DOI:10.13868/j.cnki.jcr.000001

密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2014,1(1):1–12

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

属性密码学研究*

冯登国[1,2], 陈 成[1]

1. 中国科学院软件研究所, 北京 100190
2. 北京信息科学技术研究院, 北京 100878
通讯作者: 冯登国, E-mail: fengdg@263.net

摘 要: 属性密码学作为一种新型的密码学原语, 是近年来密码学研究中的一个热门方向, 它可以有效实现细粒度的非交互访问控制机制, 并具有广泛的应用前景. 本文系统地论述了当前属性密码学的研究现状和发展趋势, 并就主流研究工作进行了深入探讨和分析, 其主要内容包括: 属性密码学基本概念、可证明安全的方案和近年来的研究进展情况, 同时, 讨论了未来需要进一步研究解决的问题.
关键词: 密码学; 属性密码学; 访问控制
中图法分类号: TP309.7 **文献标识码**: A

中文引用格式: 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1–12.
英文引用格式: Feng D G, Chen C. Research on attribute-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 1–12.

Research on Attribute-based Cryptography

FENG Deng-Guo[1,2], CHEN Cheng[1]

1. Institute of Software Chinese Academy of Sciences, Beijing 100190, China
2. Beijing Academy of Information Science and Technology, Beijing 100878, China
Corresponding author: FENG Deng-Guo, E-mail: fengdg@263.net

Abstract: As a new cryptographic primitive, attribute-based cryptography is an attractive research topic in recent years. It provides a fine-grained and non-interactive access control mechanism of encrypted data and has great potential applications. Through an in-depth study of the major work on this topic, this paper presents a survey on the research status and development trend of attribute-based cryptography. It reviews the basic concepts of attribute-based cryptography, the development of provably secure schemes and some results of the most recent research. Finally, this paper discusses some problems that need to be solved in the future.
Key words: cryptography; attribute-based cryptography; access control

1 引言

属性密码学又称基于属性的密码学, 是公钥密码学和基于身份的密码学的一种扩展, 最早的公开研究起源于属性加密[1], 后来拓展到属性签名、属性安全协议等研究内容. 与传统密码学相比, 属性密码学提

* 基金项目: 国家重点基础研究发展项目(973 计划)(2013CB338003); 国家自然科学基金项目(91118006)
收稿日期: 2013-12-15 定稿日期: 2013-12-30

供了更加灵活的操作(如加解密)关系. 例如, 在属性加密机制中, 密文和密钥都与一组属性相关, 加密者可根据要加密的内容和接收者的特征信息制定一个由属性构成的加密策略, 而产生的密文只有属性满足加密策略的用户才可以解密.

属性加密机制极大地丰富了加密策略的灵活性和用户权限的可描述性, 从以往的一对一加解密模式扩展成一对多模式. 此外, 它还具有以下 4 个特点: ①高效性. 加解密代价和密文长度仅与相应属性个数相关, 而与系统中用户的数量无关; ②动态性. 用户能否解密一个密文仅取决于他的属性是否满足密文的策略, 而与他是否在密文生成前加入这个系统无关; ③灵活性. 具体表现为加密策略可支持复杂的访问结构, 如门限、布尔表达式; ④隐私性. 加密者并不需要知道解密者的身份信息.

基于上述良好性质, 属性加密机制可以有效地实现非交互的访问控制. 在传统的访问控制系统中, 用户的权限和所有的数据都由系统管理员来分配和管理. 而随着系统中用户数量和数据量的增长, 以及用户对数据和个人隐私需求的不断提升, 对传统访问控制技术提出了新的需求和挑战. 从数据安全和隐私角度来看, 用户并不希望自己的数据对存储服务器完全透明; 另外, 一旦存储服务器被黑客攻破, 用户存储的所有数据将会被泄露. 从效率方面来看, 在传统的访问控制系统中, 服务器需要通过与每个用户进行交互来允许或限制访问者的访问能力和范围, 当用户数量很大时, 将严重影响系统效率. 属性加密机制可以很好地解决上述问题, 其解决思路是: 系统中每个权限可由一个属性表示, 由一个权威机构对所有的访问者的权限属性进行认证并颁发相应的密钥, 系统中的资源以加密形式保存在服务器中, 加密的访问策略可根据需要①由资源发布者来灵活制定, 任何人都能够公开访问加密后的资源, 但只有满足访问策略的访问者才可以通过解密来访问该资源. 例如, 一个用户想要分享一个秘密信息给拥有属性 A_3 且拥有属性 A_1 或 A_2 的用户(如图 1 所示). 他可以通过指定一个如图 1 所示的布尔表达式作为加密策略来进行加密, 实现对分享用户的访问控制.

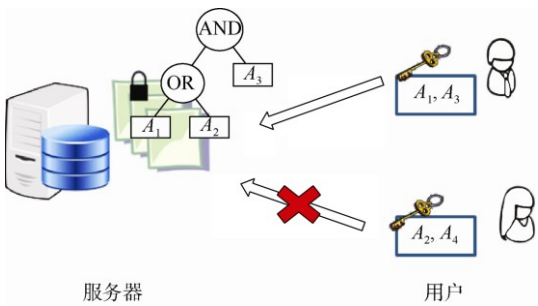


图 1 基于属性加密机制实现非交互访问控制的过程

Figure 1 Realizing a fine-grained and non-interactive access control from attribute-based encryption

这样一个系统实现了访问控制的以下基本功能: 防止非法的访问者进入受保护的网络资源; 允许合法用户访问受保护的网络资源; 防止合法的用户对受保护的网络资源进行非授权访问. 此外, 这样的系统也有效地解决了传统访问控制中存在的以下问题: 系统中服务器只负责对加密后的资源进行管理, 而不能够真正访问数据资源, 保证了用户数据的安全和隐私; 另一方面, 服务器并不需要对每个访问者进行交互, 提高了系统的效率.

