可搜索公钥加密原理与设计

方黎明 刘哲 袁瑗 葛春鹏 著

科学出版社

可搜索公钥加密原理与设计

方黎明　刘哲　袁瑗　葛春鹏　著

科学出版社
北京

内 容 简 介

带关键字搜索公钥加密研究在近些年已经取得了不少成果，但是还有很多问题亟待解决。为此，本书首先对带关键字搜索公钥加密自身的安全性问题展开研究，包括无安全信道、陷门撤销、关键字猜测攻击等问题；接着研究了带关键字搜索加密(PEKS)与公钥加密(PKE)结合的方案；最后研究了带关键字搜索加密与条件代理重加密(CPRE)结合的方案。

本书可作为高等院校网络空间安全、信息安全等相关的计算机专业的高年级本科生、研究生的参考用书，也可供从事相关行业的工程技术人员与研究人员参考，还可作为密码学爱好者的参考读物。

图书在版编目(CIP)数据

可搜索公钥加密原理与设计/方黎明等著. —北京：科学出版社，2019.9

ISBN 978-7-03-062058-3

Ⅰ. ①可… Ⅱ. ①方… Ⅲ. ①公钥密码系统-研究 Ⅳ. ①TN918.4

中国版本图书馆 CIP 数据核字(2019)第 168428 号

责任编辑：刘 博 高慧元 / 责任校对：郭瑞芝

责任印制：张 伟 / 封面设计：迷底书装

科 学 出 版 社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京凌奇印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2019 年 9 月第 一 版 开本：720×1000 1/16

2019 年11 月第二次印刷 印张：7 1/4

字数：146 000

定价：80.00 元

(如有印装质量问题，我社负责调换)

前　言

随着云计算技术的迅速发展，越来越多的用户开始将数据迁移到云端服务器，以此避免烦琐的本地数据管理并获得更加便捷的服务。为了保证数据安全和用户隐私，数据一般是以密文的形式存储在云端服务器中，但是用户将会遇到如何在密文上进行查找的难题。可搜索加密(Searchable Encryption，SE)是近年来发展起来的一种支持用户在密文上进行关键字查找的密码学原语，它能够为用户节省大量的网络和计算开销，并充分利用云端服务器庞大的计算资源进行密文上的关键字查找。

近几年，可搜索公钥加密研究已经取得了不少成果，但是还有很多问题亟待解决，相关研究者也提出了许多关于可搜索公钥加密的公开问题。为此，本书首先对可搜索公钥加密自身的安全性问题展开介绍，包括无安全信道、陷门撤销、关键字猜测攻击等问题；接着阐述了可搜索加密与公钥加密结合的方案；最后分别介绍三种可搜索加密与条件代理重加密结合的方案，并详细阐述可搜索加密自身安全性，可搜索加密与公钥加密结合的方案，可搜索加密与条件代理重加密结合的方案。本书吸收了国内外同行的研究方法及成果，并总结了自己的研究及学习成果，从而帮助读者全面了解可搜索公钥加密，由此形成了本书的内容。

本书结构合理，内容清晰，问题与方法相结合，理论与实践相结合，力求内容能够针对实际问题有一定的创新性和实用性。

在本书的研究和形成过程中，感谢我的导师王建东教授的悉心指导和帮助，是他把我引入了这个研究领域。感谢课题组成员刘哲教授、葛春鹏博士和刘亮博士等在本书内容的理论及方法上提出的建议与帮助。感谢领导和同事在本书编写和出版过程中给予的关心和帮助。

本书是在国家自然科学基金面上项目“支持多关键词复杂匹配的可搜索代理重加密研究”(No. 61872181)、国家自然科学基金项目“可搜索公钥加密关键安全性问题的研究”(No. 61300236)和江苏省基础研究(自然科学基金)项目“带多关键字搜索的公钥加密的研究”(No. BK20130809)的资助下完成的。

方黎明

2019 年 5 月

目　录

第1章 绪 论

随着云计算技术的迅速发展，用户数据在第三方存储处理的安全性问题日益凸显，而传统的加密技术无法适应这一特殊环境，很多应用中需要第三方去检测密文中是否含有特定关键字而非解密密文，为解决这一问题，带关键字搜索公钥密码被提出。本章介绍了可搜索公钥加密研究的背景，提出了可搜索公钥加密在云计算环境中的重要性，总结了相关节能协议的研究现状，分析了可搜索公钥加密体制对数据分享与处理的影响和挑战，最后给出了本书的主要研究工作及组织结构。

