基于密文策略的流程加密研究

邓宇乔[1),2)] 杨 波[2),3)] 唐春明[4)] 宋 歌[5)] 温雅敏[1)]

[1)](广东财经大学统计与数学学院 广州 510120)

[2)](陕西师范大学计算机科学学院 西安 710062)

[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)](广州大学数学与信息科学学院 广州 510006)

[5)](华南农业大学数学与计算机学院 广州 510120)

摘 要 近年来,用户通常通过云服务器与他人共享信息,以节省本地存储空间.然而,云服务提供商(CSP)不能完全被信任.实际上,在不同文献提出的各种模型中,CSP 被定义为半可信方:它是好奇但会诚实地执行程序的实体.但它可能会泄露一些用户的私人信息以谋取自己的利益.因此,用户需要在将私人内容上传到云端之前对其私密内容进行加密.但是,文件的加密形式将使得内容的共享不方便.许多文献尝试在不同的应用场景中使密文分享成为可能.为了解决上述密文共享的问题,一种基于非对称密钥的密码系统被提出,该系统被称为属性基加密(Attribute based Encryption, ABE).ABE 是一个多功能和高效的密码原语.ABE 包括以下两种类型,即密钥策略 ABE(KP-ABE)和密文策略 ABE(CP-ABE).在 KP-ABE 中,密文与属性集合相关,而秘钥与访问策略相关联.只要与密文相关的属性集合满足嵌入在秘钥中的访问策略,密文就可以被恢复.在 CP-ABE 中,密文与访问策略相关联,而密钥与一组属性相关.只要与秘钥相关的属性集合满足嵌入在密文中的访问策略,密文就可以被恢复.用户可以使用 ABE 高效地共享云中的信息,而不用担心其隐私被泄露.例如,在 CP-ABE 的环境中,用户使用指定的访问策略加密文件并将密文上传到云;则拥有访问策略中指定属性集的用户可以解密该密文.虽然 ABE 在很多应用中都很强大并且有效,但它不适用于某些特殊情况.本文研究了与流程认证有关的新应用场景.在这种场景下,数据所有者需要在用户访问加密内容之前确保用户是否满足多个流程.由于传统的 ABE 无法高效地描述流程,因此在此场景下不适用.一种基于流程的加密(Process Based Encryption, PBE)的新密码学原语被提出.PBE 被分成两类,即密钥策略的 PBE(Key-Policy PBE, KP-PBE)和密文策略的 PBE(Ciphertext Policy PBE, CP-PBE).一种 CP-PBE方案被提出.在 CP-PBE 中,加密者可以通过在加密消息时指定接收者的访问策略来细粒度地指定密文的接收者.若解密者持有的流程集满足密文中描述的访问策略时,该解密者可恢复明文消息.CP-PBE 在高效地描述各种流程方面具有优势.在标准模型中,使用双线性映射和线性秘密共享方案(LSSS)的工具构建了 CP-PBE 方案.定义了 CP-PBE 的选择性安全模型.使用分区策略提供了 CP-PBE 的安全性证明.CP-PBE 的安全性被归约到双线性 Diffie-Hellman 指数的假设上(q-BDHE).给出了 CP-PBE 和一般 CP-ABE 的效率分析.

关键词 流程加密;密文策略;属性加密;选择安全性;访问结构

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01063

Research of Ciphertext Policy Process-Based Encryption

DENG Yu-Qiao[1),2)] YANG Bo[2),3)] TANG Chun-Ming[4)] SONG Ge[5)] WEN Ya-Min[1)]

[1)](*School of Statistics and Mathematics, Guangdong University of Finance and Economics, Guangzhou* 510120)

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

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[4)](*School of Mathematics and Computer Science, Guangzhou University, Guangzhou* 510006)

[5)](*College of Mathematics and Informatics, South China Agricultural University, Guangzhou* 510120)

收稿日期:2017-08-31;在线出版日期:2018-07-11.本课题得到国家"九七三"重点基础研究发展规划项目(2017YFB0802000)、国家自然科学基金(61772147,61300204)、教育部人文社科研究项目(15YJCZH029)、广州市哲学社会科学发展"十三五"规划课题(2016GZYB25,2017GZQN05)、广东省自然科学基金重大基础研究培育项目(2015A030308016)、广东省自然科学基金(2015A030313630)、广东省教育厅基础研究重大项目(2014KZDXM044)、广东省普通高校创新团队建设项目(2015KCXTD014)、国家密码发展基金(MMJJ20170117)、广州市教育局协同创新重大项目(1201610005)、上海市信息安全综合管理技术研究重点实验室开放课题基金(AGK2015007)、广东省科技计划项目(2016A020210103,2017A020208054)资助.**邓宇乔**,博士,副教授,主要研究领域为密码学、云计算.E-mail:gdufedyq@foxmail.com.**杨 波**(通信作者),博士,教授,主要研究领域为信息安全和密码学.**唐春明**,博士,教授,主要研究领域为密码学、云计算.**宋 歌**,博士,讲师,主要研究领域为数据挖掘、密码学.**温雅敏**,博士,副教授,主要研究领域为密码学、云计算.

Abstract In recent era, users often share information with others through the cloud server, in order to save the local storages. Nevertheless, the cloud sever provider (CSP) cannot be absolutely trusted. Actually, in many models presented by different works, CSP is defined as a semi-honest party: it is curious and will perform the procedure honestly, but it may leak some user's private information for its own profit. So, it is necessary for users to encrypt their private contents before upload them to the cloud. However, the encrypted form of file makes content sharing inconvenient. Lots of attempts try to make ciphertext sharing feasible in different applications. To address the aforementioned ciphertext sharing problem, an asymmetric key cryptographic system, i.e., attribute based encryption (ABE) is proposed. ABE is a versatile and efficient cryptographic primitive. ABE includes the following two types, namely, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). The ciphertext is encrypted with a set of attribute, and the secret key is associated with the access policies in the KP-ABE. The ciphertext can be recovered, as long as the attribute set associated with the ciphertext satisfies the access polices embedded in the secret key. The ciphertext is encrypted with the access policies, and the secret key is associated with a set of attribute in the CP-ABE. The ciphertext can be recovered, as long as the attribute set associated with the secret key satisfies the access polices embedded in the ciphertext. Users can use ABE to efficiently share information in the cloud without worrying about the leakage of their privacy. For example, in the CP-ABE setting, user encrypts the file with designed access policies and uploads the ciphertext to the cloud; then, the other user can decrypt this ciphertext, if it holds the required attribute set. Although ABE is strong and efficient in many applications, it does not suited for some special scenarios. A new application scenario related to process authentication is studied in this paper. In this scenario, the data owner needs to ensure whether a user satisfies several processes, before the user accesses the encrypted contents. The classical ABE cannot be used because they cannot describe processes efficiently. A new cryptography primitive called Process-Based Encryption (PBE) is presented to address the aforementioned problem. PBE is classified into two types, i.e., Key-Policy PBE (KP-PBE) and Ciphertext Policy PBE. A CP-PBE is presented. The encryptor can specify the recipient of the ciphertext by encrypting message along with the access policies in the CP-PBE. The decryptor can recover the message if it holds the secret key associated with the desired process set. The CP-PBE has advantage in efficiently and effectively describing all kinds of processes. A CP-PBE scheme is constructed in the standard model, using the tools of bilinear maps and Linear Secret Sharing Scheme (LSSS). The selective security model of CP-PBE is defined. The security proof is provided using the partitioning strategy. The security of the CP-PBE is reduced to the q-Bilinear Diffie-Hellman Exponent Assumption (q-BDHE). The efficiency analysis of CP-PBE and general CP-ABE is presented.

Keywords process encryption; ciphertext-policy; attribute-based encryption; selective security; access structure

1 引 言

属性加密(Attribute-Based Encryption,ABE)是一种灵活的、对敏感数据的使用权限可进行控制的加密原语,其于 2005 年首先由 Sahai 和 Waters[1] 提出.由于可控制的对象可分为密文与密钥两类,因此,属性加密可分为两种基本类型,即密钥策略的属性加密(Key Policy Attribute-Based Encryption, KP-ABE)[2] 与密文策略的属性加密(Ciphertext Policy Attribute-Based Encryption, CP-ABE)[3]. KP-ABE 方案在加密明文时,把某个属性组与明文

链接，在生成密钥时，把密钥与访问策略链接；CP-ABE 方案在加密明文时，把访问策略与明文链接，在生成密钥时，把密钥与某个属性组链接. 目前，ABE 较为热门的研究思路大致有两种：一种为研究具有特定功能的 ABE，如具有短密文特性的可分层的 ABE（Hierarchical Attribute based Encryption，HABE）[4-6]、可快速解密的 ABE[7]、具有定长密文的 ABE[8]、支持“否”谓词的 ABE[9]、支持大属性域的 ABE[10]，等等[11-15]；而另一种则为研究 ABE 的安全性增强技术[16-17]. ABE 安全与高效的特点，以及灵活的权限控制方式，将可在云计算的环境下，对用户的隐私保护起到至关重要的作用.

ABE 能提供对于一般属性的较为高效的访问权限控制机制，然而，对某种“特殊”的流程属性而言，ABE 所提供的机制并不高效. 文献[18]首次提出了基于流程的加密原语，并构造了密钥策略的流程加密方案，然而，该文并未提出密文策略的流程加密方案的构造. 本文将研究密文策略的流程属性加密方案的构造过程，以下首先给出研究的动机.

1.1　一种特殊的属性——流程属性

在现实生活中，流程属性的应用场景十分常见. 例如，某高校规定只有本校新进的教职工能浏览学校的某些内部文件，而学校新进的教职工必须通过各部门共同审核，走完审核流程后方能入职. 假设该学校的新进员工需要走以下两个流程：流程 1 为该员工需要到人事处报到，随后携人事处回执到所在院系报到，最后持院系证明到校医院体检；流程 2 为员工所在院系根据该员工的当前业务能力为其初步定岗，该员工持院系开具的初步定岗证明移交人事处，人事处确认后统一上报校长办公室审批. 走完以上两个流程，该员工方可正式入职，并拥有浏览学校内部文件的权限.

