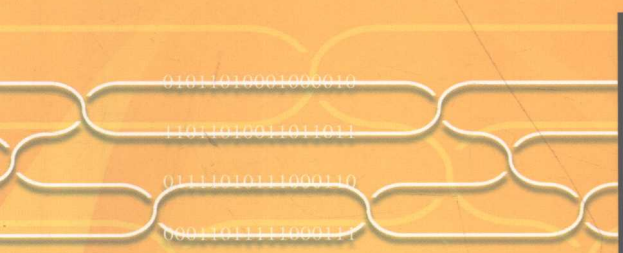
辫群密码体制的设计与分析

王励成 著



科学出版社

辫群密码体制的设计与分析

王励成　著

科学出版社

北京

内 容 简 介

本书围绕最有影响力的非交换密码系统之一——辫群密码体制的设计与分析展开研究，重点分析求解辫群共轭搜索问题的计算复杂度，设计可证明安全的辫群比特承诺协议及若干辫群数字签名方案等，并研究基于辫群的自分配系统及其相应的密码构造问题。

本书可供密码学方向的研究生或相关工程技术人员参考。

图书在版编目(CIP)数据

辫群密码体制的设计与分析/王励成著. —北京: 科学出版社, 2017. 9

ISBN 978-7-03-054570-1

Ⅰ. ①辫… Ⅱ. ①王… Ⅲ. ①密码算法 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字 (2017) 第 234166 号

责任编辑: 王 哲 霍明亮 / 责任校对: 郭瑞芝

责任印制: 张 倩 / 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

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 9 月第 一 版 开本: 720 × 1000 1/16

2017 年 9 月第一次印刷 印张: 8 3/4

字数: 164 000

定价: 55.00 元

(如有印装质量问题, 我社负责调换)

前　言

RSA (Rivest-Shamir-Adleman) 和椭圆曲线密码系统 (elliptic curve cryptosystems, ECC) 是目前使用最为广泛的两类公钥密码系统，它们均以某个交换代数结构作为工作平台，其安全性基础是相应交换代数结构上的某类难题假设。例如，RSA 密码系统假设整数分解问题是困难的，ECC 密码系统假设椭圆曲线离散对数问题是困难的。然而，随着量子计算的发展，基于这些交换代数结构的难题假设不再成立。1994 年，Shor 提出了求解整数分解问题和离散对数问题的量子算法；2003 年，Shor 的量子算法被 Proos 和 Zalka 推广到椭圆曲线上，得到了求解椭圆曲线离散对数问题的量子算法。这些量子算法无论是从其时间复杂度 (包括量子操作及附加的经典计算的时间复杂度) 来看，还是从其空间复杂度 (包括所需的量子位数和附加的经典计算的空间复杂度) 来看，都是很高效的，这些进展对目前仍在广泛使用的公钥密码系统的安全性带来了严重威胁。事实上，密码学家甚至早在 Shor 的量子算法出现之前就已经开始探索新的具有抵抗量子算法攻击潜力的密码。一方面，提出了量子密码、混沌密码、生物密码或 DNA 密码等概念，这些密码系统的安全性直接依赖于特定的物理学或生物学原理，而不再依赖于某个数学难题，因而可以称为“非数学密码”；另一方面，继续探索新型的数学密码，特别是那些既能抵抗量子算法攻击，又能在目前广泛使用的电子计算机上实现的密码。目前，密码界将这类数学密码称为后量子密码 (post-quantum cryptography)。例如，基于格的密码、基于多变量的密码、基于哈希 (Hash) 的密码、基于编码的密码等。

非交换密码也正在努力跻身于后量子密码的行列。非交换密码 (non-commutative cryptography, NCC) 是基于非交换代数结构的密码的简称。首先，从抵抗量子攻击能力上，非交换密码有望做到更高的强度。有几类数学问题当从交换代数结构中过渡到非交换代数结构中时，其求解难度显著增加。特别是，从量子算法的典型框架 —— 隐藏子群问题 (hidden subgroup problem, HSP) 的角度看，目前已经知道如何设计高效的量子算法来求解任意交换群中的隐藏子群问题，但是对于非交换群上的隐藏子群问题，量子求解算法方面的进展还十分有限，有些结果甚至是否定的。其次，密码学研究的数学平台从“交换”拓广到“非交换”是量子计算、组合群论、计算复杂性理论发展到一定阶段后多学科交叉的产物，这种拓广有着深刻的背景和丰富的内涵。从平台选择上，非交换密码拓展了密码学研究的领地。非交换代数结构中有大量的难解问题，为探索新型公钥密码提供了丰富的可供“挖掘”的“矿藏”。在非交换密码研究中，数论、组合群论、代数表示论、拓扑学甚至范畴

