基于可提取哈希证明系统的多策略加密方案

张丽娜[1,2,3],杨 波[1,3],黄梅娟[1,3,4],贾艳艳[2]
(1.陕西师范大学计算机科学学院,陕西西安 710119;2.西安科技大学计算机科学与技术学院,陕西西安 710054;
3.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093;4.宝鸡文理学院数学与信息科学学院,陕西宝鸡 721013)

摘 要: 哈希证明系统由Cramer-Shoup在2002年首次提出,到目前为止仍是密码工作者的研究热点之一.进而,Wee在2010年提出可提取哈希证明系统的概念,其可用来构造基于查找性困难假设的公钥加密方案.本文在可提取哈希证明系统之上,通过重新定义系统参数的意义,扩大了可提取哈希证明系统的密码学应用范围.我们利用可提取哈希证明系统的框架构造了一个基本的基于Diffie-Hellman关系的All-But-One可提取哈希证明系统.在此基础上细粒度了辅助输入,引入权重计算,给出了一个基于标签和可变策略的CCA加密方案,并进行了详细的安全性证明.特别的,该方案比可提取具有更丰富的抽象表达,即是All-But-N的,也即在提取模式中由标签决定的分支数量可以有n个.同时,该方案是基于困难性可搜索问题,本质上是基于计算性的Diffie-Hellman问题.

关键词: Diffie-Hellman关系; 选择密文攻击; 哈希证明系统; 可提取哈希证明系统; 多策略
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2019)02-0337-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.02.012

A Multi-Policy Encryption Scheme Based on Extractable Hash Proof Systems

ZHANG Li-na[1,2,3], YANG Bo[1,3], HUANG Mei-juan[1,3,4], JIA Yan-yan[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*;
2. *Department of Computing Science and Technology, Xi'an University of Science and Technology, Xi'an, Shaanxi*, 710054, *China*;
3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
4. *Department of Mathematics, Baoji University of Arts and Sciences, Baoji, Shaanxi* 721013, *China*)

Abstract: Hash proof systems, which was first introduced by Cramer and Shoup in 2002, is still one of the hottest research topics in cryptography. And then Wee proposed the concept of extractable hash proof system in 2010 and it is a concept extension on the hash proof system and as a paradigm of constructing PKE from search problems. On the basis of the extractable hash proof system, this paper expands the application scope of the extractable hash proof system by redefining the meaning of system parameters. We construct a basic All-But-One extractable hash proof system based on Diffie-Hellman relations by using the framework of extractable hash proof system. Based on this, fine-grained auxiliary input and weighting calculation are introduced. A new variable-policy CCA encryption scheme based on tag is proposed, and the security proof is also given in details. In particular, this scheme is a richer abstraction of extractable hash proof system that it is All-But-N, which means that the number of branches determined by the tag in the extraction mode could be n. At the same time, the scheme is based on the difficulty of the search problem and is essentially based on the computational Diffie-Hellman problem.

Key words: Diffie-Hellman relations; chosen ciphertext attack; hash proof systems; extractable Hash proof system; multi-policy

收稿日期:2018-01-22;修回日期:2018-06-22;责任编辑:蓝红杰
基金项目:国家重点研发计划(No.2017YFB0802000);国家自然科学基金(No.61572303, No.61772326);中国科学院信息工程研究所信息安全国家重点实验室开放课题(No.2017-MS-03);"十三五"国家密码发展基金(No.MMJJ20180217);中央高校基本科研业务费项目(No.GK201702004);陕西省自然科学基础研究计划(No.2017JQ6026);榆林市科技计划产学研项目(No.2014CXY-08-01)

1 引言

哈希证明系统(Hash Proof Systems)首次由 Cramer-Shoup 于 2002 年在欧洲密码年会上提出[1],它在本质上是指针对某一 NP 语言的一种公开可验证的非交互式零知识证明系统.

总体而言,哈希证明系统[1,2]建立在子集合成员关系问题之上,包括一个与该问题相关的投影哈希函数族,该系统具有"投影性"和"平滑性"两种性质. 子集合成员关系问题是指给定一个集合 X 和定义在 X 上的 NP 语言 L,区分 L 中的一个随机元素和 $X\backslash L$ 中的一个随机元素是困难的. 设投影哈希函数族的定义域为 X,值域为 Y,"投影性"是指对于属于语言 L 的 $x\in X$,利用公钥 pk 和证据 w 或者对应的私钥 sk 都可以算出对应点的哈希值,即 $y=\mathrm{H}(sk,x)=\mathrm{H}(pk,x,w)\in Y$. 但是对于不属于语言 L 的 $x\in X\backslash L$,其哈希值只能通过私钥计算. "平滑性"是指只给定公钥,对于 L 中的一个随机元素和 $X\backslash L$中的一个随机元素的哈希值是统计不可区分的.

