软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(10):2722−2736 [doi: 10.13328/j.cnki.jos.005138]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种新的密码学原语研究——流程加密*

邓宇乔[1], 唐春明[2], 宋 歌[3], 温雅敏[1]

[1](广东财经大学 数学与统计学院,广东 广州 510320)

[2](广州大学 数学与信息科学学院,广东 广州 510006)

[3](华南农业大学 数学与信息学院,广东 广州 510120)

通讯作者: 唐春明, E-mail: ctang@gzhu.edu.cn

摘 要: 在许多实际的应用场景中,当用户需要获取敏感数据时,需要判断该用户是否满足某些“流程”的要求.现存的加密方案不能有效应用到以上场景中.为了解决这一新问题,提出了一种新的加密原语:基于流程的加密(process based encryption,简称 PBE),并把 PBE 分成两种类型:密钥策略的 PBE(KP-PBE)与密文策略的 PBE(CP-PBE).运用双线性映射与线性秘密共享协议的工具,给出了一种 KP-PBE 的构造方法.随后,把 KP-PBE 方案与传统属性加密进行对比,指出在描述流程数量方面,KP-PBE 与传统属性加密方案存在数量级的差异,从而体现了 KP-PBE 方案在描述流程方面的优越性.最后,在选择性安全的模型下,证明了该方案的安全性.

关键词: 流程加密;密钥策略;密文策略;属性加密;选择性安全模型

中图法分类号: TP309

中文引用格式: 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. http://www.jos.org.cn/1000-9825/5138.htm

英文引用格式: Deng YQ, Tang CM, Song G, Wen YM. New cryptography primitive research: Process based encryption. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2722−2736 (in Chinese). http://www.jos.org.cn/1000-9825/5138.htm

New Cryptography Primitive Research: Process Based Encryption

DENG Yu-Qiao[1], TANG Chun-Ming[2], SONG Ge[3], WEN Ya-Min[1]

[1](School of Mathematics and Statistics, Guangdong University of Finance and Economics, Guangzhou 510320, China)

[2](School of Mathematics and Computer Science, Guangzhou University, Guangzhou 510006, China)

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

* 基金项目: 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); 国家自然科学基金(61772147, 61300204); 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(2016A020210103, 2017A020208054)

Foundation item: Humanities and Social Science Research Project of Ministry of Education (15YJCZH029); The Project of “the 13th Five-Year Plan” for the Development of Philosophy and Social Sciences in Guangzhou (2016GZYB25, 2017GZQN05); National Natural Science Foundation of China (61772147, 61300204); Guangdong Province Natural Science Foundation of Major Basic Research and Cultivation Project (2015A030308016); Natural Science Foundation of Guangdong Province of China (2015A030313630); Basic Research Project of Guangdong Provincial Department of Education (2014KZDXM044); Colleges and Universities Innovation Team Construction Project Guangdong Province (2015KCXTD014); National Cryptography Development Fund (MMJJ20170117); Guangzhou City Bureau of Cooperative Innovation Project (1201610005); Information Security Comprehensive Management Technology Research Key Laboratory Open Topic Fund of Shanghai (AGK2015007); Guangdong Science and Technology Plan (2016A020210103, 2017A020208054)

收稿时间: 2016-05-22; 修改时间: 2016-07-19, 2016-08-18; 采用时间: 2016-09-23

Abstract: In many applications, when a user needs to access sensitive information, it is a usual requirement to authenticate whether or not the user satisfies certain processes. Existing encryption schemes are not applicable for this scenario. To adderess this problem, a new cryptography primitive called process pased encryption (PBE) is presented. The application scenario of PBE is demonstrated. PBE is classified into two categories: Key policy process based encryption (KP-PBE) and ciphertext policy process based encryption (CP-PBE). A KP-PBE scheme is constructed utilizing the tools of bilinear map and linear secret sharing scheme (LSSS). Compared to conventional attribute based Eecryption (ABE), the performance of KP-PBE is much better on describing processes. Finally, the security of KP-PBE is proven under the selective security model.

Key words: process based encryption; key policy; ciphertext policy; attribute-based encryption; selective security model

1 引 言

尽管经典的公钥加密算法能够满足一般的加密需求,然而,在密钥管理操作中存在以下问题:由于需要给每个用户设置相应的公钥、私钥对,因此,在密钥管理服务器端需要进行大量的运算,且需要在服务器端公布大量用户的公钥,导致沉重的系统开销问题.为了解决这个问题,Shamir 于 1984 年首次提出了基于身份的密码学概念[1].利用基于身份的加密(identity based encryption,简称 IBE),服务器端无需针对每个用户公布其对应的公钥,而仅需公布若干个公共参数(公共参数的数量大大少于用户的数量).加密者可以利用公共参数以及具体用户的身份,生成仅供该用户访问的密文.IBE 与传统公钥加密相比,能使得服务器端所需时间与空间花销更少,大大提高了效率.

然而,IBE 使用单一的“身份串”对用户的身份进行描述,在对身份表达的灵活性以及用户隐私性方面存在缺陷.为了使 IBE 能够更方便地表达用户的身份,Sahai 和 Waters 在 2005 年首次提出了基于模糊身份的加密(fuzzy identity based encryption,简称 FIBE),随后,该概念被重命名为基于属性的加密(attribute-based encryption,简称 ABE)[2].作为一种密码学中强大而灵活的加密方案,属性加密引起了许多学者的研究兴趣[3−6].属性加密的原理可以简单叙述如下:给定一个秘密文档,规定一组属性 A,规定一组访问规则 B;如果属性 A 能够满足访问规则 B 的要求,则允许对秘密文档进行解密.把以上的原理应用到公钥加密机制中,必须把属性组 A、访问策略组 B 与传统的公钥加密中的两个重要的组件——密钥与密文——进行绑定.根据绑定的组件的不同,可以把 ABE 划分为以下两类[2]:密钥策略的属性加密(key-policy attribute based encryption,简称 KP-ABE)与密文策略的属性加密(ciphertext-policy attribute based encryption,简称 CP-ABE).在 KP-ABE 中,密文与属性组 A 相对应,而用户的私钥则与具体的访问策略 B 相对应;在 CP-ABE 中,密文与访问策略 B 相对应,而用户的私钥则与具体的属性组 A 相对应.ABE 具有高效、安全等优点,特别是在云计算环境下,对用户的隐私保护起到了至关重要的作用.ABE 可以在不泄露用户隐私的情况下完成秘密共享:以 CP-ABE 为例,假设内容提供者(content provider,简称 CP)使用如下访问策略加密文件:“总经理 OR(经理 AND 男性)OR(副经理 AND 男性 AND 工程师)”,而某用户又成功解密了该文件,CP 仍无法确定该人员的真实身份,因为该人员既可能是总经理,也可能是男性经理,或者是具有工程师职称的男性副经理.这样,ABE 就可以在分享秘密的同时做到保护用户的隐私.因此,近年来 ABE 一直是国内外密码学界的研究热点.

虽然 ABE 方案可以描述现实生活中绝大部分的属性,但是,对特殊属性的描述却效率不高.这种特殊的属性是一种类似于“流程”“步骤”等现实生活中经常出现的属性.虽然使用传统的 ABE 方案也能表达流程,但将使得流程的表达缺乏灵活性,同时造成非常大的冗余.基于以上分析,本文首次进行了基于流程的加密(process based encryption,简称 PBE)的研究,基于流程的加密可便利地表达流程、步骤等特殊属性,为了说明 PBE 的实用性,本文首先介绍研究的动机.

1.1 本文的动机

在现实应用中,经常需要使用到一种重要的控制手段——流程.特别是在政府部门、学校、大型企业等组织里,某个任务通常由多个部门协同合作,而与该任务相关的一些机密文档需要由指定的与任务相关的人员方可查看.为了严格地对文档进行保密,对于能够查看机密文档的人员必须进行层层验证:只有依次通过验证的人

员才具有查看文档的资格.

例如:假设国家某安全机关需要设计一个专门为专案组服务的文件加密系统,该系统中保存了绝密的与各个具体案件相关的案件资料.而能够查看某案件资料的人员必须是负责该案件的专案组成员.由于专案组的成立通常由某个部门牵头,由多个部门协同派出人手组成,因此,专案组成员的准入审核通常由各部门按照该部门与案件相关的程度从低到高的顺序审核通过.如,假设某个案件 Z 涉及到 5 个部门:A,B,C,D,E,且由部门 C,E 联合牵头组办专案组.专案组成员的加入需要满足以下的审核流程:"$A \to B \to C$"OR"$D \to E$".