论等方面的专家都可以大显身手。菲尔茨奖得主 Atiyah 曾将引入非交换性比喻为“20 世纪代数研究的面包和黄油”。我国著名密码学家曹珍富教授也期待引入非交换性能够成为“21 世纪密码学研究的面包和黄油”。

辫群密码是最有影响力的非交换密码系统之一。自从 Ko 等于 2000 年在美国密码会议上提出完整的基于辫群的公钥密码系统以来，基于辫群的公钥密码系统的发展虽然经历了不少曲折，但目前仍然是公钥密码学研究领域中十分活跃的主题之一。近年来，算法研究方面的进展对辫群密码系统的基础假设 —— 共轭搜索问题困难性假设提出了质疑，但是并未形成任何定论。另外，已经发表的基于辫群的公钥密码方案，具有可证明安全模型者甚少；即使那些底层难题最终被证明是困难的，现有的基于辫群的密码方案也不具备人们所期望的安全属性。因此，本书研究的重点是：其一，分析目前已经发表的典型的求解共轭搜索问题 (conjugator search problem, CSP) 的方法的计算复杂度；其二，研究基于辫群的数字签名体制，设计可证明具有 EUF-CMA(existentially unforgeable under adaptive chosen message attacks) 安全性 (即在自适应选择消息攻击下存在性不可伪造) 的新的签名体制；其三，研究并设计基于自分配系统的密码体制。

本书主要章节安排如下。第 1 章概括性地介绍公钥密码学的发展历史及量子攻击，并从抵抗量子攻击的角度引入本书主题 —— 辫群密码，进而介绍辫群密码系统早期的发展概况和存在的问题。在第 2 章，为求解辫群 CSP 问题的各个典型方法提供具体的算法描述和详细的复杂性分析，指出超级顶点集 (super summit subset, SSS)、极端顶点集 (ultra summit subset, USS) 和 U-轨道之间的关系，并对 USS 方法所宣称的高效性提出质疑。我们的结论是：目前发表的求解辫群 CSP 问题的方法还没有一个能够被证明是可以在多项式时间内完成的。另外，澄清了一些人关于辫群 CSP 难解性和群的小消去条件之间的关系的一个误解。在第 3 章，基于辫群 CSP 困难性假设，设计两个基于辫群的比特承诺方案：一个是标准的比特承诺方案；另一个是推广的非平衡的比特承诺方案。基于辫群实现比特承诺协议有着计算效率和安全性级别两方面的优势。第 4 章主要是围绕辫群数字签名体制的一些工作。首先，提出辫群上的密码学新问题 —— 多一匹配共轭问题，并且基于该问题的困难性假设，对 Ko 等提出的基于辫群的签名体制给出了新的安全性归约，首次证明了一个基于辫群的签名体制具有 EUF-CMA 安全性。其次，提出辫群上的另外一个密码学新问题 —— 共轭连接问题，并且基于该问题的困难性假设，设计了新的基于辫群的数字签名体制。新体制也被证明具有 EUF-CMA 安全性。最后，分别给出了基于辫群的传递数字签名体制和盲签名体制。在第 5 章，设计多个基于自分配系统的密码体制。这是首次系统地从密码设计的角度对自分配系统进行的考察。首先，设计基于 1-型左自分配 (left self-distributive, LD1) 系统的数字签名方案、基于 1-型中自分配 (central self-distributive, CD1) 系统的数字签名方案

和具有部分变色龙属性的哈希函数。其次，提出其他 14 种形式的自分配系统，包括 2-型左自分配 (LD2) 系统、3-型左自分配 (LD3) 系统、4-型左自分配 (LD4) 系统、CD2、CD3、CD4、1-型右自分配 (right self-distributive, RD1) 系统、RD2、RD3、RD4、1-型双边自分配 (bilateral self-distributive, BD1) 系统、BD2、BD3 和 BD4 等。进而，设计基于 2-型中自分配 (CD2) 系统的数字签名方案和基于 1-型右自分配 (RD1) 系统的数字签名方案与认证方案。在第 6 章，作者对辫群密码发展所面临的一些问题以及非交换密码一些新的方向提出一些思考。