目前对哈希证明系统的研究已经有很多. 在哈希证明系统中,可以用私钥来验证利用公钥计算的哈希值,也可以在安全性证明中将属于语言中的 x 用不属于语言中的 x 替换. 因此可以用来设计选择密文安全的公钥加密体制和基于身份的加密方案[3~7],还可以用于各类需要证据的安全协议设计,如基于口令的认证密钥交换协议[8~10]、不经意传输协议[11,12]、承诺协议[13,14]、损耗陷门函数和损耗加密[15,16],属性加密[17,18]等.

可提取哈希证明系统(Extractable Hash Proof Systems,简记为 EHPS)[19]的概念建立在哈希证明系统基础之上,也成为密码学界的研究热点之一. Wee 等人[19]于 2010 年首次给出了基于 CDH 假设的可提取哈希证明系统构造,在此基础上还给出了第一个基于 CDH 假设的 CCA2 加密方案. 该方案展示了如何通过可提取哈希证明系统的模块化设计方法,派生出有效的 CCA 加密机制. Chen 等[20]基于 ABO(All-But-One)的可提取哈希证明系统给出了公开可计算的伪随机函数的构造方法,还结合公开验证关系给出了公开可计算和验证函数及应用系统. Faonio 等[21]给出了可提取哈希证明系统和可预测的知识论证系统之间的联系,并指出给定一个基于某个关系 R 的可提取哈希证明系统,就可以构造一个对应关系 R'的知识论证系统. Goyal 等[22]指出利用有效的可提取哈希证明系统如文献[19]等,可构造可提取的证据加密,从而直接基于软件形式构造出基于权益证明的区块链系统一次性程序. Hu 等[23]利用可提取的哈希证明系统得到了抗泄露的适应性陷门关系,从而给出了能抵抗密钥泄露攻击的密钥封装机制构造方法.

可提取哈希证明系统本质上是将哈希证明系统中对完备性的要求(对应于平滑性)用"知识的证明"代替,因此它是一种公开可验证的知识的非交互式零知识证明系统. 在可提取哈希证明系统中,公私钥可以用哈希模式和提取模式中的一种模式生成,分别在方案具体构造和安全性证明中使用. 更进一步地说,与 Cramer-Shoup 等的哈希证明系统[1]不同,可提取的哈希证明系统是与单向关系族一起设计的,因此特别适用于查找困难性假设问题.

由此可见,可提取哈希证明系统不仅继承了哈希证明系统的性质,还具有提取性,是一种公开可验证的零知识证明系统. 该系统可以在提取模式下解密,在哈希模式中进行安全性证明,可直接用于构造公钥加密方案,也可以灵活应用于各类实际安全方案中. 本文的主要贡献在于:

本文在可提取哈希证明系统之上,扩展了辅助输入的定义域和应用,将其由有限域上的某一个数扩展为由$\{0,1\}$组成的比特串. 我们利用可提取哈希证明系统的框架构造了一个基于 Diffie-Hellman 关系的 All-But-N(ABN)可提取哈希证明系统. 在此基础上细粒度了辅助输入,在特定的应用场景中引入权重计算,将标签定义为用户属性,结合建立的属性/非属性二维权重矩阵,给出了一个基于标签和可变策略的 CCA 加密方案,并进行了详细的安全性证明. 在加密方案中利用了 Goldreich-Levin 硬核比特定理[16,24,25]和公共参数的随机性,可以从 Diffie-Hellman 关系$\{u,s\}$的 s 中提取出随机数的性质. 特别的,该方案是基于 All-But-N 可提取哈希证明系统的细粒度属性和策略隐藏的加密方案. 同时,该方案是基于困难性可搜索问题,本质上是基于计算性的 Diffie-Hellman 问题.

2 基本理论

在可提取的哈希证明系统[19]中,将某个 R 固定为一些计算困难性问题的关系[26,27]. 即 R 是一个有效的抽样,但是在给定一个随机的 u 时,找到一个 s 满足关系$(u,s)\in R$是困难的. 此外,该系统还要求在给定 PK 和用来抽样$(u,s)\in R$的随机数 r 的情况下哈希函数 $\mathrm{Pub}(PK,r)$能够被有效计算. 可提取的哈希证明系统中存在两种模式,一种是哈希模式,另一种是提取模式. 系统中用来生成公私钥对的 setup 算法属于两种模式中的一种. 在两种模式下,算法产生的公钥具有同样的分布,秘密钥提供的功能取决于产生密钥的模式. 在哈希模式下,密钥SK^*允许我们在不知道 s 或 r 的情况下,同样计算出哈希值 $\mathrm{Pub}(PK,r)$,与之对应的是,存在一个私有计算算法 Priv,对于所有$(u,s)\in R$,有$\mathrm{Priv}(\mathrm{SK}^*,u)=\mathrm{H}_{PK}(u)$. 在提取模式下,密钥 SK 允许我们验证哈

希值是否被正确计算和是否能提取出一个证据 s. 更形式化的说,存在一个提取算法 Ext,使得对于所有的 u, τ,当 $\tau = H_{PK}(u)$时,$Ext(SK,u,\tau)$输出满足$(u,s) \in R$ 的 s. 这也意味着当 R 是一个有效计算时,在给定 SK 的情况下对哈希函数值的有效验证. 更进一步的,All-But-One(ABO)可提取哈希证明系统是在可提取哈希证明系统的提取模式中,有一个由标签 TAG 决定的分支. 因此在公开计算和提取时都需要输入这个标签 TAG.

