公钥密码的实际安全性发展研究

刘亚敏[1,2]　薛海洋[1,2]　张道德[1,2,3]
[1](中国科学院数据与通信保护研究教育中心　北京　100093)
[2](信息安全国家重点实验室(中国科学院信息工程研究所)　北京　100093)
[3](中国科学院大学网络空间安全学院　北京　100080)
(ymliu@is.ac.cn)

On the Development of the Practical Security of Public Key Cryptosystems

Liu Yamin[1,2], Xue Haiyang[1,2], and Zhang Daode[1,2,3]
[1](*Data Assurance and Communication Security Research Center*, *Chinese Academy of Sciences*, *Beijing* 100093)
[2](*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)
[3](*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100093)

Abstract　Public key cryptography is an important primitive in the era of internet, and also is an important tool for protecting the data and communication in cyberspace. Currently, the three basic public key cryptographic algorithms, namely, public key encryption, digital signature and key exchange, are extensively used in various kinds of data systems and network protocols. In this paper, we introduce the definitions and security notions of the three basic public key cryptographic algorithms, especially the development of security notions from theory to practice; we also introduce several representative public key cryptosystems, for example, schemes which are considered as milestones, such as RSA encryption and RSA signature; efficient and practical schemes, such as the Cramer-Shoup hybrid encryption scheme; standardized schemes, such as RSA-OAEP, NTRU, DSA; and promising schemes with post-quantum security, such as Kyber and Frodo. We hope that the paper will benefit the researchers in the area of public key cryptology.

Key words　public key cryptology; public key encryption; digital signature; key exchange; provable security

摘　要　公钥密码是网络时代的重要原语,是保护网络空间中的数据和通信的重要工具.目前,公钥密码的三大类基础算法:公钥加密、数字签名、密钥交换,在各类数据系统和网络协议中被广泛使用.介绍了这3类基础公钥密码算法的定义和安全性概念,尤其是安全性概念从理论到实际应用的发展;着重介绍了一些具有代表性的方案,例如RSA加密和RSA签名这种具有里程碑意义的方案;Cramer-Shoup混合加密这种高效实用的方案;RSA-OAEP,NTRU,DSA这种被标准化的方案;以

收稿日期:2018-10-30
基金项目:国家自然科学基金项目(61502480,61602473,61772515)

及 Kyber,Frodo 这种具有潜力的后量子安全方案,以期对该领域的研究者有所帮助.

关键词 公钥密码学;公钥加密;数字签名;密钥交换;可证明安全

中图法分类号 TP309.7

数据保护与通信安全是信息时代的重要问题,而密码技术是信息安全的基础.从古典的斯巴达加密棍、凯撒密码等开始,传统的对称密码技术已经有数千年历史.在对称密码中,信息的发送方和接收方共享1个相同的密钥.然而,如何安全高效地共享这个密钥成为一大难题.在1976年,Diffie和Hellman[1]发表了具有划时代意义的论文"New Directions in Cryptography",文中所开创的非对称密码学,即公钥密码学,便是这个难题的一种解决之道.Diffie和Hellman也因此获得了2015年的图灵奖.

公钥密码方案使用1对相互关联但不同的密钥,分别称为公钥和私钥.其中的公钥是公开的,任何人都可以得到;私钥由其所有者保密;从公钥得到私钥在计算上是困难的.这样,公钥密码可以实现不同的功能,例如用公钥进行加密、私钥进行解密的公钥加密方案,用私钥进行签名、公钥进行验证的数字签名方案,用私钥和公钥同时参与计算,使会话双方可以建立一个共同密钥的密钥交换方案.目前,公钥密码的三大类基础算法:加密、数字签名、密钥交换,已经成为网络时代保障信息安全的基本原语,在各类数据系统和网络协议中被广泛使用.

对称加密方案的安全性通常以攻击为度量.如果某个算法能够抵抗已知的各种攻击,那么它就被认为是安全的.公钥密码方案的安全性通常由数学困难问题来保证,这使得其安全性可以有2种评估方式:一种是对其具体安全性的分析,包括对其底层的困难问题的分析和具体实现时使用的参数的分析等;另一种是其可证明安全性,即使用归约的方法,在方案的安全性和底层数学问题的困难性之间建立归约,以证明攻击方案的安全性等同于攻击底层困难问题.可证明安全的思想在1984年由Goldwasser和Micali[2]开启,Goldwasser和Micali也因此获得了2012年的图灵奖.

公钥密码自1976年提出,发展迅速,很快就形成了两大类算法:一类的困难性和整数分解问题关联,例如RSA加密/签名方案;另一类的困难性基于循环群上的离散对数问题,尤其是在椭圆曲线上的实现,具有密钥短、运算速度快的优点,例如Diffie-Hellman密钥交换.RSA和椭圆曲线离散对数密码可视为公钥密码领域第1代和第2代的工业标准,在实际应用中已经被广泛部署,例如邮件加密系统的优良保密协议(pretty good privacy, PGP)、网络中的传输层安全协议(transport layer security, TLS)协议、银行优盾等.