首先,应该注意到,如果用属性加密中的一个属性表示一个部门,是无法表达以上语义的.因为属性加密无法表达该应用中的"顺序"关系.例如,在表达流程"$D \to E$"时,如果"D"与"E"均为属性,并且在加密时用"D"与"E"对公文进行加密,而在颁发密钥时给某用户颁发"D"AND"E"的访问策略,则此加密方法仅能保证该用户通过了 D 与 E 的审查,而无法表达其通过审查的先后次序关系.此时就会造成一个潜在的重大安全漏洞:如果另外一个案件 Z'由部门 D 牵头,部门 E 作为参与部门,则该案件侦办人员通过部门 D,E 审核的顺序为"$E \to D$",此时,在属性加密方案下,无法分清流程"$D \to E$"与"$E \to D$",因此,导致侦办案件 Z'的人员也能查看案件 Z 的资料,造成严重的后果.

此外,另一种可行的途径是,把流程直接定义为一个属性.如,把流程"$D \to E$"直接定义为一个属性.但这种方法也会导致以下较为严重的问题:首先,一个属性代表一个流程,这会加大属性审核人员的负担(因为一个属性中包含过多的逻辑).另外,更为严重的是,如果在建立加密系统之初需要考虑到所有可能的流程,且为每个流程分配相应的公共参数,将会导致公共参数过多,系统效率非常低下.关于这一点的论述,将在第 3.6 节进行详细论证.

因此,本文的研究动机是:如何提出一种新的安全的加密方案,能便捷地对流程进行描述,使得加密时能对用户的准入流程进行灵活的(flexible)控制.并且,定义该方案的安全性模型,并对其进行严格的证明.

1.2 本文的创新

- 本文提出了一种新的密码学原语:PBE,并把这个模型划分为两类,即:密钥策略的基于流程的加密(key-policy process-based encryption,简称 KP-PBE)和密文策略的基于流程的加密(ciphertext-policy process-based encryption,简称 CP-PBE).
- 在 KP-PBE 方案中,密文与流程的集合相关联,而密钥与基于流程的访问结构相关联.当且仅当密文中包含的流程信息满足密钥中所描述的基于流程的访问结构时,解密方可成功.而相对应地,在 CP-PBE 方案中,密钥与流程的集合相关联,而密文与基于流程的访问结构相关联.当且仅当密钥中包含的流程信息满足密文中所描述的基于流程的访问结构时,解密方可成功.
- 运用双线性映射技术与线性秘密共享协议首次构造出一个 KP-PBE 方案,并比较了该方案在描述流程时与传统 ABE 方案的差异,分析了该方案在流程表达上的优势.最后,本文对 KP-PBE 方案进行了严格的安全性模型定义,并在该定义下证明了 KP-PBE 方案的安全性.

1.3 本文的技术

本文所借鉴的技术主要包括两大部分:线性秘密共享协议(linear secret sharing scheme,简称 LSSS)[7]和 Waters 的功能加密(functional encryption,简称 FE)[8].

首先,本文需要考虑的是如何描述流程的问题.在解决该问题的过程中,本文受到文献[7]的启发:在文献[7]中,Waters 设计了一个利用有限自动状态机来描述访问策略的功能加密方案:该方案能使有限自动状态机的读写头在接受了符号集Σ上的一个符号 w_i 后,从一个状态 D_i 跳到另一个状态 D_j,并得到一个 $e(g,D_j)^{w_i}$ 的秘密.Waters 的方案在状态转换时的机制非常类似于沿着某个流程进行"行走"的过程.因此,本文借鉴该机制的原理,对流程进行了描述.本文为每个流程都设定唯一的起点与终点.如果解密算法能从某个流程的起点依据算法设定的方案依次得到流程中各个点的值,并最终推算出该流程的终点的值,则本文认为该解密者满足流程要求.

另外,由于考虑到实际应用的复杂性,在检验流程是否满足的过程中,可能需要用逻辑运算符(如"AND""OR"等)对多个流程进行连接检验(如第 1.1 节所述的情况),因此,本文还引入了 LSSS 方案,以便对复杂流程集

合进行检验.

1.4 相关工作

文献[1]首先提出了基于身份的加密方案IBE,在IBE中,用户的身份信息(例如他的姓名和电话号码)可以嵌入到公钥里.此后,国内外的学者们在对身份加密的算法改进上做了许多有意义的工作:熊金波等人结合多级安全与IBE提出了一种面向网络内容隐私的基于身份加密的安全自毁方案[9];光焱等人利用容错学习问题构造了基于身份的全同态加密体制[10];王少辉等人结合IBE和可搜索加密的技术,提出了一种指定测试者的基于身份可搜索加密方案[11];明洋和王育民则提出了一种标准模型下可证安全的通配符基于身份加密方案[12].Cocks提出了一种基于二次剩余问题的IBE[13];Boneh和Franklin基于双线性对的工具提出了一种IBE方案[14];Waters提出了一种不基于随机预言机(random oracle,简称RO)的IBE方案[15];Shao与Cao利用层次IBE的思想提出了可重用的、单向的、基于身份的代理重加密方案[16].

Sahai和Waters改进了IBE中身份表示不灵活的特性,首次在文献[2]中提出了一种模糊身份加密方案.该方案的思想是,加密者可以设定一个谓词$f(\cdot)$,规定解密者的身份信息x必须满足该谓词的条件:即$f(x)=1$时方可解密文档.模糊身份加密的提出使公钥密码学得到了重大的改进:一方面,加密者可以非常灵活地指定解密者所应满足的特性;另一方面,解密者的身份信息相对于传统的公钥加密方案而言也更加模糊,从而可以保护用户的隐私.在文献[1]中,Sahai和Waters还提出了一个全新的密码学原语:基于属性的加密ABE.基于属性的加密方案在文献[2]中被定义为以下一种机制:用户的证书将用用户的属性集合进行描述,而谓词$f(\cdot)$则用来描述作用在这些属性上的一组规则.文献[2]中提出的模糊身份加密方案事实上就是一种原始的属性加密方案,但该方案中的规则只能用门限的方法进行描述,导致规则的灵活性较差.

随后,由Goyal等人在文献[17]中把属性加密进一步细分成密钥策略的属性加密KP-ABE与密文策略的属性加密CP-ABE.KP-ABE在密钥中包含访问结构,用以指定解密者有权限访问何种文档;而CP-ABE的访问策略则与密文相关,用以指定加密内容可被何种人群解密.在文献[17]中,提出了一种支持属性的“与”和“或”操作的KP-ABE机制,从而大大丰富了访问结构的形式.在此基础上,Bethencourt等人首次提出了一种支持“与”和“或”操作的CP-ABE方案[3],而Ostrovsky、Sahai和Waters在文献[4]中首次提出了一种支持“否”操作的ABE方案.至此,ABE方案已可支持非常灵活的访问策略定义操作.另外,Hohenberger和Waters[5]提出了一种密钥策略的、支持快速解密的属性加密方案.Chase则从另一个方面对属性加密进行研究:他提出了一种具有多认证方的属性加密方案(multi-authority attribute based encryption,简称MA-ABE)[18].MA-ABE与一般的ABE方案的不同点在于,MA-ABE方案中具有多个属性授权方,很显然,这在分布式的环境下可以使得属性授权的工作量大大地分散,从而降低单个属性授权方授权的工作量.Goyal等人[17]和Lewko等人[19]提出了具有代理功能的属性加密方案.Wan等人提出了一种具有层次特性的属性加密方案,该方案能对属性加密中的属性进行分层[20];Wang等人则提出了具有撤销功能的层次属性加密方案,该方案能使系统具有撤销用户属性的能力[21];Deng等人则提出了一种具有短密文特性的层次属性加密方案,且证明了该方案的完全安全性[22].此外,熊金波等人提出了一种基于属性加密的组合文档安全自毁方案[23],关志涛等人提出了面向云存储的基于属性加密的多授权中心访问控制方案[24],陈剑洪等人提出了密文策略的属性基并行密钥隔离加密方案[25],王鹏翩等人[26]提出了一种支持完全细粒度属性撤销的CP-ABE方案.

功能加密[27]作为一种新的加密形式,可以使得加密者在加密过程中定义任意复杂的访问逻辑.最近,功能加密研究的热点是利用不可区分的混淆(indistinguishability obfuscation,简称IO)来构造加密方案,并取得了一些有趣的结果[28].

2 背景知识

本节首先给出单调访问结构的定义,再介绍线性秘密共享协议与双线性映射的技术,最后给出本文将使用的困难性假设.

