在文献[54]中，Dodis 等人还定义了新的密码原语—真实模拟可提取的 NIZK(true-simulation extractable NIZK，tsE-NIZK)论证，除了满足上述三个安全性质之外，tsE-NIZK 论证中还存在一个 PPT 的提取器 Ext′(初始化算法会输出相应的提取陷门 ek；特别地，此处的提取器与强随机性提取器是存在本质区别的，并非同一种，为了方便区分将其表示为 Ext′)能从恶意证明者 $\mathcal{P}^*$ 输出的任意论证 π 中提取出一个证据 x'，其中 $\mathcal{P}^*$ 能够看到之前关于真实状态的模拟论证. 此外，Dodis 等人将 tsE-NIZK 扩展到关于函数 f 的可提取性，即 Ext′只需输出关于有效证据 x' 的函数值 $f(x')$，而不再直接输出证据 x' 本身.

令 $\mathcal{O}_{tk}^{\text{Sim}}(\cdot)$ 表示模拟谕言机，敌手提交二元组 (x,y) 给模拟谕言机，$\mathcal{O}_{tk}^{\text{Sim}}(\cdot)$ 检测 $(x,y)\in R$ 是否成立，若成立，则忽略 x，并输出一个由模拟器 Sim 生成的模拟论证 $\text{Sim}(y,tk)$，否则输出终止符号 $\perp$.

定义 4(真实模拟的 f-可提取性). 令 f 是确定的高效可计算的函数，$\Pi=(\text{Setup},\text{Prove},\text{Verify})$ 是关系 R 上的 NIZK 论证，当下述条件成立时，也称 Π 是真实模拟 f-可提取的(true-simulation f-extractable，f-tSE)NIZK 论证.

(1) 初始化算法 Setup 除了输出公共参考串 CRS 和陷门密钥 tk 之外，还输出一个供提取器 Ext′使用的提取密钥 ek，即

$$(CRS,tk,ek)\leftarrow\text{Setup}(1^\kappa).$$

(2) 在下列游戏中，存在一个 PPT 算法 $\text{Ext}'(y,\pi,ek)$ 使得任意的 PPT 敌手 $\mathcal{A}$ 获胜的优势是可忽略的，即有

$$\Pr[\mathcal{A}\ wins]\le\text{negl}(\kappa)$$

成立，其中 $\text{Ext}'(y,\pi,ek)$ 表示在提取密钥 ek 的作用下从 y 的论证 π 中提取出相应的证据信息.

① 密钥生成. 挑战者 $\mathcal{C}$ 运行初始化算法

$$(CRS,tk,ek)\leftarrow \mathrm{Setup}(1^{\kappa}),$$

并将 CRS 发送给敌手 $\mathcal{A}$.

② 模拟询问. 敌手 $\mathcal{A}^{\mathcal{O}_{tk}^{\mathrm{Sim}}(\cdot)}$ 可适应性地询问模拟谕言机 $\mathcal{O}_{tk}^{\mathrm{Sim}}(\cdot)$,即敌手 $\mathcal{A}$ 以二元组 (x,y) 作为输入,能够从模拟谕言机 $\mathcal{O}_{tk}^{\mathrm{Sim}}(\cdot)$ 处获得相应的模拟论证.

③ 输出. 敌手 $\mathcal{A}$ 输出 (y',π').

④ 提取. 挑战者 $\mathcal{C}$ 运行 $z'\leftarrow \mathrm{Ext}'(y',\pi',ek)$.

条件:① 状态信息 y' 未在模拟询问中出现,② $\mathrm{Verify}(\pi',y')=1$,③ 对于满足条件 $f(x')=z'$ 的 x',有 $R(x',y')=0$. 若上述条件都成立,则称敌手 $\mathcal{A}$ 在上述游戏中获胜.

f-tSE NIZK 论证的真实模拟的 f-可提取性表明关系 R 中的二元组 (x,y) 所对应的论证 π,提取操作 $\mathrm{Ext}'(y,\pi,ek)$ 能以不可忽略的概率从 π 中提取出相应的证据 x 满足 $f(x)=\mathrm{Ext}'(y,\pi,ek)$.

若敌手 $\mathcal{A}$ 仅有一次访问模拟谕言机 $\mathcal{O}_{tk}^{\mathrm{Sim}}(\cdot)$ 的机会,则称是一次性模拟可提取的;通过增强敌手 $\mathcal{A}$ 获胜的条件,可得到强模拟可提取的概念,其中敌手 $\mathcal{A}$ 输出一个新的状态、论证对而不再是单一的新状态,更详细地讲,条件①更改为 (y',π') 是新的,并且 y' 未在模拟询问中出现;并且论证 π' 与敌手 $\mathcal{A}$ 从模拟谕言机 $\mathcal{O}_{tk}^{\mathrm{Sim}}(\cdot)$ 获得的论证是不相同的. 此外,在文献[54]中,Dodis 等人指出基于任意 CCA 安全的加密机制和标准的 NIZK 论证可以来构造 f-tSE NIZK 论证.

3 身份基哈希证明系统

虽然 Alwen 等人[2]在 EUROCRYPT2010 中详细介绍了 IB-HPS 的形式化定义及安全属性,为了文章的完整性本节我们将简述上述内容.

3.1 形式化定义

一个 IB-HPS 包含五个 PPT 算法 Setup、KeyGen、Encap、Encap* 和 Decap. 算法的具体描述如下所述:

(1) $(mpk,msk)\leftarrow \mathrm{Setup}(1^{\kappa})$. 初始化算法 Setup 以系统安全参数 κ 为输入,输出相应的系统公开参数 mpk 和主密钥 msk,其中 mpk 定义了系统的用户身份空间 $\mathcal{ID}$,封装密钥空间 $\mathcal{K}$ 和用户私钥空间 $\mathcal{SK}$. 此外,mpk 是其他算法 KeyGen、Encap、Encap* 和 Decap 的隐含输入;为了方便起见,下述算法的输入列表并未将其列出.

(2) $d_{id}\leftarrow \mathrm{KeyGen}(msk,id)$. 对于输入的任意身份 $id\in\mathcal{ID}$,密钥生成算法 KeyGen 以主密钥 msk 作为输入输出身份 id 所对应的私钥 d_{id}.

(3) $(C,k)\leftarrow \mathrm{Encap}(id)$. 对于输入的任意身份 $id\in\mathcal{ID}$,有效密文封装算法 Encap 输出相应的密文和封装密钥对 (C,k).

(4) $C^*\leftarrow \mathrm{Encap}^*(id)$. 对于输入的任意身份 $id\in\mathcal{ID}$,无效密文封装算法 Encap* 输出相应的无效封装密文 C^*.

(5) $k\leftarrow \mathrm{Decap}(d_{id},C)$. 对于确定性的解封装算法,输入身份 id 所对应的密文 C(或 C^*)和私钥 d_{id},输出相应的解封装密钥 k.

3.2 安全性

一个 IB-HPS 需满足正确性、通用性、平滑性及有效密文与无效密文的不可区分性等四个安全性质.

(1) 正确性

对于任意的身份 $id\in\mathcal{ID}$,有

$$\Pr\left[k\neq k'\;\middle|\;\begin{matrix}(C,k)\leftarrow \mathrm{Encap}(id)\\ k'\leftarrow \mathrm{Decap}(d_{id},C)\end{matrix}\right]\leq \mathrm{negl}(\kappa)$$

成立,其中 $(mpk,msk)\leftarrow \mathrm{Setup}(1^{\kappa})$ 和 $d_{id}\leftarrow \mathrm{KeyGen}(msk,id)$.

(2) 通用性

对于 $(mpk,msk)\leftarrow \mathrm{Setup}(1^{\kappa})$ 和任意的身份 $id\in\mathcal{ID}$,当一个 IB-HPS 满足下属两个条件时,称该 IB-HPS 是 δ-通用的.

① 对于 $d_{id}\leftarrow \mathrm{KeyGen}(msk,id)$,有

$$H_{\infty}(d_{id})\geq\delta.$$

② 对于身份 id 对应的任意两个不同的私钥 d_{id}^1 和 d_{id}^2 $(d_{id}^1\neq d_{id}^2)$,有

$$\Pr[\mathrm{Decap}(C^*,d_{id}^1)=\mathrm{Decap}(C^*,d_{id}^2)]\leq \mathrm{negl}(\kappa),$$

其中 $C^*\leftarrow \mathrm{Encap}^*(id)$.

通用性表明 IB-HPS 的用户私钥具有一定的不可预测性;并且对于同一身份的不同私钥解封装同一个无效密文得到相同解封装结果的概率是可忽略的.

(3) 平滑性

对于任意身份 $id\in\mathcal{ID}$ 的私钥 d_{id}(其中 $d_{id}\leftarrow \mathrm{KeyGen}(msk,id)$),若有

$$\mathrm{SD}((C^*,k),(C^*,\tilde{k}))\leq \mathrm{negl}(\kappa)$$

成立,则称该IB-HPS是平滑的,其中 $C^*\leftarrow \mathrm{Encap}^*(id)$、$k\leftarrow \mathrm{Decap}(d_{id},C^*)$ 和 $\tilde{k}\leftarrow_R\mathcal{K}$.

平滑性表明无效封装密文的解封装输出与封装密钥空间中的任意随机值是不可区分的. 换句话讲,无效密文的解封装输出对任意敌手而言是完全均匀

随机的.

在平滑性的基础上，下面讨论泄露平滑性. 令函数 $f:\{0,1\}^{*}\rightarrow\{0,1\}^{\lambda}$ 是一个高效可计算的泄露函数，若有关系

$$\mathrm{SD}((C^{*},f(d_{id}),k),(C^{*},f(d_{id}),\tilde{k}))\leq\mathrm{negl}(\kappa)$$

成立，则称相应的 IB-HPS 具有抗泄露攻击的平滑性.

(4) 有效密文与无效密文的不可区分性

有效封装算法 Encap 生成的密文称为有效密文，无效封装算法 Encap* 输出的密文称为无效密文. 对于 IB-HPS 而言，有效密文和无效密文是不可区分的，即使敌手能够获得任意身份(包括挑战身份)的私钥.

有效密文和无效密文的不可区分性游戏的参与者包括挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$，上述参与者间的消息交互如下所述：

① 系统初始化. $\mathcal{C}$ 运行初始化算法 $(mpk,msk)\leftarrow\mathrm{Setup}(1^{\kappa})$，发送系统公开参数 mpk 给 $\mathcal{A}$，并秘密保存主私钥 msk.

② 阶段 1. $\mathcal{A}$ 对 $\mathcal{ID}$ 中的用户身份 $id\in\mathcal{ID}$ 进行适应性的密钥生成询问(包括挑战身份)，$\mathcal{C}$ 通过运行密钥生成算法 $d_{id}\leftarrow\mathrm{KeyGen}(msk,id)$ 返回相应的私钥 d_{id} 给 $\mathcal{A}$.

③ 挑战. 对于挑战身份 $id^{*}\in\mathcal{ID}$，$\mathcal{C}$ 首先计算 $(C_1,k)\leftarrow\mathrm{Encap}(id^{*})$ 和 $C_0\leftarrow\mathrm{Encap}^{*}(id^{*})$，然后，发送挑战密文 C_{ω} 给 $\mathcal{A}$，其中 $\omega\leftarrow_{R}\{0,1\}$.

④ 阶段 2. 与阶段 1 相类似，$\mathcal{A}$ 能够适应性的对任意身份 $id\in\mathcal{ID}$ 进行密钥生成询问(包括挑战身份)，获得 $\mathcal{C}$ 返回的相应应答 $d_{id}\leftarrow\mathrm{KeyGen}(msk,id)$.

⑤ 输出. 敌手 $\mathcal{A}$ 输出对 ω 的猜测 ω'. 若 $\omega'=\omega$，则称敌手 $\mathcal{A}$ 在该游戏中获胜，并且挑战者 $\mathcal{C}$ 输出 1，意味着 $\mathcal{C}$ 能够区分有效密文与无效密文；否则，挑战者 $\mathcal{C}$ 输出 0.