1994年Shor[3]提出了1个量子算法,能够高效地分解大整数以及解离散对数问题.这意味着一旦大规模量子计算机被制造出来,基于整数分解和离散对数的传统公钥密码方案就不再安全.因此,能够抵抗量子敌手攻击的后量子公钥密码方案在近20年成为一个研究热点.目前有5类主流的后量子公钥密码:格密码[4]、基于编码的密码[5]、基于散列函数的密码[6]、多变量密码[7]、椭圆曲线超奇异同源密码[8].这些后量子公钥密码的效率已经趋于实用化,将成为公钥密码领域第3代的工业标准.目前,由美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)、国际标准化组织(International Organization for Standardization, ISO)等机构发起的对后量子公钥密码的标准化工作正在开展中,其标准化目标包括加密、签名和密钥交换这3类基础算法.

综上,公钥密码是网络时代的重要原语,是保护网络空间中的数据和通信的重要工具.本文将对3类基础公钥密码算法,即公钥加密、数字签名和密钥交换的定义、发展和实际安全性进行详细介绍.

1 公钥加密

公钥加密(非对称加密)与对称加密类似,都是使用加密算法将明文隐藏在密文中,用解密算法从密文中恢复明文.差别在于:公钥加密的加密

密钥(公钥)和解密密钥(私钥)是不同的,因此称为非对称;而对称加密如高级加密标准(advanced encryption standard, AES),其加密密钥和解密密钥是相同的.

以下首先介绍公钥加密方案的形式化定义.

定义 1. 公钥加密.

一个公钥加密方案通常包含 3 个算法,即 $PKE=(Gen,Enc,Dec)$. 具体介绍如下:

1) 密钥生成算法 Gen. 输入安全参数 1^n,输出 1 对密钥 (pk,sk),其中公钥 pk 为加密算法使用的公钥,sk 为解密算法使用的私钥.

2) 加密算法 Enc. 输入公钥 pk 及明文 m,输出密文 $c=Enc(pk,m)$.

3) 解密算法 Dec. 输入私钥 sk 以及密文 c,输入对应的明文 $m=Dec(sk,c)$.

公钥加密方案的正确性要求是对于任意的安全参数 n,任意由密钥生成算法生成的公私钥对 (pk,sk),任意合法的明文 m,有

$$Dec(sk,Enc(pk,m))=m.$$

1.1 公钥加密的发展

在 Diffie 和 Hellman[1] 的开创性研究论文中提出了公钥加密算法的概念,但是并没有给出公钥加密算法的具体构造. 1977 年,Rivest,Shamir,Adleman 提出的 RSA 加密算法[9],是第 1 个符合 Diffie 和 Hellman 设想的公钥加密算法,他们也因此获得了 2002 年的图灵奖(实际上,英国军方也早已发现并使用了公钥加密算法,只是由于保密原因并未公开).

以下介绍 RSA 加密算法,称为“教科书式 RSA 加密”[10]. 设 $GenRSA$ 是 1 个概率多项式算法,输入安全参数 1^n,输出模数 N 以及 (e,d),其中 N 是 2 个长度为 n-比特的素数的乘积,(e,d) 是 2 个整数且满足 $ed\equiv 1 \bmod \phi(N)$. 图 1 所示为教科书式 RSA 加密方案:

- Gen:输入 1^n 运行 $GenRSA$ 得到输出 (N,e,d). 其中,验证密钥签名私钥 $sk:=(N,d)$.
- Enc:输入公钥 $pk:=(N,e)$ 和明文 $m\in\mathbb{Z}_N^*$,计算密文 $c:=m^e \bmod N$.
- Dec:输入私钥 $sk:=(N,d)$ 和密文 c,计算明文 $m:=c^d \bmod N$.

图 1 教科书式 RSA 加密方案

教科书式 RSA 加密本质上是一个确定性的单向陷门函数. 类似的加密方案还有 1979 年 Rabin[11] 提出的 Rabin 加密. Rabin 加密的安全性能够归约为大整数分解的困难性,是第 1 个可证明安全的加密方案. 而 RSA 方案的困难性和大整数分解之间的关系,还是一个开放问题.

在 RSA 和 Rabin 之后还出现了许多开创性的公钥加密方案的构造,例如基于离散对数的 El Gamal[12] 加密、基于格的后量子公钥加密 Regev[13] 加密等. 这些方案在提出之时并非是最完善的,但是其思想影响深远. 随后的公钥加密标准和候选标准都是对这些方案的扩展和具体实现.

1.2 公钥加密的安全性

单向性是对加密方案最基本的安全要求. 然而对于公钥加密来说,由于加密算法和加密密钥都是公开的,任何人都可以加密. 因此,如果明文来自较小的空间,如教科书式 RSA 加密这样的确定性单向陷门函数便毫无安全性可言:敌手只需将所有明文一一加密,与密文对比,便可确定对应的明文. 1984 年 Goldwasser 和 Micali[2] 提出了概率加密,为公钥加密引入了更强的安全目标:语义安全,即密文能保护明文的每 1 b 信息. 其等同定义是敌手不能区分 2 个已知明文的加密,这一定义被称为“不可区分性”. 由于不可区分性更容易分析,因此得到了更广泛的应用.

概率加密方案中,加密算法是 1 个概率算法. 在公钥和明文之外,加密算法还输入 1 个随机数. 这样,同一个明文可以使用不同的随机数加密成不同的密文. 目前,概率加密是公钥加密的主流做法.