2.1 单调访问结构

定义 1(访问结构[29]). 设$\{P_1,P_2,\ldots,P_n\}$是一个参与方的集合.称集合$A\subseteq 2^{\{P_1,P_2,\ldots,P_n\}}$为单调的,当且仅当对于$\forall B,C$,如果$B\in A$并且$B\subseteq C$,则有:$C\in A$成立.一个访问结构为集合$\{P_1,P_2,\ldots,P_n\}$中的非空子集$A$.包含于$A$内的集合称为授权集,不包含于$A$内的集合称为非授权集.

在本文的 KP-PBE 方案中,参与方集合所对应的是流程集合.

2.2 线性秘密共享协议

定义 2(线性秘密共享协议[29]). 假设存在一个参与方的集合P,称 II 为一个在Z_p上的线性秘密共享协议,如果满足以下条件:

(1) 协议里的所有参与方拥有一个在Z_p上的秘密分享向量.

(2) 称一个l行n列的矩阵M为一个在 II 上的秘密产生矩阵.令ρ为一个把矩阵M里的每一行的行标i通过映射$(\rho(i),i=1,\ldots,l)$映射到参与方的下标.假设参与方需要分享一个秘密$s\in Z_p$,它选定一个列向量$v=(s,r_2,\ldots,r_n)$,其中,$r_2,\ldots,r_n\in Z_p^{n-1}$是随机选定的,参与方可以通过计算得到$l$个秘密分享值:$(M_v)_i,i=1,\ldots,l$.其中,参与方$\rho(i)$拥有秘密的分割:$(M_v)_i$.

根据文献[29]中的结论,以上论述的 LSSS 方案 II 拥有一个秘密的线性重构机制,具体描述如下:令S是一个定义在A上的授权集,定义集合$I\subset(1,2,\ldots,l)$为$I\subset(i:\rho(i)\in S)$.那么,必然存在某个常数集合$w_i\in Z_p$满足以下式子:

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

另外,对于任意的关于集合I的非授权集,必然存在一个向量w满足:$w_1=1$并且$w\cdot M_i=0(i\in I)$.

2.3 双线性映射技术

设G,G_T是阶为素数q的循环乘群.令g是一个G上的群生成元,$c:G\times G\to G_T$是一个双线性映射.那么,c具有以下的性质.

(1) 双线性特性:对于任意的$u,v\in G$和$a,b\in Z_p$,有$c(u^a,v^b)=c(u,v)^{ab}$.

(2) 非退化性:$c(g,g)\neq 1$.

(3) 可计算性:$c:G\times G\to G_T$可以有效计算.同时,映射c具有对称的特性,因为$c(g^a,g^b)=c(g,g)^{ab}=c(g^b,g^a)$.

2.4 困难性假设

本文的方案是基于以下的确定性q-BDHE(q-bilinear diffie-Hellman exponent assumption).

定义 3(确定性 q-BDHE[29]). 令G是一个素数阶群,设其阶为p,g为G上的生成元,令$a,s\leftarrow Z_p$,R是群G上的一个随机元素.确定性q-BDHE 定义如下.

如果给定向量:

$$\vec{X}=G,p,g,g^s,g^a,\ldots,g^{a^q},g^{a^{q+2}},\ldots,g^{a^{2q}},$$

定义任何的概率多项式时间(probabilistic polynomial-time algorithm,简称 PPT)算法A能成功解决q-BDHE 的优势为

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

确定性q-BDHE 成立的条件是:如果对于任意的 PPT 算法A,它解决该假设的优势$Adv_{q\text{-BDHE}}$都是可忽略的.

3 KP-PBE 加密模型

3.1 流程的相关定义

在描述 KP-PBE 算法的加密模型之前,首先给出流程与线性流程的定义.

定义 4(流程(process)的定义). 设$G=\langle V,E\rangle$为有向图,其中,V表示G的顶点集合,而E表示G的有向边的集合.称P为G中的一个流程,如果满足:$P=p_1\to p_2\to\ldots\to p_n$,其中,$p_1,\ldots,p_n\in V$且$p_1\to p_2,p_2\to p_3,\ldots,p_{n-1}\to p_n\in E$.称集合

$\{p_1,\ldots,p_n\}$为流程 P 的节点集,称集合 $R=\{p_1\rightarrow p_2,p_2\rightarrow p_3,\ldots,p_{n-1}\rightarrow p_n\}$为流程 P 的关系集,称有向图中的边 $(p_i\rightarrow p_j)\in R$ 为流程 P 的关系.

注意,首先,在以上的流程定义中,流程是有向的,具体体现为流程关系集中的每个关系均为有向图中的一条有向边;其次,流程 P 中的顶点 $p_1,\ldots,p_n$ 可重复,如流程 $P'=a\rightarrow b\rightarrow c\rightarrow d\rightarrow b\rightarrow f$ 中,顶点 b 出现了两次.此时,称流程 P'中存在环.而 KP-PBE 算法处理的流程不允许出现环,因此,给出以下定义.

定义 5(线性流程(linear process)). 设 $LP=lp_1\rightarrow lp_2\rightarrow\ldots\rightarrow lp_n$ 为有向图 $G=\langle V,E\rangle$的一个流程,其中,$lp_1,\ldots,lp_n\in V$ 且 $lp_1\rightarrow lp_2,lp_2\rightarrow lp_3,\ldots,\rightarrow lp_{n-1}\rightarrow lp_n\in E$.如果对所有的 $i\neq j(i,j\in[1,\ldots,n])$,都有 $lp_i\neq lp_j$,则称 LP 为线性流程.

由定义 5 可知,线性流程不允许流程中出现环,如上文提到的流程 $P'=a\rightarrow b\rightarrow c\rightarrow d\rightarrow b\rightarrow f$ 不是线性流程(设 $lp_1=a,lp_2=b,lp_3=c,lp_4=d,lp_5=b,lp_6=f$,则有 $lp_2=lp_5=b$,可知 $b\rightarrow c\rightarrow d\rightarrow b$ 为一个环).

在 KP-PBE 中,为了判定用户是否满足一个或多个线性流程,需要由可信授权中心(trusted authorization center,简称 TAC)为用户颁发与流程相关的密钥.本文用定义 6 给出用户满足流程的条件.

定义 6(用户满足线性流程的条件(condition for the satisfaction of linear process)). 设 $LP=lp_1\rightarrow lp_2\rightarrow\ldots\rightarrow lp_n$ 为有向图 $G=\langle V,E\rangle$的一个线性流程,其中,$lp_1,\ldots,lp_n\in V$ 且 $lp_1\rightarrow lp_2,lp_2\rightarrow lp_3,\ldots,\rightarrow lp_{n-1}\rightarrow lp_n\in E$.如果用户持有流程的起点 p_1 的密钥及流程的关系集$\{lp_1\rightarrow lp_2,lp_2\rightarrow lp_3,\ldots,\rightarrow lp_{n-1}\rightarrow lp_n\}$中所有关系的密钥,则该用户满足线性流程 LP.

3.2 符号定义

本文涉及的符号定义如下所述.$x\leftarrow Z_p$ 表示从 Z_p 中随机选取一个元素,符号 $x\leftarrow Z_p^n$ 表示从 Z_p 中随机选取 n 个元素,$A\rightarrow B$ 表示点 A,B 之间存在一条有向边直接通连;$A\rightarrow\rightarrow B$ 表示点 A,B 是连通的(可能由多条有向边连通).用映射函数$\rho(\cdot)$把任意的矩阵 M 中的一行映射为一个线性流程的终点,用映射函数$\rho^{-1}(\cdot)$把一个线性流程的终点映射成矩阵 M 中的一行.

3.3 KP-PBE 加密模型

KP-PBE 总共包括 4 个子算法,分别为 Setup,Encrypt,KeyGen 和 Decrypt.需要注意的是,KP-PBE 算法在加密文件时允许对文件嵌入多个线性流程的信息,而在颁发密钥时允许密钥持有者灵活地表述其复杂的多个线性流程的持有信息.因此,在 Setup,Encrypt 和 KeyGen 算法中,可能涉及到多个线性流程的处理.下面给出算法的严格定义.

定义 7(KP-PBE 的加密定义). KP-PBE 的加密主要包括以下 4 个算法.

Setup(1^n,B,R):在 Setup 算法中,算法接受安全参数 n、线性流程的起点个数 B 以及线性流程的关系集 R 的输入.算法输出公共参数 PP 和主密钥 MSK.以上提到,Setup 算法颁发的公共参数可能需要支持多个线性流程的表达,因此,线性流程的起点个数 $B\geqslant 1$.