特别地，上述两个测试阶段，对于同一身份 $id\in\mathcal{ID}$ 的密钥生成询问，挑战者通过列表记录返回相同的私钥 $d_{id}\leftarrow\mathrm{KeyGen}(msk,id)$ 给敌手(可通过建立应答列表的方式实现). 在具体的构造中，由于 KeyGen 是随机性算法，同一身份不同时刻的私钥是不相同的.

在上述有效密文与无效密文的区分性实验中，敌手 $\mathcal{A}$ 获胜的优势定义为

$$Adv_{\text{IB-HPS}}^{\text{VI-IND}}(\kappa)=\left|\Pr[\mathcal{A}\ wins]-\frac{1}{2}\right|,$$

其中概率来自挑战者和敌手对随机数的选取. 对于任意的 PPT 敌手 $\mathcal{A}$，有

$$Adv_{\text{IB-HPS}}^{\text{VI-IND}}(\kappa)\leq\mathrm{negl}(\kappa)$$

成立.

3.3　通用性、平滑性及泄露平滑性之间的关系

下面将回顾通用性、平滑性及泄露平滑性之间的关系，其中定理 2 表明当参数满足相应的限制条件时任意一个通用的 IB-HPS 是泄露平滑的；定理 3 表明基于平均情况的强随机性提取器可将平滑的 IB-HPS 转变成泄露平滑的 IB-HPS.

定理 2.　假设封装密钥空间为 $\mathcal{K}=\{0,1\}^{l_k}$ 的 IB-HPS 是 δ-通用的，那么它也是泄露平滑的，其中泄露参数满足 $\lambda\leq\delta-l_k-\omega(\log\kappa)$.

定理 2 可由剩余哈希引理(引理 1)和广义的剩余哈希引理(引理 2)得到.

下面基于强随机性提取器给出由平滑的 IB-HPS 构造泄露平滑的 IB-HPS 的通用转换方式. 令 $\Pi'=(\mathrm{Setup}',\mathrm{KeyGen}',\mathrm{Encap}',\mathrm{Encap}'^{*},\mathrm{Decap}')$ 是封装密钥空间为 $\mathcal{K}=\{0,1\}^{l_k}$，身份空间为 $\mathcal{ID}$ 的平滑性 IB-HPS，$\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k-\lambda,\varepsilon)$-强随机性提取器，其中 λ 是泄露参数，ε 在安全参数 κ 上是可忽略的. 那么，泄露平滑的 IB-HPS 的构造 $\Pi=(\mathrm{Setup},\mathrm{KeyGen},\mathrm{Encap},\mathrm{Encap}^{*},\mathrm{Decap})$ 表述如下：

(1) $(mpk,msk)\leftarrow\mathrm{Setup}(1^{\kappa})$

输出 (mpk,msk)，其中

$(mpk,msk)\leftarrow\mathrm{Setup}'(1^{\kappa})$.

(2) $d_{id}\leftarrow\mathrm{KeyGen}(msk,id)$

输出 d_{id}，其中

$d_{id}\leftarrow\mathrm{KeyGen}'(msk,id)$.

(3) $(C,k)\leftarrow\mathrm{Encap}(id)$

随机选取 $S\leftarrow_{R}\{0,1\}^{l_t}$，并计算

$(C',k')\leftarrow\mathrm{Encap}'(id)$ 和 $k=\mathrm{Ext}(k',S)$.

输出 (C,k)，其中 $C=(C',S)$.

(4) $C^{*}\leftarrow\mathrm{Encap}^{*}(id)$

随机选取 $S\leftarrow_{R}\{0,1\}^{l_t}$，并计算

$C'^{*}\leftarrow\mathrm{Encap}'^{*}(id)$.

输出 $C^{*}=(C'^{*},S)$.

(5) $k\leftarrow\mathrm{Decap}(d_{id},C)$

计算

$k'\leftarrow\mathrm{Decap}'(d_{id},C')$ 和 $k=\mathrm{Ext}(k',S)$.

输出相应的封装密钥 k.

定理 3.　假设 Π' 是封装密钥空间为 $\mathcal{K}=\{0,1\}^{l_k}$ 的平滑性 IB-HPS，$\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k-\lambda,\varepsilon)$-强随机性提取器，那么，当 $\lambda\leq l_k-l_m-\omega(\log\kappa)$ 时，上述通用转换可生成一

个封装密钥空间为$\mathcal{K}=\{0,1\}^{l_m}$的$\lambda$-泄露平滑性IB-HPSⅡ.

定理3的证明详见附录A.

4 抗泄露的可撤销IBE机制

本节将给出RIBE机制的形式化定义和抗泄露的安全性模型.

4.1 形式化定义

一个RIBE机制包含六个PPT算法Setup、KeyGen、Enc、Dec、Revoke和KeyUpdate.各算法的具体描述如下所述:

(1)$(Params,msk)\leftarrow\text{Setup}(1^{\kappa})$.初始化算法Setup以系统安全参数$\kappa$为输入,输出相应的系统公开参数$Params$和主密钥$msk$,其中$Params$定义了身份空间$\mathcal{ID}$,私钥空间$\mathcal{SK}$和密文空间$\mathcal{M}$.同时,还定义了初始为空的用户身份撤销列表$RL$.此外,$Params$是其他算法KeyGen、Enc、Dec、Revoke和KeyUpdate的隐含输入;同样为了方便,下述算法的输入列表并未将其列出.

(2)$sk_{(id,T_i)}\leftarrow\text{KeyGen}(msk,id,RL,TL)$.输入任意身份$id\in\mathcal{ID}$,主密钥$msk$,身份撤销列表$RL$和当前时间列表$TL$,密钥生成算法KeyGen首先检测$id$是否在身份撤销列表$RL$中,若在则终止并输出$\perp$;否则,输出身份$id$在当前$T_i$时刻所对应的私钥$sk_{(id,T_i)}=(k_{id},k_{T_i})$,其中$k_{id}$是私钥$sk_{(id,T_i)}$的身份组件,$k_{T_i}$是私钥$sk_{(id,T_i)}$的时间组件.

(3)$(C_{T_i},T_i)\leftarrow\text{Enc}(id,M,T_i)$.对于输入的身份$id\in\mathcal{ID}$,明文消息$M$和时刻$T_i$,加密算法Enc输出身份$id$在$T_i$时刻对消息$M$的加密密文$C_{T_i}$.同时,一起输出$C_{T_i}$相对应的标记时戳$T_i$.

(4)$M\leftarrow\text{Dec}(sk_{(id,T_i)},C_{T_i},T_i)$.输入身份$id$在$T_i$时刻的密文$C_{T_i}$和身份$id$在$T_i$时刻的私钥$sk_{(id,T_i)}$,解密算法Dec输出相应的明文消息$M$.

(5)$RL'\leftarrow\text{Revoke}(RL,\{id_1,\cdots,id_n\})$.输入现有的撤销列表$RL$和相应的待撤销的身份集合$\{id_1,\cdots,id_n\}$,身份撤销算法Revoke输出更新后的撤销列表$RL'$.

(6)$k_{T_{i+1}}\leftarrow\text{KeyUpdate}(RL,id,T_{i+1})$.输入现有的撤销列表$RL$,身份$id$和时间戳$T_{i+1}$,密钥更新算法首先检测$id$是否在身份撤销列表$RL$中,若在则终止并输出$\perp$;否则,输出私钥$sk_{(id,T_i)}$更新后的时间组件$k_{T_{i+1}}$,即将身份$id$所对应的时间组件更新到$T_{i+1}$时刻,将用户私钥更新到$sk_{(id,T_{i+1})}=(k_{id},k_{T_{i+1}})$,实现对用户之前私钥$sk_{(id,T_i)}=(k_{id},k_{T_i})$的撤销,其中私钥的身份组件部分$k_{id}$保持不变.

4.2 安全性

RIBE机制抗泄露攻击的CCA安全游戏由模拟器$\mathcal{C}$和敌手$\mathcal{A}$执行,其中κ是安全参数,λ是泄露参数.具体的消息交互过程如下所述:

①系统初始化.该阶段通过输入安全参数κ,$\mathcal{C}$运行$\text{Setup}(1^{\kappa})$获得相应的公开参数$Params$和主密钥msk;在秘密保存msk的同时发送$Params$给$\mathcal{A}$;此外,初始化算法还定义了初始为空的身份撤销列表RL,同时设定了系统时刻列表TL.

②阶段1(训练).该阶段$\mathcal{A}$能对密钥生成、解密、泄露、身份撤销和密钥更新等询问适应性地进行多项式有界次.

密钥生成询问.对于身份id在T_i时刻密钥的生成询问,挑战者$\mathcal{C}$首先检测id是否在撤销列表RL中,若$id\in RL$,那么$\mathcal{C}$终止并输出$\perp$;否则,$\mathcal{C}$运行密钥生成算法KeyGen,输出id在T_i时刻的私钥$sk_{(id,T_i)}$,并发送给$\mathcal{A}$.

解密询问.对于$\mathcal{A}$提交的关于身份、密文和时刻三元组(id,C_{T_i},T_i)的解密询问,$\mathcal{C}$首先检测id是否在撤销列表RL中,若$id\in RL$,那么$\mathcal{C}$终止并输出$\perp$;否则,$\mathcal{C}$运行秘密钥生成算法KeyGen,产生身份id在T_i时刻所对应的私钥$sk_{(id,T_i)}$,再运行解密算法Dec,用$sk_{(id,T_i)}$解密密文C,并将相应的明文M发送给$\mathcal{A}$.

泄露询问.当收到$\mathcal{A}$提交的关于身份id在T_i时刻对应私钥$sk_{(id,T_i)}$的泄露询问,$\mathcal{C}$首先通过运行KeyGen获得相应的私钥$sk_{(id,T_i)}$,然后运行泄露谕言机$\mathcal{O}^{\lambda,\kappa}_{sk_{id,T_i}}(\cdot)$,产生$sk_{(id,T_i)}$的泄露信息$f_i(sk_{(id,T_i)})$,并把$f_i(sk_{(id,T_i)})$发送给敌手$\mathcal{A}$,其中$f_i:\{0,1\}^{*}\rightarrow\{0,1\}^{\lambda_i}$是由敌手提交的高效可计算的泄露函数;特别需要说明的是,关于同一用户私钥$sk_{(id,T_i)}$泄露信息的总量不能超过系统设定的泄露界λ,即有$\sum_{l=1}^{i}f_l(sk_{(id,T_i)})\leq\lambda$成立;否则$\mathcal{C}$将输出终止符号$\perp$给敌手$\mathcal{A}$.

身份撤销询问.对于敌手$\mathcal{A}$提交的待撤销身份集合$\{id_1,\cdots,id_n\}$,挑战者$\mathcal{C}$输出更新后的身份撤销列表$RL=RL\cup\{id_1,\cdots,id_n\}$.

密钥更新询问.对于身份id在T_{i+1}时刻的密钥更新询问,挑战者$\mathcal{C}$首先检测id是否在撤销列表RL中,若$id\in RL$,那么$\mathcal{C}$终止并输出$\perp$;否则,$\mathcal{C}$运行密钥更新算法KeyUpdate,产生身份id在T_{i+1}

时刻所对应的时间组件 $k_{T_{i+1}}$，并将其发送给 $\mathcal{A}$.

③ 挑战. 敌手 $\mathcal{A}$ 某时刻决定结束阶段 1，并输出挑战元组 (id^*, T_i, M_0, M_1)（其中 $M_0, M_1 \in \mathcal{M}$ 且 $|M_0|=|M_1|$），但是阶段 1 中不能对挑战身份 id^* 进行密钥生成询问，同时关于挑战身份 id^* 所对应私钥 sk_{id^*} 泄露信息的总量不能超过 λ. $\mathcal{C}$ 计算挑战密文 $C^*_{(v,T_i)}=\mathrm{Enc}(id^*, T_i, M_v)$，其中 $v \leftarrow_R \{0,1\}$，并将 $C^*_{(v,T_i)}$ 发送给 $\mathcal{A}$.

④ 阶段 2(训练). 敌手在该阶段除不能提交相应的泄露询问之外，将适应性地重复执行阶段 1 中的其他询问，但是相应的询问具有一定的限制条件.