在以上实例中，可将教职工入职的流程表述如下：

流程 1：人事处→院系→校医院

流程 2：院系→人事处→校长办公室

在经典的 CP-ABE 中，需要描述以上的流程，可使用如下的两种方法：

方法 1.　可为每个流程设置一个对应的属性. 如，在上例中，可设置两个属性：属性 1 和属性 2. 令属性 1 表示流程 1，属性 2 表示流程 2. 使用策略“属性 1 AND 属性 1”对消息进行加密，并向完成流程属性的用户颁发相应的属性密钥. 该方法尽管能满足上述应用的基本功能，但存在如下两点缺陷.

其一，对于参数共享类型的 CP-ABE 方案（即一个属性对应于一个公共参数、一个密文与一个密钥）而言，此方法将会导致公钥、密文和密钥的存储空间过大. 对于一些轻量级（Lightweight）的设备（如 RFID 读写器）而言，由于设备的存储空间非常有限，因此，此方法必然会限制 CP-ABE 在此类设备上的应用. 本质而言，由于该方法对流程的描述不够简练，将导致存储效率非常低. 本文将在第 1.3 节对此点予以详细说明.

其二，此方法将会造成属性密钥颁发方极大的认证负担，造成系统瓶颈. 在一般的应用中，一个流程的验证过程通常采用“多授权方”的验证模式，简述如下：用户每完成一个子流程，即可获得相应的证书（公章）. 不同的子流程，其证书（公章）由不同的部门负责颁发. 然而，若使用上述方法认证流程，将无法做到此点. 若将流程一描述为一个属性，则该属性密钥的认证（授权）方只能为一个授权中心. 因此，该中心为确认用户满足流程 1，需与人事处、院系以及校医院分别交互后，方可颁发属性密钥. 此举增加了授权中心的工作量，容易造成系统瓶颈. 因此，更为贴近的做法应为：将流程“拆分”为若干个子流程，每个子流程由特定的授权方负责授权. 每当用户完成其中的一个子流程，即可获得该子流程授权方颁发的证书（即密钥）. 若用户拥有所有子流程的证书（密钥），则认为其满足该流程. 因此，可考虑如下第 2 种描述流程的方法.

方法 2.　可将流程 1 拆分为 3 个子流程：“人事处”（流程起点）、“人事处→院系”和“院系→校医院”. 上述的 3 个子流程分别对应属性 A、属性 B 和属性 C. 由人事处、院系和校医院分别负责分配属性 A，属性 B 和属性 C 的密钥（可考虑利用现今的基于多授权方的 CP-ABE 方案进行构造）. 可见，由于为每一个子流程均指定了对应的授权方，有效地解决了方法 1 中单一授权方的认证负荷问题. 然而，以上方法也存在缺陷：导致访问结构变得非常复杂，从而影响解密效率. 因为在上述方案中，每个子流程均对应一个属性；而在经典的 CP-ABE 中，每个属性对应一个访问结构中的叶子节点（或访问矩阵中的一行），因此，当流程中包含的子流程较多时，访问结构将变得异常复杂，从而影响解密效率. 因此，本方法也不能在描述流程时取得令人满意的结果.

综上所述，本研究的动机为：设计一种便于描述流程、可支持多方共同验证流程且每个流程仅对应一种访问策略的加密方案. 该方案既解决了上述方法 1 存储效率低、不支持多方认证的问题，也同时解

决了方法 2 中访问结构过于复杂的问题.

1.2 非闭环流程——线性流程

为便于描述,本文先给出线性流程的定义.首先,本文先给出流程的一般定义.

定义 1(流程(Process)的定义). 设 $G=V,E$ 是有向图,V 为 G 的顶点集合,E 为 G 的有向边集合.称 P 是有向图 G 中的流程,若 P 满足:$P=p_1\rightarrow p_2\rightarrow\cdots\rightarrow p_n$,其中顶点集 $p_1,\cdots,p_n\in V$ 且有向边集 $p_1\rightarrow p_2,p_2\rightarrow p_3,\cdots,p_{n-1}\rightarrow p_n\in E$.称顶点集$\{p_1,\cdots,p_n\}$是流程 P 的节点集,称有向边集合 $R=\{p_1\rightarrow p_2,p_2\rightarrow p_3\cdots,p_{n-1}\rightarrow p_n\}$是流程 P 的关系集,称有向图中的边$(p_i\rightarrow p_j)\in R$ 是 P 的关系.

以下有两点需要说明:

(1)流程为有向的,因为每个流程均由有向关系(边)构成.

(2)本文所研究的流程不允许存在闭环,若有流程 $P'=a\rightarrow b\rightarrow c\rightarrow b$,该流程即为闭环流程(因为节点 b 经过了两次,如图 1 所示).

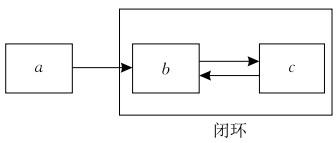

图 1 存在闭环的流程

因此,为更准确描述本文能处理的流程类型,以下给出线性流程的定义.

定义 2[18](线性流程(Linear Process)的定义). 设 $LP=lp_1\rightarrow lp_2\rightarrow\cdots\rightarrow lp_n$ 是有向图 $G=V,E$ 中满足条件 $lp_1,\cdots,lp_n\in V$ 与 $lp_1\rightarrow lp_2,lp_2\rightarrow lp_3,\cdots,lp_{n-1}\rightarrow lp_n\in E$ 的一个流程,若对所有的 $i\neq j(i,j\in[1,\cdots,n])$,都有 $lp_i\neq lp_j$,则称 LP 为线性流程.

定义 2 中对线性流程的定义限定了线性流程的特性:线性流程中不可能存在闭环——因为在线性流程中,相同的顶点不能在流程中出现多于一次.如图 2 中的闭环流程 $P'=a\rightarrow b\rightarrow c\rightarrow b$ 不是线性流程,因为若设 $lp_1=a,lp_2=b,lp_3=c,lp_4=b$,则有 $lp_2=lp_4=b$,其显然不满足线性流程的条件.

在下文中,需从加密的角度解决当用户满足了某个线性流程时,如何对其进行验证的问题.以下通过定义 3 给出用户满足线性流程的条件.

定义 3[18]. 令 $LP=lp_1\rightarrow lp_2\rightarrow\cdots\rightarrow lp_n$ 为有向图 $G=V,E$ 的一个线性流程.若用户持有该线性流程的起点 p_1 及线性流程的关系集$\{lp_1\rightarrow lp_2,lp_2\rightarrow lp_3,\cdots,lp_{n-1}\rightarrow lp_n\}$中所有关系的密钥,则该用户满足线性流程 LP.

以下对定义 3 简要注释.设有线性流程 $LP'=a\rightarrow b\rightarrow c$,若用户持有起点 a 以及关系 $a\rightarrow b,b\rightarrow c$ 的密钥,则称该用户满足线性流程 LP'.

1.3 CP-ABE 在描述线性流程属性时的缺陷

本节将对第 1.1 节中方法一的缺陷进行解释.即,对于参数共享类型的 CP-ABE 方案(一个属性对应于一个公共参数)而言,方法一将会导致公钥存储空间过大的问题;另外,对于一般的 CP-ABE 方案而言(在此暂不论述一些特殊的密钥或密文定长的 CP-ABE,在第 3.5 节将补充说明),该方案将导致密文和密钥过长的问题.

传统的 CP-ABE 可分为两种类型:基于参数共享(Parameter Sharing,PS)的类型和基于大属性域(Attributes of Large Universe,ALU)的类型.

假设系统中包含的所有属性的个数为 n_P,密钥中包含的属性个数为 n_K,密文中包含的属性个数为 n_C.则在 PS 类型的 CP-ABE 中,公共参数的长度为 $\mathcal{O}(n_P)$,而基于 ALU 类型的 CP-ABE 的公共参数长度为 $\mathcal{O}(1)$(即公共参数与属性个数无关);而无论何种类型的 CP-ABE,其密钥长度均为 $\mathcal{O}(n_K)$,其密文长度均为 $\mathcal{O}(n_C)$.因此,分析传统 CP-ABE 在描述线性流程时所需要使用的属性量是个极为关键的要素.以下试用例 1 说明,若使用定义 3 的方法描述流程,将比传统 CP-ABE 描述流程更为高效.

例 1. 如第 1.1 节所述的两个流程内共包括 4 个部门(人事处、院系、校医院和校长办公室),考虑以下两种方法描述这 4 个部门可组成的所有流程.

(1)若使用第 1.1 节所述的方法描述流程,则共有 64 种可能的线性流程(即不存在闭环的流程,若考虑闭环流程,则会有无穷多种可能的流程).

上述结果可分析如下:若流程中包含的节点(部门)只有一个,此时流程属性"退化"为普通的属性,由于共有 4 个节点,所以共有 4 种可能的流程,即 P_4^1;若流程中包含的节点有两个,此时流程中的第 1 个节点(部门)有 4 种可能性,而第 2 个节点(部门)只有 3 种可能性(去掉已选的第 1 个部门后只有 3 种可能性),所以共有 P_4^2 种可能的流程;以此类推,4 个节点可组成的流程共有 $P_4^1+P_4^2+P_4^3+P_4^4=64$ 种.

而若采取第 1.2 节定义 3 的方法描述以上所有可能的流程,则仅需 16 个参数即可.可如图 2 所示进行描述:设定人事处、院系、校医院和校长办公室均为起点,并设置 4 个部门两两之间均有双向的关系.即,设定 4 个起点:人事处、院系、校医院和校长办公室;设定关系:人事处→院系、院系→人事处、人

事处→校医院、校医院→人事处、人事处→校长办公室、校长办公室→人事处、院系→校医院、校医院→院系、院系→校长办公室、校长办公室→院系、校医院→校长办公室、校长办公室→校医院.以上关系共计 12 个(P_4^2).因此,若使用定义 3 的方式描述以上 4 个部门所有可能组成的流程,仅需使用 4 个起点与 12 个关系参数,共计 16 个参数即可.

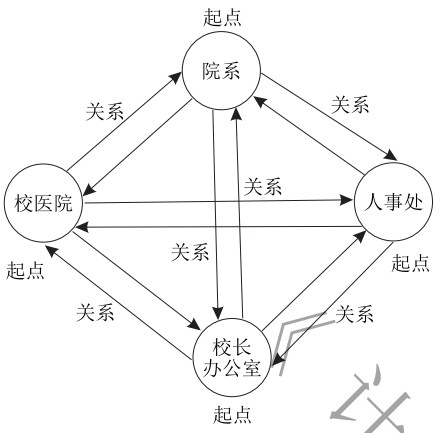

图 2　4 个节点的全线性流程设定

与上述分析类似,可将 4 个节点推广到 n 个节点的情况.以下给出定理 1.