属性密码学自从诞生以来, 就已成为密码学领域一个非常热门的研究方向, 并得到了快速发展, 在分布式文件管理、第三方数据存储、日志审计、付费电视系统、定向广播加密等领域有着良好的应用前景[2,3]. 特别是随着近几年云计算技术的发展和日益普及, 越来越多的企业和个人将自身的数据存储外包给云服

①一般来说, 加密策略可以由需要加密资源的属性或允许访问者的属性来决定.

务商, 为保护用户的数据安全和隐私, 属性密码学提供了一个很好的解决途径. 本文将对属性密码学做一个系统的综述: 首先对属性密码学的基本概念进行介绍; 其次, 对当前研究现状和相关研究成果进行归纳和总结; 最后, 对目前存在的一些未解决或尚未良好解决的公开问题进行了分析和探讨, 并指出一些未来可能的研究方向.

2 属性密码学的基本概念

本节将重点介绍属性加密、属性签名和属性安全协议等基本概念.

2.1 属性加密

一个属性加密方案主要由以下 4 个算法组成:

1) $\mathrm{Setup}(k,U)$: 该算法输入安全参数 k 和一个系统属性描述 U, 输出公共参数 PP 和一个主私钥 MSK.

2) $\mathrm{Keygen}(\mathrm{MSK},X)$: 该算法输入主私钥 MSK 和一个权限 X, 输出一个密钥 SK_X.

3) $\mathrm{Enc}(\mathrm{PP},Y,m)$: 该算法输入公共参数 PP, 一个密文索引(index) Y 和一个要加密的消息 m, 输出密文 CT_Y.

4) $\mathrm{Dec}(\mathrm{PP},\mathrm{SK}_X,\mathrm{CT}_Y)$: 该算法输入公共参数 PP, 密钥 SK_X 和密文 CT_Y, 输出解密的结果 m'.

如果一个属性加密方案是正确的, 当且仅当对任意用户权限 X 和密文索引 Y, 若 X 满足 Y, 则

$$\mathrm{Dec}\big(\mathrm{PP},\mathrm{Keygen}(\mathrm{MSK},X),\mathrm{Enc}(\mathrm{PP},Y,m)\big)=m$$

其中, 公共参数 PP 和主私钥 MSK 都是正确产生的.

文献[2]中将属性加密(Attributed based encryption, ABE)分为两类, 密钥策略的属性加密(Key-Policy ABE, KP-ABE)和密文策略的属性加密(Ciphertext-Policy ABE, CP-ABE). 在密文策略的属性加密方案中, X 为一个属性集合, 密文索引 Y 为一个访问结构, X 满足 Y 当且仅当 X 是 Y 的授权集. 在密钥策略的属性加密方案中, 正好相反, 即 Y 为一个属性集合, X 为一个访问结构, X 满足 Y 当且仅当 Y 是 X 的授权集. 访问结构的具体定义可参见文献[2,4].

为了刻画属性加密的安全性, 我们考虑一个敌手 A 和挑战者 S 之间的实验(如图 2). 最后, 敌手的优势定义为

$$\mathrm{Adv}_A(k)=\left|\Pr[b'=b]-1/2\right|$$

我们称一个属性加密方案是自适应安全的, 当且仅当任意多项式敌手的优势都是可忽略的. 在实际证明中, 常常也考虑一种弱化的安全模型, 称为选择模型. 在选择模型中要求敌手 A 必须提前选择自己的攻击目标, 即公布自己的挑战密文索引 Y (如图 2 中框内所示), 在此模型下的安全则称为选择安全.

$$\mathrm{Exp}_{\mathrm{ABE}}^{\mathrm{ind}}(k):$$
$$\boxed{Y\leftarrow A[\text{选择模型}]}$$
$$b\xleftarrow{R}\{0,1\}$$
$$\mathrm{PP},\mathrm{MSK}\xleftarrow{R}\mathrm{Setup}(k,U)$$
$$(\mathrm{Msg}_0,\mathrm{Msg}_1,Y)\xleftarrow{R}A^{\mathrm{KeyGen}(\cdot)}(\mathrm{PP})$$
$$\mathrm{CT}\xleftarrow{R}\mathrm{Enc}(\mathrm{PP},Y,\mathrm{Msg}_b)$$
$$b'\leftarrow A^{\mathrm{KeyGen}(\cdot)}(\mathrm{PP},\mathrm{CT})$$

图 2 属性加密的安全模型

Figure 2 Security model of attribute-based encryption

2.2 属性签名

一个属性签名方案主要由以下 4 个算法组成:

1) $\mathrm{Setup}(k,U)$: 该算法输入安全参数 k 和一个系统属性描述 U, 输出公共参数 PP 和一个主私钥 MSK.

2) $\mathrm{Keygen}(\mathrm{MSK},X)$: 该算法输入主私钥 MSK 和一个权限 X, 输出一个密钥 SK_X.

3) $\mathrm{Sign}(\mathrm{PP},Y,\mathrm{SK}_X,m)$: 该算法输入公共参数 PP, 一个签名策略 Y, 私钥 SK_X 和一个要签名的消息 m, 输出签名 σ_Y.

4) $\mathrm{Verify}(\mathrm{PP},\sigma_Y,m)$: 该算法输入公共参数 PP, 签名 σ_Y 和消息 m, 如果签名合法, 输出 1; 否则, 输出 0.

如果一个属性签名方案是正确的, 当且仅当对任意用户权限 X 和签名策略 Y, 若 X 满足 Y, 则

$$\mathrm{Verify}\left(\mathrm{PP},\ \mathrm{Sign}(\mathrm{PP},Y,\mathrm{SK}_X,m),\ m\right)=1$$

其中, 公共参数 PP 和主私钥 MSK 都是正确产生的.

在考虑属性签名的安全性时, 除了考虑传统签名的不可伪造性之外, 还需考虑签名者的匿名性. 这里我们分别对此进行描述.