1.1 研 究 背 景

1949 年，Shannon 发表了题为《保密通信的信息理论》的文章，为密码学的发展奠定了理论基础。到了 20 世纪 70 年代，近代密码学得到了快速发展。70 年代后期，美国国家标准学会正式公布实施了美国的数据加密标准，并批准该算法用于非保密单位及商业上的保密通信。同时，公钥密码思想被 Diffie 和 Hellman 提出，受该思想的启发，公钥密码被提出：由 Rivest 等提出的 RSA 公钥密码体制；基于合数模下求解平方根的困难性的“Rabin 体制”；基于离散对数问题的 ElGamal 公钥密码体制；基于有限域上椭圆曲线加法群离散对数问题的困难性的椭圆曲线密码系统；之后 Koblitz 又对椭圆曲线系统作了推广，提出了超椭圆曲线密码系统。

在公钥密码体制下，通常需要数字证书确认身份。然而，使用数字证书也带来了存储和管理开销的问题。为了克服这个缺点，Shamir 在 1985 年提出了基于身份的密码系统(Identity-Based Cryptosystem)的概念。其主要观点是：使用用户的唯一标识如 IP 地址、电子邮件地址等作为公钥，简化了基于证书的密码系统烦琐的密钥管理机制。

虽然对称加密算法、基于 PKI 的一般公钥加密体制以及基于身份的加密体制对保证数据保密性具有重要价值，但面对新的应用还存在很多不足。在实际应用中，很多时候需要第三方去检测或者验证密文中是否含有某些关键字而非解密密文。例如，在智能电子邮件路由选择中，服务者在收到加密的电子邮件的时候是完全随机的，但服务者需要在不解密电子邮件密文的前提下选择正确的路由。又如，对于安全数据管理来说，在分布式或者云计算环境下，数据通常在加密后由

第三方服务者保存，服务者需要对加密的数据在不解密的条件下进行管理操作，如通过关键字搜索整理文件等。带关键字搜索公钥加密方案真正实现了在不解密的条件下对密文进行是否包含某关键字的测试功能，很好地弥补了传统加密算法的不足。微软研究院密码技术小组的 Kamara 和 Lauter 在题为 *Cryptographic Cloud Storage* 的白皮书中，提出了用带关键字搜索公钥加密技术实现“虚拟的私有云服务”，这是一种由公有云使用带关键字搜索公钥加密技术实现云提供商对加密数据的安全服务，即云服务提供者可以对用户加密数据在不解密的条件下进行搜索，解决了备份、归档、健康记录系统、安全数据交换及电子发掘等安全问题。带关键字搜索公钥加密颠覆了传统加密无法对密文进行直接操作的缺陷，因此对带关键字搜索公钥加密技术进行深入研究具有重要的理论意义和应用价值。

1.2　研究现状及分析

为了实现智能加密电子邮件路由选择，即实现第三方可以检测或者验证密文中是否含有某些关键字而非解密密文，Boneh 等在 2004 年提出了带关键字搜索公钥加密方案(Public Key Encryption with Keyword Search，PEKS)。该方案的基本思想如下：Bob 发送密文 $\tilde{C}[\tilde{C}=(C_{\text{PKE}}\,\|\,C_{\text{PEKS}})=(\text{PKE}(\text{pk}_A,m)\,\|\,\text{PEKS}(\text{pk}_A,w))]$ 给 Alice，其中 pk_A 是 Alice 的公钥，C_{PKE} 是 Bob 用 pk_A 加密的密文消息，w 是 Bob 想附加在邮件中的关键字(如“紧急的”)。Alice 能够通过安全信道提供给服务者一个特定的陷门 T_w(Alice 对某个关键字 w 构造的陷门)，这使得服务者能够测试消息 C_{PEKS} 中所加密的关键字是否和 Alice 所选的关键字 w 相等。即给定密文 $\text{PEKS}(\text{pk}_A,w')$，拥有陷门 T_w 的服务者能够验证等式 $w=w'$。除了知道等式 $w=w'$ 成立与否之外，服务者不知道关于 w' 的更多的消息。简而言之，带关键字搜索公钥加密提供了这样的一个机制：通过提供给服务者关键字的陷门，Alice 能够让邮件服务者测试加密邮件是否含有某个关键字，同时，邮件服务者和除 Alice 之外其他参与方不知道邮件的任何信息。紧随 Boneh 等的开创性工作，Waters 等提出的带关键字搜索公钥加密方案，能够应用于对加密的日志进行关键字搜索，已达到对保密信息审查的目的。Golle 等与 Park 等都提出了允许对加密的数据做连接的关键字查询的方案。Zhang 等提出了更有效支持连接的关键字查询的带关键字搜索加密方案。Boneh 和 Waters 扩展了带关键字搜索公钥加密，使它支持对关键字的连接词、子集、范围比较等进行查询。之后，有学者还研究了带关键字搜索公钥加密和公钥加密(PKE)相结合方案的安全性，以及带关键字搜索公钥加密和代理重加密(PRE)结合方案的安全性。