定理 1.　n 个节点共能组成 $P_n^1+P_n^2+\cdots+P_n^n$ 种可能的流程.

简证.　如例 1 所述,若从 n 个节点中任取 i 个节点($i\leq n$)组成线性流程,则能组成 P_n^i 种可能的线性流程.因此,n 个节点共能组成的流程个数为 $P_n^1+P_n^2+\cdots+P_n^n$.

根据定理 1 可知,对于 PS 类型的 CP-ABE 而言,公共参数数量与流程数量成正比.因此,包含 n 个节点的 PS 类型的 CP-ABE 方案所需的公共参数的长度为 $\mathcal{O}(P_n^1+P_n^2+\cdots+P_n^n)>\mathcal{O}(C_n^0+C_n^1+\cdots+C_n^n)=\mathcal{O}(2^n)$,该参数长度的量级为指数级.而使用定义 3 所示方法,只需将每个节点设置为起点(长度为 $\mathcal{O}(n)$)及设置所有节点两两间均有双向的关系(长度为 $\mathcal{O}(P_n^2)=\mathcal{O}(n^2)$).故此,综合而言,使用定义 3 的方法描述流程,仅需 $\mathcal{O}(n^2)$ 的公共参数即可包含所有可能的流程.

同理,在经典的 CP-ABE 中,密钥的长度与该密钥中包含的属性个数 n_K 成正比.因此,若假设密钥(密文)中包含 n_s 个节点,则这 n_s 个节点最多共可组成 $\mathcal{O}(2^{n_s})$ 个流程,描述这些流程最长需要 $\mathcal{O}(2^{n_s})$ 长度的密钥;而使用定义 3 的方法描述这些流程,仅需 $\mathcal{O}(n_s{}^2)$ 长度的密钥.对于密文长度的分析与密钥长度的分析类似.

综上,由于定义 3 的方法在描述流程时具有比传统 CP-ABE 更便利的特点,因此,本文将依据定义 3 设计一种新型的加密方法——基于密文策略的流程加密方案(Ciphertext Policy Process-Based Encryption, CP-PBE).

1.4　本文所做的工作

本文所做的工作可描述如下:

(1)本文严格地给出了 CP-PBE 的定义,给出了其选择性的安全模型.

(2)利用双线性映射技术,在素阶群上提出了一种基于标准模型的 CP-PBE 方案,并证明了其安全性.

(3)分析了 CP-PBE 方案与一般的 CP-ABE 方案在描述流程时的时间和空间效率.

2　背景知识

本节将介绍本文所需使用到的背景知识.包括单调访问结构、线性秘密共享协议、双线性映射技术以及一个数学假设.

2.1　单调访问结构(Monotonus Access Structure)

定义 4(访问结构[3]).　令 $\{P_1,P_2,\cdots,P_n\}$ 为参与方实体组成的集合.若对于 $\forall B,C$,当 $B\in\mathbb{A}$ 且 $B\subseteq C$ 时有 $C\in\mathbb{A}$ 成立,则称 $\mathbb{A}\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$ 单调.授权集被定义为包含在 $\mathbb{A}$ 内的集合;而非授权集则被定义为不包含于 $\mathbb{A}$ 内的集合.

2.2　线性秘密共享协议(Linear Secret Sharing Scheme, LSSS)[3]

定义 5.　设集合 $P=\{P_1,P_2,\cdots,P_n\}$ 为参与方实体组成的集合,若满足以下的两个条件,则称 Π 为定义在 $\mathbb{Z}_p$ 上的 LSSS:

(1) $P_1,P_2,\cdots,P_n$ 共同持有 $\mathbb{Z}_p$ 上的一个秘密的分享向量.

(2)设 $\boldsymbol{M}$ 为一个 l 行 n 列的,定义在 Π 上的秘密的生成矩阵.ρ 为如下描述的一个映射:该映射把 $\boldsymbol{M}$ 里行标的集合映射到参与方实体的下标集合中.即,若 i 表示 $\boldsymbol{M}$ 中的一行,则 $\rho(i)$:($i\in\{1,\cdots,l\}$)表示某参与方实体的下标.若参与方集合中的某个授权集需要分享秘密值 $s\in\mathbb{Z}_p$,则他们可共同选定列向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)$,其中 $r_2,\cdots,r_n\in\mathbb{Z}_p^{n-1}$ 是随机分布的.参与方实体 $\rho(i)$ 通过计算 $(\boldsymbol{Mv})_i$:($i=1,\cdots,l$)可以得到相对应于其的秘密分割.

文献[3]指出,使用以上的 LSSS 方案,授权集合 S 内的成员可如下地恢复出秘密值 s.令集合 $I\subset$

$(1,2,\cdots,l)$为 $I=(i:\rho(i)\in S)$. 根据线性代数的知识,必能在多项式时间内搜索到常数集合 $\omega_i\in\mathbb{Z}_p$ 满足$\sum_{i\in I}\omega_i\lambda_i=s$. 且对于集合 I 的非授权集,必能在多项式时间内搜索到向量 $\boldsymbol{w}$ 且满足 $w_1=1$ 和 $\boldsymbol{w}\cdot\boldsymbol{M}_i=0:(i\in I)$.

2.3 双线性映射技术(Bilinear Maps)

选取阶为素数 q 的循环乘法群$\mathbb{G},\mathbb{G}_T$,设群$\mathbb{G}$上的一个生成元为 g. 定义 $e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$为一个双线性映射,则其具有以下性质.

(1)若有 $u,v\in\mathbb{G}$和$a,b\in\mathbb{Z}_p$, 则以下等式成立 $e(u^a,v^b)=e(u,v)^{ab}$.

(2)$e(g,g)\neq1$.

(3)$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$可高效地计算.

2.4 数学假设

以下介绍本文方案所使用到的数学假设:q-BDHE[3](q-Bilinear Diffie-Hellman Exponent Assumption).

定义 6. 设$\mathbb{G},\mathbb{G}_T$是阶为素数 q 的循环乘群. 令 g 是一个$\mathbb{G}$上的群生成元,$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$是一个双线性映射. 令$a,\gamma\leftarrow Z_p,R$ 是群$\mathbb{G}$上的一个随机元素. 判定性 q-BDHE 定义如下. 给定向量

$$\boldsymbol{X}=(\mathbb{G},p,g,g^{\gamma},g^{a},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}})$$

和群$\mathbb{G}_T$上的数 T. 定义概率多项式时间的(Probabilistic Polynomial-Time Algorithm, PPT)算法$\mathcal{A}$解决 q-BDHE 的优势为:

$$Adv_{q\text{BDHE}}=|Pr[\mathcal{A}(\boldsymbol{X},T=e(g,g)^{a^{q+1}\gamma})=0]-Pr[\mathcal{A}(\boldsymbol{X},T=R)=0]|$$

若对于任意的 PPT 算法$\mathcal{A}$,其解决 q-BDHE 的优势 $Adv_{q\text{BDHE}}$都可忽略,则判定性 q-BDHE 成立.

3 方案构造及讨论

3.1 CP-PBE 方案的定义及安全性模型

CP-PBE 共包括 4 个基本的子算法,分别为:Setup,Encrypt,KeyGen 和 Decrypt.

定义 1. CP-PBE 方案的 4 个算法分述如下.

Setup$(1^n,B,\mathfrak{R})$:Setup 算法的输入为安全参数 n,线性流程的起点个数 B 以及线性流程的关系集 $\mathfrak{R}$. 算法的输出为公共参数 PP 以及主密钥 MSK.

Encrypt. $(PP,\mathbb{A},m)$:Encrypt 算法的输入为公共参数 PP、访问结构$\mathbb{A}$以及消息 m. 算法的输出为密文 CT.

KeyGen. $(MSK,\mathfrak{B},\mathfrak{R})$:KeyGen 算法的输入为主密钥 MSK 以及线性流程的起点集$\mathfrak{B}$, 线性流程的关系集$\mathfrak{R}$. 算法的输出为私钥 SK.

Decrypt(SK,CT):Decrypt 算法的输入为密文 CT 以及私钥 SK. 算法输出明文消息 m,如果私钥中包含的流程集合满足密文中定义的访问结构$\mathbb{A}$;否则,算法将终止并输出$\perp$.

3.2 CP-PBE 的安全模型定义

本文所提的 CP-PBE 方案的安全性模型是建立在选择性安全(Selective Security)的基础上的. 以下给出 CP-PBE 的选择安全性的定义.

定义 2. (CP-PBE 的选择流程安全性的定义):CP-PBE 的选择流程安全性是敌手$\mathcal{A}$(Adversary)和挑战者$\mathcal{C}$(Challenger)之间进行的游戏,游戏的过程描述如下.

Init:敌手$\mathcal{A}$向挑战者$\mathcal{C}$公开其要挑战的访问结构$\mathbb{A}^*$.

Setup:$\mathcal{C}$生成系统的公共参数,并向敌手$\mathcal{A}$公开.

Phase 1:$\mathcal{A}$可以查询关于任意流程集合 A 的私钥,但是需要满足以下限制:流程集合 A 不能满足$\mathcal{A}$在 Init 阶段所公布的挑战的关于流程的访问结构$\mathbb{A}^*$.

Challenge:敌手$\mathcal{A}$随机选取两个等长的消息 m_0和 m_1,并向挑战者公开. 随后,挑战者通过投掷一个随机硬币 $b\in\{0,1\}$,然后利用挑战的关于流程的访问结构$\mathbb{A}^*$ 生成对消息 m_b的挑战密文. 最后,挑战者将挑战密文发给敌手.

Phase 2:敌手可以继续询问关于任意流程集合 A'的私钥,但是,和 Phase 1 一样,流程集合 A'不能满足$\mathcal{A}$在 Init 阶段所公布的挑战的关于流程的访问结构$\mathbb{A}^*$.

Guess:敌手向挑战者公开其对 b 的猜测 b'. 则易知敌手赢得该游戏的优势为:$Pr[b'=b]-\frac{1}{2}$.

定义 3(CP-PBE 的选择流程安全性定义). 若对任意的 PPT 敌手,若其对于以上游戏的优势 ε 可忽略,则 CP-PBE 方案具有语义安全性(semantic security).