为了刻画属性签名的不可伪造性, 我们考虑一个敌手 A 和挑战者 S 之间的实验(如图 3). 最后, 如果敌手输出的签名合法且他之前没有询问过, 那么我们称敌手成功. 敌手的优势定义为敌手成功的概率. 我们称一个属性签名方案是自适应不可伪造的, 当且仅当任意多项式敌手的优势都是可忽略的. 在实际证明中, 同样也考虑一种弱化的安全模型, 称为选择模型. 在选择模型中要求敌手 A 必须提前选择自己的攻击目标, 即公布将要伪造的签名策略 Y (如图 3 中框内所示), 在此模型下的安全则称为选择不可伪造.

属性签名的匿名性是指签名验证者通过签名仅能够得知签名者的属性满足签名的策略, 而无法得知其他信息, 包括签名者的具体属性信息和身份信息. 我们称一个属性签名方案具有匿名性, 当且仅当对任意权限 X_1 和 X_2、策略 Y 和消息 m, 如果 X_1 和 X_2 都满足 Y, 那么私钥 SK_{X_1} 和 SK_{X_2} 对 (Y,m) 产生的签名在敌手眼中不可区分.

$\mathrm{Exp}_{\mathrm{ABE}}^{\mathrm{ind}}(k)$:

$\boxed{Y \leftarrow A[\text{选择模型}]}$

$\mathrm{PP},\mathrm{MSK} \xleftarrow{R} \mathrm{Setup}(k,U)$

$(M,\sigma,Y) \xleftarrow{R} A^{\mathrm{KeyGen}(\cdot),\mathrm{Sign}(\cdot)}(\mathrm{PP})$

图 3 属性签名的安全模型

Figure 3 Security model of attribute-based signature

2.3 属性安全协议

在属性安全协议中, 证明方通过协议的交互向验证方证明自己的属性满足某种条件或策略来完成认证, 同时在一定程度上保护自己的隐私性. 目前, 属性安全协议主要有两类, 即属性证明协议和属性协商协议. 在属性证明协议中, 一方向另一方通过交互进行单向的认证, 来证明自己的属性满足验证策略. 在属性协商协议中, 则是通过双向的认证方式来进行, 双方都向对方指定一个策略, 只有双方的属性都满足对方指定的策略才可完成协商, 产生一个共同的会话密钥. 具体定义可参见文献[5,6].

3 属性密码学研究现状

本节将主要介绍属性密码学的研究现状, 重点侧重于属性密码学基础方案的构造, 按照时间顺序将属性密码学的发展历程划分为三个阶段, 如图 4 所示, 其中包括: 概念的提出、可证明安全的方案和近年来的研究进展.

3.1 概念的提出

在基于身份的加密机制中[7], 往往用可以唯一标识的身份信息当作公钥来进行加密. 而人的生物特征(如指纹、虹膜)被认为是很好的身份信息载体, 因为它们与生俱来, 永不失效, 并方便随身携带. 但同时在对生物信息识别时会不可避免地出现误差. 因此, 用生物特征作为身份信息需要考虑对这种误差的容忍. 2005 年, Sahai 和 Waters[1]首先考虑了基于生物特性信息的身份加密方案, 称为模糊身份加密方案(Fuzzy Identity-based Encryption, Fuzzy-IBE). 在该方案中, 用户的身份信息被特征化为一组属性, 而身份的匹配关系由原来的"完全匹配"变为"相似匹配", 即对两个由 n 个属性组成的身份信息, 它们之间匹配允许存在一些小的误差, 只需要它们之间至少存在 t 个共同的属性即可, 而 $n-t$ 则是对误差的"容忍值". 这样一个模糊身份加密方案可以看作是属性密码学的"雏形".

2006 年, Goyal, Sahai 和 Waters 等人[2]将模糊身份加密拓展为属性加密, 阐明了属性加密的概念和意义. 在属性加密机制中, 用户身份信息被泛化为用户身份相关的属性, 并根据密文和密钥表现形式和应用场景的不同分为密钥策略的属性加密(KP-ABE)和密文策略的属性加密(CP-ABE)两类. 他们从第三方存储中的访问控制问题出发, 说明了属性加密是一个可以实现细粒度访问控制的强大密码机制. 同时, 还提出了一个基本的安全要求——抗合谋性. 抗合谋性可防止用户之间通过互相合作来超越他们应有的解密能力. 例如, 在一个属性加密机制中, 张三拥有属性 A, 李四拥有属性 B, 密文加密策略为属性 A 且 B, 张三李四都不能单独解密这条密文, 但如果张三和李四可以通过"合谋"来解密密文, 那么这个系统就不满足抗合谋性. 之后, Pirretti 等人[3]利用属性加密来实现属性系统, 并指出了属性加密机制在分布式存储和社交网络等更广领域的应用.

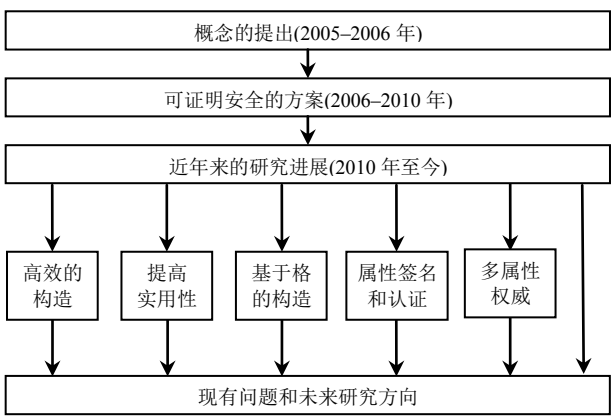


图 4 属性密码学发展历程

Figure 4 Development of attribute-based cryptography

3.2 可证明安全属性密码方案

与传统的可证明安全公钥机制相比, 属性密码机制需要支持灵活和复杂的访问策略, 并且需要具有抗合谋的安全特性. 这些因素给设计可证明安全的属性密码方案带来了困难和挑战. 本节通过一些经典的

选择安全和自适应安全的属性加密方案, 来介绍可证明安全属性密码方案的发展历程.