在考虑公钥加密方案所面临的攻击时,自然存在的一类便是选择明文攻击(chosen plaintext attack, CPA),因为敌手可以拿到公钥,自由地加密它所选择的密文. 更强的攻击有选择密文攻击(chosen ciphertext attack, CCA),并且又可以进一步区分为非自适应选择密文攻击(non-adaptive chosen ciphertext attack, CCA1)[14] 和自适应选择密文攻击(adaptive chosen ciphertext attack, CCA2)[15]. 将不可区分性和自适应选择密文攻击结合,可得到一个强安全概念:抗自适应选择密文攻击的不可区分性(indistinguishability against adaptive chosen ciphertext attack, IND-CCA2).

IND-CCA2 安全性是通过一个挑战者和敌手之间的游戏来定义的. 在游戏中,敌手可以访问一个解密谕言. 随后,敌手选择 2 个明文 m_0,m_1,发送给挑战者,并得到 1 个挑战密文 $c^*=Enc(pk, m_b)$,$b\in\{0,1\}$. 在得到挑战密文后,敌手可以继续访问解密谕言(在 CCA1 游戏中,敌手得到挑战密文 c^* 后就不能再访问解密谕言了),但是它不能请求解密挑战密文 c^*. 最后,敌手输出自己对 c^* 所加密明文的判断 b'. 如果 $b'=b$ 则称敌手攻击成功. 这一定义被认为是反映了公钥加密算法在一个复杂的系统中运行的场景.

起初,人们对于选择密文攻击的重要性并没有认识,因为它允许敌手可以有限制地使用解密功能,这在现实中看起来过于强大. 然而在 1998 年,Bleichenbacher[16]使用选择密文攻击对加密标准 PKCS ♯1 V1.5 中带简单填充的 RSA 加密进行了攻击,使人们认识到选择密文攻击的确是实际存在的. 从此,IND-CCA2 成为工业标准中对公钥加密算法的安全性准则. 构造高效率的具有 IND-CCA2 安全性的公钥加密方案也成为一个重要的研究问题.

1.3 实用的公钥加密方案

1994 年 Bellare 和 Rogaway[17]提出了第 1 个高效率的具有 IND-CCA2 安全性的公钥加密方案 RSA-OAEP(optimal asymmetric encryption padding). RSA-OAEP 也成为 PKCS ♯1 V2.0 中的加密标准. 特别地,RSA-OAEP 在随机谕言模型[18]中设计,这种方法也广泛地应用在实用化的签名和密钥交换的设计中.

1998 年,Hoffstein 等人[19]提出了 NTRU 加密方案. NTRU 方案效率很高,并且它的安全性被发现与理想格上的困难问题关联,因此是一种后量子公钥加密方案. 目前,NTRU 已经成为 IEEE P1363 中的加密标准,也是美国 NIST 的候选后量子公钥标准算法之一[20].

曾经在效率方面,公钥加密较之对称加密并没有特别的优势,通常公钥加密运算慢、密文大. 公钥加密的特色在于消息的收发双方不需要复杂的密钥分配,发送方拥有接收方的公钥即可向对方发送加密的消息. 1998 年,Cramer 和 Shoup[21]提出了混合加密(hybrid encryption)体制,即,用公钥算法来加密对称加密算法的密钥,称为“密钥封装”;然后用对称加密方案,使用所封装的密钥来加密明文数据,称为“数据封装”. 混合加密体制本质上是一个公钥加密体制,而兼具公钥加密和对称加密的优点,也是实际中常用的类型. 这样,公钥加密的设计者可以专注于密钥封装部分的设计.

在后量子公钥密码算法标准化项目的推动下,出现了许多高效率的后量子公钥加密算法,除了以上所述的 NTRU 加密,还有来自欧盟后量子旗舰项目的 Kyber[22],Frodo[23]等算法,以及我国研究人员提交的 KCL[24],Lepton[25],LAC[26]等加密算法. 这些算法的计算效率与 RSA 和椭圆曲线加密不相伯仲,只是密钥和密文的长度比传统的公钥加密大,但是也达到了现实可接受的程度.

2 数字签名

数字签名是一种用于呈现数字信息或文档真实性的数学方案,它是公钥版本的消息验证码(message authentication code, MAC). 数字签名具有真实性(消息是由已知的发送者创建的)、不可否认性(发送方不能否认消息是他发送的)、完整性(消息在传输过程中没有被改变)这 3 种性质.

数字签名是大多数密码协议组件的基础元素,比如大家最熟知的安全套接层协议(secure sockets layer, SSL)及其继任者传输层安全协议(transport layer security, TLS),数字签名在其中都扮演着至关重要的角色. 数字签名是电子签名的一种. 在一些国家,如美国和欧盟中的一些国家,电子签名与手工签名具有同样的法律效果.

首先我们介绍数字签名的形式化定义.

定义 2. 数字签名.

数字签名由算法 3 元组构成,具体介绍如下:

1) 密钥生成算法 Gen. 输入安全参数 1^n,输出 1 对密钥(vk,sk),其中 vk 为验证密钥,sk 为签名私钥.

2) 签名算法 $Sign$. 输入签名私钥 sk 以及消息 m,输出签名 $\sigma=Sign(sk,m)$.