3.3 算法构造

Setup$(1^n,B,\mathfrak{R})$:Setup 算法的输入为安全参数 n,线性流程的起点个数 B 以及线性流程的关系集$\mathfrak{R}$. 算法随机选择素数 $p>2^n$,并选取 p 阶的两个群$\mathbb{G}$,$\mathbb{G}_T$. 令 $e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$为第 2.3 节所述的双线性映射,并设群$\mathbb{G}$上的一个生成元为 g. 算法选择 B 个群$\mathbb{G}$上的元素 $h_j\in\mathbb{G}(j\in\{1,2,\cdots,B\})$,并将这些元素作为线性流程的起点. 对于关系集合$\mathfrak{R}$中任意的关

系$(t\to k)\in\mathfrak{R}$，算法相应地选取$\mathbb{G}$上的元素$r_{t,k}\in\mathbb{G}$作为其公共参数. 最后，算法随机地选择$\alpha,b\in\mathbb{Z}_p$，并计算$e(g,g)^{\alpha},g^{b}$.

算法保存其主密钥$MSK=(\alpha,b)$，并公布其公共参数

$$e(g,g)^{\alpha},g^{b},g,h_j:(j\{1,2,\cdots,B\}),r_{t,k}:\exists(t\to k\in\mathfrak{R}).$$

Encrypt$(PP,\mathbb{A},m)$：Encrypt 算法的输入为公共参数 PP、访问结构$\mathbb{A}$和消息 m. 访问结构$\mathbb{A}$包括一个ℓ行n列的访问矩阵$\boldsymbol{M}$，线性流程的起点集$\mathfrak{B}$，终点集$\mathfrak{D}$，关系集$\mathfrak{R}$以及一个单射的映射函数ρ. 其中，映射ρ将$\boldsymbol{M}$中的每一行映射到流程的每一个终点下标上.

算法选择随机数$s\in Z_p$，然后创建以下的密文：

$$C_m=m\cdot e(g,g)^{\alpha s},$$
$$C_0=g^{s}.$$

选择一个秘密向量$\boldsymbol{y}=(s,y_2,\cdots,y_n)$，其中$(y_2,\cdots,y_n)\leftarrow\mathbb{Z}_p^{n-1}$. 计算对于秘密$s$的$\ell$个分割如下：

$$\ell=(\lambda_1,\lambda_2,\cdots,\lambda_\ell)=\boldsymbol{My}$$

即，子秘密$\lambda_i(i=1,2,\cdots,\ell)$为：

$$\lambda_i=\boldsymbol{M}_{i,1}s+\boldsymbol{M}_{i,2}y_2+\cdots+\boldsymbol{M}_{i,n}y_n.$$

算法为访问结构中的每一个节点(包括线性流程的起点，内部节点与终点)均隐秘地选择一个群元素$D_i\in\mathbb{G}$.

对于线性流程的每一个起点$i\in\mathfrak{B}$，算法为其分配密文如下. 算法选取$v_i\in\mathbb{Z}_p$并计算：

$$C_i=(C_{i,1},C_{i,2})=(D_i(h_i)^{v_i},g^{v_i}).$$

对于关系$(t\to k)\in\mathfrak{R}$，选择$c_{t,k}\in Z_p$，并创建以下密文：

$$C_{t,k}=(C_{t,k,1},C_{t,k,2})=((D_t^{-1}D_k)r_{t,k}^{c_{t,k}},g^{c_{t,k}}).$$

算法对于流程集合中的每个终点$j\in\mathfrak{D}$，均如下地为其分配对应的访问权限.

$$C_{\mathrm{end},j}=g^{-b\lambda_j}D_{\rho(j)}:j\in\mathfrak{D}.$$

最后，输出密文：

$$CT=((M,\rho),C_m,C_0,$$
$$C_j:(\forall j\in\mathfrak{B}),$$
$$C_{t,k}:(\forall(t\to k)\in\mathfrak{R},$$
$$C_{end,j}:(\forall j\in\mathfrak{D})).$$

KeyGen$(MSK,\mathfrak{B},\mathfrak{R})$：KeyGen 算法的输入为主密钥 MSK，该用户包含的线性流程的起点集$\mathfrak{B}$以及关系集$\mathfrak{R}$.

选取随机数$t\in Z_p$并计算

$$K=g^{\alpha}g^{bt},$$
$$K_0=g^{t}.$$

随后，对于线性流程的起点集$\mathfrak{B}$以及关系集$\mathfrak{R}$，计算

$$K_j=h_j^{t}:(\forall j\in\mathfrak{B}),$$
$$K_{\tau,k}=r_{\tau,k}^{t}:\forall(\tau\to k)\in\mathfrak{R}.$$

算法最终输出如下密钥：

$$SK=(K,K_0),$$
$$K_j:(\forall j\in\mathfrak{B}),$$
$$K_{\tau,k}:(\forall(\tau\to k)\in\mathfrak{R}).$$

Decrypt(SK,CT)：算法接受密文CT以及私钥SK的输入.

设L为密钥SK中满足密文CT中定义的访问结构的线性流程的集合，为进一步阐明满足访问结构的流程属性的特点，以下举例简要说明之. 如图 3 所示，设L中包括两个流程，即$L_0\to L_1\to L_2$和$L_3\to L_4$. 其中，在 KeyGen 算法中，根据第 1.3 节定义 3 的描述，将会给出起点L_0，L_3和关系$L_0\to L_1$，$L_1\to L_2$，$L_3\to L_4$的密钥；而在 Encrypt 算法中，也将会给出起点L_0，L_3和关系$L_0\to L_1$，$L_1\to L_2$，$L_3\to L_4$的密文，同时，还将给出终点L_2，L_4的密文. 如上对 KeyGen 和 Encrypt 算法的要求缺一不可：若 KeyGen 算法并未颁发如上描述的密钥，则表明该用户并未同时完成流程$L_0\to L_1\to L_2$和$L_3\to L_4$；若 Encrypt 算法并未公开如上所述的密文，则表明用户是否完成以上流程与其是否能解密密文毫无关系. 若 KeyGen 和 Encrypt 算法均如上述般颁发密钥与密文，且如图 3 所示，终点L_2，L_4中包含的子秘密构成了主秘密s的合法分割，则称集合L为密钥SK中满足访问结构的线性流程的集合.

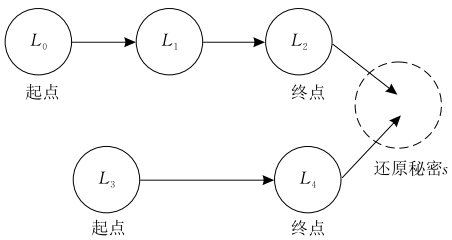

图 3　满足访问结构的流程集合L

不妨令L中的流程的起点组成的集合为$\mathfrak{B}$，终点集合为$\mathfrak{D}$.$\mathfrak{D}$中相对应的访问矩阵的行组成的集合为I，即$I\subset\{1,\cdots,\ell\}$并且$I=\{i:\rho(i)\in\mathfrak{D}\}$. 若密钥$SK$中包含的线性流程的集合满足密文$CT$中描述的访问结构$\mathbb{A}$的要求，则算法将成功解密. 以下描述解密过程.

根据 LSSS 的性质(第 2.3 节)，若集合$\{\lambda_i\}$是对秘密s的分享，则可有效地找到集合$\{\omega_i\}_{i\in I}$使式(1)

成立

$$\sum_{i\in I}\omega_i\lambda_i = s \tag{1}$$

不妨设 L 中任意的一个流程为:"$\mu_0\rightarrow\mu_1\rightarrow\cdots\rightarrow\mu_{l-1}\rightarrow\mu_l$".算法如下地进行解密操作.

算法通过以下计算推出该流程起点(即 μ_0)的秘密:

$$\begin{aligned}B_0 &= e(C_{\mu_0,1},K_0)\cdot e(C_{\mu_0,2},K_{\mu_0})^{-1}\\ &= e(D_{\mu_0}(h_{\mu_0})^{v_{\mu_0}},g^t)\cdot e(g^{v_{\mu_0}},(h_{\mu_0})^t)^{-1}\\ &= e(g,D_{\mu_0})^t:(\mu_0\in\mathfrak{B}).\end{aligned}$$

根据以上所得 μ_0 的秘密值,算法如下地进行递归计算.若假设算法已得到 $B_k=e(g,D_{\mu_k})^t(k\in\{0,\cdots,l-1\})$的秘密,则算法可如下地推导出 B_{k+1} 的值:

$$\begin{aligned}B_{k+1} &= B_k\cdot e(C_{\mu_k,\mu_{k+1},1},K_0)\cdot e(C_{\mu_k,\mu_{k+1},2},K_{\mu_k,\mu_{k+1}})^{-1}\\ &= e(g,D_{\mu_k})^t\cdot e((D_{\mu_k}^{-1}D_{\mu_{k+1}})^{r_{\mu_k,\mu_{k+1}}^t},g^t)\cdot\\ &\quad e(g^{c_{\mu_k,\mu_{k+1}}},r_{\mu_k,\mu_{k+1}}^t)^{-1}\\ &= e(g,D_{\mu_{k+1}})^t.\end{aligned}$$

上述的递归运算必然能在有限时间内推导出该流程的终点 μ_l,且该终点必与访问矩阵 $\boldsymbol{M}$ 中的一行相对应.设 $\rho(i)=\mu_l$,算法计算

$$B_l = e(g,D_{\mu_l})^t = e(g,D_{\rho(i)})^t,\ (\rho(i)\in\mathfrak{D})$$

最终,算法如下地推导出流程终点 μ_l 所对应的秘密分享值

$$\begin{aligned}&(e(C_{\mathrm{end},i},K_0)^{-1}(B_l))^{\omega_i})^{\omega_i}\\ &=(e(g^{-b\lambda_i}D_{\rho(i)},g^t)^{-1}\cdot e(g,D_{\rho(i)})^t\\ &=e(g,g)^{bt\omega_i\lambda_i}\cdot e(g,D_{\rho(i)})^{-\omega_i t}\cdot e(g,D_{\rho(i)})^{\omega_i t}\\ &=e(g,g)^{bt\omega_i\lambda_i}.\end{aligned}$$

算法可通过相似的计算步骤推导出 L 中其余流程终点所对应的秘密分享 $e(g,g)^{bt\omega_i\lambda_i}:(\forall i\in I)$.