根据上述描述,本文将涉及到基于计算问题的二元关系和可提取哈希证明系统的相关概念. 因此本章主要给出需要用到的基本理论.

2.1　基于搜索问题的二元关系

固定一个由公开参数 PP 索引的(二元)关系族 R_{PP},我们要求在给定安全参数 1^{λ} 下,PP 是一个有效的抽样,并且假定所有的算法都将 PP 作为输入参数. 我们也要求 R_{PP}能够被有效验证(可能在给定 PP 的某个陷门时)和有效采样.

根据文献[19],R_{PP}能够对应于一个计算性困难问题,也即给定随机数 u,很难去找到一个 s 满足关系$(u,s) \in R$. 更形式化的,我们说一个二元关系 R_{PP}是单向的,假如满足以下两个条件:

—在公共参数 PP 上,以极大的概率,对于所有 u,存在至多一个 s 能够满足$(u,s) \in R$.

—存在一个有效的可计算产生器 G 使得 $G_{PP}(s)$对于能够得到 PP 和 u,能够对于访问谕言机 R_{PP}(这里$(u,s) \leftarrow_R SampR(PP)$)的敌手是伪随机的.

2.2　Diffie-Hellman 关系

考虑阶为素数 q 的一系列群 G. 对于随机选取的 $g \leftarrow_R G$ 和 $\alpha \leftarrow_R Z_q$,公共参数 PP 为(g,g^{α}). 考虑 Diffie-Hellman 关系

$$R_{PP}^{dh}\{(u,s) \in G \times G : s = u^{\alpha}\}$$

相关的抽样算法 SampR 选择一个随机数 $r \leftarrow_R Z_q$,输出$(g^r,g^{\alpha r})$.

2.3　可提取的哈希证明系统

我们考虑一个由公钥 PK 索引的哈希函数族 $\{H_{PK}\}$. 一个可提取的哈希证明系统与一个单向关系 R_{PP}相关,由在公共参数 PP 上以极大概率满足下列性质的五元组(SetupExt,SetupHash,Pub,Ext,Priv)组成:

(公开可计算)对于$(PK,SK) \leftarrow SetupExt(PP)$和$(u,s) = SampR(r)$有 $Pub(PK,r) = H_{PK}(u)$. (提取模式)对于$(PK,SK) \leftarrow SetupExt(PP)$和所有$(u,\tau)$,有

$$\tau = H_{PK}(u) \Leftrightarrow (u,Ext(SK,u,\tau)) \in R.$$

(哈希模式)对于$(PK,SK^*) \leftarrow SetupHash(PP)$和所有$(u,s) \in R$,有$Priv(SK^*,u) = H_{PK}(u)$. (不可区分性)SetupExt(PP)和 SetupHash(PP)的第一个输出(即 PK)不可区分.

2.4　All-But-One 可提取的哈希证明系统

我们考虑一个由公钥 PK 索引的带辅助输入 TAG 的哈希函数族 $\{H_{PK}\}$. 更形式化的,一个 All-But-One(ABO)的可提取哈希证明系统由在公共参数 PP 上以极大概率满足下列性质的六元组(SetupExt,SetupABO,Pub,Ext,Ext^*,Priv)组成:

(公开可计算)对于所有$(u,s) = SampR(r)$,PK 和 TAG,有 $Pub(PK,TAG,r) = H_{PK}(TAG,u)$(提取模式)对于所有$(PK,SK) \leftarrow SetupExt(PP)$和所有$(TAG,u,\tau)$,有 $\tau = H_{PK}(TAG,u) \Leftrightarrow (u,Ext(SK,TAG,u,\tau)) \in R$

(All-But-One 哈希模式)对于所有的TAG^*和$(PK,SK^*) \leftarrow SetupABO(PP,TAG^*)$,对应于所有$(u,s) \in R$,有 $Priv(SK^*,TAG^*,u) = H_{PK}(TAG^*,u)$

此外,对于所有 $TAG \neq TAG^*$和所有(u,τ),有

$$\tau = H_{PK}(TAG,u) \Leftrightarrow (u,Ext^*(SK^*,TAG,u,\tau)) \in R$$

(不可区分性)对于所有的 TAG^*, SetupExt(PP) SetupABO(PP,TAG^*)和的第一个输出(即 PK)不可区分.

3　基于 Diffie-Hellman 关系的 All-But-N 可提取哈希证明系统

本节在文献[19]的基础上,扩展辅助输入 TAG 的形式,给出一个基于 Diffie-Hellman 关系的 All-But-One 可提取哈希证明系统,事实上这个分支可以达到长度 N(这里 N 为根据策略能得到相同权重值的不同标签个数),因此也可称作 All-But-N 的可提取哈希证明系统.