本书以作者的博士论文为基础，新增辫群密码近十年的发展和作者近十年来的一些成果，整理而成。因此，本书首先饱含着导师曹珍富教授的辛勤指导和谆谆教诲。记得在我刚完成博士开题答辩的那个中午，当我从食堂返回到实验室时，发现曹老师还没有去吃中饭，他一直在等着告诉我关于“如何解决辫群运算单一对密码构造制约性问题”的突发灵感 —— 这就是我们后来提出的 $\mathbb{Z}$ 模方法。这类场景举不胜举。曹老师对于科学研究的热情，一直鼓励着我坚持钻研辫群密码和非交换密码这类目前还比较偏冷的课题。我的研究也得益于上海交通大学可信任数字技术实验室师兄弟们的相互帮助。例如，曾鹏师弟在辫群基础和小消去条件理论等方面给了我许多帮助，陆荣幸和钱海峰等师兄在可证明安全理论方面则是我的启蒙者。在此一并表示感谢。

本书的出版得到国家自然科学基金面上项目“非交换密码的两个核心问题研究”(批准号：61370194) 的资助。

由于作者水平有限，书中难免有不足之处，恳请广大读者批评指正。

作　者

2017 年 8 月

主要符号对照表

$\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{R}$	分别表示整数、自然数、有理数和实数的集合
$\mathbb{Z}_n$	以 n 为模的剩余类环 $\mathbb{Z}/n\mathbb{Z}$
$\mathbb{Z}_n^*$	$\mathbb{Z}_n$ 中所有对模乘可逆元构成的集合
$\{0,1\}^*$	任意长度的比特字符串集合
$\{0,1\}^n$	长度为 n 的比特字符串集合
1^n	正整数 n 的 1 元表示
$\lvert s\rvert, \lvert\mathcal{S}\rvert$	分别表示字符串 s 的长度、集合 $\mathcal{S}$ 的规模
$a \in \mathcal{S}, a \notin \mathcal{S}$	元素 a 属于 (不属于) 集合 $\mathcal{S}$
$a \in_R \mathcal{S}, a \leftarrow \mathcal{S}$	均匀随机地在集合 $\mathcal{S}$ 中选取元素 a
$a \| b$	a 和 b 的连接
$a \oplus b$	表示相同长度的 a 和 b 按位求异或
$p(n)$	表示 n 的一个多项式
$n!$	n 的阶乘 $(= n(n-1)(n-2)\cdots 1, 0! = 1)$
$\binom{n}{k}$	n 个对象中取 k 个的取法个数 $\left(= \dfrac{n!}{k! \cdot (n-k)!}\right)$
$\exp(1), \mathrm{e}$	表示自然对数的底 $(\exp(1) = \mathrm{e} \approx 2.71826\cdots)$
log	表示以 2 为底的对数，即 $\log_2$
$\neg E$	事件 E 的补事件
$E \cup F$	事件 E 和 F 的和事件，即或者事件 E 发生，或者事件 F 发生
$E \cap F$	事件 E 和 F 的积事件，即事件 E 和事件 F 都发生
$E \subseteq F$	事件 F 包含事件 E，即事件 E 的发生蕴含事件 F 的发生
$\mathcal{O}, \mathcal{O}_{\mathrm{name}}, \mathcal{O}(n)$	分别表示随机预言机，名为 name 的随机预言机和计算复杂度 (可根据上下文区分)
$\Pr[E]$	事件 E 发生的概率
$\Pr[E \mid F]$	事件 F 发生的条件下，事件 E 发生的条件概率

目　　录

第1章 绪 论

1.1 公钥密码学

1.1.1 里程碑

如果说 Shannon 于 1949 年发表的 *Communication theory of secrecy systems* 一文[1] 标志着现代密码学的开端, 那么 Diffie 和 Hellman 于 1976 年发表的 *New directions in cryptography* 一文[2] 则标志着公钥密码学的开端。在公钥密码系统里, 用于加密信息的密钥 (公钥) 与用于解密信息的密钥 (私钥) 是完全不同的。而且要从公钥分析求解出对应的私钥, 在计算上也是不可行的。