3.2.1 选择安全的属性加密方案

Goyal, Sahai 和 Waters 等人[2]提出属性加密概念的同时, 也给出了一个可证明安全的密钥策略的属性加密方案. 该方案在双线性群上实现, 其访问结构可以支持树状访问结构(布尔表达式)②. 然而, 构造可证明安全的密文策略的属性加密方案在很长一段时间一直是一个公开难题. 相比于密钥策略的属性加密, 构造可证明安全的密文策略的属性加密要相对困难, 其主要难点在于如何防止用户之间的合谋攻击.

Bethencourt, Sahai 和 Waters[8]在 2007 年给出了第一个密文策略的属性加密的构造, 他们通过在不同密钥中引入不同随机数来防止合谋攻击. 该方案支持树状访问结构, 虽然其安全性是可证明的, 但是证明却是基于具有争议的一般群模型假设(generic group model). 同年, Cheung 和 Newport[9]在标准模型和标准假设(BDBH 假设)下给出了一个可证明安全的方案, 但是访问结构只能支持与门. Waters[4]之后构造了一系列在标准模型和合理假设下可证明安全的密文策略的属性加密方案, 这些构造都能支持一般访问结构, 并通过线性秘密共享方案(linear secret sharing scheme)来实现. 在证明过程中, 模拟者利用选择模型中敌手提供的挑战访问结构的信息, 在设置公共参数时, 将挑战访问结构嵌入公共参数中, 使得挑战者可以很容易进行挑战密文的回答. 而在产生密钥询问的回答时, 证明利用了线性秘密共享方案的性质, 使得密钥中模拟者所不能产生的部分都可以被消去, 从而实现完美模拟.

3.2.2 自适应安全的属性加密方案

在考虑自适应安全(或完全安全)时, 在基于身份的加密方案中, 常常采用一种称作“分割规约”(partitioning reduction)的证明技术. 但是, 这种证明技术并不能很好地拓展到属性密码的研究中, 因为在属性密码机制中属性集合和访问结构的空间比身份空间要大得多. 当我们尝试对属性集合和访问结构的空间进行划分时, 将不可避免地造成模拟成功的概率为一个可忽略的值, 从而导致证明无法完成.

对偶系统加密[10]的提出为解决这个问题提供了一种新的思路. 在证明中引入了半功能密钥和半功能密文的概念, 半功能密钥可以正常解密密文, 同时半功能密文也可以被正常密钥所解密, 但是半功能密钥不能解密半功能密文. 在模拟时, 对于敌手的询问和挑战密文, 模拟者不再按照正常的方式来回答, 而是分别回答半功能密钥和半功能密文. 模拟者可以“完美”产生任何半功能密钥和半功能密文, 由于敌手拿到的密钥都是半功能的, 对解密挑战半功能密文没有任何帮助.

Lewko 和 Waters 等人[11]利用对偶系统加密的思想实现了第一个自适应安全的属性加密方案. 该方案建立在合数阶的双线性群上, 在一些合理的假设下可证明安全. 其中包括合数阶上子群判定假设, 该假设要求群的阶数不可被分解. 为了保证这点, 就必须要求群的阶数十分大, 例如, 对于两个素数构成合数, 就需要阶数的长度至少为 1024 bit, 这远远大于目前常用的椭圆曲线阶数, 导致方案效率十分低下. Okamoto 和 Takashima[12]给出了第一个基于素数阶的自适应安全的属性加密方案. 该方案通过基于双线性群的“对偶向量空间”(dual paring vector space)的构造技术, 有效实现了对偶系统加密. 虽然效率比之前合数阶的方案要高得多, 但是相比于选择安全的方案还是存在差距.

3.3 近年来的研究进展

随着一些基本方案的提出和对属性密码学研究的不断深入细化, 近年来研究者们在属性密码学方面又有了许多新的理解和认识, 并提出了一些更深层次的问题和一些新的研究方向, 本节将简要介绍近年来属性密码学的研究热点和成果.

3.3.1 高效属性加密方案的构造

在考虑属性加密机制的效率问题时, 主要存在两个方面的瓶颈, 即通讯代价和计算代价. 在实际应用中, 产生的通讯代价主要由密文长度决定, 而计算代价主要包括加解密算法产生的计算消耗. 而在加解密

②树状访问结构和布尔表达式都可以等同于一般访问结构, 只是在表现形式上有所不同而已.

代价中, 减小解密代价更为重要, 一方面, 由于加解密是一对多的关系, 在系统中解密对于加密而言是一个高频行为. 另一方面, 目前绝大多数属性加密方案都基于椭圆曲线的双线性群, 解密计算中往往都存在双线性对计算, 双线性对计算在实现效率方面要远远低于其他运算(如指数运算). 在传统构造中[1,2,8,9], 密文长度和解密代价往往都与相关属性个数线性相关, 当密文中涉及很多属性时, 效率将会变得很低.

Emura 等人[13]和 Chen 等人[14]考虑了密文长度为常数的属性加密方案, 但方案中加密策略仅能支持与门访问结构. 之后, Herranz 等人[15]提出了一个访问结构支持门限密文为常数的密文策略的属性加密方案, 但访问结构还是不够丰富. Attrapadung 和 Libert[16]首次构造了一个支持一般访问结构的密钥策略的属性加密方案. 该方案的密文长度和解密代价都为常数. 上述方案都只能在选择模型下可证明安全, Chen 等人[17]在自适应安全模型下给出了一个从内积加密到属性加密的通用构造方法, 并通过高效且自适应安全的内积加密方案底层构造, 实现了支持门限访问结构自适应安全的属性加密方案, 该方案密文长度和解密代价都为常数. 最近, Hohenberger 和 Waters[18]从一些经典属性加密方案出发, 通过双线性群上的数学性质, 将方案中解密所需双线性运算次数都减小为常数.