3) 确定性验证算法 $Vrfy$. 输入验证密钥 vk、消息 m 以及签名 σ,输出 1 b 信息 b. 若签名是有效的则输出“$b=1$”,若签名是无效的,则输出“$b=0$”. 简记为 $Vrfy(vk,(m,\sigma))=b$.

要求对任意的 n，任意的由 Gen 产生的(vk,sk)，任意合法的消息 m，下面的公式成立：

$$Vrfy(vk,(m,Sign(sk,m)))=1.$$

2.1 数字签名的发展

数字签名的概念也是在 Diffie-Hellman 的开创性研究论文中介绍的，美中不足的是他们也没有给出具体的数字签名方案的构造，但他们推测数字签名方案的存在性基于单向陷门置换函数的存在性.

同样在 1977 年 Rivest 等人[9]实现了第 1 个签名方案，在本文中称之为“教科书式 RSA 签名方案”[10]. 该方案正是基于单向陷门置换而构造的. 教科书式 RSA 签名方案如图 2 所示：

- Gen：输入 1^n，运行 $GenRSA$，得到输出(N,e,d). 其中，验证密钥 $vk:=(N,e)$，签名私钥 $sk:=(N,d)$.
- $Sign$：输入签名私钥 $sk=(N,d)$和消息 $m\in\mathbb{Z}_N^*$，计算签名 $\sigma:=m^d \bmod N$.
- $Vrfy$：输入验证密钥 $vk=(N,e)$，消息 $m\in\mathbb{Z}_N^*$ 以及签名 σ，输出“1”当且仅当 $m\overset{?}{=}\sigma^e \bmod N$.

图 2　教科书式 RSA 数字签名方案

自从教科书式 RSA 数字签名方案后，涌现了大量的数字签名方案. 例如，同样基于单向陷门置换函数的 Rabin[11]签名方案、El Gamal[12]提出的 El Gamal 签名等. 1986 年 Fiat 和 Shamir[27]提出一种“Fiat-Shamir 转换”技术，可以在随机谕言模型中，将一个身份证明方案转化为一个签名方案. Schnorr[28]提出了一个高效的身份证明方案，利用“Fiat-Shamir 转换”得到了一个高效的签名方案，称之为 Schnorr 签名方案. 在这些方案中，使用最多的便是 El Gamal 签名算法的变形 DSA(digital signature algorithm). 1991 年，美国 NIST 建议将 DSA 作为其数字签名标准，并在 1994 年将其纳入 FIPS 186 标准.

2.2 数字签名的安全性

至此，另一个问题出现了，那就是“如何说明这些或者其中一部分签名方案是安全的”. 其实回答这个问题之前还有一个问题——“签名的安全性该如何定义”. 当时，部分学者认为“找到攻击的签名就是不安全的，找不到攻击的签名就是安全的”. 但是这个观点里有个时间点，如果这个时间点是“当前”，那么观点就变成了“(截至目前)找到攻击的签名就是不安全的，(截至目前)找不到攻击的签名就是安全的”. 前半句是正确的，但是后半句就有些难以让人认同. 因为截至目前找不到攻击，但可能在去往找到攻击的路上. 事实上，一些签名方案很容易找到攻击，但是这些签名方案的变种就很难找到攻击. 比如教科书式 RSA，可以很容易伪造出签名：对于消息 m，计算 $m^e \bmod N$ 并将其作为签名，可以看出这就是一个有效的伪造. 但是如果采用“hash-then-sign”技术，即签名之前需要对消息进行散列计算，该教科书式 RSA 的变种签名方案就很难再被找到有效攻击. 由此可见，签名安全性的定义以及证明需要新的理论与技术.

20 世纪 80 年代，大量的密码学者投入到了“可证明安全理论”的研究工作中. 在数字签名的可证明安全理论研究工作中，Goldwasser 等人[29]首先给出了数字签名安全性的定义. 该定义也是通过挑战者和敌手之间的游戏来给出的. 挑战者给敌手模拟签名方案的环境并赋予敌手一定的能力(简称“敌手能力”)，敌手(可以看成一个概率多项式的算法)期望最终达到他的目标(简称“敌手目标”)，比如给出一个有效的签名.

敌手能力分为以下 2 类：

1) 仅知密钥攻击，敌手只知道签名方案的验证密钥.

2) 消息攻击，在敌手试图攻击方案之前，敌手可以检查一些与已知或选择的消息相对应的签名.

根据敌手看到的签名对应的消息是如何选择的，消息攻击分为以下 4 类：

1) 已知消息攻击，敌手可以获得一些消息的签名，但消息是由挑战者选择的；

2) 一般选择消息攻击，敌手可以获得一些消息的签名，而且消息是由敌手在看到验证密钥之前选择的；

3) 直接选择消息攻击，与一般选择消息攻击类似，不过消息是在敌手看到验证密钥之后以及看到任何签名之前一起选择的；

4) 选择消息攻击(adaptive chosen-message attack)，敌手可以在看到验证密钥之后，适应性地选择一些消息然后获得签名. 可以看出，敌手能力是越来越强的.

敌手目标可以分为以下4类：

1）完全攻破. 敌手获得签名密钥.