密钥生成询问. 对除挑战身份 id^* 之外的任何身份 $id(id \neq id^*)$ 进行密钥产生询问. 挑战者 $\mathcal{C}$ 以阶段 1 中的方式进行回应.

解密询问. 敌手提交关于 (id, C) 的解密询问，其中 $(id, C) \neq (id^*, C^*_{(v,T_i)})$. $\mathcal{C}$ 将使用与阶段 1 相类似的方法返回相应的明文消息.

身份撤销询问和密钥更新询问的应答方式与阶段 1 的相应询问相类似，但询问的身份中不能涉及挑战身份.

⑤ 猜测. 敌手 $\mathcal{A}$ 输出对随机数 v 的猜测 v'，如果 $v=v'$，则敌手 $\mathcal{A}$ 攻击成功.

敌手 $\mathcal{A}$ 在上述游戏中获胜的优势定义为

$$Adv^{\text{LR-CCA}}_{\text{RIBE},\mathcal{A}}(\kappa,\lambda)=\left|\Pr[v=v']-\frac{1}{2}\right|.$$

其中概率来自于模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 对随机数的使用.

定义 5(抗泄露 RIBE 机制的 CCA 安全性，LR-CCA 安全性). 若对任意的 PPT 敌手 $\mathcal{A}$，其在上述游戏中获胜的优势 $Adv^{\text{LR-CCA}}_{\text{RIBE},\mathcal{A}}(\kappa,\lambda)$ 是可忽略的，那么相应的 RIBE 机制是抗泄露选择密文攻击安全的.

相类似地，在抗泄露 RIBE 机制的 CPA 安全性游戏中，敌手能够执行除解密询问之外的其他询问，且限制条件与 CCA 安全性游戏相一致.

5　CPA 安全的抗泄露 RIBE 机制

基于 IB-HPS，本节将给出 CPA 安全的抗泄露 RIBE 机制的通用构造；并基于底层 IB-HPS 的安全性，给出我们通用构造的形式化证明过程.

5.1　具体构造

令 $\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_v}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k+l_v-\lambda,\varepsilon)$-强随机性提取器，其中 λ 是泄露参数，ε 在安全参数 κ 上是可忽略的，$\{0,1\}^{l_t}$ 是提取器的随机种子空间. 令 $\Pi_1=(\mathrm{Setup}_1, \mathrm{KeyGen}_1, \mathrm{Encap}_1, \mathrm{Encap}_1^*, \mathrm{Decap}_1)$ 是封装密钥空间为 $\mathcal{K}_1=\{0,1\}^{l_k}$、身份空间为 $\mathcal{ID}_1$ 的平滑性 IB-HPS. 令 $\Pi_2=(\mathrm{Setup}_2, \mathrm{KeyGen}_2, \mathrm{Encap}_2, \mathrm{Encap}_2^*, \mathrm{Decap}_2)$ 是封装密钥空间为 $\mathcal{K}_2=\{0,1\}^{l_v}$、身份空间为 $\mathcal{ID}_2$ 的平滑性 IB-HPS. 令 $\mathcal{H}:\mathcal{ID}_1\times\mathcal{T}\rightarrow\mathcal{ID}_2$ 是抗碰撞的单向哈希函数，其中 $\mathcal{T}$ 表示时刻列表 TL 中的时刻.

CPA 安全的抗泄露 RIBE 机制通用构造 $\mathcal{E}'=(\mathrm{Setup}', \mathrm{KeyGen}', \mathrm{Enc}', \mathrm{Dec}', \mathrm{Revoke}', \mathrm{KeyUpdate}')$ 的具体算法如下所述：

(1) $(Params, msk)\leftarrow\mathrm{Setup}'(1^\kappa)$

输出 $Params=(mpk_1, mpk_2)$ 和 $msk=(msk_1, msk_2)$，其中

$$(mpk_1, msk_1)\leftarrow\mathrm{Setup}_1(1^\kappa)\text{和}$$

$$(mpk_2, msk_2)\leftarrow\mathrm{Setup}_2(1^\kappa).$$

特别地，该算法还定义了初始为空的身份撤销列表 RL，并且初始化了时间列表 TL.

(2) $(sk_{(id,T_i)}, T_i)\leftarrow\mathrm{KeyGen}'(msk, id, RL, TL)$

对于身份 id 的密钥生成，PKG 首先检测身份 id 是否在撤销列表 RL 中，若 $id\in RL$，算法 KeyGen 输出 $\perp$；否则 PKG 执行下述操作：

计算

$$d^1_{id}\leftarrow\mathrm{KeyGen}_1(msk_1, id)$$

从时间列表 TL 中读取当前时戳 T_i，并计算 $id'=\mathcal{H}(id, T_i)$ 和 $d^2_{id}\leftarrow\mathrm{KeyGen}_2(msk_2, id')$.

输出身份 id 在 T_i 时刻的私钥

$$sk_{(id,T_i)}=(k_{id}, k_{T_i})=(d^1_{id}, d^2_{id}),$$

其中 $k_{id}=d^1_{id}$ 是私钥 $sk_{(id,T_i)}$ 的身份组件，$k_{T_i}=d^2_{id}$ 是私钥 $sk_{(id,T_i)}$ 的时间组件.

(3) $(C_{T_i}, T_i)\leftarrow\mathrm{Enc}'(M, id, T_i)$

对于一个消息 $M\in\mathcal{M}=\{0,1\}^{l_m}$，时间戳 T_i 和身份 $id\in\mathcal{ID}$，加密者进行下述运算：

计算

$$id'=\mathcal{H}(id, T_i).$$

计算

$$(c_1, k_1)\leftarrow\mathrm{Encap}_1(id)\text{和}(c_2, k_2)\leftarrow\mathrm{Encap}_2(id').$$

随机选取 $S\leftarrow_R\{0,1\}^{l_t}$ 后计算

$$c_3\leftarrow\mathrm{Ext}(k_1, k_2, S)\oplus M.$$

输出密文 $C_{T_i}=(c_1, c_2, c_3, S)$，即密文 C_{T_i} 是身份 id 在 T_i 时刻对消息 M 的加密密文.

(4) $M\leftarrow\mathrm{Dec}'(C_{T_i}, sk_{(id,T_i)})$

对于身份 id 在 T_i 时刻的秘钥 $sk_{(id,T_i)}=(d^1_{id}, d^2_{id})$ 和加密密文 $C_{T_i}=(c_1, c_2, c_3, S)$，解密者进行下述运算：

计算

$k_1=\mathrm{Encap}_1(c_1,d_{id}^1)$和$k_2=\mathrm{Encap}_2(c_2,d_{id}^2)$.

计算

$$M=\mathrm{Ext}(k_1,k_2,S)\oplus c_3.$$

输出密文$C=(c_1,c_2,c_3,S)$所对应的明文消息M.

(5) $RL'\leftarrow\mathrm{Revoke}'(RL,\{id_1,\cdots,id_n\})$

若集合$\{id_1,\cdots,id_n\}$中的身份将被撤销,那么PKG通过下述操作对身份撤销列表进行更新.

$$RL'=RL\bigcup\{id_1,\cdots,id_n\}.$$

(6) $k_{T_{i+1}}\leftarrow\mathrm{KeyUpdate}'(RL,id,T_{i+1},msk)$

当收到身份$id\in\mathcal{ID}$在时间戳T_{i+1}时刻的密钥更新询问时,PKG首先检测身份id是否在撤销列表RL中,若存在则PKG输出$\perp$,并终止;否则PKG进行下列运算:

计算

$id'=\mathcal{H}(id,T_{i+1})$和$d_{id}^2\leftarrow\mathrm{KeyGen}_2(msk_2,id')$.

输出$k_{T_{i+1}}=d_{id}^2$.那么身份id所对应的密钥由T_i时刻的$sk_{(id,T_i)}=(k_{id},k_{T_i})$更新为$T_{i+1}$时刻的$sk_{(id,T_{i+1})}=(k_{id},k_{T_{i+1}})$,随着时间戳$T_i$的递增,用户之前的私钥$sk_{(id,T_i)}$相继被撤销.

5.2 安全性证明

上述通用构造的正确性可由底层IB-HPS的正确性获得,下面将给出上述通用构造安全性的形式化证明过程.

定理4. 假设Π_1和Π_2是两个平滑性IB-HPS,$\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_v}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$是平均情况的$(l_k+l_v-\lambda,\varepsilon)$-强随机性提取器.那么,对于任意的泄露参数$\lambda\leq l_k+l_v-l_m-\omega(\log\kappa)$,上述构造$\mathcal{E}'$是CPA安全的抗泄露RIBE机制的通用构造.

定理4的证明详见附录B.

5.3 改进的构造

抗有界泄露攻击的密码机制要求相应机制的运行过程中敌手仅能获得有界的泄露信息;然而,在密码机制的实际应用中,敌手往往能够通过各种物理攻击(如边信道攻击、冷启动攻击等)进行持续的泄露攻击,使得传统抗有界泄露攻击的密码机制不具备其所声称的安全性,那么研究密码机制的抵抗连续泄露攻击的能力可以增强传统密码机制的实用性.

在FOCS2010中,Dodis等人[9]指出当一个密码原语在满足下属两个条件时,该机制具有抵抗连续泄露攻击的能力:(1)在保证公开参数和性能不变的前提下,密钥能够进行周期性更新,并且外界无法识别该更新;(2)在连续泄露攻击中,只要相应密码机制在两次密钥更新间隔内当前私钥的泄露总量未超过系统设定的安全参数,则相应的机制依然保持其所声称的安全性.此外,Zhou等人[26]提出了一个新的密码学原语,称为U-IB-HPS;该原语在IB-HPS的基础上,增加了一个额外的密钥更新算法,在保持公开参数不变的前提下,对用户密钥进行周期性更新,基于新的随机数产生与原始密钥不可区分的新密钥(特别地,U-IB-HPS基于IB-HPS设计,本文不再赘述它的形式化定义和安全属性,详见文献[26]).

特别地,定理3表明可用泄露平滑的IB-HPS来直接构造抗泄露的身份基密码机制;由于泄露平滑的IB-HPS输出的封装密钥具有抗泄露攻击的能力,因此在这种情况下不再使用随机性提取器.

综上所述,为增强RIBE机制的实用性,我们能够直接使用具有泄露平滑性质的U-IB-HPS构造CPA安全的抵抗连续泄露攻击的RIBE机制的通用构造$\mathcal{E}''=(\mathrm{Setup}'',\mathrm{KeyGen}'',\mathrm{Enc}'',\mathrm{Dec}'',\mathrm{Update}'',\mathrm{Revoke}'',\mathrm{KeyUpdate}'')$,具体描述如下:

令$\Pi_1=(\mathrm{Setup}_1,\mathrm{KeyGen}_1,\mathrm{Encap}_1,\mathrm{Encap}_1^*,\mathrm{Decap}_1,\mathrm{Update}_1)$是封装密钥空间为$\mathcal{K}=\{0,1\}^{l_m}$的$l_k$-泄露平滑性U-IB-HPS.令$\Pi_2=(\mathrm{Setup}_2,\mathrm{KeyGen}_2,\mathrm{Encap}_2,\mathrm{Encap}_2^*,\mathrm{Decap}_2,\mathrm{Update}_2)$是封装密钥空间为$\mathcal{K}=\{0,1\}^{l_m}$的$l_v$-泄露平滑性U-IB-HPS.令$\mathcal{H}:\mathcal{ID}_1\times\mathcal{T}\rightarrow\mathcal{ID}_2$是抗碰撞的单向哈希函数,其中$\mathcal{T}$表示时刻列表$TL$中的时刻.

(1) $(Params,msk)\leftarrow\mathrm{Setup}''(1^\kappa)$

输出$Params=(mpk_1,mpk_2)$和$msk=(msk_1,msk_2)$,其中

$$(mpk_1,msk_1)\leftarrow\mathrm{Setup}_1(1^\kappa)\text{和}$$

$$(mpk_2,msk_2)\leftarrow\mathrm{Setup}_2(1^\kappa).$$

此外,初始化算法还定义了初始为空的身份撤销列表RL,并且初始化了时间列表TL.