虽然 Diffie 和 Hellman 在当时并未构造出具体的公钥密码系统, 但是他们宣布了一个信念: 只要找到合适的单向陷门函数, 就可以构造出公钥密码系统。随后, 他们的工作引起了密码学界的广泛关注。很快, 到了 1978 年, Rivest 等 [3] 就给出了第一个实用的公钥密码体制 —— 即大家最为熟悉的 RSA 体制。近三十多年来, RSA 不断接受实践的考验, 目前仍然是应用最为广泛的密码体制之一。除了 RSA 密码体制, 其他学者基于另外的计算问题提出了大量的公钥密码算法。其中具有代表意义的密码体制有: 基于整数分解的改进 RSA 算法[4] 和 Rabin 算法[5], 基于有限域上离散对数相关难题的 ElGamal 算法[6] 以及目前被普遍看好的基于椭圆曲线的方案 [7–9]。

Diffie 与 Hellman 甚至在正式发表*New directions in cryptography*一文之前, 就发明了数字签名的概念[10, 11]。在一个数字签名系统中, 公钥与私钥的运作顺序正好与公钥密码系统相反, 发送者首先通过自己的私钥对消息进行数字签名, 随后, 当接收者收到消息及其对应的数字签名之后, 利用发送者的公钥来证实这个数字签名的正确性。数字签名可以确保信息的鉴别性、完整性及不可否认性。所谓数字签名的不可否认性是指: 签名的接收者能够证实发送者的身份, 发送者不能否认其曾签署过的签名, 其他任何人不能伪造和篡改签名[11, 12]。

第一个数字签名方案也是由 Rivest、Shamir 和 Adleman 三位密码学家[3] 首先提出的。之后, 数字签名的理论与技术在密码学界受到了广泛的重视。具有代表意义的数字签名体制有基于整数分解问题的改进的 RSA 签名[4] 和 Rabin 签名[13]、基于有限域上离散对数相关难题的 ElGamal 签名方案[6] 及两个著名的变形 ——Schnorr 签名方案[14, 15] 以及美国国家数字签名标准 DSS(digital signature

standard)[16−18]。

在公钥密码体制的密钥生成过程中，通常先随机产生私钥，之后通过私钥产生对应的公钥，这样产生的公钥将是一段随机的乱码，因此如何将公钥与其对应的实体的身份进行绑定就成为一个棘手的问题。为了解决这个问题，Kohnfelder 在 1979 年提出了“公钥证书”的概念[11]。公钥证书通常包含这样的一些内容：由公钥持有实体的身份信息、公钥参数信息，以及由可信第三方 (称为证书权威机构 (certificate authority, CA)) 对该 (证书) 消息的一个数字签名。目前最为流行的基于目录的公钥认证框架是 X.509 证书框架[19]。然而，它的建立和维护异常复杂，且成本昂贵。

1984 年，Shamir[20] 突破基于目录的公钥认证框架的束缚，提出了基于身份的 (identity-based) 公钥密码系统的思想。在这种公钥密码系统的密钥生成过程中，公钥直接为公钥拥有实体的身份信息，因此基于身份的公钥密码系统可以很自然地解决公钥与实体身份的绑定问题。基于身份的密码系统之所以可直接将身份信息作为公钥，是因为在其密钥产生过程中，先由实体的身份信息产生公钥，然后再由公钥产生对应的私钥。在文献 [20] 中，Shamir 基于 RSA 假设[3] 给出了一个基于身份的签名方案。在随后的几年里，其他学者又提出了一些优秀的基于身份的数字签名体制 [21−24]。但是基于身份的加密方案却在很长时间内没有人提出。

Shamir 基于身份的公钥密码系统的思想发表 17 年之后，即到了 2001 年，Boneh 和 Franklin 两位学者[25] 基于双线性配对技术提出了第一个实用的基于身份的密码方案。同年，Cocks[26] 也基于二次剩余理论提出了另外一个基于身份的加密方案。这两个密码方案都完全符合 Shamir[20] 基于身份密码系统的设想。此后，双线性配对技术[27] 成为构造基于身份密码体制的主流，这方面也已经发表了很多优秀的成果 [28−35]。