2）无条件伪造. 敌手可以伪造出任何消息的签名.

3）选择性伪造. 敌手可以伪造出事先选择的消息的签名.

4）存在性伪造(existential forgery). 至少伪造出一个消息的签名，该消息可能是随机的，也可能是以前询问过签名的(在此前况下，签名应该是新的)，可以看出，敌手目标是越来越小的.

根据敌手能力以及敌手目标，签名的安全性可以定义为“敌手目标(不可实现)+敌手能力”，可以简单理解为在此能力的敌手攻击下，敌手攻击签名方案的目标是不可实现的. 可以看出，赋予的敌手能力越强，敌手目标越小，定义的数字签名安全性越强. 那么数字签名最强安全性为：抗适应性选择消息攻击的存在性不可伪造(existential unforgery against adaptive chosen-message attack, EUF-aCMA). 目前该安全性是默认的数字签名安全性的要求. 该安全性的形式化定义如下：

定义 3. EUF-aCMA 安全性定义.

如果对于任意的概率多项式敌手 A，存在可忽略函数 $negl(n)$，使得以下公式成立：

$$Pr[Sig\_forge_{A,\Pi}(n)=1]\leqslant negl(n).$$

那么，我们称该签名方案 $\Pi=(Gen,Sign,Vrfy)$ 是 EUF-aCMA 安全的，其中 $Sig\_forge_{A,\Pi}(n)$ 如图3所示：

签名实验 $Sig\_forge_{A,\Pi}(n)$：
- 运行 $Gen(1^n)$，获得(vk,sk).
- 将验证密钥 vk 发送给敌手 A，并且敌手可以询问签名谕言 $Sign(sk,\cdot)$(该签名谕言是将敌手选择的消息 m 的签名 $Sign(sk,m)$返回给敌手). 最终敌手输出(m^*,σ^*). 设 Q 为敌手 A 询问过签名谕言 $Sign(sk,\cdot)$的消息组成的集合.
- 该实验最终输出“1”当且仅当：
  $Vrfy(vk,(m^*,\sigma^*))=1$ 以及 $m^*\notin Q$.

图3 签名方案的 EUF-aCMA 实验

2.3 数字签名的安全性证明

至此，数字签名的安全性定义已经给出，剩下需要解决的问题是“如何说明提出的所有签名方案或者其中的一部分是安全的”.

Bellare 和 Rogaway[30] 证明采用“hash-then-sign”技术后的教科书 RSA 和 Rabin 变形签名方案是随机谕言模型下 EUF-aCMA 安全的. 随后，Coron[31] 对教科书式 RSA 变形签名方案给出了更紧凑的安全性证明.

Fiat 和 Shamir[27] 声称经过“Fiat-Shamir 转换”得到的签名方案是安全的，但是他们没有给出安全性证明. 随后，Pointcheval 和 Stern[32] 在随机谕言模型下证明了“Fiat-Shamir 转换”的安全性，同时简单声明 Schnorr 签名方案是 EUF-aCMA 安全的. Seurin[33] 于 2012 年给出了详细的 Schnorr 签名方案可证明安全过程.

此外，Pointcheval 和 Stern[32] 说明了原始的 El Gamal 签名方案是不安全的，并且在随机谕言模型下证明了 ElGamal 签名方案的一个变形是 EUF-aCMA 安全的. 该变形的 El Gamal 签名方案与 DSA 签名方案非常类似，但是截至目前 DSA 签名方案的可证明安全还是一个公开问题.

在理论方面，密码学者想利用更弱的密码原语构造具有强安全性的签名方案. 比如 Lamport[34] 利用单向函数构造一次签名方案；Naor 和 Yung[35] 证明单向置换足以构造可以签署任意长度消息的一次性签名，这一点得到了 Rompel[36] 的改进，他证明了只利用单向函数就足够；Merkle[37] 证明了利用一次签名就可以构造出具有 EUF-aCMA 安全性的数字签名方案. 由此可以得出，EUF-aCMA 安全的数字签名方案的存在性可以归结于单向函数的存在性.

综上所述，数字签名的研究已经非常成熟了. 与公钥加密的情况类似，签名领域目前的一个重点研究方向也是后量子签名算法的设计，例如基于格上的困难问题和基于散列函数等. 尤其基于散列函数的签名方案，很有希望成为未来的签名标准算法.

3 密钥交换

密钥交换协议旨在让两方或者多方在不安全的信道上协商共享会话密钥，从而建立安全的加密通信. 为了在公开的、不安全的通信信道中实现安全的通信，1976 年 Diffie 和 Hellman[1] 还提出了著名的 Diffie-Hellman 密钥交换协议. 随后在学术研究中有一系列成果出现，包括实用化方案

的构造与安全性证明；在工业方面也在广泛的应用，例如 TLS，SSL 等协议.

然而基础的密钥交换协议只能提供建立共享密钥的功能，并不能抵抗中间人攻击，同时也不能提供相互认证的安全保障. 后续工作考虑了带认证功能的密钥交换协议[38]，然而和加密方案相比，该协议面对的攻击形式与种类多样而繁杂，给认证密钥交换协议的分析和设计工作带来较大的难度. 本节旨在通过对已有工作的梳理和分析，为认证密钥交换协议的设计和安全性证明梳理出一个清晰的思路和方法.