Baek等发现Boneh等带关键字搜索公钥加密方案需要在接收者和邮件服务者之间建立一个安全信道，这使得带关键字搜索公钥加密方案不太实用，因为接收者和服务者之间需要安全信道意味着接收者不能利用正常的不安全信道，如4G和Wi-Fi，或者至少需要一个安全的SSL连接，这是相当昂贵的。为了解决安全信道问题，Baek等给出了无安全信道的带关键字搜索公钥加密(Secure Channel Free Public Key Encryption with Keyword Search，SCF-PEKS)方案的定义和相应的构造，该方案有时也被称为指定测试者的带关键字搜索公钥加密方案(Searchable Public Key Encryption with Designated Tester，DPEKS)。然而，Baek等的构造依赖于随机预言机，这并不能反映现实世界中的安全性。2007年，Gu等提出了一个更有效的随机预言机模型下的无安全信道的带关键字搜索公钥加密方案。2009年，Rhee等增强了Baek等的安全模型，即允许攻击者获得非挑战密文和陷门之间的关系(即获得测试查询的结果)，并提出了一个增强模型下基于随机预言模型的无安全信道的带关键字搜索公钥加密方案。

在实际应用中，每个人都会使用众所周知的关键字(Low Entropy)，如“紧急的”，附加在加密的邮件中。这个特性导致了带关键字搜索公钥加密的一个重要的攻击，称为关键字猜测攻击(Keyword Guessing Attack，KGA)，在这种攻击中，一个恶意的攻击者能够成功地猜测一些候选的关键字，并且以离线的方式验证他的猜测。通过这种离线的关键字猜测攻击，恶意攻击者能够获得加密邮件的相关信息，从而获得关键字。这个攻击最初是由Byun等在2006年提出来的，他们观察到Merriam-Webseter的学术字典仅仅包含225000个关键字的定义，也就意味着通常的关键字来源于此。更进一步，Byun等还指出了Boneh等的方案不能抵抗关键字猜测攻击。如果在带关键字搜索公钥加密方案中，关键字猜测攻击能够被成功地实施，那么攻击者就能够知道哪个关键字是接收者和发送者所用的关键字。因此，攻击者破坏了带关键字搜索公钥加密方案的安全性。受Byun等工作的启发，Yau等提出了离线关键字猜测攻击一些最新的带关键字搜索公钥加密方案。

尽管带关键字搜索公钥加密体制的研究已经取得不少成果，但是还有很多问题亟待解决，具体问题如下。

(1)标准模型。一个好的加密算法首先应该是安全的，而安全问题的研究首先要归结到安全模型上，恰当的安全模型能够很好地体现安全目标。传统加密系统的安全模型已经被广泛深入地研究，如何把这些安全模型扩展到带关键字搜索公钥加密系统环境中，建立带关键字搜索公钥加密系统安全模型是证明一个带关键字搜索公钥加密算法是否安全的基础。而现有的方案在证明过程中通常会依赖随机预言模型(Random Oracle Model，ROM)来完成，因为在随机预言模型中，哈希

函数通常被理想化为完全随机均匀的，即输入和输出之间不存在确定的关系，证明者可以按需构造，因此容易实现对方案安全性证明。现有的无安全信道的带关键字搜索公钥加密方案都是在随机预言模型下可证安全的。然而，随机预言模型有其局限性，因为存在在随机预言模型下可证安全的但在实际应用时却是不安全的方案。因此，实际应用中迫切需要在标准模型(Standard Model，SM)下可证安全的方案。