(2) $(sk_{(id,T_i)},T_i)\leftarrow\mathrm{KeyGen}''(msk,id,RL,TL)$

对于身份id的密钥生成,PKG首先检测身份id是否在撤销列表RL中,若$id\in RL$,算法KeyGen输出$\perp$;否则PKG执行下述操作:

计算

$$d_{id}^1\leftarrow\mathrm{KeyGen}_1(msk_1,id)$$

从时间列表TL中读取当前时戳T_i,并计算

$id'=\mathcal{H}(id,T_i)$和$d_{id}^2\leftarrow\mathrm{KeyGen}_2(msk_2,id')$.

输出身份 id 在 T_i 时刻所对应的私钥 $sk_{(id,T_i)}=(k_{id},k_{T_i})=(d_{id}^1,d_{id}^2)$，其中 $k_{id}=d_{id}^1$ 是私钥 $sk_{(id,T_i)}$ 的身份组件，$k_{T_i}=d_{id}^2$ 是私钥 $sk_{(id,T_i)}$ 的时间组件.

(3) $sk'_{id}\leftarrow\text{Update}''(sk_{id},id,T_i)$

对 T_i 时刻身份 id 的密钥进行更新 $sk_{id}=(k_{id},k_{T_i})$，PKG 首先检测身份 id 是否在撤销列表 RL 中，若 $id\in RL$，输出 $\perp$；否则 PKG 执行下述操作：

计算

$$d'^1_{id}\leftarrow\text{Update}_1(k_{id},id)$$

计算

$id'=\mathcal{H}(id,T_i)$ 和 $d'^2_{id}\leftarrow\text{Update}_2(k_{T_i},id')$.

输出 $sk'_{(id,T_i)}=(k'_{id},k'_{T_i})=(d'^1_{id},d'^2_{id})$.

特别地，用户私钥的更新操作并非是私钥的撤销操作，因为 T_i 时刻的私钥 $sk_{(id,T_i)}$ 更新后的输出依然是 T_i 时刻的有效用户私钥 $sk'_{(id,T_i)}$，即更新操作生成了某一时刻用户的新私钥，使得该时刻之前私钥的泄露信息对新的私钥不起作用. 然而，用户私钥的撤销更新则是将当前 T_i 时刻的私钥撤销 $sk_{(id,T_i)}$，由下一 T_{i+1} 时刻的有效私钥 $sk_{(id,T_{i+1})}$ 替换.

(4) $(C_{T_i},T_i)\leftarrow\text{Enc}''(M,id,T_i)$

对于一个消息 $M\in\mathcal{M}=\{0,1\}^{l_m}$，时间戳 T_i 和身份 $id\in\mathcal{ID}$，加密者进行下述运算：

计算

$$id'=\mathcal{H}(id,T_i).$$

计算

$(c_1,k_1)\leftarrow\text{Encap}_1(id)$ 和 $(c_2,k_2)\leftarrow\text{Encap}_2(id')$.

计算

$$c_3\leftarrow k_1\oplus k_2\oplus M.$$

输出身份 id 在时刻 T_i 对明文消息 M 的加密密文 $C_{T_i}=(c_1,c_2,c_3)$.

(5) $M\leftarrow\text{Dec}''(C,sk_{id},T_i)$

对于相对于身份 id 和时间戳 T_i 的私钥 $sk_{(id,T_i)}=(d_{id}^1,d_{id}^2)$ 和密文 $C_{T_i}=(c_1,c_2,c_3)$，解密者进行下述运算：

计算

$k_1=\text{Encap}_1(c_1,d_{id}^1)$ 和 $k_2=\text{Encap}_2(c_2,d_{id}^2)$.

计算

$$M=k_1\oplus k_2\oplus c_3.$$

输出密文 $C=(c_1,c_2,c_3)$ 所对应的明文消息 M.

运行密钥更新算法 $sk'_{id}\leftarrow\text{Update}''(sk_{id},id,T_i)$ 生成新的用户私钥 sk'_{id} 参与下一轮的计算(即下一轮的解密运算将使用 sk'_{id})，使得之前关于 sk_{id} 的泄露信息对新的私钥 sk'_{id} 是无任何意义的，即敌手获得的泄露信息将重新开始计数.

(6) $RL'\leftarrow\text{Revoke}''(RL,\{id_1,\cdots,id_n\})$

若集合 $\{id_1,\cdots,id_n\}$ 中的身份将被撤销，那么 PKG 通过下述操作对身份撤销列表进行更新.

$$RL'=RL\cup\{id_1,\cdots,id_n\}.$$

(7) $k_{T_{i+1}}\leftarrow\text{KeyUpdate}'(RL,id,T_{i+1},msk)$

当收到身份 $id\in\mathcal{ID}$ 在时间戳 T_{i+1} 时的密钥更新询问时，PKG 首先检测身份 id 是否在撤销列表 RL 中，若存在则 PKG 输出 $\perp$，并终止；否则 PKG 进行下列运算：

计算

$id'=\mathcal{H}(id,T_{i+1})$ 和 $d^2_{id}\leftarrow\text{KeyGen}_2(msk_2,id')$.

输出 $k_{T_{i+1}}=d^2_{id}$.

定理 5.　假设 Π_1 和 Π_2 分别是两个 l_k 和 l_v-泄露平滑的 U-IB-HPS. 那么，对于任意的轮泄露参数 $\lambda\leq l_k+l_v-\omega(\log\kappa)$，上述构造 $\mathcal{E}''$ 是 CPA 安全的抵抗连续泄露攻击的 RIBE 机制的通用构造.

定理 5 的证明与定理 4 的证明相类似，本文不再赘述. 由 Dodis 等人[9]的结论可知连续泄露攻击的最大优势是可将连续泄露攻击的问题转化为单轮的有界泄露容忍性问题，因此定理 5 可在证明有界泄露容忍的前提下，基于附加的密钥更新算法获得机制的抗连续泄露性. 特别地，抗连续泄露的 RIBE 机制中，通过附加的密钥更新算法将整个 RIBE 机制分成了不同的周期，每个周期结束时通过运行密钥更新算法生成新的用户密钥，使得该周期内产生的泄露信息对新密钥是无意义的.

6　CCA 安全的抗泄露 RIBE 机制

对于一个加密机制而言，CCA 安全性是一个非常实用且重要的安全属性. 因此，本节将基于 CPA 安全的抗泄露 RIBE 机制，给出 CCA 安全的抗泄露 RIBE 机制的通用构造.

为方便机制的设计，对 CPA 安全的抗泄露 RIBE 机制的加密算法进行简单的修改，即加密算法所使用的随机数来自于算法输入，则相应的加密算法可表示为

$$C\leftarrow\text{Enc}(M,id,T_i,r),$$

其中 r 表示加密算法运算过程中所使用的随机数.

6.1　具体构造

令 $\mathcal{E}'=(\text{Setup}',\text{KeyGen}',\text{Enc}',\text{Dec}',\text{Revoke}',$

KeyUpdate′)是一个 CPA 安全的抗泄露 RIBE 机制,$\Pi'_{\text{nizk}}=(\text{Setup},\text{Prove},\text{Verify})$是关系 R_{enc} 上的强一次性 f-tSE NIZK 论证,其中

$$R_{\text{enc}}=\{(M,r),(id,T_i,C')\mid C'=\text{Enc}'(M,id,T_i,r)\}.$$

此外,在提取操作中,f-tSE NIZK 论证中的提取器 Ext′只需要输出消息 M,无需输出加密所需的随机数 r,即 $f(M,r)=M$.

CCA 安全的抗泄露 RIBE 机制通用构造 $\mathcal{E}'''=(\text{Setup}''',\text{KeyGen}''',\text{Enc}''',\text{Dec}''',\text{Revoke}''',\text{KeyUpdate}''')$ 的具体算法表述如下:

(1) $(Params,msk)\leftarrow\text{Setup}'''(1^\kappa)$

输出 $Params=(Params',CRS)$ 和 $msk=msk'$,其中

$(Params',msk')\leftarrow\text{Setup}'(1^\kappa)$ 和

$(CRS,tk,ek)\leftarrow\text{Setup}(1^\kappa)$.

(2) $sk_{id}\leftarrow\text{KeyGen}'''(msk,id,T_i)$

输出 $sk_{(id,T_i)}=sk'_{(id,T_i)}$,其中

$sk'_{(id,T_i)}\leftarrow\text{KeyGen}'(msk,id,T_i)$.

(3) $C_{T_i}\leftarrow\text{Enc}'''(M,id,T_i)$

从相应的空间中选取一个随机数 r,并计算

$$C'\leftarrow\text{Enc}'(M,id,T_i,r).$$

生成 C' 所对应的 NIZK 论证 π,即

$$\pi\leftarrow\text{Prove}((M,r),(C',id,T_i)).$$

输出密文 $C_{T_i}=(C',\pi)$.

(4) $M/\perp\leftarrow\text{Dec}'''(C_{T_i},sk_{(id,T_i)},T_i)$

接收者首先验证

$$\text{Verify}(\pi,(C',id,T_i))=1$$

是否成立,若成立则输出 $M\leftarrow\text{Dec}'(C',sk_{(id,T_i)})$;否则输出 $\perp$.

(5) $RL'\leftarrow\text{Revoke}'''(RL,\{id_1,\cdots,id_n\})$

若集合 $\{id_1,\cdots,id_n\}$ 中的身份将被撤销,那么 PKG 通过下述操作对身份撤销列表进行更新.

$$RL'\leftarrow\text{Revoke}'(RL,\{id_1,\cdots,id_n\}).$$

(6) $k_{T_{i+1}}\leftarrow\text{KeyUpdate}'''(RL,id,T_{i+1},msk)$

当收到身份 $id\in\mathcal{ID}$ 在 T_{i+1} 时刻的密钥更新询问时,PKG 首先检测身份 id 是否在撤销列表 RL 中,若存在则 PKG 输出 $\perp$,并终止;否则 PKG 计算:

$$k_{T_{i+1}}\leftarrow\text{KeyUpdate}'(RL,id,T_{i+1},msk).$$

输出身份 id 在 T_{i+1} 时刻私钥 $sk_{(id,T_{i+1})}$ 的时间组件 $k_{T_{i+1}}$.

6.2 安全性证明

上述通用构造的正确性可由底层 CPA 安全的抗泄露 RIBE 机制和 f-tSE NIZK 论证的正确性获得.本节将对上述构造 $\mathcal{E}'''$ 抗泄露攻击的 CCA 安全性进行形式化证明.

定理 6. 假设 $\mathcal{E}'$ 是一个 CPA 安全的抗泄露 RIBE 机制,Π'_{nizk} 是相应关系上的强一次性 f-tSE NIZK 论证.那么,上述构造 $\mathcal{E}'''$ 是 CCA 安全的抗泄露 RIBE 机制的通用构造.

定理 6 的证明详见附录 C.

6.3 性能扩展

类似地,借鉴上述 CCA 安全的抗泄露 RIBE 机制的设计思路,将底层 IB-HPS 更换为 U-IB-HPS 即可得到 CCA 安全的抵抗连续泄露攻击的 RIBE 机制的通用构造.

此外,为了方便读者了解构造 CCA 安全的抗泄露 RIBE 机制时 NIZK 和 OT-LF 的区别与联系,本文在附录 D 中给出了基于 OT-LF 设计 CCA 安全的抗泄露 RIBE 机制的具体构造,由于 OT-LF 在抗泄露 IBE 机制的构造中已有相应的使用,因此本文仅给出了具体的构造,省略了证明过程.

7 实例化

本文以 f-tSE NIZK 论证、IB-HPS 和 U-IB-HPS 作为底层基础工作设计了 CPA/CCA 安全的抗(连续)泄露攻击的 RIBE 机制的通用构造.由于本文抗泄露 RIBE 机制的通用构造具有模块化的结构,并且各模块已有相应的具体实例相继被提出,因此,基于上述各底层工具的具体构造即可设计出本文抗泄露 RIBE 机制的具体实例.由于底层基础工具的实例化问题并非本文的重点研究内容,我们在本文不再设计底层工具的具体实例.