系统参数设置 选取阶为素数 q 的群 G,其对应的生成元为 g. 系统选取特定的 l 对默认参数 ***Weight*** = $\begin{bmatrix} W_{10} & W_{20} & \cdots & W_{l0} \\ W_{11} & W_{21} & \cdots & W_{l1} \end{bmatrix} \in Z_q^{2*l}$. 计算对应的矩阵 $\begin{bmatrix} g^{W_{10}} & g^{W_{20}} & \cdots & g^{W_{l0}} \\ g^{W_{11}} & g^{W_{21}} & \cdots & g^{W_{l1}} \end{bmatrix} \in Z_q^{2*l}$

公共参数 PP 为$(g,g^a,(g^{aW_{i,0}},g^{aW_{i,1}})_{i=1}^{l})$.

私有参数 SP 为 a 和$(W_{i,0},W_{i,1})_{i=1}^{l}$.

根据 Diffie-Hellman 关系可定义抽样函数 SampR$(r) = (g^r,g^{ra})$,这里 $r \leftarrow_R Z_q$.

则可定义公开函数

$$\tau = H_{PK}(u) = (\prod g^{aW_{i,tag_i}} \cdot PK)r$$

这里 $u = g^r$.

公开计算/可提取

(1) $SetupExt: PK = g^{SK}, SK \leftarrow_R Z_q$

(2) $Pub(PK,TAG,r) = (\prod_{i=1}^{l} g^{aW_{i,tag_i}} \cdot PK)^r$

(3) $Ext(SK,TAG,u,\tau) = (\tau \cdot u^{-SK})^{(\sum_{i=1}^{l} W_{i,tag_i})^{-1}}$

上式中提取模式的正确性可以通过下式验证得到.

$$\tau = \mathrm{H}_{\mathrm{PK}}(\mathrm{TAG},u) = (\prod_{i=1}^{l} g^{a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i})} \cdot \mathrm{PK})r$$

$$= (g^{a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i})} \cdot g^{\mathrm{SK}})r = u^{a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i})+\mathrm{SK}}$$

$$\Leftrightarrow (\tau \cdot u^{-\mathrm{SK}})^{(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i})^{-1}} = u^{a}$$

ABO 提取模式

(1) $\mathrm{SetupABO}(\mathrm{PP},\mathrm{TAG}^*)$:

$$\mathrm{PK}^* = g^{\mathrm{SK}^*} \cdot g^{-a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})}, \mathrm{SK}^* \leftarrow_R Z_q$$

(2) $\mathrm{Priv}(\mathrm{SK}^*,u) = u^{\mathrm{SK}^*}$

(3) $\mathrm{Ext}^*(\mathrm{SK}^*,\mathrm{TAG}^*,u,\tau)$

$$= (\tau \cdot u^{-\mathrm{SK}^*})^{(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i} - (\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*}))^{-1}}$$

在 ABO 的提取模式中,当 TAG 和TAG^*根据策略能得到相同权重值时,其公开计算的函数和私有计算的函数计算出来的结果是相等的. 即

$$\mathrm{Pub}(\mathrm{PK}^*,\mathrm{TAG},r) = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK}^*)r$$

$$= (g^{a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})} \cdot g^{SK^*-a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})})r$$

$$= u^{\mathrm{SK}^*} = \mathrm{Priv}(\mathrm{SK}^*,u)$$

在 ABO 的提取模式中,对于所有不满足策略的 TAG 和TAG^*,其提取算法的正确性可以通过下式验证得到,

$$\tau = \mathrm{H}_{\mathrm{PK}}(\mathrm{TAG},u) = (\prod_{i=1}^{l} g^{a\mathrm{W}_{i,\mathrm{tag}_i}} \cdot \mathrm{PK}^*)r$$

$$= (g^{a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i}} \cdot g^{\mathrm{SK}^*-a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})})^{r}$$

$$= u^{a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i} - a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})} \cdot u^{\mathrm{SK}^*}$$

$$\Leftrightarrow (\tau \cdot u^{-\mathrm{SK}^*})^{(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i} - (\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*}))^{-1}} = u^{a}$$

从上式可以看出,在 ABO 的提取模式中,可能有 N 个TAG^*均能满足基于 TAG 的策略要求,即可能有 N 个分支都能使得 $\sum_{i=1}^{l} W_{i,\mathrm{tag}_i} = \sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*}$ 成立,因此可用 ABN 来表示.

4 基于 ABN 可提取哈希证明系统的多策略 CCA 加密方案

本方案是在第 3 节给出的基于 Diffie-Hellman 关系的 ABN 可提取哈希证明系统的基础上给出的. 在本方案中,参数 ***Weight*** 是一个二维矩阵,里面的每一个元素 W_{i0}, W_{i1} 可以表示一个属性值的两种情况,W_{i1} 表示拥有这个属性对应的权值,对应的 W_{i0} 表示不拥有这个属性对应的权值. 此种形式可以用来表示单调的属性访问策略.

例如,当前系统里的属性集合为 ***Attribute*** = {男,大学生,计算机科学专业,身高 170cm 以上,通过英语四级},给出属性对应的权值矩阵 ***Weight*** = $\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 3 & 1 \end{bmatrix} \in Z_q^{2*5}$.