随后,算法进行如下运算

$$\begin{aligned}e(K,C_0) &= e(g^a g^{bt},g^s)\\ &= e(g,g)^{as}\cdot e(g,g)^{bts}.\end{aligned}$$

由于 $\lambda_i(i\in I)$ 是对秘密 s 的分享,因此,根据式(1),算法可得到

$$\begin{aligned}\prod_{i\in I}e(g,g)^{bt\omega_i\lambda_i} &= e(g,g)^{bt\sum_{i\in I}\omega_i\lambda_i}\\ &= e(g,g)^{bts}.\end{aligned}$$

最终,算法通过以下的式(2)计算出明文:

$$C_m/(e(K,C_0)/\prod_{i\in I}e(g,g)^{bt\omega_i\lambda_i}) = m \tag{2}$$

讨论. 以下对 CP-PBE 方案的一些特性进行论述.

1)如第 1.2 节定义 3 所述,CP-PBE 在描述流程时,与经典的 CP-ABE 有较大相异:CP-ABE 在 Setup 阶段需要为每个流程分配一个公共参数;而 CP-PBE 在 Setup 阶段仅需为流程的起点以及流程节点间的关系分配公共参数.因此,根据定理 1,大大节省了公共参数的数量.

2)KeyGen 算法在颁发用户的密钥时(实际上是向用户完成的流程颁发密钥),与 Setup 算法类似,仅需颁发流程起点与关系的密钥;而 Encrypt 算法的作用为,指定拥有何种流程的用户方能访问本加密文件,其同样需要给定流程的起点以及关系的密文部分,所不同的是,Encrypt 算法还包括了流程终点的密文部分(即 $C_{\mathrm{end},j}$)——该部分主要用于为该流程分配访问权限之用.

3)CP-PBE 亦可"退化"成普通的 CP-ABE——当流程属性仅含一个节点时,该属性即为 CP-ABE 中的普通属性.在 Encrypt 算法中,若定义某个节点为起点,同时又指定其为终点时,该节点实际上即为仅包含一个节点的流程,其"退化"成了普通的属性.

3.4 安全性证明

CP-PBE 的安全性可通过以下的定理 2 进行说明.

定理 2. 设 CP-PBE 的挑战访问矩阵的列数为 n,且有 $n\leq q$.若 q-BDHE 假设为困难的,则不存在 PPT 的敌手 $\mathcal{A}$ 能以不可忽略的优势赢得本文第 3.2 节所定义的游戏.

定理 2 的详细证明过程请参见附录 1.

3.5 效率分析

本文将对 CP-PBE 与几种 CP-ABE 的时间和空间效率进行比较和分析,其结果在附录 2 中给出.

4 结论

本文对经典 CP-ABE 方案进行了扩展,将 CP-ABE 方案中的一般属性扩展成流程属性,首次提出了一种 CP-PBE 方案.CP-PBE 方案能让加密方精准控制其密文能被完成何种流程的用户解密.

本文对 CP-PBE 方案的应用场景进行了论述,定义了 CP-PBE 方案以及其选择流程的安全性模型,并借用双线性映射的理论提出了一种基于标准模型的 CP-PBE 方案,同时,基于数学假设证明了其安全性.

尽管本文证明了 CP-PBE 方案的安全性,但其安全性是基于选择安全的,在理论上存在一定的欠缺,因而,如何提出具有完全安全性的 CP-PBE 是一个较为有趣的问题.另外,本文方案的解密需要进行

多个双线性运算操作，效率存在一定问题，因而，如何尽量缩减解密的双线性操作，也是一个较有意义的研究方向.

参 考 文 献

[1] Sahai A, Waters B. Fuzzy identity-based encryption// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457-473

[2] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[3] Waters B. Ciphertext policy attribute based encryption: An expressive, efficient, and provably secure realization// Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 53-70

[4] Deng Hua, Wu Qian-Hong, Qin Bo, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences, 2014, 275: 370-384

[5] Wan Z, Liu J E, Deng R H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754

[6] Wang G, Liu Q, W U J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 2011, 30(5): 320-331

[7] Hohenberger S, Waters B. Attribute-based encryption with fast decryption//Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography. Nara, Japan, 2013: 162-179

[8] Attrapadung N, Libert B, de Panafieu E. Expressive key-policy attribute based encryption with constant-size ciphertexts// Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 90-108

[9] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures//Proceedings of the 2007 ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 195-203

[10] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption// Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. Berlin, Germany, 2013: 463-474

[11] Guan Z T, Yang T T, Xu R Z, et al. Multi-authority attribute-based encryption access control model for cloud storage. Journal of Communications, 2015, 36(6): 116-126(in Chinese)
(关志涛，杨亭亭，徐茹枝，王竹晓. 面向云存储的基于属性加密的多授权中心访问控制方案. 通信学报，2015，36(6)：116-126)

[12] Chen J H, Chen K F, Long Y, et al. Ciphertext policy attribute-based parallel key insulated encryption. Journal of Software, 2012, 23(10): 2795-2804(in Chinese)
(陈剑洪，陈克非，龙宇等. 密文策略的属性基并行密钥隔离加密. 软件学报，2012，23(10)：2795-2804)

[13] Wang P P, Feng D G, Zhang L W. CP-ABE scheme supporting fully fine-grained attribute revocation. Journal of Software, 2012, 23(10): 2805-2816(in Chinese)
(王鹏翩，冯登国，张立武. 一种支持完全细粒度属性撤销的CP-ABE方案. 软件学报，2012，23(10)：2805-2816)

[14] Zhang K, Gong J, Tang S, et al. Practical and efficient attribute-based encryption with constant-size ciphertexts in outsourced verifiable computation//Proceedings of the 11th ACM Asia Conference on Computer and Communications Security. Xi'an, China, 2016: 269-279

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 2012 IEEE Symposium on Security and Privacy (2007). Berkeley, USA, 2007: 321-334

[16] Benson K, Shacham H, Waters B. The k-bdh assumption family: Bilinear map cryptography from progressively weaker assumptions//Proceedings of the Cryptographers' Track at the RSA Conference 2013. San Francisco, USA, 2013: 310-325

[17] Deng Y Q, Song G. Scalable attribute-based encryption under the strictly weaker assumption family. Cryptology ePrint Archive: Report 2016/1029

[18] Deng Y Q, Tang C M, Song G, Wen Y M. New cryptography primitive research: Process based encryption. Journal of Software, 2017, 28(10): 2722-2736(in Chinese)
(邓宇乔，唐春明，宋歌，温雅敏. 一种新的密码学原语研究——流程加密. 软件学报，2017，28(10)：2722-2736)

[19] Odelu V, Das A K, Rao Y S, et al. Pairing-based cp-abe with constant-size ciphertexts and secret keys for cloud environment. Computer Standards & Interfaces, 2016, 54 (P1): 3-9

附录 1.

定理 2. 设 CP-PBE 的挑战访问矩阵的列数为 n，且有 $n \leq q$. 若 q-BDHE 假设为困难的，则不存在 PPT 的敌手 $\mathcal{A}$ 能以不可忽略的优势赢得本文第 3.2 节所定义的游戏.

证明. 假定存在 PPT 的敌手 $\mathcal{A}$ 在选择性安全模型下能以不可忽略的优势 $\varepsilon = Adv_{\mathcal{A}}$ 攻破 CP-PBE 系统，则必存在一个挑战者 $\mathcal{C}$，其可在多项式时间内求解判定性 q-BDHE 假设.

游戏开始前，$\mathcal{C}$ 将获取 q-BDHE 假设的参数 $\boldsymbol{X} = (\mathbb{G}, p, g, g^{\gamma}, g^{a}, \cdots, g^{a^{q}}, g^{a^{q+2}}, \cdots, g^{a^{2q}})$ 和 T，其中 $T = e(g,g)^{a^{q+1}\gamma}$，或为群 $\mathbb{G}_T$ 上的随机数.

Init：敌手 $\mathcal{A}$ 公布一个将要挑战的访问结构 $\mathbb{A}^*$，敌手 $\mathcal{A}$ 将于本模拟游戏的 Challenge 阶段询问关于挑战访问结构 $\mathbb{A}^*$ 的密文，其中，挑战访问结构 $\mathbb{A}^*$ 应包括：一个挑战的 ℓ 行 n 列的访问矩阵 $\boldsymbol{M}^*$，其中 $n \leq q$；挑战的流程起点集 $\mathfrak{B}^*$、终点集 $\mathfrak{D}^*$、关系集 $\mathfrak{R}^*$ 和一个单射的映射函数 ρ.

Setup：挑战者 $\mathcal{C}$ 如下设置公共参数 $e(g,g)^{a}$ 和 g^{b}：

$$e(g,g)^{a} = e(g^{a^{q}}, g^{a}), \quad g^{b} = g^{a}.$$

在以上设置中，挑战者秘密地令 $a=a^{q+1}$，$b=a$.

对于挑战终点集$\mathfrak{D}^*$中的每一个终点 d，必定唯一对应挑战矩阵 $\boldsymbol{M}^*$中的一行，不妨设该行为 $\rho^{-1}(d)$.

挑战者分如下情况设置起点参数 h_j：

(1) 若 $j\notin\mathfrak{D}^*$，即起点 j 不属于挑战终点集时，挑战者选择随机数 $z_j\in Z_p$，并设置 $h_j=g^{z_j}$.

(2) 若 $j\in\mathfrak{D}^*$，即起点 j 属于挑战终点集时(注意，如第 3.3 节所述，起点可同时设置为终点，此时的流程属性“退化”为普通属性)，挑战者选择随机数 $z_j\in Z_p$，并设置：

$$\begin{aligned}h_j&=g^{z_j}\cdot g^{\boldsymbol{M}^*_{\rho^{-1}(j),1}a+\boldsymbol{M}^*_{\rho^{-1}(j),2}a^2+\cdots+\boldsymbol{M}^*_{\rho^{-1}(j),n}a^n}\\&=g^{z_j}\cdot(g^a)^{\boldsymbol{M}^*_{\rho^{-1}(j),1}}(g^{a^2})^{\boldsymbol{M}^*_{\rho^{-1}(j),2}}\cdots(g^{a^n})^{\boldsymbol{M}^*_{\rho^{-1}(j),n}}\end{aligned}\tag{3}$$

注意到以下三点：(1) 在式(3)中，由于 $j\in\mathfrak{D}^*$，因此，j 为某个终点，且根据前文论述，其唯一对应挑战访问矩阵的一行，即为 $\rho^{-1}(j)$；(2) h_j 的构造中，其指数部分实际为挑战访问矩阵的第 $\rho^{-1}(j)$ 行的元素与向量 $(a,a^2,\cdots,a^n)$ 的内积值；(3) 由于有 $n\leq q$，因此，挑战者知道所有的 $(g^a,g^{a^2},\cdots,g^{a^n})$ 值，因此，挑战者能成功构造式(3).