换句话讲,本文的通用构造的基础模块是:f-tSE NIZK 论证、IB-HPS 和 U-IB-HPS,然而上述基础模块的具体实例已被多位研究者相继提出,其中 Dodis 等人在文献[54]中指出能够基于任意 CCA 安全的加密机制和标准的 NIZK 论证来构造 f-tSE NIZK 论证;Chow 等人[19]和 Chen 等人[20-21]给出了多个 IB-HPS 的构造,甚至是匿名的 IB-HPS;Zhou 等人[22,55-56]给出了 U-IB-HPS 的具体实例.然而,为保持文章的完整性,在 Chow 等人[19]实例的基础上,我们将在附录 E 中给出一个泄露平滑的 IB-HPS 的具体实例,方便读者了解 IB-HPS 的具体构造.

8　应用探索

本节将以数据授权机制为例，简述抗(连续)泄露 RIBE 机制在现实环境中的应用情况.

令 $\mathcal{E}=$ Setup, KeyGen, Enc, Dec, Revoke, KeyUpdate)是抗泄露的 RIBE 机制. 如图 2 所示，数据拥有者$\mathcal{U}_0$将自己的数据授权给云计算环境中集合$\{\mathcal{U}_1,\mathcal{U}_2,\cdots,\mathcal{U}_n\}$中的用户使用，具体可撤销的抗泄露数据授权机制的工作流程如下所述：

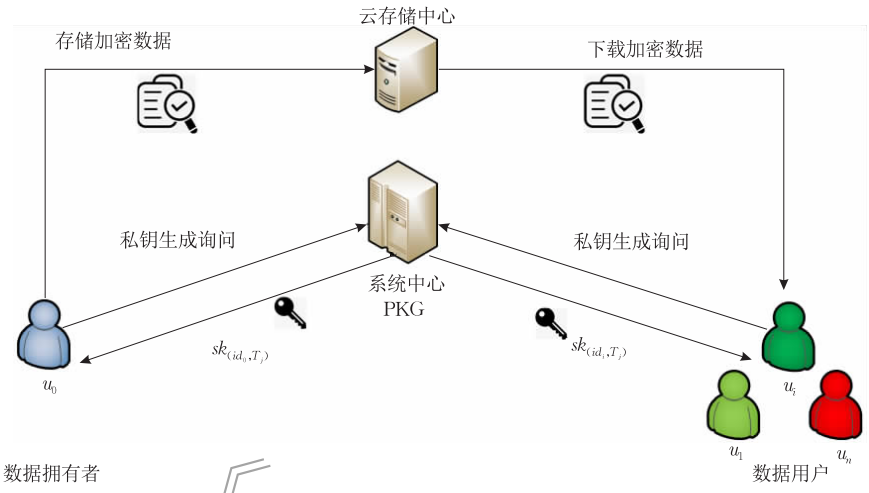

图 2 可撤销的抗泄露数据授权机制

(1) 系统建立. 系统中心 PKG 运行初始化算法建立系统公开参数，即

$$(Params,msk)\leftarrow \text{Setup}'''(1^\kappa).$$

秘密保存主密钥 msk 的同时，对外公布 $Params$ 和当前系统时刻 T_j. 此外，为系统中的用户 id_i 生成 T_j 时刻的私钥 $sk_{(id_i,T_j)}$，即

$$sk_{(id_i,T_j)}\leftarrow \text{KeyGen}(msk,id_i,T_j).$$

(2) 数据共享. 数据拥有者$\mathcal{U}_0$使用相应用户$\mathcal{U}_i(1\leq i\leq n)$的身份信息 id_i 和系统中心 PKG 公布的当前时刻 T_j 对相应的共享数据 m_i 进行加密，然后将加密后的数据 $C^i_{T_j}$ 存储到相应的云数据库中，其中

$$C^i_{T_j}=\text{Enc}(id_i,T_j,m_i).$$

特别地，当 $n=1$ 时，数据拥有者仅对一个用户进行授权；否则，是对多个用户进行授权.

(3) 数据使用. 数据用户$\mathcal{U}_i(1\leq i\leq n)$从云数据库中下载相应的加密数据 $C^i_{T_j}$，使用自己在 T_j 时刻的私钥 $sk_{(id_i,T_j)}$ 解密 $C^i_{T_j}$ 即可获得相应的明文数据 m_i，其中

$$m_i=\text{Dec}(sk_{(id_i,T_j)},C^i_{T_j},T_j).$$

(4) 用户撤销. 当系统中出现身份需撤销的用户时，PKG 执行用户撤销操作，对用户撤销列表 RL 进行更新，将撤销用户的身份信息$\{id_1,\cdots,id_m\}$添加到 RL 中，输出更新后的撤销列表 RL'，即 PKG 执行

$$RL'\leftarrow \text{Revoke}(RL,\{id_1,\cdots,id_m\}).$$

撤销列表 RL 更新后，PKG 将当前的系统时刻调整为 T_{j+1}，并为系统中未撤销的用户 id_t 分发私钥的时间组件 $k_{T_{j+1}}$，即

$$k_{T_{j+1}}\leftarrow \text{KeyUpdate}(RL,id_t,T_{i+1},msk).$$

用户id_t设置新的私钥为 $sk_{(id_t,T_{j+1})}=(k_{id_t},k_{T_{i+1}})$. 因此，被撤销用户 id_η 的原始私钥 $sk_{(id_\eta,T_j)}$ 将失效，其无法完成对后续加密数据的解密，即使数据拥有者$\mathcal{U}_0$在未知情的前提下为其进行了授权，输出了加密数据 $C^\eta_{T_{j+1}}$，但是用户 id_η 依然无法解密 $C^\eta_{T_{j+1}}$. 由于底层的 RIBE 机制具有抗泄露的性质，因此上述授权数据访问机制能够抵抗泄露攻击.

此外，也可考虑为每个用户设置时刻信息，对撤销用户的时刻进行更替，使得过去时刻的私钥失效，而对于非撤销用户的时刻信息可不用进行更新，这样 PKG 就无需对非撤销用户的时间组件进行更新，一定程度上能降低 PKG 的执行复杂度. 为防止敌手获得私钥的过多泄露信息，PKG 可周期性的对系统当前未撤销用户的时刻信息进行更替，并为他们生成新的时间组件，这样即可用新的私钥替换原始的旧私钥，使得之前私钥的泄露对当前私钥不起作用，而且在一定程度上达到了抵抗连续泄露攻击的效果.

9 结束语

可撤销 IBE 机制作为一种较为理想的数据加密机制,其安全性和实用性对其实际应用有着至关重要的作用.本文针对传统 RIBE 机制无法抵抗泄露攻击的不足,基于现有的 IB-HPS 和 U-IB-HPS 分别设计了抗泄露 RIBE 机制和抗连续泄露 RIBE 机制的通用构造,并基于底层技术的安全性对本文通用构造相应的 CPA 安全性进行了形式证明.为进一步增强上述通用构造的安全性,在现有构造的基础上引入 NIZK 论证实现密文元素间的防扩展性,设计了 CCA 安全的抗泄露 RIBE 机制,并基于 IB-HPS 和 NIZK 论证的安全性对所提出构造的安全性进行了形式化证明.分析表明我们的构造具有抵抗秘密信息泄露的能力,在信息可泄露的环境中依然保持其所声称的安全性.此外,本文通用构造中所使用的基础工作,目前已有多位研究者提出了多个具体构造,因此本文的通用构造是可实例化的,具有较强的实用性.

参 考 文 献

[1] Naor M, Segev G. Public-key cryptosystems resilient to key leakage//Proceedings of the Advances in Cryptology—CRYPTO 2009, 29th Annual International Cryptology Conference. Santa Barbara, USA, 2009: 18-35

[2] Alwen J, Dodis Y, Naor M, et al. Public-key encryption in the bounded-petrieval model//Proceedings of the Advances in Cryptology—EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Monaco, 2010: 113-134

[3] Liu Shengli, Weng Jian, Zhao Yunlei. Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks //Proceedings of the Topics in Cryptology—CT-RSA 2013-The Cryptographers' Track at the RSA Conference 2013. San Francisco, USA, 2013: 84-100

[4] Qin Baodong, Liu Shengli. Leakage-resilient chosen-ciphertext secure public-key encryption from Hash proof system and one-time lossy filter//Proceedings of the Advances in Cryptology—ASIACRYPT 2013-19th International Conference on the Theory and Application of Cryptology and Information Security. Bengaluru, India, 2013: 381-400

[5] Qin Baodong, Liu Shengli. Leakage-flexible CCA-secure public-key encryption: Simple construction and free of pairing //Proceedings of the Public-Key Cryptography—PKC 2014-17th International Conference on Practice and Theory in Public-Key Cryptography. Buenos Aires, Argentina, 2014: 19-36

[6] Li Sujuan, Zhang Futai, Sun Yinxia, Shen Limin. Efficient leakage-resilient public key encryption from DDH assumption. Cluster Computing, 2013, 16(4): 797-806

[7] Zhang Ming-Wu, Chen Mi-Wen, He De-Biao, et al. An efficient leakage-resilient and CCA2-secure PKE system. Chinese Journal of Computers, 2016, 39(3): 492-502(in Chinese)
(张明武, 陈泌文, 何德彪等. 高效弹性泄漏下 CCA2 安全公钥加密体制. 计算机学报, 2016, 39(3): 492-502)

[8] Wang Zhi-Wei, Li Dao-Feng, Zhang Wei, et al. CCA secure PKE with auxiliary input. Chinese Journal of Computers, 2016, 39(3): 562-570(in Chinese)
(王志伟, 李道丰, 张伟等. 抗辅助输入 CCA 安全的 PKE 构造. 计算机学报, 2016, 39(3): 562-570)

[9] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Cryptography against continuous memory attacks//Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010), Las Vegas, USA, 2010: 511-520

[10] Li Su-Juan, Zhang Ming-Wu, Zhang Fu-Tai. Security analysis and improvement of CCA secure PKE with (continual) auxiliary input. Chinese Journal of Computers, 2018, 41(12): 2823-2832(in Chinese)
(李素娟, 张明武, 张福泰. 抗(持续)辅助输入 CCA 安全的 PKE 构造方案的分析及改进. 计算机学报, 2018, 41(12): 2823-2832)

[11] Zhou Yanwei, Yang Bo, Zhang Wenzheng, Mu Yi. CCA2 secure public-key encryption scheme tolerating continual leakage attacks. Security and Communication Networks, 2016, 9(17): 4505-4519

[12] Zhou Yanwei, Yang Bo. Continuous leakage-resilient public-key encryption scheme with CCA security. The Computer Journal, 2017, 60(8): 1161-1172

[13] Yang Rupeng, Xu Qiuliang, Zhou Yongbin, et al. Updatable Hash proof system and its applications//Proceedings of the Computer Security—ESORICS 2015-20th European Symposium on Research in Computer Security. Vienna, Austria, 2015: 266-285

[14] Li Jiguo, Teng Meilin, Zhang Yichen, Yu Qihong. A leakage-resilient CCA-secure identity-based encryption scheme. The Computer Journal, 2016, 59(7): 1066-1075

[15] Zhang Ming-Wu, Wang Chun-Zhi, Yang Bo, et al. Key leakage-resilient secure cryptosystem with hierarchical wildcard pattern delegation. Journal of Software, 2015, 26(5): 1196-1212(in Chinese)
(张明武, 王春枝, 杨波等. 密钥弹性泄漏安全的通配模板层次委托加密机制. 软件学报, 2015, 26(5): 1196-1212)

[16] Zhang Yinghui, Yang Menglei, Zheng Dong, et al. Leakage-resilient hierarchical identity-based encryption with recipient anonymity. International Journal of Foundations of Computer Science, 2019, 30(4): 665-681

[17] Sun Shifeng, Gu Dawu, Liu Shengli. Efficient chosen ciphertext secure identity-based encryption against key leakage attacks. Security and Communication Networks, 2016, 9(11): 1417-1434

[18] Sun Shifeng, Gu Dawu, Huang Zhengan. Fully secure wicked identity-based encryption against key leakage attacks. The Computer Journal, 2015, 58(10): 2520-2536

[19] Chow S S M, Dodis Y, Rouselakis Y, Waters B. Practical leakage-resilient identity-based encryption from simple assumptions//Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010). Chicago, USA, 2010: 152-161