当用户情况为{男,非大学生,非计算机科学专业,身高不足 170cm,通过英语四级},可用 ***Attribute*** = {1,0,0,0,1} 表示. 因此当用户 1 的属性设置为 ***Attribute***1 = {1,0,0,0,1} 和用户 2 的属性设置为 ***Attribute***2 = {0,0,0,1,0} 时,用户 1 和用户 2 利用公式 $\sum_{i=1}^{l} W_i \, Attr_{i,\mathrm{tag}_i}$ 可以计算出相同的值.

在上例中,可以改变系统的策略,对非属性也给出对应权值. 例如可以令属性对应的权值矩阵为 ***Weight*** = $\begin{bmatrix} -2 & 0 & 0 & -3 & 1 \\ 2 & 1 & 1 & 3 & 1 \end{bmatrix} \in Z_q^{2*5}$,当用户 1 的属性为 ***Attribute***1 = {0,0,0,1,1} 和用户 2 的属性为 ***Attribute***2 = {0,1,0,1,0} 时,用户 1 和用户 2 也可以利用公式 $\sum_{i=1}^{l} W_i \, Attr_{i,\mathrm{tag}_i}$ 计算出相同的值.

在本方案中,同样存在一个辅助输入标签 TAG = $\mathrm{tag}1,\mathrm{tag}2,\cdots,\mathrm{tag}_l \in \{0,1\}^l$,作为用户的属性值.

4.1 方案构造

首先需要进行系统参数的设置,选取阶为素数 q 的一系列群 G. 随机选取 $g \leftarrow_R G$. 与第 3 节类似,标签 TAG = $\mathrm{tag}1,\mathrm{tag}2,\cdots,\mathrm{tag}_l \in \{0,1\}^l$,表示长度为 l 的比特串. 系统选取特定的 l 对默认属性 ***Weight*** = $\begin{bmatrix} W_{10} & W_{20} & \cdots & W_{l0} \\ W_{11} & W_{21} & \cdots & W_{l1} \end{bmatrix} \in Z_q^{2*l}$. 计算对应的矩阵 $\begin{bmatrix} g^{W_{10}} & g^{W_{20}} & \cdots & g^{W_{l0}} \\ g^{W_{11}} & g^{W_{21}} & \cdots & g^{W_{l1}} \end{bmatrix} \in Z_q^{2*l}$

公共参数 PP 为$(g, g^a, (g^{aW_{i,0}}, g^{aW_{i,1}})_{i=1}^{l})$. 私有参数 SP 为 a 和$(W_{i,0}, W_{i,1})_{i=1}^{l}$.

我们的加密方案由以下三元组(Gen, Enc, Dec)组成:

(1) $\mathrm{Gen}(\mathrm{PP})$: $\mathrm{PK} = g^{\mathrm{SK}}, \mathrm{SK} \leftarrow_R Z_q$

(2) $\mathrm{Enc}(\mathrm{PK},\mathrm{TAG},b)$:随机取 $r \leftarrow_R Z_q$,输出对应密文为:

$$C = \{c_1 = g^r, c_2 = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})^r, c_3 = G((g^a)^r)b\}$$

(3) $\mathrm{Dec}(\mathrm{SK},\mathrm{TAG},c)$:将 C 分割为$\{c_1,c_2,c_3\}$,验证 $c_2 = c_1^{a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i}+\mathrm{SK}}$,若等式不成立则输出 $\perp$,若等式成立则输出解密结果 $b' = G((c_1^{-\mathrm{SK}} \cdot c_2)^{(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i})^{-1}}) \oplus c_3$.

上述方案是逐比特加密的形式,可以通过将加密

方案中的随机数 $r \leftarrow_{Rq}$ 扩展为 n 个,即 $r_1, r_2, \cdots r_n \leftarrow_R Z_q^n$ 来直接得到明文定义域为 Z_q^* 下的加密方案.

4.2 方案的正确性和安全性分析

本方案的正确性可以直接由第 3 节给出的 ABN 可提取哈希证明系统中,提取模式的正确性得到.

下面我们将利用一系列的 GAME 游戏来完成安全性证明. 在真实游戏GAME_0 中,C_b 代表挑战密文,其中 C_0 是真实密文,C_1 是随机生成的密文. 在GAME_4 中,C_0 和 C_1 都将被替换成均匀分布的随机值. 我们将展示所有的游戏都是计算不可区分的.

GAME_0:本游戏为真实游戏.

选取阶为素数 q 的一系列群 G. 随机选择标签 $\mathrm{TAG} = \mathrm{tag1}, \mathrm{tag2}, \cdots, \mathrm{tag}_l \in \{0,1\}^l$,随机选取 $g \leftarrow_R G$. 随机选取$(W_{i,0}, W_{i,1}) \leftarrow_R Z_q$,这里 $i \in [1, l]$. 公共参数 PP 为$(g, g^a, (g^{aW_{i,0}}, g^{aW_{i,1}})_{i=1}^l)$. 私有参数 SP 为 a 和$(W_{i,0}, W_{i,1})_{i=1}^l$.