随后，挑战者选择随机数 $v_{\tau,k}\in Z_p$，并进行以式(4)的设置：

$$r_{\tau,k}=g^{v_{\tau,k}}\cdot(h_k/h_\tau)\tag{4}$$

由于 $v_{t,k}$ 为挑战者自己选取的值，且挑战者已成功构造出所有的 h_j 值(即挑战者可知 (h_k/h_τ) 部分的值)，因此，挑战者能成功构造出式(4)的参数.

Phase 1,2：在这一步中，敌手 $\mathcal{A}$ 可以向挑战者 $\mathcal{C}$ 询问关于任意线性流程集合 A 的私钥：敌手需给出该线性流程集合 A 中的起点集合$\mathfrak{B}$以及关系集合$\mathfrak{R}$，但需符合以下设定——流程集合 A 不满足挑战的访问结构$\mathbb{A}^*$.

不妨设流程集合 A 中所有节点的集合为 ζ. 定义集合：

$$\xi=\zeta\cap\mathfrak{D}^*,$$

其中$\mathfrak{D}^*$为敌手在 Init 阶段公布的挑战访问结构$\mathbb{A}^*$ 中的流程终点的集合. 即集合 ξ 中的节点同时在集合 ζ 中和集合$\mathfrak{D}^*$中出现. 集合 ξ 中的节点实际上有两种含义：(1) 集合 ξ 中的节点必为挑战访问结构中的流程终点；(2) 集合 ξ 中的节点同时又在目前的询问阶段，作为流程中的一个节点出现. 因此，集合 ξ 中的节点在挑战访问结构$\mathbb{A}^*$中，其所对应的访问矩阵中的行必定不能满足挑战访问结构的要求(否则，敌手询问的该流程集合 A 的密钥将满足挑战访问结构$\mathbb{A}^*$，与本安全模型的假设矛盾).

令集合 I'为

$$I'=\{i\mid\forall\rho(i)\in\xi\},$$

以上的集合 I'表示集合 ξ 中节点相对应的挑战访问矩阵中行组成的集合.

根据上文论述，由于集合 I'中的行不满足挑战访问矩阵的访问结构(即集合 I'中的行不构成对访问矩阵中共享秘密的合法分割)，因此，根据文献[3]结论，对于所有的 $i\in I'$，必然存在向量 $\boldsymbol{w}=(w_1,\cdots,w_n)^\perp$，其中 $w_1=-1$，使得式(*)成立：

$$\boldsymbol{M}^*_i\cdot\boldsymbol{w}=0\tag{*}$$

利用向量 $\boldsymbol{w}$，挑战者隐蔽地设置秘密参数 t 如下：

$$\begin{aligned}t&=w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n}\\&=-a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n}.\end{aligned}$$

随后，挑战者将可如下地设置密钥参数. 首先，挑战者设置：

$$\begin{aligned}K&=g^ag^bt\\&=g^{a^{q+1}}g^{a\cdot(w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n})}\\&=g^{a^{q+1}}g^{a\cdot(-a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n})}\\&=(g^{a^q})^{w_2}\cdot(g^{a^{q-1}})^{w_3}\cdots(g^{a^{q+2-n}})^{w_n}.\end{aligned}$$

在以上的设置中，尽管存在挑战者未知的参数 $g^a=g^{a^{q+1}}$，但由于 g^{bt} 中正好存在 $g^{-a^{q+1}}$ 的项，因而，能将挑战者未知的项抵消.

随后，挑战者设置：

$$\begin{aligned}K_0&=g^t\\&=g^{w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n}}\\&=g^{-a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n}}\\&=(g^{-a^q})\cdot(g^{a^{q-1}})^{w_2}\cdots(g^{a^{q+1-n}})^{w_n}\end{aligned}$$

挑战者将分以下两种情况设置起点参数 $K_j=h_j^t$：$(\forall j\in\mathfrak{B})$：

(1) 若 $j\notin\xi$，此种情况表明起点 j 不是挑战访问矩阵中的终点，即有 $j\notin\mathfrak{D}^*$，因此，根据以上的设置，有 $h_j=g^{z_j}$，可知 h_j 中不存在挑战者未知的指数. 挑战者可简单地设置如下：

$$\begin{aligned}K_j&=h_j^t\\&=g^{z_j(w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n})}\\&=((g^{a^q})^{w_1}\cdot(g^{a^{q-1}}{}^{w_2}\cdots(g^{a^{q+1-n}})^{w_n})^{z_j}.\end{aligned}$$

(2) 若 $j\in\xi$，此种情况表明节点 j 是挑战访问矩阵中的终点，即有 $j\in\mathfrak{D}^*$，此时有：

$$\begin{aligned}K_j&=h_j^t\\&=g^{(z_j+\boldsymbol{M}^*_{\rho^{-1}(j),1}a+\boldsymbol{M}^*_{\rho^{-1}(j),2}a^2+\cdots+\boldsymbol{M}^*_{\rho^{-1}(j),n}a^n)(w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n})}\\&=g^{z_j(w_1a^q+w_2a^{q-1}+\cdots+w_na^{q+1-n})}\cdot\prod_{\substack{1\leq u\leq n,\\1\leq v\leq n,\\u\neq v}}\boldsymbol{M}^*_{\rho^{-1}(j),u}w_va^{q+1+u-v}.\end{aligned}$$

注意到，在上式中，可能会出现挑战者未知的项 $g^{a^{q+1}}$，且通过观察易知，$g^{a^{q+1}}$ 项的系数为：

$$\boldsymbol{M}^*_{\rho^{-1}(j),1}w_1+\boldsymbol{M}^*_{\rho^{-1}(j),2}w_2+\cdots+\boldsymbol{M}^*_{\rho^{-1}(j),n}w_n=\boldsymbol{M}^*_{\rho^{-1}(j)}\boldsymbol{w}.$$

但因 $j\in\xi$，因此，$\rho^{-1}(j)\in I'$(集合 I'的含义)，所以，根据式(*)，有

$$\boldsymbol{M}^*_{\rho^{-1}(j)}\cdot\boldsymbol{w}=0.$$

因此，所有的 $g^{a^{q+1}}$ 项均被抵消. 挑战者能成功构造出该 K_j 项.

最后，挑战者还将设置项 $K_{\tau,k}=r_{\tau,k}^t$：$\forall(\tau\to k)\in\mathfrak{R}$. 根据以上的论述可知，挑战者设置 $r_{\tau,k}=g^{v_{\tau,k}}\cdot(h_k/h_\tau)$. 因此，易知：

$$\begin{aligned}K_{\tau,k}&=r_{\tau,k}{}^t\\&=(g^{v_{\tau,k}}\cdot(h_k/h_\tau))^t\\&=g^{t\cdot v_{\tau,k}}\cdot(h_k^t/h_\tau^t)\\&=((g^{a^q})^{w_1}\cdot(g^{a^{q-1}})^{w_2}\cdots(g^{a^{q+1-n}})^{w_n})^{v_{\tau,k}}\cdot(h_k^t/h_\tau^t)\end{aligned}$$

在上式中，$v_{\tau,k}$ 为挑战者自选的已知数，而项 h_k^t，h_t^t 即为挑战者已成功在以上构造出的密钥参数 $K_k=h_k^t$，$K_\tau=h_\tau^t$.

Challenge：挑战者抛掷硬币 $\beta\in\{0,1\}$，并生成密文如下：

$$C_m=m_\beta\cdot T,\quad C_0=g^\gamma\tag{5}$$

以下，挑战者将构造关于挑战访问结构$\mathbb{A}^*$的密文参数. 挑战者首先设置挑战的访问结构中每个节点的秘密 D_i，该设置又可分为以下两种情况：

(1) 若 $i\notin\mathfrak{D}^*$，即节点 i 不为挑战流程终点时，挑战者选

择整数 $d_i \in Z_p$，并设置 $D_i = g^{d_i}$.

(2) 若 $i \in \mathfrak{D}^*$，即节点 i 为挑战流程终点时，挑战者选择整数 $d_i \in Z_p$，并隐秘地设置：

$$D_i = g^{d_i} \cdot g^{\boldsymbol{M}^*_{\rho^{-1}(i),1} a + \boldsymbol{M}^*_{\rho^{-1}(i),2} a^2 + \cdots + \boldsymbol{M}^*_{\rho^{-1}(i),n} a^n) \gamma}.$$

根据以上设置，挑战者分如下两种情况构造关于起点集合 $\mathfrak{B}$ 的密文参数 $C_i = (C_{i,1}, C_{i,2}) : (i \in \mathfrak{B})$.