[20] Chen Yu, Zhang Zongyang, Lin Dongdai, Cao Zhenfu. Generalized (identity-based) hash proof system and its applications. Security and Communication Networks, 2016, 9(12): 1698-1716

[21] Chen Yu, Zhang Zongyang, Lin Dongdai, Cao Zhenfu. Anonymous identity-based hash proof system and its applications //Proceedings of the Provable Security-6th International Conference(ProvSec 2012). Chengdu, China, 2012: 143-160

[22] Zhou Yanwei, Yang Bo, Hou Hong-Xia, et al. Continuous leakage-resilient identity-based encryption with tight security. The Computer Journal, 2019,62(8): 1092-1105

[23] Zhou Yanwei, Yang Bo, Mu Yi. Continuous leakage-resilient identity-based encryption without random oracles. The Computer Journal, 2018, 61(4): 586-600

[24] Zhou Yanwei, Yang Bo, Mu Yi, et al. Identity-based encryption resilient to continuous key leakage. IET Information Security, 2019, 13(5): 426-434

[25] Zhou Yanwei, Yang Bo, Mu Yi. Continuous leakage-resilient identity-based encryption with leakage amplification. Designs, Codes and Cryptography, 2019, 87(9): 2061-2090

[26] Zhou Yanwei, Yang Bo, Mu Yi. The generic construction of continuous leakage-resilient identity-based cryptosystems. Theoretical Computer Science, 2019, 772: 1-45

[27] Zhang Leyou, Shang Yujie. Leakage-resilient attribute-based encryption with CCA2 security. International Journal of Network Security, 2019, 21(5): 819-827

[28] Zhang Jie, Chen Jie, Gong Junqing, et al. Leakage-resilient attribute based encryption in prime-order groups via predicate encodings. Designs, Codes and Cryptography, 2018, 86(6): 1339-1366

[29] Zhang Leyou, Zhang Jingxia, Mu Yi. Novel leakage-resilient attribute-based encryption from hash proof system. The Computer Journal, 2017, 60(4): 541-554

[30] Qin Yan-Lin, Wu Xiao-Ping, Hu Wei. Leakage-resilient certificateless signcryption scheme. Journal on Communications, 2017, 38(S2): 43-50(in Chinese)
(秦艳琳，吴晓平，胡卫. 抗密钥泄露的无证书签密方案. 通信学报，2017, 38(S2): 43-50)

[31] Zhou Yan-Wei, Yang Bo, Wang Qing-Long. Provably secure leakage-resilient certificateless hybrid signcryption scheme. Journal of Software, 2016, 27(11): 2898-2911(in Chinese)
(周彦伟，杨波，王青龙. 可证安全的抗泄露无证书混合签密机制. 软件学报，2016, 27(11): 2898-2911)

[32] Zhou Yanwei, Yang Bo. Continuous leakage-resilient certificateless public key encryption with CCA security. Knowledge Based Systems, 2017, 136: 27-36

[33] Zhou Yanwei, Yang Bo. Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing. Information Processing Letters, 2018, 130: 16-24

[34] Li Jiguo, Guo Yuyan, Yu Qihong, et al. Continuous leakage-resilient certificate-based encryption. Information Sciences, 2016, 355-356: 1-14

[35] Yu Qihong, Li Jiguo, Zhang Yichen. Leakage-resilient certificate-based encryption. Security and Communication Networks, 2015, 8(18): 3346-3355

[36] Yu Qihong, Li Jiguo, Zhang Yichen, et al. Certificate-based encryption resilient to key leakage. Journal of Systems and Software, 2016, 116: 101-112

[37] Huang Jianye, Huang Qiong, Susilo Willy. Leakage-resilient group signature: Definitions and constructions. Information Sciences, 2020, 509: 119-132

[38] Huang Jianye, Huang Qiong, Susilo Willy. Leakage-resilient ring signature schemes. Theoretical Computer Science, 2019, 759: 1-13

[39] Ruan Ou, Zhang Yuanyuan, Zhang Mingwu, et al. After-the-fact leakage-resilient identity-based authenticated key exchange. IEEE Systems Journal, 2018, 12(2): 2017-2026

[40] Chen Rongmao, Mu Yi, Yang Guomin, et al. Strongly leakage-resilient authenticated key exchange//Proceedings of the Topics in Cryptology－CT-RSA 2016-The Cryptographers' Track at the RSA Conference 2016. San Francisco, USA, 2016: 19-36

[41] Zhang Ming-Wu, Chen Mi-Wen, Li Fa-Gen, et al. A strongly leakage-resilient and unconditionally secure dynamic secret-sharing scheme. Journal of Cryptologic Research, 2016, 3(4): 361-373(in Chinese)
(张明武，陈泌文，李发根等. 强抗泄漏的无条件安全动态秘密共享方案. 密码学报，2016, 3(4): 361-373)

[42] Shen Hua, Chen Mi-Wen, Zhang Ming-Wu. Leakage-resilient verifiable multi-secret sharing scheme. Journal of Beijing University of Posts and Telecommunications, 2016, 39(1): 87-91(in Chinese)
(沈华，陈泌文，张明武. 抗泄漏可验证多秘密共享方案. 北京邮电大学学报，2016, 39(1): 87-91)

[43] Shamir A. Identity-based cryptosystems and signature schemes //Proceedings of the Advances in Cryptology－CRYPTO'84. Santa Barbara, California, USA,1984: 47-53

[44] Boneh D, Franklin M K. Identity-based encryption from the weil pairing//Proceedings of the Advances in Cryptology－CRYPTO 2001, 21st Annual International Cryptology Conference. Santa Barbara, USA, 2001: 213-229

[45] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation//Proceedings of the 2008 ACM Conference on Computer and Communications Security (CCS 2008). Alexandria, USA, 2008: 417-426

[46] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the Advances in Cryptology—EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, USA, 2005: 457-473

[47] Libert B, Vergnaud D. Adaptive-ID secure revocable identity-based encryption//Proceedings of the Topics in Cryptology—CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009. San Francisco, USA, 2009: 1-15

[48] Seo J H, Emura K. Revocable identity-based encryption revisited: Security model and construction//Proceedings of the Public-Key Cryptography—PKC 2013-16th International Conference on Practice and Theory in Public-Key Cryptography. Nara, Japan, 2013: 216-234

[49] Seo J H, Emura K. Efficient delegation of key generation and revocation functionalities in identity-based encryption//Proceedings of the Topics in Cryptology—CT-RSA 2013-The Cryptographers' Track at the RSA Conference 2013. San Francisco, USA, 2013: 343-358

[50] Lee K, Choi S G, Lee D H, et al. Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency. Theoretical Computer Science, 2017, 667: 51-92

[51] Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption//Proceedings of the Advances in Cryptology—CRYPTO 2012-32nd Annual Cryptology Conference. Santa Barbara, USA, 2012: 199-217

[52] Lee K, Lee D H, Park J H. Efficient revocable identity-based encryption via subset difference methods. Designs, Codes and Cryptography, 2017, 85(1): 39-76

[53] Lee K, Park S. Revocable hierarchical identity-based encryption with shorter private keys and update keys. Designs, Codes and Cryptography, 2018, 86(10): 2407-2440

[54] Dodis Y, Haralambiev K, López-Alt A, Wichs D. Efficient public-key cryptography in the presence of key leakage//Proceedings of the Advances in Cryptology—ASIACRYPT 2010-16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore, 2010: 613-631

[55] Zhou Yanwei, Yang Bo, Xia Zhe, et al. Anonymous and updatable identity-based hash proof system. IEEE Systems Journal, 2019, 13(3): 2818-2829

[56] Zhou Yanwei, Yang Bo, Wang Tao, Mu Yi. Novel updatable identity-based hash proof system and its applications. Theoretical Computer Science, 2020, 804: 1-28

附录 A. 定理 3 的证明.

证明. 机制 Π 的正确性、平滑性、通用性及有效密文与无效密文的不可区分性均可由底层的 IB-HPSΠ′获得. 下面将详细证明泄露平滑性.

令函数 $f:\{0,1\}^*\to\{0,1\}^\lambda$ 是输出长度为 λ 的任意泄露函数. 此外,定义一个函数 $f'(C,k)$,它通过输入私钥 d_{id} 运行解封装算法 Decap 从密文中输出相应的封装秘钥 k,同时输出私钥的泄露信息 $f(d_{id})$,也就是说

$$f'(C,k)\equiv\{\text{输出 } k=\text{Encap}(d_{id},C)\text{和 } f(d_{id})\}.$$

对于任意确定的 $(mpk,msk)\leftarrow\text{Setup}(1^\kappa)$ 和身份 id,我们有

$$\begin{aligned}(C,f(d_{id}),k)&\equiv(C,f(d_{id}),k=\text{Ext}(k',S))\\&\equiv(C,f'(C,k'),k=\text{Ext}(k',S))\\&\approx(C,f'(C,U_k),k=\text{Ext}(U_k,S))\\&\approx(C,f'(C,U_k),\tilde{k})\\&\approx(C,f'(C,k'),\tilde{k})\\&\equiv(C,f(d_{id}),\tilde{k}),\end{aligned}$$

其中 $d_{id}=\text{KeyGen}(id,msk)$,$C=\text{Encap}(id)$,$k'=\text{Decap}(C,d_{id})$,$U_k\leftarrow\{0,1\}^{l_m}$ 和 $\tilde{k}\leftarrow_R\{0,1\}^{l_v}$. 此外,S 是强随机性提取器的种子.

第一和第三个约等号成立是基于底层 IB-HPS 的平滑性;强随机性提取器的安全性保证了第二个约等号成立. 因此,可得到

$$\text{SD}((C,f(d_{id}),k),(C,f(d_{id}),\tilde{k}))\leq\text{negl}(\kappa).$$

由于底层的 $\text{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_t}\to\{0,1\}^{l_m}$ 是一个平均情况的$(l_k-\lambda,\varepsilon)$-强随机性提取器,那么,可知关系

$$\lambda\leq l_k-l_m-\omega(\log\kappa)$$

成立.

综上所述,任意平滑的 IB-HPS,可借助强随机性提取器转化为泄露平滑的 IB-HPS. 证毕.

附录 B. 定理 4 的证明.

证明. 本文通用构造$\mathcal{E}'$的安全性,将通过一系列游戏论证来证明.

Game 0. 这个游戏是抗泄露 RIBE 机制原始的 CPA 安全性游戏. 该游戏中,挑战身份 id^* 在 T_i 时刻所对应的挑战密文 $C^*_{(v,T_i)}=(c'_1,c'_2,c'_3,S)$通过下述计算生成:

① 计算

$$\overline{id}^*=\mathcal{H}(id^*,T_i).$$

② 计算

$(c'_1,k_1)\leftarrow\text{Encap}_1(id^*)$和$(c'_2,k_2)\leftarrow\text{Encap}_2(\overline{id}^*)$.

③ 随机选取 $S\leftarrow_R\{0,1\}^{l_t}$ 和 $v\leftarrow_R\{0,1\}$后,计算

$$c_3' \leftarrow \mathrm{Ext}(k_1, k_2, S) \oplus M_v.$$

由 RIBE 机制原始抗泄露的 CPA 安全性游戏的定义可知：

$$\mathrm{Adv}_{\mathrm{RIBE},\mathcal{A}}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda) = \left| \Pr[\mathcal{A}\ wins\ \text{in Game 0}] - \frac{1}{2} \right|.$$

Game 1. 该游戏与 Game 0 相类似，修改挑战密文的生成过程. 在 Game 1 中，使用挑战身份 id^* 在 T_i 时刻的私钥 $sk_{(id^*,T_i)} = (d_{id^*}^1, d_{id^*}^2)$ 去生成挑战密文，即挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$(c_1', k_1) \leftarrow \mathrm{Encap}_1(id^*) \text{ 和 } (c_2', k_2) \leftarrow \mathrm{Encap}_2(\overline{id}^*).$$

③ 计算

$$k_1' \leftarrow \mathrm{Decap}_1(c_1', d_{id^*}^1).$$

④ 随机选取 $S \leftarrow_R \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2, S) \oplus M_v.$$

由底层 IB-HPSΠ_1 的解封装操作的正确性可知 $k_1 = k_1'$，那么 Game 0 和 Game 1 是不可区分的.

