Broadview
www.broadview.com.cn

安全技术大系

# 中国密码学发展报告2010

中国密码学会 组编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

# 中国密码学发展报告2010

中国密码学会 组编

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

# 前 言

学术，是人类智慧与经验的积累和升华[1]。学术的历史反映了学术发展的内在逻辑。

密码学是一门发展中的交叉学科，《中国密码学发展报告》致力于阐述密码学发展过程中的内在逻辑，以指导和促进我国密码学研究。

从第一期的《中国密码学发展报告 2007》出版以来，密码学的研究经历了很大的变化，我国密码工作者对密码学的认识也在不断深化和提高，每期《中国密码学发展报告》都试图从不同的视角对密码学的最新进展做出独到的观察。

《中国密码学发展报告 2007》着重介绍了密码学基础理论方面的内容，以及在密码学基础理论研究方面的学术热点，这是对密码学的一个全景式的展望。

《中国密码学发展报告 2008》侧重于介绍密码学的另一个重要特点——应用，对密码学应用方面的内容做了全面详细的介绍。特别对当时受人关注的可信计算问题，专门开辟章节进行论述。

《中国密码学发展报告 2009》以密码学中所涉及的数学门类为主线展开，全面深刻地介绍了密码学中所需要的数学基础，以及在和密码学的互动过程中产生的研究成果。

本册《中国密码学发展报告 2010》则瞄准密码学的最新进展，以探索的眼光审视密码学最新、最活跃的研究方向。在密码学深度发展的同时，新的应用和新的思想激发了密码学的新方向。虽然有些研究方向还不是很成熟，但是我们可以看到它们旺盛的生命力，看到它们在顽强地成长。

从生物特征密码学、轻量级密码学、视觉密码学的发展过程中，我们可以看到，现实的需求和实际的需要是怎么刺激密码学发展的。同时也可以看到，“对合适的应用给予合适的安全”的理念是密码学研究中创造力的重要起点。从 DNA 密码、后量子密码等的发展可以看到，新的计算能力对密码学发展的推动。但是，从另一方面我们也可以看到，即使是量子计算机这种强有力的计算工具，也不像有些人想象的那样会成为传统密码学的终结者，因为量子并行计算不能把 NP 问题归结到 P 问题。所谓后量子密码学的发展就是这个事实在密码学中的反映。零知识证明、安全多方计算、同态密码学是近年来发展较快、研究深入的密码学方向，尤其是在零知识证明方面，我国密码学家有着不俗的表现。密码算法公开征集是密码学发展中的一个重要驱动力量，

---

[1] 《犯罪侦查学》，翁里主编，浙江大学出版社，2004 年

对国际上密码算法公开征集活动的体制、机制研究有利于推动和指导我国开展自主密码算法征集活动。

在本册《中国密码学发展报告 2010》中，我们邀请到十多位工作在本学科前沿的中国学者来讲述这些迷人的故事。

一般认为量子计算的发展会对传统密码学产生巨大威胁，因此人们开始关注后量子时代密码学。后量子时代密码学包括两个方面的内容：其一是利用量子信息技术设计量子密码算法和协议；其二是设计抵抗量子计算机攻击的基于经典计算的密码算法和协议。武汉大学张焕国教授等完成的《抗量子密码体制的研究现状》重点介绍了基于 Hash 函数的数字签名、基于纠错码的公钥密码体制、基于格的密码体制，以及多变量公钥密码体制等抗量子密码体制，并指出了一系列值得研究的公开问题。

视觉密码是最近十多年间逐渐发展起来的新型密码学分支，它将传统的一次一密加密方式与图片相结合，并利用人们的视觉直接进行解密。视觉密码具有解密设备简单、视觉解密、秘密共享和无条件安全等特点。中国科学院软件研究所刘峰副研究员完成的《视觉密码学研究进展》详细介绍了视觉密码的原理机制、评价标准，并讨论了当今流行的几种构造方案及各个热点的研究进展。

零知识证明理论在现代密码学中处于基础性地位，中国科学院信息安全国家重点实验室邓燚副研究员完成的《零知识证明理论研究进展》从零知识协议的可合成性、可重置性、并发零知识、精确零知识，以及非交互零知识等方面对零知识证明的最新研究进展进行了介绍。

生物特征密码学是一门涉及生物特征识别技术、密码技术等多学科的交叉学科。生物特征加密同时要考虑安全性、准确率、可用性等多方面的技术指标。中国科学院自动化研究所田捷研究员完成的《生物特征密码学研究进展》介绍了生物特征加密中的一些主流技术及其应用，并对该技术的未来发展进行了展望。

DNA 密码是近年来发展起来的一个新分支，上海交通大学来学嘉教授等完成的《DNA 密码研究综述》介绍了 DNA 计算的基本原理及 DNA 密码的基本概念，界定了 DNA 密码和生物特征密码的区别；同时，详细介绍了 DNADES 对称加密算法、DNA-PKC 非对称加密算法、DNA 一次一密方案、DNA 加密及 DNA 秘密共享方案；讨论了 DNA 密码研究中遇到的困难和问题，并对 DNA 密码的发展前景做了展望。

轻量级密码成为近几年密码学领域的一个研究热点，其原因是 RFID、无线传感器网络应用等实际需求的推动。中国科学院信息安全国家重点实验室吴文玲研究员等完成的《轻量级分组密码研究进展》介绍了轻量级分组密码的研究进展，并重点介绍了自主设计的“鲁班锁”轻量级分组密码算法。同时，对轻量级分组密码算法的实现效