1.1.2　安全模型

人们对公钥密码系统安全性的研究，是随着对攻击方式理解的逐渐加深而日趋严谨的。最初，人们认识到的攻击手段只有被动攻击，即攻击者只能窃听密文，不能运用自己掌握的数据操纵或修改密文[11, 36]。而且对密码方案的破解方式的认识也仅限于密码体制的完全破解，即已知密码算法及其输出的密文，攻击者的攻击目标是恢复密文对应的完整明文信息；或者攻击者通过对自己选择的明文/密文对的分析，来达到获取密钥的目标。事实上，真实世界中的攻击者不可能那么被动，他们完全有可能对密文进行修改、替换或伪造。至于用“对密码方案的完全攻击”来描述攻击者的行为，在现实世界中更是不可想象的：现实中的攻击者不一定要完全破译窃听到的密文或攻破密钥，也许只要推知密文中的部分信息就可以获得很大的利益。

1982 年，Goldwasser 和 Micali[37] 提出了比特安全性的概念：公钥密码系统

的安全性应该使得密文在遭受被动攻击时不能泄露一比特。他们的想法可形式化描述为[38]：假设攻击者已知两条等长的明文消息 M_0 和 M_1，又已知 c 是这两条明文消息之一的密文，那么该攻击者利用任何概率多项式时间算法来判断 c 是由哪一条明文对应的密文，与同“抛币”的方法猜测相比较，其正确的概率“几乎”一样，或者用他们论文中的说法就是其获得的优势是多项式不可区分的。这个概念又被他们称为语义安全性，或称为选择明文攻击下的不可区分 (indistinguishable against chosen plaintext attack, IND-CPA) 安全。在他们的论文中还有一个非常重要的成果就是引入了“概率加密”的技术，使得相同的明文每次加密后的结果是不一样的，这就有效抵抗了存储密文攻击。

Goldwasser 和 Micali 的成果更正了人们对公钥密码安全性方面的一个错误观念，即攻击者对密码方案的破解方式不仅仅限于完全攻击，因而密码系统安全必须做到比特级别的安全。用语义安全的概念来审视以前的一些公钥密码体制[3, 5, 39]就会发现，这些体制不是语义安全的。幸运的是，关于 RSA 加密函数有一条非常有用的性质：如果一条 RSA 密文是对事先不可猜测的信息进行加密，那么从密文中提取一比特的明文信息就同提取整个明文组一样困难[11, 40, 41]。因此，只要采用合适的概率加密技术，那么这些方案都可以改造为语义安全的方案[41, 42]。

语义安全虽然使人们对公钥密码系统安全性的认识更进了一步，但是，在这个概念中，还是只将攻击者定位在被动攻击的行为上。1990 年，Naor 和 Yung[43] 引入了不可区分选择密文攻击 (indistinguishability against chosen ciphertext attacks, IND-CCA) 安全的概念。在这个概念中，攻击者可以选择自己需要的密文，并得到解密服务，产生相应的明文，即攻击者可以实施选择密文攻击。Naor 和 Yung 还在他们的论文中提到，原本语义安全的一些密码体制[37, 40, 44] 不是 IND-CCA 安全的。

1991 年，Rackoff 和 Simon[16] 提出了一种更强的安全性概念 —— 不可区分适应性选择密文攻击 (IND-CCA2) 安全。在这个概念中，攻击者在得到他感兴趣的密文 c 后，还可以继续获得除 c 之外的解密服务。Rackoff 和 Simon 的成果彻底更正了语义安全概念中所认为的攻击者的被动攻击行为。

2001 年，Boneh 和 Franklin[25] 在基于身份的密码系统环境中给出了基于身份的不可区分选择明文攻击 (ID-IND-CPA) 安全性的概念和基于身份的不可区分适应性选择密文攻击 (ID-IND-CCA2) 安全性的概念，在这些概念中，攻击者除了可以拥有对应的攻击手段，还可以获得针对除了攻击目标用户的其他用户的私钥提取询问服务。