(1) 若 $i \notin \mathfrak{D}^*$，即起点 i 不是挑战流程的终点时，挑战者随机选择 $v'_i \in Z_p$，并设置 $v_i = v'_i$. 挑战者生成：

$$C_{i,1} = g^{d_i} \cdot g^{z_i v'_i}, \quad C_{i,2} = g^{v'_i}$$

(2) 若 $i \in \mathfrak{D}^*$，即起点 i 同时也是挑战流程的终点时，挑战者随机选择 $v'_i \in Z_p$，并隐蔽地设置 $v_i = -\gamma + v'_i$. 挑战者生成：

$$\begin{aligned} C_{i,1} &= D_i (h_i)^{v_i} \\ &= (g^{d_i} \cdot g^{(\boldsymbol{M}^*_{\rho^{-1}(i),1} a + \boldsymbol{M}^*_{\rho^{-1}(i),2} a^2 + \cdots + \boldsymbol{M}^*_{\rho^{-1}(i),n} a^n) \gamma}) \cdot \\ &\quad g^{(z_j + \boldsymbol{M}^*_{\rho^{-1}(i),1} a + \boldsymbol{M}^*_{\rho^{-1}(i),2} a^2 + \cdots + \boldsymbol{M}^*_{\rho^{-1}(i),n} a^n)(-\gamma + v'_i)} \\ &= g^{d_i} \cdot ((g^a)^{\boldsymbol{M}^*_{\rho^{-1}(i),1}} (g^{a^2})^{\boldsymbol{M}^*_{\rho^{-1}(i),2}} \cdots (g^{a^n})^{\boldsymbol{M}^*_{\rho^{-1}(i),n}})^{v'_i} \cdot \\ &\quad (g^{\gamma})^{-z_j} \cdot g^{z_j v'_i} \\ C_{i,2} &= g^{v_i} \\ &= g^{-\gamma + v'_i} = g^{-\gamma} \cdot g^{v'_i}. \end{aligned}$$

在以上设置中，当 $i \in \mathfrak{D}^*$ 时，尽管挑战者无法“显式”构造出秘密 D_i 的值(只能隐秘地设置)：因为 D_i 中含有 $g^{a^p \gamma}$：($p \in \{1, 2, \cdots, n\}$) 这样挑战者未知的量，但挑战者可通过巧妙地设置 v_i 的值将 D_i 中未知的量抵消，如上所述.

与以上构造方法类似，挑战者按以下两种情况构造密文参数 $C_{t,k}$.

(1) 若 $t \notin \mathfrak{D}^* \wedge k \notin \mathfrak{D}^*$，此时由于 $D_t = g^{d_t}$，$D_k = g^{d_k}$，可见，D_t，D_k 中不含有挑战者未知的值，因此，挑战者可随机挑选 $c'_{t,k} \in Z_p$，令 $c_{t,k} = c'_{t,k}$，并设置：

$$C_{t,k} = (C_{t,k,1}, C_{t,k,2}) = ((g^{d_k} / g^{d_t}) r^{c'_{t,k}}_{t,k}, g^{c'_{t,k}}).$$

注意，在以上的设置中，$r_{t,k}$ 的值在 Setup 阶段挑战者已成功构造.

(2) 若 $t \in \mathfrak{D}^* \vee k \in \mathfrak{D}^*$，此种情况又可分成 3 种情况：$t \in \mathfrak{D}^* \wedge k \notin \mathfrak{D}^*$、$t \notin \mathfrak{D}^* \wedge k \in \mathfrak{D}^*$ 和 $t \in \mathfrak{D}^* \wedge k \in \mathfrak{D}^*$. 3 种情况的构造原理均类似，现以最具代表性的第 3 种情况，即 $t \in \mathfrak{D}^* \wedge k \in \mathfrak{D}^*$ 情况予以说明. 若 $t \in \mathfrak{D}^* \wedge k \in \mathfrak{D}^*$，则根据前文的设置，终点 D_t，D_k 中将含有挑战者未知的项 $g^{a^p \gamma}$：($p \in \{1, 2, \cdots, n\}$)，特别地，有：

$$D_i = g^{d_i} \cdot g^{(\boldsymbol{M}^*_{\rho^{-1}(i),1} a + \boldsymbol{M}^*_{\rho^{-1}(i),2} a^2 + \cdots + \boldsymbol{M}^*_{\rho^{-1}(i),n} a^n) \gamma} : (i \in \{t, k\}).$$

然而，与上述密文参数 C_i 的构造类似，挑战者可随机选择 $c'_{t,k} \in Z_p$，隐蔽地设置 $c_{t,k} = -\gamma + c'_{t,k}$，并生成：

$$\begin{aligned} C_{t,k,1} &= (D_t^{-1} D_k) r^{c'_{t,k}}_{t,k} \\ &= g^{(d_k - d_t) + ((\boldsymbol{M}^*_{\rho^{-1}(k),1} - \boldsymbol{M}^*_{\rho^{-1}(t),1}) a + \cdots + (\boldsymbol{M}^*_{\rho^{-1}(k),n} - \boldsymbol{M}^*_{\rho^{-1}(t),n}) a^n) \gamma} \cdot \\ &\quad g^{(v_{t,k} + (\boldsymbol{M}^*_{\rho^{-1}(k),1} - \boldsymbol{M}^*_{\rho^{-1}(t),1}) a + \cdots + (\boldsymbol{M}^*_{\rho^{-1}(k),n} - \boldsymbol{M}^*_{\rho^{-1}(t),n}) a^n) \cdot (-\gamma + c'_{t,k})} \\ &= g^{(d_k - d_t) + v_{t,k}) \cdot c'_{t,k}} \cdot (g^{\gamma})^{-v_{t,k}} \cdot \\ &\quad ((g^a)^{(\boldsymbol{M}^*_{\rho^{-1}(k),1} - \boldsymbol{M}^*_{\rho^{-1}(t),1})} \cdots (g^{a^n})^{(\boldsymbol{M}^*_{\rho^{-1}(k),n} - \boldsymbol{M}^*_{\rho^{-1}(t),n})})^{c'_{t,k}} \\ C_{t,k,2} &= g^{c_{t,k}} \\ &= g^{-\gamma} \cdot g^{c'_{t,k}}. \end{aligned}$$

从上式易知，D_t，D_k 中未知的项被 $r^{c_{t,k}}_{t,k}$ 抵消. 其中，根据上文的设置，当 $t \in \mathfrak{D}^* \wedge k \in \mathfrak{D}^*$ 时，有：

$$\begin{aligned} r_{t,k} &= g^{v_{t,k}} \cdot (h_k / h_t) \\ &= g^{v_{t,k}} \cdot ((g^a)^{\boldsymbol{M}^*_{\rho^{-1}(k),1}} \cdots (g^{a^n})^{\boldsymbol{M}^*_{\rho^{-1}(k),n}} / \\ &\quad (g^a)^{\boldsymbol{M}^*_{\rho^{-1}(t),1}} \cdots (g^{a^n})^{\boldsymbol{M}^*_{\rho^{-1}(t),n}}) \\ &= g^{v_{t,k}} \cdot ((g^a)^{(\boldsymbol{M}^*_{\rho^{-1}(k),1} - \boldsymbol{M}^*_{\rho^{-1}(t),1})} \cdots \\ &\quad (g^{a^n})^{(\boldsymbol{M}^*_{\rho^{-1}(k),n} - \boldsymbol{M}^*_{\rho^{-1}(t),n})}) \end{aligned}$$

最后，挑战者将设置密文参数 $C_{\mathrm{end},j} = g^{-b\lambda_j} D_{\rho(j)} : j \in \mathfrak{D}^*$. 挑战者随机选择 $n-1$ 个整数 $(y'_2, y'_3, \cdots, y'_n) \in Z_p^{n-1}$，并隐秘地设置秘密共享向量为：

$$\boldsymbol{y} = (s, y_2, \cdots, y_n) = (\gamma, a\gamma + y'_2, a^2\gamma + y'_3, \cdots, a^{n-1}\gamma + y'_n)$$

根据 LSSS 的性质，以上的共享向量所生成的子秘密 λ_i ($i = 1, 2, \cdots, \ell$) 为：

$$\begin{aligned} \lambda_i &= \boldsymbol{M}^*_{i,1} s + \boldsymbol{M}^*_{i,2} y_2 + \cdots + \boldsymbol{M}^*_{i,n} y_n \\ &= \boldsymbol{M}^*_{i,1} \gamma + \boldsymbol{M}^*_{i,2} (a\gamma + y'_2) + \cdots + \boldsymbol{M}^*_{i,n} (a^{n-1}\gamma + y'_n) \\ &= (\boldsymbol{M}^*_{i,1} \cdot \gamma + \boldsymbol{M}^*_{i,2} \cdot a\gamma + \cdots + \boldsymbol{M}^*_{i,n} \cdot a^{n-1}\gamma) + \\ &\quad (\boldsymbol{M}^*_{i,2} \cdot y'_2 + \cdots + \boldsymbol{M}^*_{i,n} \cdot y'_n). \end{aligned}$$

注意，在上式中，挑战者实际上隐秘地设置了 $s = \gamma$. 挑战者将如下地设置 $C_{\mathrm{end},j}$：

$$\begin{aligned} C_{\mathrm{end},j} &= g^{-b\lambda_j} D_{\rho(j)} \\ &= g^{-a((\boldsymbol{M}^*_{i,1} \cdot \gamma + \boldsymbol{M}^*_{i,2} \cdot a\gamma + \cdots + \boldsymbol{M}^*_{i,n} \cdot a^{n-1}\gamma) + (\boldsymbol{M}^*_{i,2} \cdot y'_2 + \cdots + \boldsymbol{M}^*_{i,n} \cdot y'_n))} \cdot \\ &\quad g^{d_{\rho(j)}} \cdot g^{(\boldsymbol{M}^*_{i,1} a + \boldsymbol{M}^*_{i,2} a^2 + \cdots + \boldsymbol{M}^*_{i,n} a^n) \gamma} \\ &= g^{(\boldsymbol{M}^*_{i,2} \cdot y'_2 + \cdots + \boldsymbol{M}^*_{i,n} \cdot y'_n)} \cdot g^{d_{\rho(j)}}. \end{aligned}$$

在上式中，如前文所述，尽管 $D_{\rho(j)}$ 中存在挑战者未知的项 $g^{a^p \gamma}$：($p \in \{1, 2, \cdots, n\}$)，但挑战者可通过巧妙地设置秘密共享向量的方式将未知项全部抵消.

Guess：$\mathcal{A}$ 向挑战者公开其猜测的比特 β'. 若 $\beta = \beta'$，挑战者输出 0(代表其猜测 $T = e(g, g)^{a^{q+1} \gamma}$)，否则，挑战者输出 1(代表其猜测 T 为群上的随机数).

注意，在 Challenge 阶段的设置中，除式(5)外，其余的设置均为合法的. 以下分析式(5)中对于参数 C_m 设置的合法性. 在式(5)中，挑战者实际上隐秘地设置了 $s = \gamma$. 由于在 Setup 阶段设置了 $\alpha = a^{q+1}$，因此，若 $T = e(g, g)^{a^{q+1} \gamma} = e(g, g)^{\alpha s}$，此时，挑战者对参数 C_m 的设置是合法的；若 $T = e(g, g)^{a^{q+1} \gamma} \cdot R$，其中 $R \in \mathbb{G}_T$ 为某随机数(表示 T 亦为群 $\mathbb{G}_T$ 上的随机数)，则显然挑战者并未合法地设置参数 C_m.