(2)安全信道问题。带关键字搜索公钥加密方案中，需要安全信道来传送陷门，但构建安全信道通常需要付出较大的代价，能否在公开信道直接传送陷门呢？

(3)关键字猜测攻击问题。带关键字搜索公钥加密容易遭受关键字猜测攻击，微软研究院密码技术小组的 Kamara 和 Lauter 在题为 *Cryptographic Cloud Storage* 的白皮书中，提出了用带关键字搜索公钥加密技术实现加密的存储服务，同时该文把关键字猜测攻击作为一个影响应用的关键问题。而 Byun 等在 SDM 2006 上把关于构造抗关键字猜测攻击的带关键字搜索公钥加密方案作为公开问题。

(4) Trapdoor 撤销问题。在带关键字搜索公钥加密系统中，接收者根据需要的关键字产生相应的 Trapdoor，并发送给相应的服务者来测试，撤销发送给服务者的 Trapdoor 相当于撤销关键字，而关键字信息大多是不容易改变的，因此 Trapdoor 撤销是带关键字搜索公钥加密系统面临的另一重要难题。在 PKI 系统中，公钥证书起着非常重要的作用，陌生实体能够通过证书验证过程实现互相信任、安全通信。证书通常由权威机构 CA 来签名，在证书的生命周期内绑定用户名和公钥。由于存在用户私钥泄露或者用户工作调动等原因，原有的证书必须被提前废除，因而需要一种高效的证书撤销机制来安全地发布证书状态信息，供用户实体在验证数字证书有效性时查询数字证书状态。在 PKI 体制中，目前提出了许多方案来撤销证书。但是在带关键字搜索公钥加密系统中，这一方法是行不通的。因为一方面实现关键字证书系统需要很大的开销，另一方面接收者并不希望关键字被公开，关键字证书实际上破坏了带关键字搜索公钥加密的安全性。所以，简单而有效的 Trapdoor 撤销方法也是带关键字搜索公钥加密系统必须研究的重要问题。

(5)带关键字搜索公钥加密与公钥加密相结合的安全性问题。通常带关键字搜索公钥加密算法只是加密了关键字，并没有加密实际的消息明文，也就是缺少密文的解密功能。在实际的应用中，需要带关键字搜索公钥加密算法跟公钥加密算法结合。然而，简单的结合会破坏原有公钥密码算法的安全性，例如，一个安全的带关键字搜索公钥加密算法简单结合一个 CCA 安全的公钥加密方案后却不一定是 CCA 安全的加密算法了。同样，Fuhr 和 Paillier 在 ProvSec 2007 会议上提出了一个关于构造标准模型下的可解密的带关键字搜索公钥加密的公开问题。

(6)带关键字搜索公钥加密与条件代理重加密相结合安全性问题。带关键字搜

索公钥加密系统已经得到广泛关注，也在智能电子邮件路由选择和加密数据管理中得到了应用。但在条件代理重加密的应用环境中，需要代理者搜索的关键字与服务器存储的关键字相匹配才能进行重加密，这就需要把重加密与带关键字搜索公钥加密相结合。本书介绍了带关键字搜索的条件代理重加密方案，解决了 Weng 等在 AsiaCCS 2009 年会上提出的关于构造匿名条件代理重加密方案的公开问题。

综上所述，带关键字搜索公钥加密的关键安全问题已经影响了带关键字搜索公钥加密的应用，所以对上述关键问题进行深入研究是非常有意义的。

1.3 本书的主要研究工作及组织结构

1.3.1 主要研究工作

本书针对带关键字搜索公钥加密系统中存在的问题进行深入研究，具体工作如下。

进一步研究带关键字搜索公钥加密体制的安全目标及其数学定义，分析在不同攻击模型下各种安全目标之间的关系；深入研究带关键字搜索公钥加密体制安全性证明常用的两种数学模型，即随机预言模型和标准模型，并研究在这两种模型下进行安全性证明的归约证明方法。

深入研究带关键字搜索公钥加密方案，分析研究现有的方案及其存在的缺陷，解决 Trapdoor 传送的安全信道问题，本书致力于阐述标准模型下无安全信道的带关键字搜索公钥加密方案。