人们对数字签名体制安全性的认识也是逐渐完善起来的。人们对伪造者的攻击手段的认识经历了这样几个过程[11, 45]。

(1) 已知公钥攻击。伪造者在攻击的整个过程中只知道签名人的公钥。

(2) 已知消息攻击。伪造者在整个攻击过程中可以利用一些已经存在的由被攻击的签名人产生的消息/签名对。

(3) 适应性选择消息攻击。在整个攻击过程中，伪造者随时可以得到签名人对由伪造者所选择消息的签名。

同样，人们对签名体制的破解方式的认识也经历过如下几个阶段[5,6,39,45–48]。

(1) 完全破解。伪造者经过整个攻击过程后得到签名人的私钥。

(2) 通用性伪造。发现一个算法，这个算法和签名人的签名算法是等价的。

(3) 选择性伪造。在攻击过程开始之前，伪造者选择了一个目标消息，在攻击过程结束以后，伪造者能够伪造出这个消息的签名。

(4) 存在性伪造。经过整个攻击过程之后，伪造者至少可以伪造出一个消息/签名对 (m, σ)。当然在整个攻击过程中，伪造者没有就消息 m 向签名人询问过签名，而且消息 m 也许是伪造者预先无法知道的，也许是随机的、无意义的，伪造的后果也许对签名人不会构成一点点伤害。

(5) 强存在性伪造。经过整个攻击过程之后，伪造者至少可以伪造出一个消息/签名对 (m, σ)。而且消息 m 也许是攻击者预先无法知道的，也许是随机的、无意义的，伪造的后果也许对签名人不会构成一点点伤害。与存在性伪造不同之处在于，攻击者在攻击过程中可以就消息 m 向签名人询问过签名，但是签名 σ 不能包含在关于 m 的询问结果中。

可以看出，从完全破解到强不可伪造性，对破解的要求是逐渐降低的。人们当然希望数字签名体制在拥有最强攻击手段的攻击者面前也不会以最容易的破解方式遭到攻击①。对于数字签名体制，最基本也最常用的安全性概念是由 Goldwasser 等[45] 于 1988 年提出的：适应性选择消息攻击下的存在性不可伪造 (existential unforgeable against adaptively chosen message attack, EUF-CMA)。这个概念非常适合于现实世界的情况[11]。此后，An 等 [46] 提出了一个更强的数字签名概念，即适应性选择消息攻击下的强存在性不可伪造的数字签名的概念。

2003 年，Cha 和 Choen[31] 与 Dodis 等[49] 分别在 Goldwasser 等的工作基础上，提出了基于身份的适应性选择密文攻击下的不可存在性伪造的数字签名的安全性概念，在这些概念中，攻击者除了具有适应性选择密文攻击的手段，还可以获得针对除了攻击目标用户的其他用户的私钥提取询问服务。

1.1.3　典型的方案构造技术和安全性证明方法

早期的 IND-CCA2 安全的公钥密码方案[16, 43, 50] 都普遍依赖于非交互零知识 (non-interactive zero knowledge, NIZK) 技术，这些方案效率很低，不实用。

① 一些攻击手段与破解方式在概念上是有矛盾的。例如，适应性选择消息攻击和选择性伪造就不能搭配起来。

1991 年，Damgard[51] 摒弃了 NIZK 技术，提出了一个重要的设计方法：为了防止攻击者对密文的篡改，保证密文数据的完整性，可在一般的公钥密码方案中加入验证方程。虽然 Damgard 当时利用这种方法设计的方案只能达到 IND-CCA 安全而不是 IND-CCA2 安全的[52]，但是他的这种设计思想却成为以后设计 IND-CCA2 安全的密码方案的主流思想。随后，许多基于这种思想的密码方案被设计出来，其中 Zheng 和 Seberry[52, 53] 提出采用哈希函数来进行密文的完整性保护的方法，从效率上对 Damgard 的方法进行了非常有意义的改进。

1993 年，Bellare 和 Rogaway 在 Zheng-Seberry 方法的基础上，结合 Fiat-Shamir 的预言机[22] 的思想，提出了在随机预言模型 (random oracle model, ROM) 下证明 IND-CCA2 安全性的方法[54]。他们的工作开辟了密码学可证安全的一个方向，即基于随机预言模型的可证明安全性。