具体到带认证功能的密钥交换协议，包括两大类：一类是假设交互双方各自具有高熵的私钥，通过与临时私钥的组合生成高熵会话密钥；另外还有一类是基于共享弱口令的认证密钥交换协议，其假设双方只具有弱的共享口令，通过交互生成高熵会话密钥. 本文分别分析这 2 类密钥交换协议的设计方法与安全证明.

3.1 高熵私钥的密钥交换协议

与其他密码方案发展规律类似，密钥交换协议的前期设计工作只进行启发式的安全说明，缺乏严格的安全性证明，具有代表性的就是 MTI 协议[39]和 MQV 协议[40]. 该方法明显和致命的缺点就是不断有新的未预料的攻击出现. 后续研究者逐渐针对认证密钥交换协议提出了一些严格的安全模型，并采用可证明安全的方法证明所设计的方案符合某个安全模型的安全定义，其中具有代表性的就是 HMQV[41]，OAKE[42]等方案.

3.1.1 安全模型

在可证明安全的理论中，安全模型大致分为方案的功能性、敌手攻击能力以及安全目标的刻画. 认证密钥交换协议的安全模型也包含这 3 个要素，只是密钥交换协议有一些自己的特征而已. 针对这 3 个要素分别出现了 BR，CK，eCK，CK＋安全模型，以及基于口令密钥交换协议的 BPR 安全模型.

Bellare 和 Rogaway[43]首次将可证明安全思路引入到密钥交换协议的安全模型中，并提出了 BR 模型系列（包括 BR93 和 BR95 模型）. 不过在 BR 安全模型中敌手的能力有很大的限制，例如不能访问协议参与方的内部状态. 针对此，Canetti 和 Krawczyk[44]提出了 CK 模型，考虑能力更强的敌手，允许敌手访问协议的内部状态. Krawczyk[41]在 2005 年分析了各种针对 MQV 方案的攻击，并在 CK 安全模型的基础上进一步增加敌手的能力，包括分析前向安全性（PFS）、密钥冒充攻击（KCI）等. 后续还有加强的 eCK（扩展）模型[45]和 CK＋模型[46].

3.1.2 学术界构造与工业应用

在高熵私钥认证密钥交换协议的构造方面有两大类：其中一类是使用密码学中的签名、认证码等组件进行的显式认证；一类是隐式认证.

在显式认证密钥交换协议方面的研究比较清晰彻底，其中以 Canetti 和 Krawczyk[44]提出的 SIGMA 协议为主要代表，后续在工业应用标准中，互联网密钥交换协议（Internet key exchange，IKE）、TLS 协议、安全套接层协议（SSL）等基本是在该框架基础上进行优化和改进. 在刚发布的 TLS 1.3 中，删除了对于 RSA 等弱密钥传输方案的支持，并重点考虑了 0-RTT 的前向安全性.

在隐式认证密钥交换协议方面，MQV[40]协议曾被 IEEE Std 1363—2000 纳入为标准协议. 然而后续研究发现各种针对该协议的攻击层出不穷. Krawczyk[41]提出的 HMQV 协议和 Zhao 等人[42]提出的 OAKE 方案等都是后续的改良协议.

3.1.3 后量子安全方案

在面对量子计算机带来的威胁时，由于加密可以使用对称加密方案、签名的验证功能具有时效性，因此密钥交换协议的更新换代最为迫切. 近年在后量子密钥交换协议的设计方面涌现大量的工作，包括基于格、超奇异同源和编码的构造. 基于格困难问题所设计的密钥交换协议[47-48]兼具安全性和高效性，其中 Ding-KE[49]，NewHope[50-51]，Frodo[23]，Kyber[22]最具代表性. Zhang 等人[52]也基于环上带错误的学习问题（ring learning with errors，环 LWE）给出一种类 HMQV 的方案，其满足 BR 安全性与弱前向安全性.

3.2 基于口令的密钥交换

高熵私钥密钥交换协议中假设双方具有高熵的私钥，然而还有一种类型是假设双方共享低熵的口令，适用于服务器客户端的连接情形，其仅通过共享的弱口令进行认证，并协商会话密钥. Bellovin 和 Merritt[53]在 1992 年首次提出基于口令的认证密钥交换协议（password-based authenticated key exchange，PAKE），称为 BM 方案. 后续有很

多对于 BM 方案的改进，直到 2000 年，Boyko 等人[54]提出了基于口令的认证密钥交换协议的安全模型-BPR 模型.

在随机谕言模型下，比较高效且可证明安全的方案是 SPAKE 方案[55]. 在标准模型下，Goldreich 和 Lindell[56]给出了基于单向函数和零知识的解决方案，但是该方案以及后续的理论构造都不实用. Katz 等人[57]借助公共参考串，首次给出可证安全的实用的基于口令的安全方案. Gennaro 和 Lindell [58]在 2003 年把 KOY 方案推广到基于光滑射影散列系统和选择密文安全加密方案的一般性构造. 后续有很多基于该方案的工作，其中文献[59-60]中的方案最为高效.