Encrypt(PP,B,R,m):在 Encrypt 算法中,算法接受公共参数 PP、本次加密所需要用到的线性流程的起点集 B、线性流程的关系集 R 和消息 m 的输入.算法输出密文 CT.

KeyGen(MSK,A):在 KeyGen 算法中,算法接受主密钥 MSK 以及与线性流程相关的访问结构 A 的输入.算法输出私钥 SK.

Decrypt(SK,CT):在 Decrypt 算法中,算法接受密文 CT 以及私钥 SK 的输入,如果私钥的集合满足访问结构 A,算法输出明文 m,否则,算法输出$\perp$.

3.4 KP-PBE 的安全性模型定义

本小节详细讨论 KP-PBE 方案的安全性模型.KP-PBE 的安全模型主要建立在两个角色之间,这两个角色分别为:

(1) 方案的攻击者,即敌手 A(attacker).敌手 A 的任务是对 KP-PBE 方案进行攻击.

(2) 难题挑战者 C(challenger).难题挑战者的任务是在与敌手 A 进行交互的过程中,利用敌手 A 来攻破一个

困难的问题.

本文所提出的 KP-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.选择性安全模型虽然比现今的另一种安全性模型:完全安全性模型[30]的安全归约要弱,但相对完全安全性模型,建立在选择性安全模型下的系统的效率更高.因此,本文将在选择性安全模型下设计 KP-PBE 方案.

定义 8(KP-PBE 的安全模型定义). KP-PBE 的安全模型是方案攻击者 A 和难题挑战者 C 之间的游戏,游戏主要包括下面的步骤.

Init:方案攻击者 A 公布他要挑战的线性流程集 A^*,并把 A^*发给挑战者 C.

Setup:挑战者 C 调用 Setup 算法生成公共参数,并把公共参数 PP 发给攻击者.

Phase 1:攻击者 A 可以查询任意的访问结构 $A_1,\ldots,A_{q1}$ 的私钥集合:$SK_1,\ldots,SK_{q1}$,但需要满足以下限制:A 在 Init 阶段所公布的属性集合 A^*不能满足访问结构集 $A_1,\ldots,A_{q1}$ 中任一访问结构.

Challenge:攻击者生成两个等长的消息 m_0 和 m_1 并提交给挑战者,挑战者通过投掷一个随机硬币 $b\in\{0,1\}$,然后利用挑战属性集 A^*生成对消息 m_b 的挑战密文并将其发给攻击者.

Phase 2:攻击者可以重复 Phase 1 多次,但是,和 Phase 1 一样,攻击者在 Init 时公布的属性集 A^*都不能满足这些访问结构: $A_{q_1+1},\ldots,A_q$.

Guess:最终,敌手会输出一个对 b 的猜测,记为 b'.敌手赢得这个游戏的优势记为 $\Pr[b'=b]-\frac{1}{2}$.

定义 9(方案安全的定义). 如果对于任意的概率多项式时间(probability polynomial time,简称 PPT)的敌手能赢得以上游戏的优势 ε均为可忽略的,则称 KP-PBE 方案为语义安全(semantic security)的.

3.5 方案构造

下面首先给出方案的构造过程,随后在选择性安全模型下证明方案的安全性.

3.5.1 算法构造

Setup(1^n,B,R):在 Setup 算法中,算法接受安全参数 n、线性流程的起点个数 B 以及线性流程的关系集 R 的输入.算法选择素数 $p>2^n$,创建阶为 p 的群 G,G_T.令 $c:G\times G\to G_T$ 是一个双线性映射.$g\in G$ 为群 G 上的生成元.算法选择 B 个群 G 中的元素 $h_j\in G(j\in\{1,2,\ldots,B\})$作为线性流程起点的公共参数.如果在关系集合 R 中存在关系 $(t\to k)\in R$,算法选择 G 中的元素 $r_{t,k}\in G$ 作为流程节点间关系的公共参数.最后,算法选取随机数 $\alpha\in Z_p$,计算 $c(g,g)^a$.

本算法的主密钥为 $MSK=g^a$,公共参数为对群 G 的描述以及:

$$PP=(e(g,g)^{\alpha},g,$$
$$h_j:(j\in\{1,2,\ldots,B\}),$$
$$r_{t,k}:\exists(t\to k)\in\Re).$$

Encrypt(PP,B,R,m):在 Encrypt 算法中,算法接受公共参数 PP、本次加密所需线性流程的起点集 B、线性流程的关系集 R 和消息 m 的输入.

算法选择随机数 $s\in Z_p$,然后创建以下密文.

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

随后,算法创建与线性流程相关的密文部分,这包括线性流程的起点集 $\mathfrak{B}$ 的密文以及线性流程的关系集 $\Re$ 的密文.

$$C_j=h_j^s:(\forall j\in B),$$
$$C_{t,k}=r_{t,k}^s:\forall(t\to k)\in R.$$

最后,算法输出密文.

$$C_T=(C_m, C_0,$$
$$C_j:(\forall j\in B),$$
$$C_{t,k}:(\forall(t\to k)\in R).$$

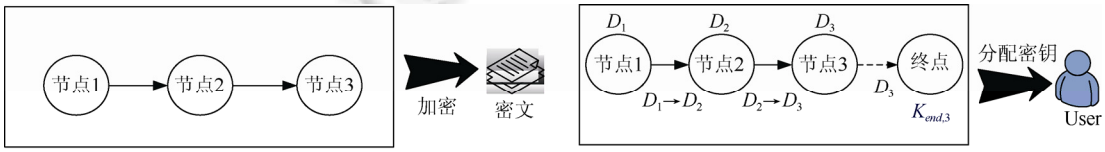
KeyGen(*MSK*,*A*):算法接受主密钥 *MSK* 以及访问结构 *A* 的输入.其中,*A* 中应该包括:一个 *l* 行 *n* 列的访问矩阵 *M*、线性流程的起点集 *B*、线性流程的终点集 *D*、线性流程的关系集合 *R* 以及一个映射函数ρ,映射函数ρ的作用为把 *M* 中的每一行映射到线性流程的每一个终点,且该映射函数为单射(injective).

注意到,在 KeyGen 算法中,存在着线性流程的终点集 *D*,而该集合在 Setup 与 Encrypt 算法中并未出现.终点集出现的目的是为了对用户满足流程与否进行验证.如图 1 所示,在 Setup 与 Encrypt 算法中,需要给出的参数为起点 Node 1 以及关系 1→2,2→3 对应的项;而在 KeyGen 算法中,除了需要给出 Node 1 以及关系 1→2,2→3 对应的项外,还需要构造一个终点项:$K_{end,3}$.且在 KeyGen 算法中,每个流程节点将被分配一个独立的秘密(即图 1(b)所示中的 D_1,D_2,D_3).事实上,KeyGen 算法使用了以下的机制把流程的秘密嵌入到密钥中:起点 Node 1 的密钥中嵌入秘密 D_1,关系 1→2 的密钥中嵌入能从 D_1 推出 D_2 的秘密,关系 2→3 的密钥中嵌入能从 D_2 推出 D_3 的秘密,最后,终点 $K_{end,3}$ 中嵌入 D_3 与访问矩阵的权限秘密.如果用户能推出 D_3,则表示该用户经历了从起点 Node 1 到 Node 3 的过程,则该用户能获得相关的权限秘密.因此,终点 $K_{end,3}$ 是基于节点 Node 3 而存在的.

算法选择一个秘密向量 $\vec{y}=(\alpha, y_2,..., y_n)$, 其中, $(y_2,..., y_n)\leftarrow Z_p^{n-1}$. 算法计算对于秘密$\alpha$的 *l* 个分割如下:

$$\vec{\lambda}=(\lambda_1,\lambda_2,...,\lambda_l)=M\vec{y}.$$

令 $M_{i,j}$ 表示矩阵 *M* 中的第 *i* 行第 *j* 列的元素.注意,这里,算法不能直接得到$\lambda_i=M_{i,1}\alpha+M_{i,2}y_2+\ldots+M_{i,n}y_n$ 的值,因为算法只知道私钥 $MSK=g^{\alpha}$ 的值而不知道α的值.但是算法可以计算出 $g^{\lambda_i}=(g^{\alpha})^{M_{i,1}}+...+g^{M_{i,n}y_n}$ 的值.