3.3.2 属性加密方案的实用性改进

在属性加密方案中, 按属性的“容量”大小可分为两类: 支持大属性集合的方案和支持小属性集合的方案. 在支持小属性集合的方案中, 所有属性在公共参数建立时就已经确定, 不能额外再加入更多的属性. 而在支持大属性集合的方案中, 方案中可用的属性是“无限”的(超多项式大小), 可以随时加入新的属性. 相比之下, 支持大属性集合的方案更能满足实际需求, 但构造难度也更大. 在最初的一些文献中[2,4]提出了从支持小属性集合方案构造支持大属性集合方案的转化方法, 但是得到的方案却对加密属性个数进行限制. Lew 等人[19,20]首先考虑了属性个数完全不受限制(unbounded)的方案, 但证明较为复杂并且方案的效率也不高. 最近, Rouselakis 和 Waters[21]给出了一个更加“简洁”且高效的构造.

另一方面, 一些属性加密方案限制每个属性在访问结构中至多能出现一次. 当需要属性能够支持访问结构中出现多次时, 常常通过将一个属性用多个“属性”来表示以解决这个问题: 访问结构中第一次出现某个属性, 用“属性 A_1”来表示, 第二次则用“属性 A_2”来表示, 以此类推. 这样做并没有从本质上解决问题, 支持将原来只能出现一次变为只能出现 k 次(k 受公共参数限制). 另外, 这样做将导致效率的降低. Waters[3]首先在选择模型下解决了这个问题, 提出了一个支持属性可以在访问结构中重复出现任意多次的方案. 在证明中, 通过引入一个 q -Parallel BDHE 假设证明了其安全性.而在自适应安全模型下构造这种方案更为困难, 因为在经典对偶系统加密证明中都存在一个统计意义下的假设,而对于属性出现多次的情形, 这个假设不再能被满足, 导致无法完成证明[11,12]. Lewko 和 Waters[22]结合对偶系统加密和选择安全方案[2,3]的证明技巧, 首次在自适应模型下给出了一个支持属性在访问结构中重复出现任意多次的方案.

3.3.3 基于格的属性加密方案的构造

格密码被认为是能够抵抗量子攻击的一种密码机制, 至今不存在可行的量子算法能破解格上的困难问题. 同时, 格上的运算简单, 计算量小, 与传统公钥密码机制相比实现效率高. 基于以上优点, 构造基于格的属性加密方案也是近年来的研究热点问题之一. Agrawal 等人[23]首先基于 LWE 困难问题给出了一个访问策略为门限的属性加密方案. 此外, 还探讨了在基于格上构造支持一般访问结构的困难性. 之后, Zhang 等人[24]将 Agrawal 等人[23]的结果推广至密文策略的属性加密. Boyen[25]在格上给出了第一个支持一般布尔表达式的构造. 最近, Gorbunov 等人[26]将访问结构做到了能够支持一般电路函数, 而以往所有属性加密只能支持 NC1 电路函数, 即电路深度受限. Garg 和 Gentry 等人[27]也利用格上的“多线性映射”(multi-linear maps)给出了一个类似的结果.

3.3.4 属性签名

Maji 等人[28]首先给出了属性签名的概念和安全性定义. 在属性签名中, 签名者通过一条消息和一个策略生成一个属性签名, 验证者通过验证可确认这条消息是否由属性满足这个策略的人所产生. 相比于传

统的属性证明系统(如 U-PROVE 证明[29]), 属性签名还具有更强的匿名性, 即签名验证者通过签名仅能够得知签名者的属性满足签名的策略, 而无法得知其他信息, 包括签名者的属性和身份信息. 同时, 属性签名还具有“不可链接性”(unlinkability)和抗合谋性. 而相比于传统匿名性签名方案(如群签名、环签名), 属性签名还能够提供很丰富的签名策略. Zhang 等人[30]针对文献[28]中的属性签名方案给出了一个伪造攻击, 同时提出了一个新的可证明安全的高效属性签名方案. 对于门限式访问结构 ABS, 给出了一个常数签名长度的属性签名方案. 文献[31–33]中也提出了一些属性签名方案, 这些方案是否安全还有待于进一步研究.

3.3.5 属性安全协议

Ateniese 等人[34]首先提出了一个属性秘密握手机制, 该机制可以看作是属性安全协议的“雏形”. Wang 等人[35]首先提出了属性密钥协商协议的概念并给出了一个基于 BR 模型的构造, 之后 Yoneyama[6]和 Li 等人[36]分别在安全模型、效率、访问策略的灵活性等方面进行了优化改进. 最近, Anada 等人[5]也将属性密码概念推广到身份识别协议(identification)中, 给出了一个属性身份识别协议. 并说明这种协议在云服务的付费服务中有着广阔的应用前景. 在可信计算技术中, 为了实现远程证明的真实性和平台配置的隐私保护使用了一种协议, 人们把这种协议称之为属性证明协议(Property-based Attestation Protocol), 也可以视为这里所讲的属性安全协议. 值得一提的是,可用属性签名来构造属性证明协议.