Game 2. 该游戏与 Game 1 相类似，修改挑战密文的生成过程. 该游戏中，挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$(c_1', k_1) \leftarrow \mathrm{Encap}_1(id^*) \text{ 和 } (c_2', k_2) \leftarrow \mathrm{Encap}_2(\overline{id}^*).$$

③ 计算

$$k_1' \leftarrow \mathrm{Decap}_1(c_1', d_{id^*}^1) \text{ 和 } k_2' \leftarrow \mathrm{Decap}_2(c_2', d_{id^*}^2).$$

④ 随机选取 $S \leftarrow_R \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2', S) \oplus M_v.$$

由底层 IB-HPSΠ_2 的解封装操作的正确性可知 $k_2 = k_2'$，那么 Game 1 和 Game 2 是不可区分的.

Game 3. 该游戏与 Game 2 相类似，修改挑战密文的生成过程. 在 Game 3 中，使用无效密文去生成挑战密文，即挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$c_1' \leftarrow \mathrm{Encap}_1^*(id^*) \text{ 和 } (c_2', k_2) \leftarrow \mathrm{Encap}_2(\overline{id}^*).$$

③ 计算

$$k_1' \leftarrow \mathrm{Decap}_1(c_1', d_{id^*}^1) \text{ 和 } k_2' \leftarrow \mathrm{Decap}_2(c_2', d_{id^*}^2).$$

④ 随机选取 $S \leftarrow_{0R} \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2', S) \oplus M_v.$$

由底层 IB-HPSΠ_1 的有效密文与无效密文的不可区分性可知 Game 2 和 Game 3 是不可区分的.

Game 4. 该游戏与 Game 3 相类似，修改挑战密文的生成过程，即挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$c_1' \leftarrow \mathrm{Encap}_1^*(id^*) \text{ 和 } c_2' \leftarrow \mathrm{Encap}_2^*(\overline{id}^*).$$

③ 计算

$$k_1' \leftarrow \mathrm{Decap}_1(c_1', d_{id^*}^1) \text{ 和 } k_2' \leftarrow \mathrm{Decap}_2(c_2', d_{id^*}^2).$$

④ 随机选取 $S \leftarrow_R \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2', S) \oplus M_v.$$

由底层 IB-HPSΠ_2 的有效密文与无效密文的不可区分性可知 Game 3 和 Game 4 是不可区分的.

Game 5. 该游戏与 Game 4 相类似，修改挑战密文的生成过程. 在 Game 5 中，使用随机数去生成挑战密文，即挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$c_2' \leftarrow \mathrm{Encap}_2^*(\overline{id}^*).$$

③ 计算

$$k_1' \leftarrow \{0,1\}^{l_k} \text{ 和 } k_2' \leftarrow \mathrm{Decap}_2(c_2', d_{id^*}^2).$$

④ 随机选取 $S \leftarrow_R \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2', S) \oplus M_v.$$

由底层 IB-HPSΠ_1 的平滑性可知 Game 4 和 Game 5 是不可区分的.

Game 6. 该游戏与 Game 5 相类似，修改挑战密文的生成过程，即挑战密文 $C_{(v,T_i)}^* = (c_1', c_2', c_3', S)$ 通过下述计算生成：

① 计算

$$\overline{id}^* = \mathcal{H}(id^*, T_i).$$

② 计算

$$k_1' \leftarrow \{0,1\}^{l_k} \text{ 和 } k_2' \leftarrow \{0,1\}^{l_v}.$$

③ 随机选取 $S \leftarrow_R \{0,1\}^{l_t}$ 和 $v \leftarrow_R \{0,1\}$ 后计算

$$c_3' \leftarrow \mathrm{Ext}(k_1', k_2', S) \oplus M_v.$$

由底层 IB-HPSΠ_2 的平滑性可知 Game 6 和 Game 5 是不可区分的.

综上所述，对于任意的敌手而言，Game 0 和 Game 6 是不可区分的. 特别地，在 Game 6 中挑战密文完全由随机数生成，使得挑战密文中不包含随机数 v 的任何信息，则任意敌手在 Game 6 中获胜的优势趋是可忽略的. 因此，任意敌手在 Game 0 中获胜的优势趋是可忽略的，即有

$$Adv_{\mathrm{RIBE},\mathcal{A}}^{\mathrm{LR\text{-}CPA}}(\kappa,\lambda) \leq \mathrm{negl}(\kappa).$$　　证毕.

附录 C.　定理 5 的证明.

证明.　底层机制 $\mathcal{E}'$ 的正确保证了通用构造 $\mathcal{E}'''$ 的正确性. 安全性将通过一系列游戏来证明.

Game 0. 该游戏是抗泄露 RIBE 机制原始的 CCA 安全性游戏.

(1)初始化. 挑战者$\mathcal{C}$输入安全参数κ运行初始化算法$(Params,msk)\leftarrow\text{Setup}(1^{\kappa})$,发送系统公开参数$Params$给敌手$\mathcal{A}$,并秘密保存主私钥$msk$.

(2)阶段 1. 敌手$\mathcal{A}$能够适应性的对身份空间$\mathcal{ID}$中的任意身份$id\in\mathcal{ID}$进行下述询问:

①密钥生成询问. 收到身份id在T_i时刻的密钥生成询问时,挑战者$\mathcal{C}$通过运行密钥生成算法$sk_{(id,T_i)}\leftarrow\text{KeyGen}(msk,id,T_i)$返回$id$在$T_i$时刻所对应的私钥$sk_{(id,T_i)}$给敌手$\mathcal{A}$.

②解密询问. 收到关于(C_{T_i},id,T_i)的解密询问时,$\mathcal{C}$返回相应的明文消息$M=\text{Dec}(C_{T_i},sk_{(id,T_i)},T_i)$给敌手$\mathcal{A}$,其中$sk_{(id,T_i)}\leftarrow\text{KeyGen}(msk,id,T_i)$.

③泄露询问. 敌手$\mathcal{A}$提交身份时戳二元组(id,T_i)和多项式可计算的函数$f_i:\{0,1\}^*\rightarrow\{0,1\}^{\lambda_i}(i\geq1)$给挑战者进行泄露询问,$\mathcal{C}$返回私钥$sk_{(id,T_i)}$的泄露信息$f_i(sk_{(id,T_i)})$,但关于$sk_{(id,T_i)}$的泄露总长度不能超过系统设定的泄露界$\lambda$,否则$\mathcal{C}$忽略本次询问.

身份撤销询问. 对于敌手$\mathcal{A}$提交的待撤销身份集合$\{id_1,\cdots,id_n\}$,挑战者$\mathcal{C}$输出更新后的身份撤销列表$RL=RL\cup\{id_1,\cdots,id_n\}$.

④密钥更新询问. 对于身份id在T_{i+1}时刻的密钥更新询问,挑战者$\mathcal{C}$首先检测id是否在撤销列表RL中,若$id\in RL$,那么$\mathcal{C}$终止并输出$\perp$;否则,$\mathcal{C}$运行算法$k_{T_{i+1}}\leftarrow\text{KeyUpdate}'(RL,id,T_{i+1},msk)$,产生身份$id$在$T_{i+1}$时刻所对应的时间组件$k_{T_{i+1}}$,并将其发送给$\mathcal{A}$.

(3)挑战. 对于挑战身份$id^*\in\mathcal{ID}$和时间戳T_i,挑战者$\mathcal{C}$计算挑战密文$C^*_{(v,T_i)}=(C',\pi^*)$,其中

$v\leftarrow_R\{0,1\},C'\leftarrow\text{Enc}'(M_v,id^*,T_i,r)$和

$\pi^*\leftarrow\text{Prove}((M_v,r),(C',id,T_i))$.

(4)阶段 2. 与阶段 1 相类似,但该阶段敌手不能对挑战身份进行秘钥生成询问,并且不能对挑战密文和挑战身份对进行解密询问;此外,不能对挑战身份进行身份撤销和密钥更新询问. 同时,该阶段敌手不能进行泄露询问.

(5)输出. 敌手$\mathcal{A}$输出对v的猜测v'. 若$v'=v$,则称敌手$\mathcal{A}$在该游戏中获胜.

综上所述,在 Game 0 中有

$$Adv^{\text{LR-CCA}}_{\text{R-IBE},\mathcal{A}}(\kappa,\lambda)=\left|\Pr[\mathcal{A}\ wins]-\frac{1}{2}\right|.$$

Game 1. 该游戏与 Game 0 相类似,修改挑战密文$C^*_{(v,T_i)}$的生成过程. 在 Game 1,使用模拟谕言机$\mathcal{O}^{\text{Sim}}_{tk}(\cdot)$生成挑战密文,即真实论证变换为模拟论证. 更详细地讲,T_i时刻的挑战密文$C^*_{(v,T_i)}=(C',\pi^*)$由下述计算生成:

$v\leftarrow_R\{0,1\},C'\leftarrow\text{Enc}'(M_v,id^*,T_i,r)$和$\pi^*\leftarrow\text{Sim}_{tk}(id^*,C')$.

由底层f-tSE NIZK 论证Π_{nizk}的零知识性可知 Game 0 和 Game 1 是不可区分的.

Game 2. 该游戏与 Game 1 相类似,修改解密询问的应答方式. 对于敌手提交的关于(C_{T_i},id,T_i)的解密询问,挑战者运行提取器Ext'从论证π中提取出相应的明文$f(M,r)=M$,即对于敌手提交的任意解密询问(C_{T_i},id,T_i),挑战者$\mathcal{C}$通过计算提取操作$\text{Ext}'((C',id),\pi,ek)$返回相应的询问应答.

由底层f-tSE NIZK 论证的强一次性模拟可提取性可知 Game 1 和 Game 2 是不可区分的. f-tSE NIZK 论证能以不可忽略的概率从论证π中提取出相应的M. 在f-tSE NIZK 论证中,敌手只能获得一个关于真实状态(C,id)的模拟论证,因此对于新的状态论证对$((C,id),\pi)\neq((C',id^*),\pi^*)$中的证据$\pi$即使通过验证,提取器$\text{Ext}'$也无法提取出相应的消息.

Game 3. 该游戏与 Game 2 相类似,修改挑战密文$C^*_{(v,T_i)}$的生成方式. 在 Game 3,使用明文空间$\mathcal{M}$中的任意随机消息生成挑战密文,即$C^*_{(v,T_i)}=(C',\pi^*)$由下述计算生成:

$M'\leftarrow_R\mathcal{M},C'\leftarrow\text{Enc}'(M',id^*,T_i,r)$和$\pi^*\leftarrow\text{Sim}_{tk}(id^*,C')$.

由底层抗泄露 RIBE 机制的 CPA 安全性可知 Game 2 和 Game 3 是不可区分的.

综上所述,对于任意的敌手而言,Game 0 和 Game 3 是不可区分的. 此外,由于在 Game 3 中完全由明文空间$\mathcal{M}$中的随机消息生成了挑战密文,因此挑战密文不包含随机值v的任何信息,那么任意敌手在 Game 3 中获胜的优势是可忽略的. 因此,任意敌手在 Game 0 中获胜的优势是可忽略的,即有

$$Adv^{\text{LR-CCA}}_{\text{R-IBE},\mathcal{A}}(\kappa,\lambda)\leq\text{negl}(\kappa).$$

证毕.

附录 D. 基于 OT-LF 的 RIBE 机制.

令$\text{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_v}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$是平均情况的$(l_k+l_v-\lambda,\varepsilon)$-强随机性提取器,其中$\lambda$是泄露参数,$\varepsilon$在安全参数$\kappa$上是可忽略的. 令$\Pi_1=(\text{Setup}_1,\text{KeyGen}_1,\text{Encap}_1,\text{Encap}_1^*,\text{Decap}_1)$是封装密钥空间为$\mathcal{K}_1=\{0,1\}^{l_k}$、身份空间为$\mathcal{ID}_1$的平滑性 IB-HPS. 令$\Pi_2=(\text{Setup}_2,\text{KeyGen}_2,\text{Encap}_2,\text{Encap}_2^*,\text{Decap}_2)$是封装密钥空间为$\mathcal{K}_2=\{0,1\}^{l_v}$、身份空间为$\mathcal{ID}_2$的平滑性 IB-HPS. 令$\mathcal{H}:\mathcal{ID}_1\times\mathcal{T}\rightarrow\mathcal{ID}_2$是抗碰撞的单向哈希函数,其中$\mathcal{T}$表示时刻列表$TL$中的时刻. 令$LF=(\text{LF.Gen},\text{LF.Eval},\text{LF.Tag})$是一个$(\mathcal{K}_1\times\mathcal{K}_2,l_{LF})$-OT-LF.