随后，Bellare 和 Rogaway 又在随机预言模型中提出了明文感知 (plaintext awareness，PA) 的概念[55]。他们的思想是：如果一个公钥密码方案是明文感知的，则攻击者得到一个密文蕴涵着此攻击者预先知道这个密文对应的明文。换句话说，如果一个公钥密码方案是 PA 的，那么攻击者得到的解密服务对他的破译工作没有任何帮助，因此如果一个公钥密码方案是 IND-CPA 安全的，而且是 PA 的，那么该密码方案就是 IND-CCA2 安全的。PA 的思想丰富了基于 ROM 的可证明安全性的方法和内容。作为 PA 概念应用的例子，他们在这篇文章中，给出了一个著名的公钥密码方案 RSA-OAEP。这个方案的安全性证明路线就是 IND-CPA + PA $\Rightarrow$ IND-CCA2。然而，他们在当时提出的 PA 的概念并不完善，此证明后来也被 Shoup[56] 找出了漏洞。在 1998 年，他们对 PA 的概念进行了修正[57]。2001 年，Fujisaki 等[58] 采用修正后的 PA 概念证明了 RSA-OAEP 方案确实是 IND-CCA2 安全的。

1998 年，Cramer 和 Shoup[59] 给出了实用的公钥密码方案，并在标准模型下证明了该方案是 IND-CCA2 安全的。所谓标准模型是指安全性的形式化证明只依赖于方案所依赖的单向陷门函数的困难性和单向哈希函数的不可逆性，以及哈希函数的一些其他在真实世界中可以实现的特性。当然，在 Cramer-Shoup 方案提出以前，也有一些基于标准模型下可证 IND-CCA2 安全的方案[16, 50]，但是这些方案都是基于 NIZK 实现的，正如前面所讨论的，这些方案不实用。Cramer-Shoup 方案是第一个实用的基于标准模型的可证明具有 IND-CCA2 安全性的密码方案。此后，Shoup 还提出了这个密码方案的变形[60]。

1999 年和 2000 年，Fujisaki 和 Okamoto 先后发表了两篇文章[61, 62]，给出了通用的而且是比较高效的方法，使得我们可以在 ROM 假设下，对一个 IND-CPA 安全的密码方案进行适当改造，使其具有 IND-CCA2 安全性。2001 年，Boneh 和 Franklin[25] 在提出他们的基于身份的密码方案的时候，其实就使用了 Fujisaki-Okamoto 转换方法。

最近，Shoup[63]、Bellare 和 Rogaway[64] 都对可证明安全的方法进行了系统的总结，尤其对证明过程中所普遍采用的“挑战者 — 模拟器 — 攻击者”之间通过玩游戏 (game playing) 来进行归约的思路进行了深入分析，总结了游戏序列 (game sequence) 定义的一些技巧和原则，使人们对可证明安全的方法和思路有更加系统的认识。特别是，可证明安全方法也已经被广泛地应用于诸如秘密分享 [65]、环签名 [66]、群签名 [67]、代理签名 [68]、盲签名 [69] 等密码体制和协议的安全性证明中。

1.2　量子计算的发展及其对公钥密码学的启示

目前，许多未被攻破的公钥密码体制的安全性假设均依赖于某个特定的计算难题。迄今为止，最典型的两类安全性假设仍然是整数分解难题和离散对数难题，以及它们的某些变种和推广。基于整数分解问题困难性假设的体制，包括 RSA[3]、Rabin-Williams[5, 70]、LUC[71]、Cocks 基于二次剩余的 IBE(identity-based encryption)[4] 等；基于离散对数计算困难性假设的体制①，包括 ElGamal[6]、椭圆曲线密码系统 ECC[7, 9]、二次域理想类群上的密码系统[72, 73]、Boneh 和 Franklin 基于配对的 IBE[25] 等。

然而，量子计算的快速发展，使得这些目前仍然活跃的公钥密码体制面临威胁。1994 年, Shor[74] 提出了大整数分解和离散对数计算的概率量子算法。1995 年, Kitaev[75] 给出了另外一种大整数分解的量子算法。2003 年, Proos 和 Zalka[76] 将 Shor 的量子算法推广到了椭圆曲线上，得到了求解椭圆曲线上的离散对数问题的量子算法。这些算法都具有多项式复杂度②。因此，在量子计算环境下，上述许多现存的未被攻破的公钥密码体制都将土崩瓦解。虽然许多专家预测量子计算机离我们至少还有 20 年的距离，但是这已经足以使我们产生紧迫感：现存的许多密码体制不再固若金汤了。