(a) Setup和Encrypt 算法流程　　(b) KeyGen算法流程

Fig.1　The model of KP-PBE

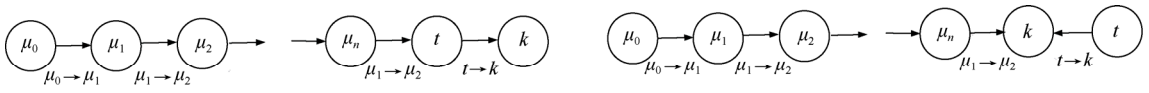
图 1　KP-PBE 模型

对于用户所具有的线性流程的每一个节点(包括起点,普通节点与终点),算法秘密地选取一个群元素 $D_i\in G$. 算法首先给线性流程的每一个起点 $i\in B$ 分配密钥如下:算法选取 $v_i\in Z_p$ 并计算:

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

随后,算法用以下方式递归地为用户颁发密钥:对于线性流程的关系集合 *R* 中的任意一个关系:$(t\to k)\in R$,如果用户申请该关系的密钥,需要满足以下条件:该用户已存在起点 μ_0,且存在关系 $\mu_0\to\mu_1,\mu_1\to\mu_2,\ldots,\mu_n\to t$ 的密钥,即必须满足 $\mu_0\to\to t$,算法方可为该用户颁发关系 $t\to k$ 的密钥.

图 2 所示为一个例子,图 2 中,公式或箭头表示用户已拥有的密钥部分(拥有起点 μ_0 及关系 $\mu_0\to\mu_1,\mu_1\to\mu_2,\ldots,\mu_n\to t$),箭头 $t\to k$ 表示需要颁发的关系密钥.图 2(a)为可颁发的情况(表示用户已完成流程 $\mu_0\to\mu_1\to\mu_2,\ldots,\to\mu_n\to t$,如果用户通过关系 $t\to k$ 的验证,则表示该用户完成流程 $\mu_0\to\mu_1\to\mu_2,\ldots,\to\mu_n\to t\to k$).而图 2(b)为不可颁发的情况(因为不存在某个起点 *O* 满足 $O\to\to t$).这种颁发策略是符合实际情况的:因为图 2(b)中的情形相当于该用户尚未完成节点 *t* 之前的流程(否则,必然持有从某个起点到 *t* 的路径的所有密钥),因此,自然无法颁发 *t* 之后的流程密钥.



(a) 可颁发的流程密钥 (b) 不可颁发的流程密钥

Fig.2 The rule for assigning paivate keys of KP-PBE

图 2 KP-PBE 颁发密钥的规则

算法选择 $c_{t,k}\in Z_p$,并创建以下私钥:

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

最后,算法为线性流程集合中的每个终点 $j\in D$ 分配其对应的访问权限.对于访问矩阵 M 中的一行 $j\in\{1,\ldots,l\}$,用映射函数ρ能把该行映射到一个线性流程的终点$\rho(j)$上,此时,算法选取 $r_j\in Z_p$,并计算:

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

算法公布私钥如下:

$$\begin{aligned}SK=((M,\rho),&\\ &K_i,i\in B,\\ &K_{t,k}:(t\to k\in R),\\ &K_{end,j}:j\in D).\end{aligned}$$

Decrypt(*SK*,*CT*):算法接受密文 *CT* 以及私钥 *SK* 的输入.设 *L* 为满足访问结构的线性流程的集合,设 *B* 表示由 *L* 中的线性流程的起点组成的集合,设 *D* 表示 *L* 所对应的线性流程的终点集合.设集合 *I* 表示 *D* 所对应的访问矩阵的行所组成的集合,即 $I\subset\{1,\ldots,l\}$且 $I=\{i:\rho(i)\in D\}$.如果密文 *CT* 中包含的线性流程的集合满足密钥 *SK* 中描述的访问结构 *A* 的要求,则算法将成功解密.

根据第 2.3 节中的描述,对于访问矩阵 *M* 而言,如果集合$\{\lambda_i\}$是对该矩阵秘密α的合法分割,则必然存在常数集合$\{\omega_i\}_{i\in I}$,使得式(1)成立.

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

对于 *L* 中任意一个线性流程,不妨设该流程为 $\mu_0\to\mu_1\ldots\to\mu_{l-1}\to\mu_l$.算法将如下地恢复该流程所对应的秘密.

算法首先计算该流程起点的秘密.

$$B_0=e(K_{\mu_0,1},C_0)e(K_{\mu_0,2},C_{\mu_0})^{-1}=e(g,D_{\mu_0})^s,(\mu_0\in B).$$

然后,从起点 μ_0 开始,算法递归地进行如下计算:如果算法已经得到了 $B_k=e(g,D_{\mu_k})^s(k\in\{0,\ldots,l-1\})$ 的值,则算法将采用如下方式计算 B_{k+1} 的值.

$$B_{k+1}=B_k\cdot e(C_0,K_{\mu_k,\mu_{k+1},1})e(C_{\mu_k,\mu_{k+1}},K_{\mu_k,\mu_{k+1},2})^{-1}=e(g,D_{\mu_{k+1}})^s.$$

根据上面的描述,*L* 中流程的终点必然对应于访问矩阵 *M* 中的一行,因此,不妨设$\rho(i)=\mu_l$,即,访问矩阵中的第 *i* 行对应本线性流程的终点,此时,根据以上的递归计算,算法最终能得到: $B_l=e(g,D_{\mu_l})^s=e(g,D_{\rho(i)})^s(\rho(i)\in D)$ 的值.

最后,算法计算:

$$(e(C_0,K_{end,i})^{-1}(B_l))^{\omega_i}=e(g,g)^{\omega_i\lambda_i s}.$$

以上为对于 *L* 中任意一个线性流程,算法通过递归运算最终得出其对应的子秘密.通过相似的计算步骤,算法能得到 *L* 中其他线性流程的子秘密.如果 $\lambda_i(i\in I)$是对访问矩阵 *M* 的秘密α的合法分割,则算法最终能通过式(2)计算出明文.

$$C_m\Big/\left(e(g,g)^{\sum_{i\in I}\omega_i\lambda_i s}\right)=me(g,g)^{\alpha s}/e(g,g)^{\alpha s}=m \tag{2}$$

3.6 方案特性讨论

在 KP-PBE 方案中,需要对以下几点加以说明.

● 本方案设置为只允许描述线性流程,是为了避免多义性的问题.为了说明这一点,首先介绍回溯攻击的原理[7].回溯攻击是指,如果用户能根据密钥和密文,利用双线性对的运算从节点 k 推出节点 k+1 的秘密,则该用户能反过来应用双线性对的运算从节点 k+1"回溯"到节点 k.举例而言,在解密的递归公式 $B_{k+1}=B_k\cdot e(C_0,K_{\mu_k,\mu_{k+1},1})e(C_{\mu_k,\mu_{k+1}},K_{\mu_k,\mu_{k+1},2})^{-1}=e(g,D_{\mu_{k+1}})^s$ 中,由于用户已知 B_k,并可从 B_k 通过上式的计算得到 B_{k+1},则该用户显然可以声称其能从 B_{k+1} 通过"反向"递推得到 B_k(可简单地通过以下公式计算: $B_{k+1}e(C_0,K_{\mu_k,\mu_{k+1},1})^{-1}e(C_{\mu_k,\mu_{k+1}},K_{\mu_k,\mu_{k+1},2})=B_k$).因此,假设给定起点 1 与关系 1→2,2→3 以及终点 3 的密钥,如果 KP-PBE 方案允许存在环流程,则用户既可证明其满足流程 1→2→3,也可证明其满足流程 1→2→3→2→3,1→2→3→2→3→2→3,….因此,用户满足的流程无法唯一标识,即流程的表达存在多义性.而如果规定 KP-PBE 不允许出现环形流程,则不存在歧义.

● 其次,本文下面将分析 KP-PBE 在描述流程时的便捷性.在第 1.1 节中,给出了一种用属性加密方法描述流程的平凡方法:即把每一个流程设置为一个属性.而用此方法描述流程将造成公共参数过于冗余的后果.下面将加以阐述.

设某组织内部共有 n 个部门,不失一般性,不妨用{1,2,…,n}表示部门编号.下面考察这 n 个部门共有几种可能的办事流程(假设办事流程均为线性流程).以下用定理 1 给出分析结果.

定理 1(线性流程的数目). 设节点集合内共有 n 个节点,则该节点集合共能产生 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 种流程.其中,符号 C,P 分别表示组合、排列的符号.

证明:不失一般性,考虑节点 1 作为起点,节点 2 作为终点这样的设置下可能存在的流程个数,此时可分成下面几种情况.

➢ 节点 1 作为起点,节点 2 作为终点,中间无任何节点,此时只有 1 种可能的流程:1→2,即 P_{n-2}^1.