CCA 安全的抗泄露 RIBE 机制通用构造$\mathcal{E}=(\text{Setup},\text{KeyGen},\text{Enc},\text{Dec},\text{Revoke},\text{KeyUpdate})$的具体算法如下所述:

(1)$(Params,msk)\leftarrow\text{Setup}(1^{\kappa})$

输出$Params=(mpk_1,mpk_2,F_{pk})$和$msk=(msk_1,msk_2)$,其中

$(mpk_1,msk_1)\leftarrow\text{Setup}_1(1^{\kappa})$、$(mpk_2,msk_2)\leftarrow\text{Setup}_2(1^{\kappa})$和

$(F_{pk},F_{td})\leftarrow\text{LF.Gen}(1^{\kappa})$.

特别地,该算法还定义了初始为空的身份撤销列表RL,并且初始化了时间列表TL. 此外,算法$\text{LF.Gen}(1^{\kappa})$还定义了 OT-LF 的公开标签空间$\mathcal{T}_C$.

(2) $(sk_{(id,T_i)},T_i)\leftarrow \mathrm{KeyGen}'(msk,id,RL,TL)$

对于身份 id 的密钥生成，PKG 首先检测身份 id 是否在撤销列表 RL 中，若 $id\in RL$，算法 KeyGen 输出 $\perp$；否则 PKG 执行下述操作：

① 计算

$$d_{id}^1\leftarrow \mathrm{KeyGen}_1(msk_1,id)$$

② 从时间列表 TL 中读取当前时戳 T_i，并计算

$id'=\mathcal{H}(id,T_i)$ 和 $d_{id}^2\leftarrow \mathrm{KeyGen}_2(msk_2,id')$.

③ 输出身份 id 在 T_i 时刻的私钥

$$sk_{(id,T_i)}=(k_{id},k_{T_i})=(d_{id}^1,d_{id}^2),$$

其中 $k_{id}=d_{id}^1$ 是私钥 $sk_{(id,T_i)}$ 的身份组件，$k_{T_i}=d_{id}^2$ 是私钥 $sk_{(id,T_i)}$ 的时间组件.

(3) $(C_{T_i},T_i)\leftarrow \mathrm{Enc}'(M,id,T_i)$

对于一个消息 $M\in\mathcal{M}=\{0,1\}^{l_m}$，时间戳 T_i 和身份 $id\in\mathcal{ID}$，加密者进行下述运算：

① 计算

$$id'=\mathcal{H}(id,T_i).$$

② 计算

$(c_1,k_1)\leftarrow \mathrm{Encap}_1(id)$ 和 $(c_2,k_2)\leftarrow \mathrm{Encap}_2(id')$.

③ 随机选取 $S\leftarrow_R\{0,1\}^{l_t}$ 后计算

$c_3\leftarrow \mathrm{Ext}(k_1,k_2,S)\oplus M$ 和 $v=\mathrm{LF.Eval}(F_{pk},t,k_1,k_2)$，其中 $t=(t_a,t_c)$，$t_a=(c_1,c_2,c_3)$ 和 $t_c\leftarrow_R\mathcal{T}_C$.

④ 输出密文 $C_{T_i}=(c_1,c_2,c_3,v,t_c,S)$，即密文 C_{T_i} 是身份 id 在 T_i 时刻对消息 M 的加密密文.

(4) $M\leftarrow \mathrm{Dec}'(C_{T_i},sk_{(id,T_i)})$

对于身份 id 在 T_i 时刻的秘钥 $sk_{(id,T_i)}=(d_{id}^1,d_{id}^2)$ 和加密密文 $C_{T_i}=(c_1,c_2,c_3,v,t_c,S)$，解密者进行下述运算：

① 计算

$k_1'=\mathrm{Encap}_1(c_1,d_{id}^1)$ 和 $k_2'=\mathrm{Encap}_2(c_2,d_{id}^2)$.

② 计算

$$v'=\mathrm{LF.Eval}(F_{pk},t,k_1',k_2'),$$

其中 $t=(t_a,t_c)$ 和 $t_a=(c_1,c_2,c_3)$.

③ 如果 $v'=v$，则计算 $M=\mathrm{Ext}(k_1,k_2,S)\oplus c_3$，输出密文 $C_{T_i}=(c_1,c_2,c_3,v,t_c,S)$ 所对应的明文消息 M；否则输出特殊的终止符 $\perp$.

(5) $RL'\leftarrow \mathrm{Revoke}'(RL,\{id_1,\cdots,id_n\})$

若集合 $\{id_1,\cdots,id_n\}$ 中的身份将被撤销，那么 PKG 通过下述操作对身份撤销列表进行更新.

$$RL'=RL\bigcup\{id_1,\cdots,id_n\}.$$

(6) $k_{T_{i+1}}\leftarrow \mathrm{KeyUpdate}'(RL,id,T_{i+1},msk)$.

当收到身份 $id\in\mathcal{ID}$ 在时间戳 T_{i+1} 时刻的密钥更新询问时，PKG 首先检测身份 id 是否在撤销列表 RL 中，若存在则 PKG 输出 $\perp$，并终止；否则 PKG 进行下列运算：

计算

$id'=\mathcal{H}(id,T_{i+1})$ 和 $d_{id}^2\leftarrow \mathrm{KeyGen}_2(msk_2,id')$.

输出 $k_{T_{i+1}}=d_{id}^2$. 那么身份 id 所对应的密钥由 T_i 时刻的 $sk_{(id,T_i)}=(k_{id},k_{T_i})$ 更新为 T_{i+1} 时刻的 $sk_{(id,T_{i+1})}=(k_{id},k_{T_{i+1}})$，随着时间戳 T_i 的递增，用户之前的私钥 $sk_{(id,T_i)}$ 相继被撤销.

定理 7. 假设 Π_1 和 Π_2 是两个平滑性 IB-HPS，$\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_v}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k+l_v-\lambda,\varepsilon)$-强随机性提取器，LF 是一个 $(\mathcal{K}_1\times\mathcal{K}_2,l_{LF})$-一次性损耗滤波器. 那么，对于任意的泄露参数 $\lambda\leq l_k+l_v-l_{LF}-l_m-\omega(\log\kappa)$，上述构造 $\mathcal{E}$ 是 CCA 安全的抗泄露 RIBE 机制的通用构造.

定理 7 的证明过程可参考 OT-LF 在抗泄露 IBE 机制构造中的证明，详见文献[26].

附录 E. 泄露平滑的 IB-HPS.

本节在 Chow 等人[19]提出的 IB-HPS 实例的基础上，给出一个泄露平滑的 IB-HPS 机制的具体构造. 令 $(q,G,G_T,g,e)\leftarrow\Gamma(1^\kappa)$，其中循环群 G 的生成元是 g，阶是大素数 q，$e:G\times G\rightarrow G_T$ 是双线性映射. 令 $\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k-\lambda,\varepsilon)$-强随机性提取器，泄露平滑的 IB-HPS 的具体构造如下所述：

(1) $(mpk,msk)\leftarrow \mathrm{Setup}(1^\kappa)$.

随机选取 $\alpha,\beta\leftarrow_R Z_q^*$ 和 $u,h\leftarrow_R G$，并输出 $mpk=(q,G,G_T,g,e,u,h,e(g,g)^\alpha,e(g,g)^\beta,\mathrm{Ext})$ 和 $msk=(g^\alpha,g^\beta)$.

(2) $d_{id}\leftarrow \mathrm{KeyGen}(msk,id)$.

随机选取 $r,t\leftarrow_R Z_q^*$，并输出

$$sk_{id}=(s_1,s_2,s_3)=(g^\alpha g^{-\beta t}(u^{id}h)^r,g^{-r},t).$$

(3) $(C,k)\leftarrow \mathrm{Encap}(id)$.

随机选取 $z\leftarrow_R Z_q^*$ 和 $S\leftarrow_R\{0,1\}^{l_t}$，并输出封装秘钥 $k=\mathrm{Ext}(e(g,g)^{\alpha z},S)$ 和相应的封装密文

$$C=(c_1,c_2,c_3,S)=(g^z,(u^{id}h)^z,e(g,g)^{\beta z},S).$$

(4) $C^*\leftarrow \mathrm{Encap}^*(id)$.

随机选取 $z,z'\leftarrow_R Z_q^*(z\neq z')$ 和 $S\leftarrow_R\{0,1\}^{l_t}$，并输出

$$C=(c_1,c_2,c_3,S)=(g^z,(u^{id}h)^z,e(g,g)^{\beta z'},S).$$

(5) $k\leftarrow \mathrm{Decap}(d_{id},C)$.

输出

$$k=\mathrm{Ext}(e(c_1,s_1)e(c_2,s_2)c_3^{s_3},S).$$

由本文定理 3 和文献[19]中的定理 3.1 可知若 $\mathrm{Ext}:\{0,1\}^{l_k}\times\{0,1\}^{l_t}\rightarrow\{0,1\}^{l_m}$ 是平均情况的 $(l_k-\lambda,\varepsilon)$-强随机性提取器，对于任意的泄露参数 $\lambda\leq l_k-l_m-\omega(\log\kappa)$，上述构造是泄露平滑的 IB-HPS.

ZHOU Yan-Wei, Ph. D., senior engineer, master supervisor. His research interests include cryptography and anonymous communication.

YANG Bo, Ph. D., professor, doctoral supervisor. His research interests include information security and cryptography.

XIA Zhe, Ph. D., associate professor, master supervisor. His research interests include information security.

LAI Qi-Qi, Ph. D., lecturer. His current research interests include information security and cryptography.

ZHANG Ming-Wu, Ph. D., professor, doctoral supervisor. His current research interests include information security and cryptography.

MU Yi, Ph. D., professor, doctoral supervisor. His current research interests include information security and cryptography.

Background

In the traditional security model, it is assumed that only legitimate participants possess the internal secret states (e. g., the user's private key), and these states are completely inaccessible to the adversary. However, in many real-world applications, these states could be leaked through various leakage attacks, such as side-channel attacks, cold boot attacks, etc. Therefore, if an adversary obtains some information of the internal secret states, the cryptographic schemes may fail to achieve their claimed security. In other words, traditional cryptographic assumptions are insufficient in the leakage setting. To solve this problem, leakage-resilient cryptography has been advocated to maintain the security properties for real world applications, and several concrete constructions were proposed to capture the leakage-resilience requirement, such as leakage-resilient public-key encryption, leakage resilient identity-based encryption, leakage-resilient authenticated key exchange, leakage resilient certificate-based encryption, etc.

In this paper, in order to provide leakage resilience for the revocable identity-based encryption (RIBE) scheme, a generic construction of chosen-plaintext attack (CPA) secure leakage-resilient RIBE scheme was created based on the identity-based hash proof system (IB-HPS), and the CPA security of proposed system was proved from the security of the underlying IB-HPS. To further achieve security, a new construction was proposed from the IB-HPS and the non-interactive zero-knowledge (NIZK) argument, which can achieve chosen-ciphertext attack (CCA) security, which can be proved from the security of IB-HPS and the NIZK argument. In addition, a continuous leakage-resilient proposal of RIBE scheme was designed based on the updatable identity-based hash proof system (U-IB-HPS), in which, an additional key update algorithm can push some new randomness into the private key of user, and the leakage of the previous private key does not affect the security of the updated private key.

This work is supported by the National Key R&D Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (61802242, 61772326, 61802241), the National Cryptography Development Foundation during the 13th Five-year Plan Period (MMJJ20180217), the Research Funds for Guangxi Key Laboratory of Trusted Software (KX202002), and the Fundamental Research Funds for the Central Universities (GK202003079, GK202007033).