选取 $r \leftarrow_R Z_q$,给定 $\mathrm{SampR}(r) = (g^r, g^{ra}) = (u, s)$ 满足 Diffie-Hellman 假设的单向关系. 给定 $\tau = H_{PK}(u) = (\prod_{i=1}^{l} g^{aW_{i,tag_i}} \cdot \mathrm{PK})^r$.

由 $\mathrm{Gen}(\mathrm{PP})$产生公私钥对 $\mathrm{PK} = g^{SK}, \mathrm{SK} \leftarrow_R Z_q$.

在给出挑战密文前,敌手访问加密谕言机 Enc 可得到明文对应的密文. 敌手访问解密谕言机 Dec 可得到密文对应的解密结果.

挑战者选定 $b_i \leftarrow_R \{0,1\}$. 生成挑战密文

$$C_{b_i} = \{c_1 = g^r, c_2 = (\prod_{i=1}^{l} g^{aW_{i,tag_i}} \cdot \mathrm{PK})^r, c_3 = G((g^a)^r) \oplus b_i\}$$

,敌手被给定 C_{b_i},然后输出一比特 b'. 假如 $b' = b_i$,则敌手获胜.

GAME_1:将GAME_0 中由 SetupExt 产生的公私钥对更改为由 SetupABO 产生的公私钥对$(\mathrm{PK}^*, \mathrm{SK}^*)$. 在回答所有对 SK 产生密文的问询时,用 SK^* 产生的密文代替. 具体过程如下所示.

按照 SetupABO 产生公私钥对 $\mathrm{SK}^* \leftarrow_R Z_q, \mathrm{PK}^* = g^{\mathrm{SK}^*} \cdot g^{-a(\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*})}$.

利用 PK 访问加密谕言机 Enc 产生密文

$$C_{b_i} = \{c_1 = g^r, c_2 = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})r, c_3 = G((g^a)^r) \oplus b_i\}$$

这里

$$c_2 = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})^r = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot g^{SK^* - \sum_{i=1}^{l} \alpha_{i,\mathrm{tag}_i^*}})^r$$

利用 SK^* 访问解密谕言机 Dec′可得到密文对应的解密结果. Dec′的具体内容如下:

当 $\mathrm{TAG} = \mathrm{TAG}^*$ 时,Dec′输出解密结果为 $\perp$.

当 $\mathrm{TAG} \neq \mathrm{TAG}^*$ 时,Dec′利用 ABO 提取模式中的 $\mathrm{Ext}^*(\mathrm{SK}^*, \mathrm{TAG}^*, u, \tau)$进行计算. 即

$$c_2 = \tau = \mathrm{H}_{PK}(\mathrm{TAG}, u) = u^{a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i} - a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*}} \cdot u^{\mathrm{SK}^*}$$

GAME_2:我们将密文中的 c_2 部分由 $c_2 = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})^r$ 改为 $c_2 = (g^{a\sum_{i=1}^{l} W_{i,tag_i^*} + \mathrm{SK}})^r$,即由 Pub 模式改为 Priv 模式. 也即在游戏模拟的密文讯问中,我们将密文改为

$$C^* = \{c_1 = g^r, c_2 = (g^{a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*} + \mathrm{SK}^*})r, c_3 = G((g^a)^r) \oplus b_i\}$$

GAME_3:我们将密文的第三部分 c_3 用产生的随机数 $c_3 \leftarrow_R Z_q$ 代替.

由于GAME_3 中的挑战信息与 b 无关,因此敌手运行GAME_3 的获胜优势为 0. 下面证明若存在基于 Diffie-Hellman 假设的单向关系,则对于 $i = 0, 1, 2$,不存在多项式时间的敌手能够以不可忽略的优势区分GAME_i 和GAME_{i+1}.

***i* = 0 时**:本过程是用 SetupABO 产生的公私钥对$(\mathrm{PK}, \mathrm{SK}^*)$代替 SetupExt 产生的公私钥对$(\mathrm{PK}, \mathrm{SK})$. 两种模式的不可区分蕴含了$\mathrm{GAME}_0$ 和GAME_1 对于

$$(\mathrm{PK}, C = \{c_1 = g^r, c_2 = (\prod_{i=1}^{l} g^{aW_{i,tag_i}} \cdot \mathrm{PK})r, c_3 = g^{ar} \oplus b_i\})$$

的视图是相同的,也即对于所有的 PK,$\mathrm{Dec}(\mathrm{SK}, \cdot)$和 $\mathrm{Dec}'(\mathrm{SK}^*, \cdot)$对于所有满足二元关系的输入$(u, \tau)$的解密结果是相同的. 具体为:

当 $\mathrm{TAG} = \mathrm{TAG}^*$ 时,Dec′和 Dec 的输出解密结果均为 $\perp$.