深入研究 Byun 等在 SDM 2006 提出的关于构造抗关键字猜测攻击的带关键字搜索公钥加密方案的公开问题，分析了对已知的带关键字搜索公钥加密方案的关键字猜测攻击类型，并重点研究形式化地定义抗关键字猜测攻击的无安全信道的带关键字搜索公钥加密方案的安全模型，并在这一模型下构造新的加密方案并证明其安全性。

深入研究带关键字搜索公钥加密方案的 Trapdoor 撤销问题，分析现有的方案存在 Trapdoor 无法撤销的缺陷，即带关键字搜索公钥加密方案中接收者在发出 Trapdoor 给服务者之后，无法高效地撤销发送出去的 Trapdoor。本书将重点研究高效安全的 Trapdoor 撤销方式，并致力于构造标准模型下安全的、可撤销的带关键字搜索公钥加密方案。

通常的带关键字搜索公钥加密方案并不提供加解密数据，为满足搜索到带有

关键字的数据后对其解密的应用需要，要把带关键字搜索公钥加密方案和公钥加密方案结合起来，即构造可解密的带关键字搜索公钥加密方案。本书将重点研究可解密的带关键字搜索公钥加密方案，并致力于构造标准模型下安全、高效、可解密的带关键字搜索公钥加密方案。

1.3.2　本书的创新点

本书主要创新点如下。

本书构造了首个标准模型下的无安全信道的带关键字搜索公钥加密方案。另外，Baek 等的无安全信道的带关键字搜索公钥加密方案的安全模型缺少合理的测试查询，本书通过增加这一合理查询增强了安全模型，并提出了在增强安全模型下安全的、新的加密方案。针对关键字猜测攻击，本书给出了抗关键字猜测攻击的无安全信道的带关键字搜索公钥加密方案安全模型的首次形式化定义，并在这一模型下构造了加密方案并证明其安全性。解决了 Byun 等在 SDM 2006 提出的关于构造抗关键字猜测攻击的带关键字搜索公钥加密方案的公开问题。

针对带关键字搜索公钥加密方案中接收者在发出 Trapdoor 给服务者之后，无法高效地撤销发送出去的 Trapdoor 的问题，本书介绍的一种计算复杂性仅为关键字 Trapdoor 个数的对数的撤销方式，很好地解决了 Trapdoor 撤销这一问题。

通常的带关键字搜索公钥加密方案并不提供加解密数据的功能，本书阐述了一种在标准模型下高效的、可解密的带关键字搜索公钥加密方案。

本书将带关键字搜索公钥加密方案与条件代理重加密方案相结合，很好地解决了 Weng 等在 AsiaCCS 2009 年会上提出的匿名条件代理重加密这一公开问题，使得条件代理重加密方案可以实现代理者在不知道关键字的前提下完成关键字匹配搜索并实现重加密。

1.3.3　本书的组织结构

本书的主线如下。

本书针对包含三个关于带关键字搜索公钥加密公开问题的若干个关键问题开展研究。首先针对带关键字搜索公钥加密体制本身的安全问题进行研究，主要工作体现在第 3 章和第 5 章；其次分析带关键字搜索公钥加密与其他加密方案结合的安全问题，如第 4 章分析带关键字搜索公钥加密与公钥加密结合的方案，第 6 章分析带关键字搜索公钥加密与条件代理重加密结合的方案。

本书后续章节的安排如下。

第 2 章首先介绍本书所使用的记号及复杂性假设，其次介绍基于身份加密和

带关键字公钥搜索加密的定义，并重点分析两者的关系，即由匿名基于身份加密方案来构造带关键字公钥搜索加密方案。

第3章首先介绍本书构造的标准模型下安全有效的无安全信道的带关键字搜索公钥加密方案，其次介绍增强的安全模型，最后介绍抗关键字猜测攻击的无安全信道的带关键字搜索公钥加密方案。

第4章主要介绍可解密的带关键字搜索公钥加密方案。

第5章讨论带关键字搜索公钥加密方案中高效地撤销 Trapdoor 的问题。

第6章讨论将带关键字搜索公钥加密方案用在代理重加密方案中，以解决匿名条件代理重加密这一问题。

第7章给出本书的工作总结和对今后进一步研究的展望。

第2章 前沿知识

公钥加密算法是当前应用最广泛的加密算法之一。本章基于已有的理论，介绍了本书用到的记号、双线性对、复杂性假设、可证安全性的基本理论。然后阐述基于身份的加密和带关键字搜索公钥加密，并重点讨论了两者之间的关系。