3.3.6 多属性权威系统

在某些场景下, 单个属性权威的属性密码系统不能满足大规模分布式应用对不同机构协作的需求, 同时, 这个属性权威容易受到集中攻击; 属性权威管理系统中所有属性需要为用户认证属性颁发密钥, 工作量大, 成为系统的性能瓶颈. 多属性权威属性密码系统可由一个中心权威(Certificate Authority, CA)和多个分管不同属性的属性权威(Attribute Authority, AA)组成, 并共同来为每个用户颁发密钥. 在考虑安全性时, 需要考虑属性权威被腐化(corrput)时, 以及不同用户间合谋恢复 AA 的密钥问题. 这是多属性权威属性密码系统的研究难点. Chase 等人[37,38]考虑了如何通过多个中心权威来防止单个权威被腐化的问题, 采用用户全局唯一标识(Globally Unique Identifier, GUID)的方法, 防止了用户间的合谋. 为避免使用 CA 带来的安全脆弱性, Lewko 等人[39]首先考虑了“分中心”的场景, 在这样一个场景中, 不再存在 CA, 用户可以根据实际情况来选择相信某些 AA, 并用这些 AA 颁发的属性来进行加密或使用他们所颁发的密钥. 之后, Liu 等人[40]在标准模型下给出了一个实现.

4 属性密码学研究展望

就目前属性密码学发展现状和当今研究中存在的一些不足, 本节将给出一些我们认为需要进一步研究解决的问题.

4.1 密钥和属性撤销

在一个属性密码机制中, 随着时间流逝, 由于用户权限发生变化以及密钥泄露等因素存在, 不可避免地要考虑密钥和属性的撤销问题. 在最初的文献[2,3]中, 给出了一个解决方法, 其解决思路是: 通过给每个用户颁发一个额外的终止日期的属性, 来限制密钥的使用时间. 之后, 也有一些工作进一步考虑了密钥撤销问题, 但所采用的更新方式都不能满足实际应用需求. 在更新密钥时, 密钥更新机构的工作量与系统中用户数量线性相关, 并且还要求密钥更新机构与每个用户之间存在一个安全信道.

为了减小密钥更新机构的负担, 消除加密方与密钥更新机构的协调, Sahai 等人[41]采用二叉树思想, 将每个用户设置为与二叉树的叶节点相关, 使得密钥更新数量与用户数量呈对数关系, 并结合“密文代理”(ciphertext delegation)的性质, 提出了一个高效的可撤销的属性加密方案. 在该方案中, 权威机构只需要定期发送一个更新密钥的广播, 即可完成密钥的更新, 并不需要用户与权威机构间进行交互或存在安全信道. 但是, 这种撤销本质上是对用户密钥的完全撤销, 在现实中, 常常需要对用户属性进行细粒度撤销而不是撤销用户所有权限, 例如, 用户身份的变化导致其不再拥有某个属性. 此外, 还存在另一种撤销场

景, 称之为“直接撤销”, 即由一个可信第三方公布撤销用户的名单, 用户在加密时直接排除被撤销用户来进行撤销. Atrapadung 等人, Li 等人[42]和 Wang 等人[43,44]针对这一问题进行了深入研究和探索, 取得了一些重要进展, 但在效率方面还有待于进一步提升和改进. 另外, 在如何防止用户滥用密钥, 即追踪那些公开自己密钥的用户的问题上, Liu 等人[45,46]分别在黑盒和白盒追踪场景下给出了一些结果, 该结果具有实际意义, 但仍然存在很大的改进空间, 这是由于所提出的方案的公共参数和代价都与系统用户数量相关, 这在一定意义下违背了属性密码的初衷. 如何让系统用户数量不受限制以及提高系统的效率, 使得其不与系统用户数量相关, 都是未来需要解决的问题.

4.2 隐藏加密策略

在属性加密中, 出于隐私性考虑, 有时加密者需要将自己的加密策略进行隐藏. 同时, 隐藏策略的属性加密在可验证外包计算中也有着重要作用[47]. 在身份加密和内积加密[48]中, 这些问题已经得到了较好的解决, 并已有很多高效的构造. 而对于属性加密而言, 密文中常常会泄露密文策略的信息. 虽然已有一些工作考虑了对加密策略的隐藏, 但访问结构只能支持与门或只能部分隐藏访问结构[49]. 对于较为丰富的访问结构, 实现策略的隐藏具有很大难度, 因为在现有的构造中, 都要求解密时输入加密策略, 而密文的策略一旦被隐藏, 解密者将无法完成解密. 如何更好的实现隐藏策略的属性加密机制, 也是另一个目前尚未很好解决的难题.

4.3 优化密文策略的属性加密方案构造

相比于密钥策略的属性加密, 目前密文策略的属性加密构造还有很多不足. 在密文长度方面,现有方案还无法将密文做到常数并同时能够支持一般访问结构. 具体而言, 在密文策略的属性加密中, 如果密文中访问结构复杂, 会导致密文很难通过某种方式进行“压缩”或“聚合”. 另外, 在安全性证明方面, 文献[4]中提出的密文策略的属性加密分别基于 n -BDHE 和 n -parallel BDHE 假设, 这些都不是标准的假设, 虽然也给出了一个基于标准假设(DBDH 假设)的构造, 但是方案效率太过低下, 密文长度与相关属性的个数呈二次相关, 并且访问结构还受到限制. 之后, Okamoto 和 Takashima 虽然给出了基于 DLIN 假设的构造[12], 但是该方案的访问结构同样受限, 每个属性在访问结构中只能出现一次. 迄今为止, 在密文策略的属性加密中, 还不存在访问结构不受限制且基于标准假设或密文长度为常数的密文策略的构造. 这些都是很具有挑战性的研究问题.

4.4 更为高效实用的属性密码方案构造

在目前属性密码构造中, 由于访问结构的复杂性, 方案的计算代价和通讯代价往往都比较高. 虽然现有工作已经在效率方面进行了一些提高, 如减小密文长度、减少计算量等, 但对于实际应用, 无论是现有的属性加密方案还是属性签名方案或属性安全协议, 都还远远不够高效, 无法为实际所用. 而现有的绝大多数工作都是在标准模型下进行构造, 而如果考虑一些较强的假设, 如随机预言模型、一般群模型, 或者通过适当降低原有安全需求, 如限制敌手询问密钥次数或允许敌手一定程度的合谋, 通过这些安全性的“放松”, 是否能有更加高效的构造? 因为在某些实际应用场景中, 这些假设和安全性都是可以接受的.