当 $\mathrm{TAG} \neq \mathrm{TAG}^*$ 时,假如 $\tau = \mathrm{H}_{PK}(u)$ 即 $c_2 = (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})^r$ 时,由提取模式的正确性可知

$$(c_1^{-\mathrm{SK}} \cdot c_2) = (g^r)^{-\mathrm{SK}} \cdot (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot \mathrm{PK})^r = g^{ra}$$

同样的,由 ABO 模式的正确性可知$(c_1^{-\mathrm{SK}^*} \cdot c_2) = (g^r)^{-\mathrm{SK}^*} \cdot (\prod_{i=1}^{l} g^{aW_{i,\mathrm{tag}_i}} \cdot g^{SK^* - a\sum_{i=1}^{l} W_{i,\mathrm{tag}_i^*}})r = g^{ra}$

因此 Dec′ 与 Dec 的输出解密结果相同. 所以GAME_0 与GAME_1 是计算不可区分的.

***i* = 1 时**:本过程是在游戏模拟的密文询问中,将密文中的 c_2 部分由 $c_2 = (\prod_{i=1}^{l} g^{aW_{i,tag_i}} \cdot \mathrm{PK})^r$ 改为 $c_2 = (g^{a\sum_{i=1}^{l} W_{i,tag_i^*} + \mathrm{SK}})^r$,也即由 Pub 模式改为 Priv 模式. 由第四节中 ABO 模式的正确性可知,GAME_1 与GAME_2 是计算不可区分的.

$i=2$ 时:由于 $G((g^a)^r)$ 是从 g^{ar} 中提取的硬核比特,具有随机性,与随机选取的 1 比特是不可区分的. 因此$GAME_2$ 和$GAME_3$ 是相同的. 因此得证.

4.3 效率分析与对比

下面将本方案与文献[18]提出的 CP-ABE 方案、文献[19]中的两个方案(记为文献[19]-1 和文献[19]-2)进行对比与分析. 表 1 列出了本方案与其他三种方案在安全模型、安全假设、是否具有多策略性,公钥长度及密文长度等方面的对比结果. 为简化说明,表格中用 l 来表示标签的比特长度及明文的长度,用 R_T 和 R 分别表示文献[18]中两个群中群元素的大小.

表 1 相关方案性能对比结果

方案名称	安全模型	安全假设	多策略	公钥长度	密文长度
文献[18]	标准模型	SDP	是	$2R_T+(2+l)R$	$R_T+(1+2l)R+l$
文献[19]-1	标准模型	HOF	否	$2+2l$	$1+l$
文献[19]-2	标准模型	CDH	否	6	$3l$
本方案	标准模型	CDH	是	$3+2l$	$3l$

由表 1 可看出,四种方案均为标准模型. 对于安全假设,文献[18]的方案是在合数阶双线性群上基于子群不可区分性问题(Subgroup decision problem,简记为 SDP)假设构造的. 文献[19]-1 基于因式分解的困难性问题(Hardness of factoring,简记为 HOF),文献[19]-2 和本方案则是基于更弱的查找性假设(Computational Diffie-Hellman problem 简记为 CDH). 文献[18]利用了基于属性的访问控制结构参与运算,因此表达形式更丰富,具有多策略性,但由于方案建立在合数阶双线性群上,因此公钥和密文长度会略多. 本文第四节的方案中,则是将访问控制策略嵌入参数中,利用标签来控制访问分支. 在本文给出的方案是逐比特加密形式,其密文长度为 3 个群元素,当本方案扩展为明文定义域为 Z_q^* 下的加密方案时,密文长度为 $3l$. 为与表格中其他方案一致和便于比较,在表 1 中将本方案的密文长度直接写为了 $3l$. 文献[19]中的相关方案与本文相比公钥长度会略短,但是并未考虑多策略性问题.

5 结论与展望

为了建立基于查找性假设的安全方案,本文首先利用基于搜索问题的二元关系,给出了一个基于 Diffie-man 关系的 ABN 可提取哈希证明系统. 作为对该方案的一个扩展,本文还给出了一个基于权重和多策略的加密方案,并利用一系列的 GAME 游戏来完成安全性证明. 根据 Goldreich-Levin 硬核比特定理,当参与运算的随机数是一个有限域中的元素时,本文从二元关系的 s 中能够提取出 1 比特随机量,只有当将随机参数扩展为一个向量时,才能够提取出多项式随机量. 因此如何构造紧致参数下基于计算性假设的有效 CCA 加密方案是下一步的研究方向. 此外如何将本方案中具有 All-But-N 性质的 CCA 加密方案提升为具有选择打开安全的加密方案或具有多个损耗分支 All-But-M 方案也是值得研究的一个问题.

参考文献

[1] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption [A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2002. 45-64.

[2] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack [A]. Annual International Cryptology Conference [C]. Berlin Heidelberg: Springer, 1998. 13-25.

[3] Alwen J, Dodis Y, Naor M, Segev G, Walfish S, Wichs D, Walfish, S, Wichs, D. Public-key encryption in the bounded-retrieval model[A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques [C]. Berlin Heidelberg: Springer, 2010. 113-134.

[4] Chen Y, Zhang ZY, Lin DD, Cao ZF. Generalized(identity-based) Hash proof system and its applications[J]. Security and Communication Networks, 2016, 9(12): 1698-1716.