因此，若敌手 $\mathcal{A}$ 返回的比特 β' 与挑战者选定的比特 β 相同，挑战者可认为 $T = e(g, g)^{a^{q+1} \gamma}$(表示其对 C_m 进行了合法的设置)；若 $\mathcal{A}$ 返回的比特 β' 与挑战者选定的比特 β 相异，挑战者可认为 T 为随机数(表示其对 C_m 进行了非法的设置，导致敌手猜错).

以下分析挑战者 $\mathcal{C}$ 攻破 qq-BDHE 假设的优势. 令事件 $\eta = 0$ 表示 $\mathcal{C}$ 接收到的 $T = e(g, g)^{a^{q+1} \gamma}$，令事件 $\eta = 1$ 表示 $\mathcal{C}$ 接收到的 $T = R$. 令事件 *success* 表示 $\mathcal{C}$ 成功攻破 qq-BDHE 假设. 则有：

$$\begin{aligned} Pr[success] &= Pr[success \mid \eta = 0] Pr[\eta = 0] + \\ &\quad Pr[success \mid \eta = 1] Pr[\eta = 1] \\ &= \left(\frac{1}{2} + \varepsilon\right) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \end{aligned}$$

$$=\frac{1}{2}+\frac{\varepsilon}{2}$$

故，$\mathcal{C}$成功解决qq-BDHE 假设的优势为 $Adv_{q\text{-DBDH}}=Pr[success]-\frac{1}{2}=\frac{\varepsilon}{2}$. 综上，若敌手能以不可忽略的优势 ε 赢得本游戏，则挑战者将能以不可忽略的优势 $\varepsilon/2$ 解决判定性 q-BDHE.

附录 2.

本节比较几种相似方案的效率，参与比较的方案包括本文的 CP-PBE、Waters 提出的 CP-ABE[3]、Deng 等人[4]提出的密文策略的基于层次的属性加密(CP-HABE)以及 Odelu 等人[19]提出的密钥和密文均为恒量的 CP-ABE 方案. 本节用 n 表示系统中的总节点数；用 n_h 表示密文中包含的节点数；用 n_s 表示密钥中包含的节点数；用 n_ε 表示密钥中符合访问结构的最少流程集合中包含的节点数；用 T 表示密钥中符合访问结构的最少属性数；用 L 表示 CP-HABE 中属性能被划分的最大层次数. 比较结果如附表 1 和 2 所示.

附表 1 CP-PBE 与运行在第 1.1 节方法 1 中的 CP-ABE 的效率比较

方案	公共参数长	最大密文长	最大密钥长	解密时间	安全模型	分布式验证
CP-PBE(本文方案)	$\mathcal{O}(n^2)$	$\mathcal{O}(n_h^2)$	$\mathcal{O}(n_s^2)$	$\mathcal{O}(n_\varepsilon)$	标准模型	支持
文献[3]方案 1	$\mathcal{O}(2^n)$	$\mathcal{O}(2^{n_h})$	$\mathcal{O}(2^{n_s})$	$\mathcal{O}(T)$	标准模型	不支持
文献[4]方案	$\mathcal{O}(L)$	$\mathcal{O}(2^{n_h})$	$\mathcal{O}(2^{n_s})$	$\mathcal{O}(T)$	标准模型	不支持
文献[19]方案	$\mathcal{O}(2^n)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(T)$	RO 模型	不支持

附表 2 CP-PBE 与运行在第 1.1 节方法 2 中的 CP-ABE 的效率比较

方案	公共参数长	最大密文长	最大密钥长	访问结构长度	解密时间	逻辑电路	分布式验证
CP-PBE(本文方案)	$\mathcal{O}(n^2)$	$\mathcal{O}(n_h^2)$	$\mathcal{O}(n_s^2)$	$\mathcal{O}(T)$	$\mathcal{O}(n_\varepsilon)$	“与或”门	支持
文献[3]方案 1	$\mathcal{O}(n^2)$	$\mathcal{O}(n_h^2)$	$\mathcal{O}(n_s^2)$	$\mathcal{O}(n_\varepsilon)$	$\mathcal{O}(n_\varepsilon)$	“与或”门	支持
文献[4]方案	$\mathcal{O}(L)$	$\mathcal{O}(n_h^2)$	$\mathcal{O}(n_s^2)$	$\mathcal{O}(n_\varepsilon)$	$\mathcal{O}(n_\varepsilon)$	“与或”门	支持
文献[19]方案	$\mathcal{O}(n^2)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	—	$\mathcal{O}(n_\varepsilon)$	“与”门	支持

附表 1 为 CP-PBE 方案与文献[3-4,19]所提方案的效率对比，且假定文献[3-4,19]方案均通过第 1.1 节所述的方法一描述流程. 首先，必须指出，本文方案在解密的时间复杂度上较此方法下的 CP-ABE 方案要高：这是由于此方法下的 CP-ABE 方案用一个属性表示一个流程，因而解密的时间与流程个数相关；而 CP-PBE 的解密时间与流程的节点个数相关. 然而，由表可知，尽管存在特殊的某类参数为定长(如公共参数定长[4]、密钥定长和密文定长[19])的 CP-ABE 方案，但目前尚不存在这 3 种参数均为定长的 CP-ABE，因此，本文提出的 CP-PBE 方案必在某类参数上存在存储空间上的优势. 另外，如第 1.1 节所述，本文方案支持多授权方验证流程的机制，而运用此方法的 CP-PBE 并不支持多授权方验证的设定，因而会增加单授权服务器的负载.

附表 2 为 CP-PBE 方案与文献[3-4,19]所提方案的效率对比，且假定文[3-4,19]方案均通过第 1.1 节所述的方法 2 描述流程. 在附表 2 中可见，由于此时采取了和 CP-PBE 相似的策略，因此，CP-ABE 与本文的 CP-PBE 方案具有近似的参数长度. 但如第 1.1 节所分析，由于每个节点(对应一个属性)均需携带一个访问权限，因此，一般 CP-ABE 的访问结构复杂度(或访问矩阵的行数)是与流程中所有的节点数相关的，因而，访问结构相当复杂；而 CP-PBE 的访问结构仅与流程数相关(因为每个流程对应一个访问权限). 所以，CP-PBE 比运行在第 1.1 节方案 2 下的一般的 CP-ABE 的加解密效率明显更高. 需要注意的是，文献[19]方案的 CP-PBE 具有密钥和密文定长的特性，似乎比本文的 CP-PBE 性能更优. 但注意到以下几点：(1)该方案在存储上比 CP-PBE 有优势，但由于其同样需要为每个属性分配一个访问权限，因而，在加解密效率上比本文的 CP-PBE 更差；(2)该方案仅支持“与”门的逻辑电路，因而，在描述关于“或”门的访问策略时需要用非常复杂的逻辑方能实现；(3)该方案的安全性是基于随机预言机(Random Oracle，RO)模型的，RO 模型尽管在理论上具有较为重要的价值，但在实用性方面尚存疑.

DENG Yu-Qiao, Ph. D., associate professor. His research interests include cryptography and cloud computing.

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

TANG Chun-Ming, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and cloud computing.

SONG Ge, Ph. D., lecturer. Her research interests include data mining and cryptography.

WEN Ya-Min, Ph. D., associate professor. Her research interests include cryptography and cloud computing.

Background

Privacy preserving theories and technologies in cloud environment attract great interests in recent era. The requirements for secure storing, accessing and deleting data in cloud server become natural and necessary. Classical cryptographic theory becomes inadequacy in some sense. For example, classical public key encryption (PKE) is not applicable for cloud sharing, because every public key/secret key pair is issued by the certificate authority (CA); the key management becomes difficult and inefficient.

Identity-based encryption (IBE) is proposed to convenient the key management process. The public key is described by the identity of the user in IBE, and thus this novel scheme sharply decreases the complexity of the key generation. As a variant of IBE, attribute-based encryption (ABE) is proposed to obtain fine-grained access control. The identity of decryptor is described as a set of attributes or some access policies. ABE makes the identity authentication much scalable than IBE.

A new application scenario related to process authentication is studied in this paper. In this scenario, the data owner needs to ensure whether a user satisfies several processes, before the user accesses the encrypted contents. The classical ABE cannot be used because they cannot describe processes efficiently. A new cryptography primitive called Process-Based Encryption (PBE) is presented to address the aforementioned problem. PBE is classified into two types, i.e., Key-Policy PBE (KP-PBE) and Ciphertext Policy PBE. A CP-PBE is presented. The encryptor can specify the recipient of the ciphertext by encrypting message along with the access policies in the CP-PBE. The decryptor can recover the message if it holds the secret key associated with the desired process set. The CP-PBE has advantage in efficiently and effectively describing all kinds of processes. A CP-PBE scheme is constructed in the standard model, using the tools of bilinear maps and Linear Secret Sharing Scheme (LSSS). The selective security model of CP-PBE is defined. The security proof is provided using the partitioning strategy. The security of the CP-PBE is reduced to the q-Bilinear Diffie-Hellman Exponent Assumption (q-BDHE). The efficiency analysis of CP-PBE and general CP-ABE is presented.

This work is supported by National Key R&D Program of China (No. 2017YFB0802000), National Natural Science Foundation of China (Nos. 61772147 and 61300204); Humanities and Social Science Research Project of Ministry of Education (No. 15YJCZH029); Project of "the 13th Five-year Plan" for the Development of Philosophy and Social Sciences in Guangzhou (Nos. 2016GZYB25 and 2017GZQN05); Guangdong Province Natural Science Foundation of Major Basic Research and Cultivation Project (No. 2015A030308016); Natural Science Foundation of Guangdong Province (No. 2015A030313630); Basic Research Project of Guangdong Provincial Department of Education (No. 2014KZDXM044); Colleges and Universities Innovation Team Construction Project Guangdong province (No. 2015KCXTD014); National Cryptography Development Fund (No. MMJJ20170117); Guangzhou City Bureau of Cooperative Innovation Project (No. 1201610005); Information Security Comprehensive Management Technology Research Key Laboratory Open Topic Fund of Shanghai (No. AGK2015007) and Project of Guangdong Science and Technology Plan (Nos. 2016A020210103 and 2017A020208054).