5 结束语

属性密码学是一个较新的研究方向, 它拥有许多良好的性质, 能够有效实现细粒度的非交互访问控制机制, 并在许多领域具有良好的应用前景[2,3,5,47,50]. 虽然在理论研究方面已经取得了丰硕的成果, 但就目前而言还并没有得到广泛的实际应用. 作者团队近几年非常关注属性密码学的研究与应用, 在理论研究方面, 尽力完善属性密码学的理论体系, 取得了一些比较好的理论结果; 在应用研究方面, 结合跨域和匿名认证、细粒度访问控制等技术以及云计算、可信计算等应用环境进行了实用性研究, 给出了一些比较实用的解决方案. 由于篇幅所限, 这里就不再罗列和赘述作者团队的这些研究成果. 本文从作者的认识深度

和角度, 系统地介绍了属性密码学的研究背景、发展历程、主要研究方向、重要结果和当今存在的一些问题. 关于属性密码学 2005 年至 2010 年的研究状况亦可参阅文献[51,52]. 对可信计算技术中研究的属性证明协议感兴趣的读者可参阅文献[53]. 希望能够通过同行们的共同努力, 进一步解决当前存在的瓶颈问题, 使得属性密码学能够得到更大的发展, 能够真正为实际所用.

References

[1] Sahai A, Waters B. Fuzzy identity-based encryption[C]. In: Advances in Cryptology-EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457–473.

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006: 89–98.

[3] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems[C]. In: ACM Conference on Computer and Communications Security-CCS 2006. 2006: 99–112.

[4] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]. In: Public Key Cryptography-PKC 2011. Springer Berlin Heidelberg, 2011: 53–70.

[5] Anada H, Arita S, Handa S, et al. Attribute-based identification: definitions and efficient constructions[C]. In: Information Security and Privacy. Springer Berlin Heidelberg, 2013: 168–186.

[6] Yoneyama K. Strongly secure two-pass attribute-based authenticated key exchange[C]. In: Pairing-Based Cryptography-Pairing 2010. Springer Berlin Heidelberg, 2010: 147–166.

[7] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]. In: Advances in Cryptology-CRYPTO 2001. Springer Berlin Heidelberg, 2001: 213–229.

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]. In: IEEE Symposium on Security and Privacy, 2007- SP'07. IEEE, 2007: 321–334.

[9] Cheung L, Newport C. Provably secure ciphertext policy ABE[C]. In: Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 456–465.

[10] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]. In: Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009: 619–636.

[11] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]. In: Advances in Cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 62–91.

[12] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption[C]. In: Advances in Cryptology-CRYPTO 2010. Springer Berlin Heidelberg, 2010: 191–208.

[13] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[M]. In: Information Security Practice and Experience. Springer Berlin Heidelberg, 2009: 13–23.

[14] Chen C, Zhang Z F, Feng D G. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost[M]. In: Provable Security. Springer Berlin Heidelberg, 2011: 84–101.

[15] Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption[C]. In: Public Key Cryptography-PKC 2010. Springer Berlin Heidelberg, 2010: 19–34.

[16] Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts[C]. In: Public Key Cryptography-PKC 2011. Springer Berlin Heidelberg, 2011: 90–108.

[17] Chen C, Chen J, Lim H W, et al. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures[C]. In: Topics in Cryptology-CT-RSA 2013. Springer Berlin Heidelberg, 2013: 50–67.

[18] Hohenberger S, Waters B. Attribute-based encryption with fast decryption[C]. In: Public-Key Cryptography-PKC 2013. Springer Berlin Heidelberg, 2013: 162–179.

[19] Lewko A, Waters B. Unbounded HIBE and attribute-based encryption[C]. In: Advances in Cryptology-EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 547–567.

[20] Okamoto T, Takashima K. Fully secure unbounded inner-product and attribute-based encryption[C]. In: Advances in Cryptology-ASIACRYPT 2012. Springer Berlin Heidelberg, 2012: 349–366.

[21] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption[C]. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013: 463–474.

[22] Lewko A, Waters B. New proof methods for attribute-based encryption: achieving full security through selective techniques[C]. In: Advances in Cryptology-CRYPTO 2012. Springer Berlin Heidelberg, 2012: 180–198.

[23] Agrawal S, Boyen X, Vaikuntanathan V, et al. Functional encryption for threshold functions (or fuzzy IBE) from lattices[C]. In: Public Key Cryptography-PKC 2012. Springer Berlin Heidelberg, 2012: 280–297.

[24] Zhang J, Zhang Z F, Ge A J. Ciphertext policy attribute-based encryption from lattices[C]. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012: 16–17.