[5] 来齐齐,杨波,陈原,韩露露,白健. 格上基于身份哈希证明系统的新型构造[J]. 软件学报,2018, http://www.jos.org.cn/1000-9825/5357.html.
Lai QQ, Yang Bo, Chen Y, Han LL, Bai Jian. Novel construction of identity-based hash proof system based on lattices[J]. Journal of Software, 2018, http://www.jos.org.cn/1000-98255357.htm. (in Chinese)

[6] Zhu D, Zhang R, Jia D. Public-key encryption with simulation-based sender selective-opening security[A]. International Conference on Provable Security[C]. Cham: Springer, 2017. 361-380.

[7] Wee H. KDM-security via homomorphic smooth projective hashing[A]. IACR International Workshop on Public Key Cryptography[C]. Berlin Heidelberg: Springer, 2016. 159-179.

[8] Abdalla M, Benhamouda F, Pointcheval D. Disjunctions for

hash proof systems: New constructions and applications [A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2015. 69 – 100.

[9] Benhamouda F, Blazy O, Chevalier C, et al. New techniques for SPHFs and efficient one-round PAKE protocols [A]. Annual International Cryptology Conference [C]. Berlin Heidelberg: Springer, 2013. 449 – 475.

[10] Katz J, Vaikuntanathan V. Smooth projective Hashing and password-based authenticated key exchange from lattices [A]. International Conference on the Theory and Application of Cryptology and Information Security [C]. Berlin Heidelberg: Springer, 2009. 636 – 652.

[11] Blazy, O, Pointcheval, D, & Vergnaud, D. (2012, March). Round-optimal privacy-preserving protocols with smooth projective hash functions [A]. Theory of Cryptography Conference [C]. Berlin Heidelberg: Springer, 2012. 94 – 111.

[12] Kalai Y T. Smooth projective hashing and two-message oblivious transfer [A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2005. 78 – 95.

[13] Garg S, Gentry C, Sahai A, et al. Witness encryption and its applications[A]. Proceedings of the forty-fifth annual ACM symposium on Theory of computing[C]. New York USA: ACM, 2013. 467 – 476.

[14] Abdalla M, Chevalier C, Pointcheval D. Smooth projective hashing for conditionally extractable commitments [A]. Annual International Cryptology Conference [C]. Berlin Heidelberg: Springer, 2009. 671 – 689.

[15] Hemenway B, Ostrovsky R. Lossy trapdoor functions from smooth homomorphic Hash proof systems[J]. Electronic Colloquium on Computational Complexity, 2009, 16 (127): 127 – 127.

[16] Wee H. Dual projective hashing and its applications—lossy trapdoor functions and more [A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2012. 246 – 262.

[17] Zhang M, Zhang Y, Su Y, et al. Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments [J]. IEEE Systems Journal, 2017, 11(2): 1018 – 1026.

[18] Zhang L, Zhang J, Mu Y. Novel leakage-resilient attribute-based encryption from hash proof system[J]. The Computer Journal, 2016, 60(4): 541 – 554.

[19] Wee H. Efficient chosen-ciphertext security via extractable hash proofs[A]. Annual International Cryptology Conference[C]. Berlin Heidelberg: Springer, 2010. 314 – 332.

[20] Chen Y, Zhang Z. Publicly evaluable pseudorandom functions and their applications[J]. Journal of Computer Security, 2016, 24(2): 289 – 320.

[21] Faonio A, Nielsen J B, Venturi D. Predictable arguments of knowledge[A]. IACR International Workshop on Public Key Cryptography [C]. Berlin Heidelberg: Springer, 2017. 121 – 150.

[22] Goyal R, Goyal V. Overcoming cryptographic impossibility results using blockchains[A]. Theory of Cryptography Conference[C]. Cham: Springer, 2017. 529 – 561.

[23] Hu C, Liu P, Guo S. Public key encryption secure against related-key attacks and key-leakage attacks from extractable hash proofs[J]. Journal of Ambient Intelligence and Humanized Computing, 2016, 7(5): 681 – 692.

[24] Goldreich O, Levin L A. A hard-core predicate for all one-way functions[A]. Proceedings of the twenty-first annual ACM symposium on Theory of computing[C]. Seattle, Washington: ACM, 1989. 25 – 32.

[25] Dodis Y, Goldwasser S, Kalai Y, et al. Public-key encryption schemes with auxiliary inputs[A]. Theory of Cryptography Conference [C]. Berlin Heidelberg: Springer, 2010. 361 – 381.

[26] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption[A]. International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin Heidelberg: Springer, 2004. 207 – 222.

[27] Cash D, Kiltz E, Shoup V. The twin Diffie – Hellman problem and applications [J]. Journal of Cryptology, 2009, 22(4): 470 – 504.

作者简介

张丽娜　女,1981 年出生,博士,副教授,研究方向为密码学、信息安全.
E-mail: zhangln@ xust. edu. cn

杨　波(通信作者)　男,1963 年出生,教授、博士生导师,陕西省“百人计划”特聘教授,研究方向为密码学、信息安全.
E-mail: byang@ snnu. edu. cn