➢ 节点 1 作为起点,节点 2 作为终点,中间通过 1 个节点,此时有 n–2 种可能的流程:1→3→2,1→4→2,…,1→n→2,即 P_{n-2}^1.

➢ 节点 1 作为起点,节点 2 作为终点,中间通过 2 个节点,此时有(n–2)(n–1)种可能的流程:

$1\to 3\to 4\to 2,1\to 3\to 5\to 2,...,1\to 3\to n\to 2,...,1\to 4\to 3\to 2,1\to 4\to 5\to 2,...,$ 1→4→n→2,…,1→n→n–1→2.实质上,此情况相当于固定 1,2 两个点,在 1,2 两点间有序地"填入"不重复的两个数(线性流程的性质不允许流程中的节点重复),且这两个数为集合{3,...,n}中的任意两个元素,这个排列共有(n–2)(n–1)种情况,即 P_{n-2}^2.

➢以同样的方法分析,以节点 1 作为起点,节点 2 作为终点,中间通过 k($0\leqslant k\leqslant n$–2)个节点,此时有(n–2)(n–1)…(n–2–k+1)种可能的流程,即 P_{n-2}^k.

因此,明显地,在集合{1,2,...,n}中,以节点 1 作为起点,节点 2 作为终点所有可能的流程为 $P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2}$ 种.

而由于在集合{1,...,n}中任选两个有序的不重复的节点共有 P_n^2 种情况,又,根据上面分析,选定两个节点分别作为起点、终点后,可生成 $P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2}$ 种流程,因此,总流程共有 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 种. □

由定理 1 可知,如果用普通的属性加密方案加密流程,在一个有 n 个部门的组织中,共存在 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 种可能的流程.为了区分这些流程,传统的属性加密[17,29]在设置公共参数时,必须定义 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 个相对应的公共参数.

而使用 KP-PBE 方案,若要表示这 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 种流程,则只需要在设置公共参数时进行以下设置.

✧ 在集合{1,2,...,n}中,为每个节点分配一个起点的公共参数(即公布起点的公共参数集合{$h_1,h_2,...,h_n$},对应于每个节点).

✧ 对于集合{1,2,…,n}中的任意两个节点 t,k,分配两个关系的公共参数 $r_{t,k},r_{k,t}$ 分别对应于关系 $t\to k$,$k\to t$.

若把{1,…,n}这 n 个节点的集合想象成一个有向图 $G=(V,E)$,设$|V|$表示图中顶点的个数,而$|E|$表示图中有向边的条数.通过以上对公共参数的设置,事实上,使得公共参数的集合组成了一个有向完全图(即任意两个节点间都有两条有向边连接的图).且该有向完全图中任意一个起点均可作为流程的起点,因此,这样的设置使得公共参数能够描述所有的存在于图中的流程.

而在有向完全图中,容易知道$|E|=|V|(|V|-1)$.因此,当 KP-PBE 方案表示 n 个节点间任意的线性流程时,需要 n 个起点参数以及 $n(n-1)$个关系参数,共需要 $n+n(n-1)=n^2$ 个参数.

根据以上分析,在表达同样数量的流程时(流程数为 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$), 传统的属性加密方案需要 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 个公共参数,而 KP-PBE 方案仅需 n^2 个公共参数.而显然,n^2 为多项式级的,而又有:

$$P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})>P_n^2(C_{n-2}^0+C_{n-2}^1+...+C_{n-2}^{n-2})=P_n^2 2^{n-2} \tag{3}$$

由式(3)可知,数 $P_n^2(P_{n-2}^0+P_{n-2}^1+...+P_{n-2}^{n-2})$ 为指数级的.因此,使用 KP-PBE 方案表示流程的效率比平凡地使用传统属性加密的效率要高许多.

3.7 安全性证明

KP-PBE 方案的正确性是显然的,以下证明该方案的安全性.KP-PBE 方案的安全性主要由以下定理保证.

定理 2(KP-PBE 的选择性安全模型). 设 KP-PBE 的所有线性流程共包含$|B^*|$个起点及$|R^*|$个关系.假设确定性 q-BDHE 成立,则不存在 PPT 的攻击者 A 能选择性地攻破 KP-PBE 系统,其中,$|B^*|+|R^*|\leqslant q$.

证明:假定存在概率多项式时间的攻击者 A 能在选择性安全模型下以不可忽略的优势$\varepsilon=Adv_A$攻破 KP-PBE 系统.那么,我们可以构造出一个挑战者 C 来解决确定性 q-BDHE.

Init:挑战者 C 首先获取确定性 q-BDHE 的参数 $\vec{X}=(\mathbb{G},p,g,g^s,g^a,...,g^{a^q},g^{a^{q+2}},...,g^{a^{2q}})$ 和 T,其中,$T=e(g,g)^{a^{q+1}s}$ 或为群 G 上的随机数.

随后,攻击者 A 公布一个挑战的线性流程集合 A^*.根据定义 6,由于一个线性流程由流程起点以及流程的关系集合组成,因此,A 需要公布的挑战的线性流程集合 A^*必须包括:A^*中所有流程的起点集 B^*以及 A^*中所有流程的关系集 R^*.

Setup:挑战者 C 设置:

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

由上可知,尽管挑战者并不知道 a^{q+1} 的值,但仍然可以秘密地设置$\alpha=a^{q+1}$.

挑战者设置其余公共参数如下.根据假设条件,设 KP-PBE 的所有线性流程共包含$|B^*|$个起点及$|R^*|$个关系,则有下式成立: $|B^*|+|R^*|\leqslant q$.因此,可以设定一个单射的映射.

$$\pi: B^*\cup R^*\to\{1,2,...,q\}.$$

即,该映射的输入值为起点集 B^*或关系集 R^*中的元素,输出值为集合{1,...,q}中的元素.

对于任意的线性流程的起点 j,挑战者把其分为属于挑战流程集内的起点($j\in B^*$)与不属于挑战流程集内的起点($j\notin B^*$),随后,挑战者选择随机数 $z_j\in Z_p$ 并进行式(4)的设置.

$$h_j=\begin{cases}g^{z_j}, & j\in B^*\\ g^{z_j}g^{a^{\pi(j)}}, & j\notin B^*\end{cases} \tag{4}$$

随后,挑战者选择随机数 $v_{t,k}\in Z_p$ 并进行式(5)的设置.

$$r_{t,k}=\begin{cases}g^{v_{t,k}}, & (t\to k)\in R^*\\ g^{v_{t,k}}g^{a^{\pi(t\to k)}}, & (t\to k)\notin R^*\end{cases} \tag{5}$$

在上面的设置中,由于映射π的目标集合中的元素都小于 q+1,因此,挑战者可以顺利地进行设置(因为不会出现 $g^{a^{q+1}}$ 这样挑战者无法得到的值).

Phase 1,2:在这一步中,攻击者 A 可以向挑战者 C 询问任意关于线性流程的访问结构 A 的私钥,但必须符合以下限制:挑战的线性流程集合 A^*不能满足访问结构 A.

设挑战的流程集合中所有的节点组成的集合为 R^*.根据 KeyGen 算法的规定,R^*中每一个终点必然对应于访问矩阵 M 中的一行.而由于挑战流程集合 A^*不能满足访问结构 A,所以根据文献[29]中的结论,对于所有的满足条件$\rho(i)\in R^*$的 i,必然存在向量 $\vec{w}=(w_1,...,w_n)^{\perp}$, 其中, $w_1=1$, 使得下式成立:

$$M_i\cdot\vec{w}=0 \tag{*}$$

利用向量 $\vec{w}$,攻击者 A 隐蔽地设置秘密向量 $\vec{y}$ 如下:

$$\vec{y}=a^{q+1}\vec{w}+(0,y_2,...,y_n)^{\perp},\{y_2,...,y_n\}\leftarrow Z_p^{n-1}.$$

以上的向量 $\vec{y}$ 的设置是均匀分布的,因为除了它的第 1 个分量是 $\alpha=g^{a^{q+1}}$ 以外(因为 $w_1=1$),其余的分量都被随机数 $y_2,...,y_n$ 随机化了.因此,可以推导出:

$$\lambda_i=M_i\vec{y}=M_i\vec{w}a^{q+1}+M_i(0,y_2,...,y_n)^{\perp}=M_i\vec{w}a^{q+1}+\lambda_i' \tag{**}$$

其中, $\lambda_i'=M_i\cdot(0,y_2,...,y_n)^{\perp}$.