4 总　　结

本文对 3 类基础公钥算法：加密、签名和密钥交换的定义、实际安全性和发展进行了介绍. 这 3 类基础算法应用最为广泛，且出现在各类工业标准中. 实际上，公钥密码极大地丰富了网络中的各类应用，例如全同态加密可以在云计算中保护隐私，环签名可以用来构建虚拟货币系统等. 本文限于篇幅，对这些并未能详述. 目前，公钥密码的整体发展趋势是转向安全高效的后量子公钥密码方案的设计.

参　考　文　献

[1] Diffie W, Hellman M E. New directions in cryptography [J]. IEEE Trans on Information Theory, 1976, 22(6): 644-654

[2] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and Systems Sciences, 1984, 28(2): 270-299

[3] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring [C] //Proc of FOCS 1994. Piscataway, NJ: IEEE, 1994: 124-134

[4] Ajtai A. Generating hard instances of lattice problems [C] //Proc of STOC 1996. New York: ACM, 1996: 99-108

[5] Berlekamp E R, McEliece R, van Tilborg H. On the inherent intractability of certain coding problems [J]. IEEE Trans on Information Theory, 1978, 24(3): 384-386

[6] Merkle R C. Secrecy, authentication, and public key systems [D]. Stanford: Stanford University, 1979

[7] Patarin J. Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms [G] //LNCS 1070: Proc of Eurocrypt 1996. Berlin: Springer, 1996: 33-48

[8] Feo L D, Jao D, Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [J]. Journal of Mathematical Cryptology, 2014, 8(3): 209-247

[9] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126

[10] 毛文波. 现代密码学理论与实践[M]. 北京：电子工业出版社, 2004

[11] Rabin M O. Digitalized signatures and public-key functions as intractable as factorization [R]. Cambridge: MIT Press, 1979

[12] El Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [G] //LNCS 196: Proc of CRYPTO 1984. Berlin: Springer, 1984: 10-18

[13] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C] //Proc of STOC 2005. New York: ACM, 2005: 84-93

[14] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks [C] //Proc of STOC 1990. New York: ACM, 1990: 427-437

[15] Rackoff C, Simon D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack [G] //LNCS 576: Proc of CRYPTO 1991. Berlin: Springer, 1991: 433-444

[16] Bleichenbacher D. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1 [G] //LNCS 1462: Proc of CRYPTO 1998. Berlin: Springer, 1998: 1-12

[17] Bellare M, Rogaway P. Optimal asymmetric encryption: How to encrypt with RSA [G] //LNCS 950: Proc of EUROCRYPT 1994. Berlin: Springer, 1995: 92-111

[18] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols [C] //Proc of ACM CCS 1993. New York: ACM, 1993: 62-73

[19] Hoffstein J, Pipher J, Silverman J H. NTRU: A new high speed public key cryptosystem [G] //LNCS 1423: Proc of Algorithmic Number Theory (ANTS III). Berlin: Springer, 1998: 267-288

[20] Chen Cong, Hoffstein J, Whyte W, et al. NIST PQ Submission: NTRUEncrypt—A lattice based encryption algorithm [EB/OL]. (2017-11-30)[2018-10-30]. https://www.onboardsecurity.com/nist-post-quantum-crypto-submission

[21] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack [G] //LNCS 1462: Proc of CRYPTO 1998. Berlin: Springer, 1998: 13-25

[22] Bos J W, Ducas L, Kiltz E, et al. Crystals-kyber: A cca-secure module-lattice-based kem [EB/OL]. 2017[2018-10-30]. https://eprint.iacr.org/2017/634.pdf

[23] Bos J W, Costello C, Ducas L, et al. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE [C] //Proc of ACM CCS 2016. New York: ACM, 2016: 1006-1018

[24] Zhao Yunlei, Jin Zhengzhong, Gong Boru, et al. KCL: Key consensus from lattice [EB/OL]. 2017[2018-10-30]. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[25] Yu Yu, Zhang Jiang. Lepton: LPN-based KEMs with post-quantum security [EB/OL]. 2017 [2018-10-30]. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[26] Lu Xianhui, Liu Yamin, Jia Dinging, et al. LAC [EB/OL]. 2017[2018-10-30]. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[27] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems [G] //LNCS 263: Proc of CRYPTO 1986. Berlin: Springer, 1986: 186-194

[28] Schnorr C. Efficient identification and signatures for smart cards [G] //LNCS 435: Proc of CRYPTO 1989. Berlin: Springer, 1989: 239-252

[29] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks [J]. SIAM Journal of Computing, 1988, 17(2): 281-308

[30] Bellare M, Rogaway P. The exact security of digital signatures—How to sign with RSA and Rabin [G] //LNCS 1070: Proc of EUROCRYPT 1996. Berlin: Springer, 1996: 399-416

[31] Coron J. On the exact security of full domain hash [G] //LNCS 1880: Proc of CRYPTO 2000. Berlin: Springer, 2000: 229-235

[32] Pointcheval D, Stern J. Security proofs for signature schemes [G] //LNCS 1070: Proc of EUROCRYPT 1996. Berlin: Springer, 1996: 387-398

[33] Seurin Y. On the exact security of Schnorr-type signatures in the random oracle model [G] //LNCS 7237: Proc of EUROCRYPT 2012. Berlin: Springer, 2012: 554-571

[34] Lamport L. Constructing digital signatures from a one-way function, CSL-98 [R]. 1978 [2018-10-30]. https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf

[35] Naor M, Yung M. Universal one-way hash functions and their cryptographic applications [C] //Proc of STOC 1989. New York: ACM, 1989: 33-43

[36] Rompel J. One-way functions are necessary and sufficient for secure signatures [C] //Proc of STOC 1990. New York: ACM, 1990: 387-394

[37] Merkle R C. A certified digital signature [G] //LNCS 435: Proc of CRYPTO 1989. Berlin: Springer, 1989: 218-238

[38] Diffie W, van Oorschot P, Wiener M. Authentication and authenticated key exchanges [J]. Designs, Codes and Cryptography, 1992, 2(2): 107-125

[39] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key distribution systems [J]. Trans on IECE of Japan, 1986, E69(2): 99-106

[40] Law L, Menezes A, Qu M, et al. An efficient protocol for authenticated key agreement [J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134

[41] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol [G] //LNCS 3621: Proc of CRYPTO 2005. Berlin: Springer, 2005: 546-566

[42] Yao Andrew Chi-Chih, Zhao Yunlei. OAKE: A new family of implicitly authenticated Diffie-Hellman protocols [C] //Proc ACM CCS 2013. New York: ACM, 2013: 1113-1128

[43] Bellare M, Rogaway P. Entity authentication and key distribution [G] //LNCS 773: Proc of CRYPTO 1993. Berlin: Springer, 1993: 273-289

[44] Canetti R, Krawczyk H. Security analysis of IKEs signature-based key-exchange protocol [G] //LNCS 2442: Proc of CRYPTO 2002. Berlin: Springer, 2002: 143-161

[45] Lamacchia B, Lauter K, Mityagin A, Stronger security of authenticated key exchange [G] //LNCS 4784: Proc of ProvSec 2006. Berlin: Springer, 2006: 1-16

[46] Fujioka A, Koutarou S, Xagawa K, et al. Strongly secure authenticated key exchange from factoring, codes, and lattices [G] //LNCS 7293: Proc of PKC 2012. Berlin: Springer, 2012: 467-484

[47] Peikert C. Lattice cryptography for the internet [G] //LNCS 8772: Proc of PQCrypto 2014. Berlin: Springer, 2014: 197-219

[48] Stebila D, Mosca M. Post-quantum key exchange for the internet and the open quantum safe project [EB/OL]. 2016 [2018-10-30]. http://eprint.iacr.org/2016/1017

[49] Ding Jintai, Xie Xiang, Lin Xiaodong. A simple provably secure key exchange scheme based on the learning with errors problem [EB/OL]. 2012 [2018-10-30]. https://eprint.iacr.org/2012/688.pdf

[50] Alkim E, Ducas L, Pöppelmann T, et al. Post-quantum key exchange-a new hope [C] //Proc of USENIX Security 2016. Berkeley, CA: USENIX Association, 2016: 327-343

[51] Alkim E, Ducas L, Pöppelmann T, et al. Newhope without reconciliation [EB/OL]. 2016 [2018-10-30]. http://eprint.iacr.org/2016/1157

[52] Zhang Jiang, Zhang Zhenfeng, Ding Jintai, et al. Authenticated key exchange from ideal lattices [G] //LNCS 9057: Proc of EUROCRYPT 2015, Part II. Berlin: Springer, 2015: 719-751

[53] Bellovin M, Merritt M. Encrypted key exchange: Password-based protocols secure against dictionary attacks [C] //Proc of SP 1992. Piscataway, NJ: IEEE, 1992: 72-84

[54] Boyko V, MacKenzie P, Patel S. Provably secure password authenticated key exchange using Diffie-Hellman [G] //LNCS 1807: EUROCRYPT 2000. Berlin: Springer, 2000: 156-171

[55] Abdalla M, Pointcheval D. Simple password-based encrypted key exchange protocols [G] //LNCS 3376: Proc of CT-RSA 2005. Berlin: Springer, 2005: 191-208

[56] Goldreich O, Lindell Y. Session-key generation using human passwords only [G] //LNCS 2139: Proc of CRYPTO 2001. Berlin: Springer, 2001: 408-432

[57] Katz J, Ostrovsky R, Yung M. Effcient password-authenticated key exchange using human-memorable passwords [G] //LNCS 2045: Proc of EUROCRYPT 2001. Berlin: Springer, 2001: 475-494

[58] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange [G] //LNCS 2656: Proc of EUROCRYPT 2003. Berlin: Springer, 2003: 524-543

[59] Jiang Shaoquan, Gong Guang. Password based key exchange with mutual authentication [G] //LNCS 3357: Proc of SAC 2004. Berlin: Springer, 2004: 267-279

[60] Groce A, Katz J. A new framework for effcient password-based authenticated key exchange [C] //Proc of ACM CCS 2010. New York: ACM, 2010: 516-525

刘亚敏

博士，助理研究员，主要研究方向为公钥密码算法的设计以及可证明安全理论.

ymliu@is.ac.cn

薛海洋

博士，助理研究员，主要研究方向为公钥密码算法的设计以及可证明安全理论.

xuehaiyang@iie.ac.cn

张道德

博士研究生，主要研究方向为可证明安全公钥密码学.

zhangdaode@iie.ac.cn