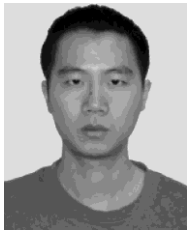
[25] Boyen X. Attribute-based functional encryption on lattices[M]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2013: 122–142.
[26] Gorbunov S, Vaikuntanathan V, Wee H. Attribute-based encryption for circuits[C]. In: Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing. ACM, 2013: 545–554.
[27] Garg S, Gentry C, Halevi S, et al. Attribute-based encryption for circuits from multilinear maps[J]. IACR Cryptology ePrint Archive, 2013, 2013: 128.
[28] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures[C]. In: Topics in Cryptology-CT-RSA 2011. Springer Berlin Heidelberg, 2011: 376–392.
[29] Credentica web site[EB/OL]. http:. www.u-prove.com.
[30] Zhang Y, Feng D G, Zhang Z F, et al. On the security of an efficient attribute-based signature[M]. In: Network and System Security. Springer Berlin Heidelberg, 2013: 381–392.
[31] Escala A, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model[C]. In: Progress in Cryptology-AFRICACRYPT 2011. Springer Berlin Heidelberg, 2011: 224–241.
[32] Li J, Au M H, Susilo W, et al. Attribute-based signature and its applications[C]. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 60–69.
[33] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model[C]. In: Public Key Cryptography-PKC 2011. Springer Berlin Heidelberg, 2011: 35–52.
[34] Ateniese G, Kirsch J, Blanton M. Secret handshakes with dynamic and fuzzy matching[C]. In: NDSS. 2007, 7: 1–19.
[35] Wang H, Xu Q L, Ban T. A provably secure two-party attribute-based key agreement protocol[C]. In: Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009, IIH-MSP '09. IEEE, 2009: 1042–1045.
[36] Li Q, Feng D G, Zhang L W, et al. Enhanced attribute-based authenticated key agreement protocol in the standard model[J]. Chinese Journal of Computer, 2013, 36(10): 2156–2167.
李强, 冯登国, 张立武, 等. 标准模型下增强的基于属性的认证密钥协商协议[J]. 计算机学报, 2013, 36(10): 2156–2167.
[37] Chase M. Multi-authority attribute based encryption[M]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2007: 515–534.
[38] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption[C]. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, 2009: 121–130.
[39] Lewko A, Waters B. Decentralizing attribute-based encryption[C]. In: Advances in Cryptology-EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 568–588.
[40] Liu Z, Cao Z F, Huang Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[C]. In: Computer Security-ESORICS 2011. Springer Berlin Heidelberg, 2011: 278–297.
[41] Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption[C]. In: Advances in Cryptology-CRYPTO 2012. Springer Berlin Heidelberg, 2012: 199–217.
[42] Li Q, Feng D G, Zhang L W. An attribute based encryption scheme with fine-grained attribute revocation[C]. In: Global Communications Conference -GLOBECOM 2012. IEEE, 2012: 885–890.
[43] Wang P P, Feng D G, Zhang L W. CP-ABE scheme supporting fully fine-grained attribute revocation[J]. Journal of Software, 2012, 23(10): 2805–2816.
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[J]. 软件学报, 2012, 23(10): 2805–2816.
[44] Wang P P, Feng D G, Zhang L W. Towards attribute revocation in key-policy attribute based encryption[M]. In: Cryptology and Network Security. Springer Berlin Heidelberg, 2011: 272–291.
[45] Liu Z, Cao Z F, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions onInformation Forensics and Security, 2013, 8(1–2): 76–88.
[46] Liu Z, Cao Z F, Wong D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay[C]. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013: 475–486.
[47] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: verifiable computation from attribute-based encryption[M]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2012: 422–439.
[48] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[C]. In: Advances in Cryptology-EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 146–162.
[49] Lai J Z, Deng R H, Li Y J. Expressive CP-ABE with partially hidden access structures[C]. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012: 18–19.
[50] Zhang Y, Feng D G. Efficient attribute proofs in anonymous credential using attribute-based cryptography[M]. In: Information and Communications Security. Springer Berlin Heidelberg, 2012: 408–415.
[51] Martin P D. Attribute-based encryption: an overview[EB/OL]. [2014-01-12]. http://pauldmartin.org/2011/12/a-survey-of-attribute-based-encryption/.
[52] Su J S, Cao D, Wang X F, et al. Attribute based encryption schemes[J]. Journal of Software, 2011, 22(6): 1299–1315.

苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299–1315.

[53] Feng D G. Security Protocol-heory and Practice[M]. In: Beijing: Tsinghua University Press, 2011: 477–485.
冯登国. 安全协议——理论与实践[M]. In: 北京: 清华大学出版社, 2011: 477–485.

作者信息

冯登国(1965–), 陕西靖边人, 博士, 研究员, 中国密码学会副理事长. 主要研究领域为信息安全, 可信计算.
E-mail: fengdg@263.net



陈成(1986–), 博士, 主要研究领域为密码学与安全协议.
E-mail: chencheng@tca.iscas.ac.cn

中国密码学会 2014 年会征文通知

中国密码学会 2014 年会(ChinaCrypt2014)将于 2014 年 8 月 27–30 日在河南省郑州市举行. 本届会议由中国密码学会主办, 信息工程大学承办. 会议旨在汇聚国内密码学领域中从事学术研究和应用技术开发的专家教授、研究学者、行业精英、工程技术人员和在校研究生, 共同探讨密码学领域各方向的最新成果、学术热点、学术动态及发展趋势, 促进密码学术界和产业界的相互交流与合作.

为保证本次会议的学术质量, 吸引更多的高水平学术论文, 现面向全国从事密码学研究和信息安全领域的专家学者、科研工作者、工程技术人员以及在校研究生公开征稿.

征文内容涵盖密码学理论和应用的各个分支. 主要征文范围包括: 对称密码、公钥密码、数字签名、杂凑函数、安全协议、密钥管理、量子密码、密码芯片应用、工业智能终端安全、云计算与物联网安全等.

会议将编辑学术年会论文集(不正式出版, 允许再投稿), 投稿论文可以是已向重要学术刊物或国际会议投稿, 或新近发表的研究成果.

论文投稿截止时间: 2014 年 5 月 30 日

论文录用通知时间: 2014 年 7 月 16 日

投稿要求:

1. 通过 E-mail 发送电子稿, 投稿信箱为 crypt2014@163.com;
2. 来稿内容应属于作者本人的科研成果, 数据真实、可靠, 具有较重要的学术价值或推广应用价值;
3. 论文一般不超过 7000 字, 一律用 word 格式排版. 另附作者信息, 包括论文题目、作者、单位、电子邮件、通信地址、电话等;
4. 论文编排顺序 ①标题; ②作者; ③单位; ④中文摘要、关键词; ⑤英文摘要、关键词; ⑥正文; ⑦参考文献;

中国密码学会 2014 年会网站已于 2014 年 1 月 10 日正式运行.

会议网址: http://cacr2014.cacrnet.org.cn/

中国密码学会 2014 年会程序委员会

2014 年 1 月 10 日