随后,挑战者将设置被询问的线性流程集合中每个节点所对应的秘密值.设集合 B 表示攻击者 A 所询问的访问结构中流程的起点集合,设集合 D 表示攻击者 A 所询问的访问结构中流程的终点集合.挑战者选择随机数 $\theta_i\in Z_p$,并隐藏地对每个流程节点相对应的秘密 D_i 进行式(6)的设置.

$$D_i=\begin{cases}g^{\theta_i}, & i\notin D\vee i\in R^*\\ g^{\theta_i}g^{\langle M_{\rho^{-1}(i)}\cdot\vec{w}\rangle a^{q+1}}, & i\in D\wedge \mathrm{i}\notin R^*\end{cases} \tag{6}$$

在以上的构造中,映射$\rho^{-1}(i)$的意思是把流程终点 i 的标号转换为访问矩阵 M 上的行的标号.该设置把秘密 D_i 的值分为两大类:一类为 D_i 所对应的节点 i 是流程的终点,并且该终点并未出现在挑战流程集合所包含的点集中,此时,设置 $D_i=g^{\theta_i}g^{\langle M_{\rho^{-1}(i)}\cdot\vec{w}\rangle a^{q+1}}$; 而另一类为 D_i 所对应的节点 i 不是流程的终点,或是终点但该终点出现在挑战流程集合所包含的点集中,此时,设置 $D_i=g^{\theta_i}$.

以下挑战者生成关于线性流程起点与线性流程关系的密钥.

- 如果 $i\in B$,即当 i 为线性流程中的起点时,挑战者挑选随机数 $v_i'\in Z_p$, 生成密钥如下:

$$K_i=\left(K_{i,1},K_{i,2}\right)=(g^{\theta_i}h_i^{v_i'},g_i^{v_i'}).$$

注意到,当 $i\in B$ 时,必然满足条件 $i\in D\vee i\in R^*$(由于线性流程的起点不可能为该流程的终点,因此,必然满足条件 $i\notin D$),因此,根据以上设置,有 $D_i=g^{\theta_i}$. 由于 D_i 中没有出现挑战者不知道的项 $g^{a^{q+1}}$, 因此,挑战者可以很简单地构造这个参数.

- 当攻击者 A 询问关系$(t\rightarrow k)\in R$ 的密钥时,挑战者挑选随机数 $c_{t,k}'\in Z_p$, 生成密钥如下:

$$K_{t,k}=\left(K_{t,k,1},K_{t,k,2}\right)=\begin{cases}g^{\theta_k-\theta_t}g^{v_{t,k}e_{t,k}a^{(q+1-\pi(t\rightarrow k))}},g^{e_{t,k}a^{(q+1-\pi(t\rightarrow k))}}, & (t\in D\wedge t\notin R^*)\vee(k\in D\wedge k\notin R^*)\\ g^{\theta_k-\theta_t}g^{v_{t,k}c_{t,k}'},g^{c_{t,k}'}, & \text{else}\end{cases} \tag{7}$$

分配关系密钥时,情况比较复杂.特别需要注意的是,只要节点 t,k 中有一个节点是流程的终点,且该终点并未出现在挑战流程中(即满足逻辑表达式$(t\in D\wedge t\in R^*)\vee(k\in D\wedge k\notin R^*)$),则根据式(6)对 D_i 的设置, $D_t^{-1}D_k$ 中必然存在 $g^{a^{q+1}}$ 这个挑战者无法构造的项.又,只要节点 t,k 中有一个节点是流程的终点,且该终点并未出现在挑战流程的节点集合中,则关系 $t\rightarrow k$ 不可能为挑战流程中的关系(挑战流程中的关系必然是从挑战流程中的某个节点到挑战流程中的另一个节点的关系).因此,逻辑表达式$(t\in D\wedge t\notin R^*)\vee(k\in D\wedge k\notin R^*)$蕴含了逻辑表达式$(t\rightarrow k)\notin R^*$.因此,此时可以设置式(7)中的 $e_{t,k}$ 用以消掉项 $g^{a^{q+1}}$, 从而能使挑战者可以产生关系 $t\rightarrow k$ 的密钥.具体分为以下 3 种情况.

(1) 当 $(t\in D\wedge t\notin R^*)\wedge(k\notin D\vee k\in R^*)$ 时,只有 D_t 含有 $g^{a^{q+1}}$ 项.因此, $D_t^{-1}D_k=g^{\theta_k-\theta_t}g^{-\langle M_{\rho^{-1}(t)}\vec{w}>a^{q+1}}$, 我们只要设置 $c_{t,k}=a^{\langle M_{\rho^{-1}(t)}\vec{w}\rangle(q+1-\pi(t\rightarrow k))}$, 即得:

$$K_{t,k,1}=(D_t^{-1}D_k)r_{t,k}^{c_{t,k}}=g^{\theta_k-\theta_t}g^{-\langle M_{\rho^{-1}(t)}\vec{w}\rangle a^{q+1}}(g^{v_{t,k}}g^{a^{\pi(t\to k)}})^{\langle M_{\rho^{-1}(t)}\vec{w}\rangle a^{(q+1-\pi(t\to k))}}=g^{\theta_k-\theta_t}g^{v_{t,k}\langle M_{\rho^{-1}(t)}\vec{w}\rangle a^{(q+1-\pi(t\to k))}},$$

$$K_{t,k,2}=g^{c_{t,k}}=g^{a^{\langle M_{\rho^{-1}(t)}\vec{w}\rangle(q+1-\pi(t\to k))}}.$$

因此,此时式(2)中的 $e_{t,k}=\langle M_{\rho^{-1}(t)}\vec{w}\rangle$.

(2) 当 $(k\in D\wedge k\notin R^*)\wedge(t\notin D\vee t\in R^*)$ 时,与情况 1 使用相似的构造方法即可消去项 $g^{a^{q+1}}$,此时,式(7)中的 $e_{t,k}=-\langle M_{\rho^{-1}(k)}\vec{w}\rangle$.

(3) 当 $(t\in D\wedge t\notin R^*)$ 而 $(k\in D\wedge k\notin R^*)$ 时,与情况 1 使用相似的构造方法即可消去项 $g^{a^{q+1}}$,此时,式(7)中的 $e_{t,k}=\langle M_{\rho^{-1}(t)}\vec{w}\rangle-\langle M_{\rho^{-1}(k)}\vec{w}\rangle$.

当以上 3 种情况皆未发生时,即 $(t\notin D\vee t\in R^*)\wedge(k\notin D\vee k\in R^*)$ 时(亦即满足式(7)中的 else 的情况),项 $D_t^{-1}D_k$ 中不存在挑战者不知道的项 $g^{a^{q+1}}$,因此挑战者选择随机数 $c'_{t,k}$ 即可简单地完成密钥构造.

● 最后,挑战者需要设置访问结构中每个终点对应的密钥.由于每个终点都与访问矩阵中的一行相对应,设需要生成终点 d 的密钥,且设 $\rho(i)=d$,即终点 d 与访问矩阵的行 i 相对应.挑战者生成密钥如下:

$$K_{end,d}=g^{-\lambda'_d}g^{\theta_{\rho(d)}}.$$

以上的设置基于以下事实:

(1) 根据式(6),当终点 d 满足 $\rho(d)\in R^*$ 时,$D_i=D_{\rho(d)}=g^{\theta_{\rho(d)}}$,而同时根据式(*),又有 $M_i\cdot\vec{w}=0$,因此,$K_{end,d}$ 中不存在 $g^{a^{q+1}}$ 这样挑战者无法构造的项.

(2) 当终点 d 满足 $\rho(d)\notin R^*$ 时,根据式(6),$D_i=D_{\rho(d)}=g^{\theta_{\rho(d)}}g^{\langle M_d\cdot\vec{w}\rangle a^{q+1}}$,而根据式(**),$\lambda_d=M_d\vec{w}a^{q+1}+\lambda'_d$,因此,挑战者不知道的项 $g^{a^{q+1}}$ 被顺利消去,挑战者亦能成功生成该密钥.

综上,挑战者成功构造了攻击者需要的密钥.