2.1 记 号

本书使用大写字母命名一个集合，如 $M=\{m_1,m_2,\cdots\}$ 的集合。$|M|$ 为集合的元素个数，$m_1\in M$ 意味着 m_1 是集合 M 的成员。如果 M、R 是集合，$M\subseteq R$ 表示 M 是 R 的子集，$M\subset R$ 表示 M 是 R 的真子集，即 $M\subseteq R$ 且 $M\neq R$。最后，N、R、Z 分别表示非负整数集、实数集、整数集。

函数或映射 $f:M\to R$ 是一种规则，其中 M、R 是集合，对每一个 $m\in M$ 赋值一个精确的 $r\in R$。

当涉及算法时，$S_I(\cdot)$ 表示算法有个输入，$S_I(\cdot,\cdot,\cdots)$ 表示不只一个输入。$Y\leftarrow S_I(x)$ 表示算法 S_I 输入 x 时输出 y。如果 S_I 是概率性的，y 则为一个随机变量。字符 A 表示恶意参与者执行的算法，通常是指攻击者。

最后，$\perp$ 表示算法或协议终止。

2.2 双线性对和复杂性假设

定义 2.1 双线性对(Bilinear Pairings)。

G_1 是阶为素数 p 的循环群，g 为 G_1 中的生成元，G_2 是乘法循环群，且与 G_1 同阶。双线性对是指满足以下性质的映射 $e:G_1\times G_1\to G_2$。

(1) 双线性。对于任意的 $a,b\in Z_p$，$g_1,g_2\in G_1$，有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

(2) 非退化性。任意的 $g_1,g_2\in G_1$，使得 $e(g_1,g_2)\neq I_G$，其中 I_G 为群 G_2 的单位元。

(3) 可计算性。对于任意 $g_1,g_2\in G_1$，存在高效的算法计算 $e(g_1,g_2)$。

可以利用椭圆曲线上的 Weil 对和 Tate 对来构造有效的双线性对。

定义 2.2 DBDH 假设。

$e:G_1\times G_1\to G_2$ 是一个双线性对，定义敌手 B 的优势函数 $\mathrm{Adv}_{G_1,B}^{\mathrm{DBDH}}(\lambda)$ 如下：

$$|\Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc})]=1-\Pr[B(g,g^a,g^b,g^c,e(g,g)^r)]=1|$$

其中，$a,b,c,r\in Z_v$ 是随机选取的。如果对于所有的 PPT(Probabilistic Polynomial-Time)敌手 B，$\mathrm{Adv}_{G_1,B}^{\mathrm{DBDH}}(\lambda)$ 是可忽略的，则 DBDH 假设成立。

定义 2.3 Truncated (Decisional) q-ABDHE 假设。

$e:G_1\times G_1\to G_2$ 是一个双线性对，定义敌手 B 的优势函数 $\mathrm{Adv}_{G_1,B}^{q-\mathrm{ABDHE}}(\lambda)$ 如下：

$$\begin{aligned}&|\Pr[B(g,g^x,\cdots,g^{x^q},g^z,g^{zx^{q+2}},e(g,g)^{zq^{q+1}})]|\\&=1-|\Pr[B(g,g^x,\cdots,g^{x^q},g^z,g^{zx^{q+2}},e(g,g)^r)]=1|\end{aligned}$$

其中，$x,z,r\in Z_v$ 是随机选取的。如果对于所有的 PPT 敌手 B，$\mathrm{Adv}_{G_1,B}^{q-\mathrm{ABDHE}}(\lambda)$ 是可忽略的，则判定性 Truncated q-ABDHE 假设成立。优势函数中上边的分布记为 $P_{q-\mathrm{ABDHE}}$，下边的分布记为 $R_{q-\mathrm{ABDHE}}$。

定义 2.4 强不可伪造一次签名。

强不可伪造一次签名包含一个三元组算法 $\mathrm{Sig}=(G,S,V)$。输入全参数 λ、G 产生一对密钥 $(\mathrm{ssk},\mathrm{svk})$。同时对于任何消息 M，当 $\sigma=S(\mathrm{ssk},M)$ 时 $V(\mathrm{svk},\sigma)=1$，否则 $V(\mathrm{svk},\sigma)=0$。强不可伪造一次签名指任何 PPT 攻击者 A 无法伪造一个新的签名，即使是对已经签名过的消息。