能否发展新的公钥密码系统，使其可以抵抗已有的量子攻击呢？根据目前的量子计算复杂性理论，人们确实找到了一些计算难题，它们即使到了量子计算时代，也仍然是困难的。人们也基于这些难题，设计了新的公钥密码系统，例如，基于格的公钥密码系统[77] 等。

①基于配对的各类密码体制的安全性也依赖于离散对数计算困难性假设。

②对于量子计算而言，由于量子比特的制备十分昂贵，算法的量子空间复杂度 (即所需要的量子比特的数量) 是首先要考虑的问题。而量子时间复杂度主要是指量子操作 (即对量子寄存器执行测量) 的次数。另外，目前的量子算法都是一种混合机制：即少量的量子操作附加一定的经典计算和推导。因此，一个量子算法具有多项式复杂度的含义是：算法所需的量子比特数以输入问题规模的某个多项式为界。典型地，Shor 算法所需要的量子比特数为 $\mathcal{O}(\log N)$；算法所需要的量子操作次数也以输入问题规模的某个多项式为界。典型地，Shor 算法需要的量子操作次数为 $\mathcal{O}((\log N)^2(\log\log N)(\log\log\log N))$；算法所需的附加经典计算的空间复杂度和时间复杂度以问题的输入规模的某个多项式为界。

2004 年，Lee[78] 提出建议：我们不要把所有的“鸡蛋”都放到一个“篮子”里，而是应该努力寻找新的不同的公钥密码系统的实现平台。现存的公钥密码系统，更多地是以某个特定的有限交换群 (或环、或域) 为基础，尤其是更多地依赖于数论上的某些计算难题。而目前发展起来的几个典型的量子算法，恰恰是专门针对这几个数论问题而设计的。因此，为了抵抗已知的量子算法的攻击，设计非基于数论的甚至非基于交换代数系统的公钥密码体制，不失为有意义的研究思路之一。而且，人们在这方面确实已经做出了一些优秀的工作。例如，基于一般非交换群的密码[79]、基于辫群的密码[80]、基于有限非交换群的 MOR 密码[81]、基于非交换群的同态密码[82]、基于汤普森群 (也是非交换的) 的密码[83]、基于自分配系统的密码[84] 和基于 e 变换的密码[85](后面两者均为非交换的代数系统，且一般不构成群) 等。

2007 年，Cao 等[86] 提出了基于非交换环的公钥密码系统。这篇文章针对一般非交换环，定义了多项式及其赋值的概念，进而提出了其上的密码学难题假设；然后在这些假设之下，给出了 Diffie-Hellman 类型的密钥协商协议和 ElGamal 类型的加密方案。最后，该方法还被推广到了一般的非交换群和非交换半群上。

量子计算也在发展，这些新兴的密码系统，多数并未被证明一定能够抵抗所有的量子攻击，但是有一点是肯定的：现有的量子算法对这些系统尚不构成威胁。

1.3 辫群密码系统简介

基于辫群的公钥密码系统可以说正是 Lee[78] 所建议的“篮子”外面的“鸡蛋”之一。自从 2000 年 Ko 等[80] 提出基于辫群的公钥密码系统以来，基于辫群的公钥密码系统的发展也经历了不少曲折。在辫群密码诞生之初，立刻出现了一个研究辫群密码的小高潮，许多新的体制不断被提出 [79,87–89]。2000 年 ~2007 年, 在美国密码会议、欧洲密码会议、亚洲密码会议等一些重要的密码学会议上, 均有不少关于辫群密码的文章发表 [80,90–92]。然而, 几乎在基于辫群的密码系统诞生的同时，人们就陆续发表了一些分析辫群密码体制的文章 [91–100], 而且算法研究方面的进展也对辫群上的一些基础难题假设提出了质疑 [101–104]。这些都迅速减弱了人们最初寄予辫群密码的热情。但是最近又有不少基于辫群的密码体制的文章出现 [105–109]。尤其是人们已经开始以研究辫群密码体制为起点, 逐渐展开对其他非交换群或半群的考察，以寻求适合构造密码系统的新的数学平台。在这个时候, 我们可以说, 辫群只是非交换群的一个代表。辫群密码已经不仅仅局限于只在辫群上构造密码体制。可以说，目前基于各种非交换群上的共轭搜索问题、求根问题等困难性假设的密码系统都可以称为基于辫群的密码系统。