Challenge:在这一步中,挑战者通过投掷随机硬币得到值 $b\leftarrow\{0,1\}$,并生成密文如下:

$$C_m=m_b\cdot T,$$

$$C_0=g^s,$$

$$C_j=(g^s)^{z_j}\ (j\in B^*),$$

$$C_{t,k}=(g^s)^{v_{t,k}}\ ((t\to k)\in R^*).$$

Guess:最终,攻击者 A 输出一个比特 b'.如果 $b=b'$,挑战者输出 0(表示它猜测 $T=e(g,g)^{a^{q+1}}$,否则,输出 1(表示它猜测 T 是群上的一个随机数).如果敌手 A 能以不可忽略的优势 ε 攻破 KP-PBE 系统,那么挑战者将能以不可忽略的优势 ε 解决确定性 q-BDHE.证毕. □

4 结论与展望

本文首次研究了一种新的密码学原语:基于流程的加密——PBE,并把 PBE 进一步划分为密钥策略的流程加密——KP-PBE 和密文策略的流程加密——CP-PBE.随后,应用双线性对原理及线性秘密共享机制构造出一个 KP-PBE 的算法,KP-PBE 与传统 ABE 方案相比,在处理流程的效率上有数量级的提高(把指数级别的流程数降低为多项式级别的流程数),大大降低了系统冗余.最后,在选择性安全模型下,给出了 KP-PBE 的安全性证明.

KP-PBE 作为一种新兴的密码学原语,具有许多全新的挑战:首先,最为明显地,如何在 KP-PBE 方案的基础上提出 CP-PBE 方案是一个挑战.另外,如何利用一些现有的安全性证明技术,如双系统加密的技术(dual system encryption[30])来证明 KP-PBE 或 CP-PBE 的完全安全性(fully secure);而且,KP-PBE 方案只能由一个可信中心进行密钥颁发工作,如何构造出可容纳多个可信中心共同颁发密钥的 PBE 方案,也是一个挑战.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the CRYPTO 1984. Berlin, Heidelberg: Springer-Verlag, 1985. 19–22. [doi: 10.1007/3-540-39568-7_5]

[2] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 457–473. [doi: 10.1007/11426639_27]

[3] Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption. In: Proc. of the Int'l Colloquium on Automata, Languages & Programming. Berlin, Heidelberg: Springer-Verlag, 2008. 579–591. [doi: 10.1007/978-3-540-70583-3_47]

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Computer Society, 2007. 321–334. [doi: 10.1109/SP.2007.11]

[5] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the ACM Conf. on Computer and Communications Security. ACM, 2007. 195–203. [doi: 10.1145/1315245.1315270]

[6] Hohenberger S, Waters B. Attribute-Based encryption with fast decryption. In: Proc. of the PKC 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 162–179. [doi: 10.1007/978-3-642-36362-7_11]

[7] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Haifa: Technion, 1996.

[8] Waters B. Functional encryption for regular languages. In: Proc. of the CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 218–235. [doi: 10.1007/978-3-642-32009-5_14]

[9] Xiong JB, Yao ZQ, Ma JF, Li FH, Liu XM. A secure self-destruction scheme with IBE for the Internet content privacy. Chinese Journal of Computers, 2014,37(1):139–150 (in Chinese with English abstract).

[10] Guang Y, Zhu YF, Fei JL, Gu CX, Zheng YH. Identity-Based fully homomorphic encryption from learning with error problem. Journal of Communications, 2014,35(2):111–117 (in Chinese with English abstract).

[11] Wang SH, Han ZJ, Xiao F, Wang RZ. Identity-Based searchable encryption scheme with a designated tester. Journal of Communications, 2014,35(7):22–32 (in Chinese with English abstract).

[12] Ming Y, Wang YM. Provable secure identity-based encryption scheme with wildcard in the standard model. Acta Electronica Sinica, 2013,41(10):2082–2086 (in Chinese with English abstract).

[13] Cocks C. An identity based encryption scheme based on quadratic residues. In: Proc. of the IMA Conf. on Cryptography and Coding. Berlin, Heidelberg: Springer-Verlag, 2001. 360–363. [doi: 10.1007/3-540-45325-3_32]

[14] Boneh D, Franklin MK. Identity-Based encryption from the weil pairing. In: Proc. of the CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 213–229. [doi: 10.1007/3-540-44647-8_13]

[15] Waters B. Efficient identity-based encryption without random oracles. In: Proc. of the EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 114–127. [doi: 10.1007/11426639_7]

[16] Shao J, Cao Z. Multi-Use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 2012,206:83–95. [doi: 10.1016/j.ins.2012.04.013]

[17] Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the ACM Conf. on Computer and Communications Security. ACM, 2006. 89–98. [doi: 10.1145/1180405.1180418]

[18] Chase M. Multi-Authority attribute based encryption. In: Proc. of the TCC 2007. Berlin, Heidelberg: Springer-Verlag, 2007. 515–534. [doi: 10.1007/978-3-540-70936-7_28]

[19] Lewko AB, Waters B. Unbounded HIBE and attribute-based encryption. In: Proc. of the EUROCRYPT 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 547–567. [doi: 10.1007/978-3-642-20465-4_30]

[20] Wan Z, Liu JE Deng RH. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans. on Information Forensics and Security, 2012,7(2):743–754. [doi: 10.1109/TIFS.2011.2172209]

[21] Wang G, Liu Q, WUJ, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 2011,30(5):320–331. [doi: 10.1016/j.cose.2011.05.006]

[22] Deng H, Wu Q, Qin B, Josep D, Lei Z, Liu JW, Shi WC. Ciphertext-Policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences, 2014,275(12):370–384. [doi: 10.1016/j.ins.2014.01.035]

[23] Xiong JB, Yao ZQ, Ma JF, Li FH, Liu XM, Li Q. A secure self-destruction scheme for composite documents with attribute based encryption. Acta Electronica Sinica, 2014,42(2):366–376 (in Chinese with English abstract).

[24] Guan ZT, Yang TT, Xu RZ, Wang ZX. Multi-Authority attribute-based encryption access control model for cloud storage. Jounnal of Communications, 2015,36(6):116–126 (in Chinese with English abstract).

[25] Chen JH, Chen KF, Long Y, Wan ZM, Yu K, Sun CF, Chen LQ. Ciphertext policy attribute-based parallel keyinsulated encryption. Ruan Jian Xue Bao/Journal of Software, 2012,23(10):2795–2804 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4183.htm [doi: 10.3724/SP.J.1001.2012.04183]

[26] Wang PP, Feng DG, Zhang LW. CP-ABE scheme supporting fully fine-grained attribute revocation. Ruan Jian Xue Bao/Journal of Software, 2012,23(10):2805–2816 (in Chinese with English abstract).). http://www.jos.org.cn/1000-9825/4184.htm [doi: 10.3724/SP.J.1001.2012.04184]

[27] Boneh D, Sahai A, Waters B. Functional encryption: Definitions and challenges. In: Proc. of the TCC 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 253–273. [doi: 10.1007/978-3-642-19571-6_16]

[28] Goldwasser S, Goyal V, Jain A, Sahai A. Multi-Input functional encryption. IACR Cryptology ePrint Archive, 2013, 727. http://eprint.iacr.org/2013/727

[29] Waters B. Ciphertext policy attribute based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the PKC 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 53–70. [doi: 10.1007/978-3-642-19379-8_4]

[30] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Proc. of the CRYPTRO 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 619–636. [doi: 10.1007/978-3-642-03356-8_36]

附中文参考文献:

[9] 熊金波,姚志强,马建峰,李凤华,刘西蒙.面向网络内容隐私的基于身份加密的安全自毁方案.计算机学报,2014,37(1):139–150.

[10] 光焱,祝跃飞,费金龙,顾纯祥,郑永辉.利用容错学习问题构造基于身份的全同态加密体制.通信学报,2014,35(2):111–117.

[11] 王少辉,韩志杰,肖甫,王汝传.指定测试者的基于身份可搜索加密方案.通信学报,2014,35(7):22–32.

[12] 明洋,王育民.标准模型下可证安全的通配符基于身份加密方案.电子学报,2013,10:2082–2086.

[23] 熊金波,姚志强,马建峰,李凤华,刘西蒙,李琦.基于属性加密的组合文档安全自毁方案.电子学报,2014,42(2):366–376.

[24] 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.

[25] 陈剑洪,陈克非,龙宇,万中美,于坤,孙成富,陈礼清.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. http://www.jos.org.cn/1000-9825/4183.htm [doi: 10.3724/SP.J.1001.2012.04183]

[26] 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. http://www.jos.org.cn/1000-9825/4184.htm [doi: 10.3724/ SP.J.1001.2012.04184]

邓宇乔(1980－),男,广东湛江人,博士,副教授,主要研究领域为密码学,信息安全.

宋歌(1984－),女,博士,讲师,主要研究领域为密码学,数据挖掘,大数据处理.

唐春明(1972－),男,博士,教授,博士生导师,主要研究领域为密码学.

温雅敏(1981－),女,博士,副教授,主要研究领域为隐私保护密码学协议的设计与可证明安全.