如果下面事件对于任何 PPT 伪造者 F 的发生概率是可忽略的，则 $\mathrm{Sig}=(G,S,V)$ 是一个强不可伪造一次签名：

$$\begin{aligned}\mathrm{Adv}^{\mathrm{OTS}}=\Pr[&(\mathrm{ssk},\mathrm{svk})\leftarrow G(\lambda);(m,\mathrm{St})\leftarrow F(\mathrm{svk});\sigma\leftarrow S(\mathrm{ssk},m)\\&(m',\sigma')\leftarrow F(m,\sigma,\mathrm{svk},\mathrm{St},):V(\mathrm{svk},\sigma',m')=1\wedge(m',\sigma')\neq(m,\sigma)]\end{aligned}$$

其中，St 表示各个阶段 F 所获得的状态信息。

定义 2.5 3-QDBDH 假设。

$e:G_1\times G_1\to G_2$ 是一个双线性对，定义 PPT 敌手 B 的优势函数 $\mathrm{Adv}_{G,B}^{3-\mathrm{ODBDH}}(\lambda)$ 如下：

$$\left|\Pr\left[B\left(g,g^x,g^{x^2},g^{x^3},g^z,e(g,g)^{\frac{z}{x}}\right)\right]=1-\Pr[B(g,g^x,g^{x^2},g^{x^3},g^z,e(g,g)^r)]=1\right|$$

其中，$x,z,r\in Z_p$ 是随机选取的。如果对于所有的 PPT 敌手 B，$\mathrm{Adv}_{G,B}^{3-\mathrm{ODBDH}}(\lambda)$ 是可忽略的，则 3-QDBDH 假设成立。Dodis 和 Yung 证明了这个问题在一般的群上是困难的。

2.3 可证安全性

可证安全性是指协议或方案的安全性可以被“证明”。可证安全性是指先确定

安全协议或方案的安全目标。然后构建一个形式敌手的攻击模型，在攻击模型中定义敌手的攻击能力。对于特定的安全协议或方案，最后将攻破方案的唯一方法归约为破解某个难解的数学问题或者困难性假设。

2.3.1 随机预言模型

很多密码体制都要用到哈希函数，目的是缩短签名消息的长度，并取得完整性与不可抵赖性。随着密码学的发展，密码专家意识到哈希函数在密码系统的安全性中有更重要的作用。即哈希函数在证明过程中被假设为一个随机函数。Fiat 和 Shamir 用上述思想证明了签名方案的安全性。之后，Bellare 和 Rogaway 形式化了这种思想，抽象出随机预言模型。主要思想在于哈希函数首先被认为是随机函数——随机预言机(Random Oracle，RO)。

定义 2.6 随机预言机。

哈希函数 $H:\{0,1\}^n \to \{0,1\}^{k'}$，假设输入为长度为 n 的{0,1}字符串，输出为长度为 k' 的{0,1}字符串，如果满足以下性质。

(1)均匀性。预言机 H 的输出在 $\{0,1\}^{k'}$ 上均匀分布。

(2)确定性。对于相同输入，H 的输出值必定是相同的。

(3)有效性。给定一个输入 x，$H(x)$ 的计算可以在多项式时间内完成，则 H 称为随机预言。

显然，上述函数是一种很强的、虚构的函数。

2.3.2 公钥加密方案的安全性

按照 Naor 的观点，加密方案的安全目标主要有以下两种。

不可区分性(Indistinguishable，IND)安全：给定已知的两个明文，加密者随机地选择其中之一进行加密，攻击者无法从密文中猜出是对哪个明文的加密。

非延展性(Non-Malleable，NM)安全：攻击者无法构造与已给密文相适应的新密文。

接下来介绍公钥密码体制中的几种攻击类型。

针对加密体制，相应的攻击者攻击能力类型，分为如下两类。

(1)选择明文攻击(Chosen Plaintext Attack，CPA)。选择明文攻击的攻击者可以获得公钥信息，并恶意对不同明文进行加密。

(2)选择密文攻击(Chosen Ciphertex Attack，CCA)。选择密文攻击的攻击者可以进行解密查询，即输入密文，获得对应的明文。但是攻击者不能对“挑战密文”进行解密预言机的查询。

进一步可以把攻击分为非适应性攻击和适应性攻击。