率和安全性等重要指标的评价方法做出了系统全面的总结。

全同态加密的思想源自20世纪70年代，但一直没有被构造出来。直到2009年才由Gentry构造了第一个全同态加密方案，结束了这一密码学领域的悬疑。全同态加密方案在云计算等新环境中的应用是传统密码方案无可比拟的。中国科学院软件研究所周永彬副研究员完成的《同态密码学研究进展》，为读者讲述了这一迷人的密码学故事。

安全多方计算主要解决的问题是两个或者多个参与方共同完成一个任务，其中每个参与方持有保密的私有输入。其目标是正确地完成任务，并且不能泄露各个参与方自己的私有输入。当参与方中的一个或者几个有攻击行为时，要正确地完成任务而同时又保持私有输入的秘密就更加困难。而安全多方计算的理论表明，在合理的条件下，这个看似不可能的任务是可以完成的。中国科学院研究生院徐海霞副教授完成的《安全多方计算》综述了安全多方计算的基本理论及研究进展。包括所需的理论基础、基本设计思想、构造方法，以及当前活跃的研究领域，如对于敌手模型的泛化及全面化的研究、对于协议设计的高效性和广泛适用性的研究等。

密码算法征集是目前产生实用密码算法的最有效的方法，反映了一个国家或地区的综合实力。我国虽然目前还没有启动自己的密码算法征集活动，但是这一天的到来已为期不远。为了参考其他国家的征集活动的经验和教训，我们专门开辟一章论述密码算法征集的发展状况，并邀请中国科学院DCS中心荆继武教授撰写了《密码算法征集评估及标准化发展概况》，概括地介绍了国际上开展的系列密码算法征集活动。

学术的发展需要学术的传承，组织出版《中国密码学发展报告》为我国密码学学术传承奠定了坚实的基础。希望本发展报告能够对密码科研工作者有参考价值。中国科学院DCS中心为本报告的出版提供了资金资助，在此表示感谢！

冯登国

中国密码学会学术工作委员会

2011年3月于北京

# 目　　录

# 抗量子密码体制的研究现状

张焕国*[1,2] 管海明[3] 王后珍[1,2]

1. 武汉大学计算机学院，武汉 430072

2. 空天信息安全与可信计算教育部重点实验室，武汉 430072

3. 中国电子设备系统工程公司通信研究所，北京 100039

E-mail: liss@whu.edu.cn

**摘要**：量子计算机的发展，对目前广泛应用的RSA、ECC 等公钥密码体制构成了严重的威胁，面临量子计算机的挑战，国际上掀起了抗量子计算公钥密码的研究热潮. 本文介绍了常见的几种抗量子公钥密码体制，对这些方案做出了较为详细的评述，并对这一领域的研究与发展给出了展望，同时指出了一系列值得研究的开放问题。

**关键词**：密码学；量子计算；抗量子密码学。

# A Survey of Post-quantumCryptography

Huanguo Zhang[1,2] Haiming Guan[3] Houzhen Wang[1,2]

1. Computer School of Wuhan University, Wuhan 430072, China

2. The Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan 430072, China

3. Chinese Electronic Equipment System Corporation, Beijing 100039, China

**Abstract**: Public key cryptosystems have become a key technology for making the Internet and otherIT infrastructures secure. However, advances in quantum computers threaten to break the currentlyused public key cryptographic algorithms such as RSA. This paper provides a survey of some ofthe quantum resistant public key cryptographic algorithms, and presents more detailed review andprospects of these schemes. Finally, discusses a series of open problem that we need to consider in thefuture.

**Key words**: Cryptography; Quantum Computation; Post-quantum Cryptography.

*本文得到国家自然科学基金项目（批准号：60970115, 60970116, 61003267, 61003268）、国家863高技术研究发展计划项目（批准号：2007AA01Z411）和中国科学院数学机械化重点实验室开放课题（批准号：KLMM0903）资助。

# 1 引言

21 世纪是信息的时代，除了电子信息科学技术继续高速发展之外，量子和生物等新型信息科学正在建立和发展。量子信息科学的研究和发展催生了量子计算机、量子通信和量子密码的出现。历史上，电子计算机一出现，便被用于密码破译。同样，量子计算机一出现也将会用于密码破译。值得注意的是，许多在电子计算机环境下是安全的密码，在量子计算机模型下却是可破译的。

近年来，Shor 算法的研究还在纵向发展[47, 39]，已由量子傅里叶变换推广到一般情况下的 HSP 问题（Hidden Subgroup Problem），绝大数能归结到 HSP 的公钥密码方案均不能抵抗量子计算机的攻击[66]，包括 RSA、ElGamal 和 ECC。这意味着一旦量子计算机走向实用，那么目前这些广泛应用的公钥密码体制将遭受致命攻击。

美国、日本等国正在加紧研发量子计算机。例如，美国早已认识到量子计算机的战略意义，并已率先投入了巨大资金、启动了 5 个量子计算研究计划：美国国防高级研究计划局的“量子信息科学和技术发展规划”，美国国家安全局的 ARDA5（Advanced Researchand Development Activity）计划；美国科学基金会的 QuBIC（Quantum and BiologicallyInspired Computing）计划；美国宇航局的 Quantum Computing Technology Group 计划；以及美国国家标准与技术研究院的 Physics Laboratory Quantum Information 计划。上述这些计划正在加紧进行，但具体进展情况严格保密。根据公开的资料信息，目前量子计算机的研发工作已取得了突破性的进展，如 2001 年 IBM 公司率先研制成功了 7 量子比特的示例性量子计算机[94]、2008 年加拿大 D-wave 公司宣布研制成功 48qubit 量子计算机系统[46]。我国在量子计算和量子通信领域的研究起步不晚、成果喜人。例如，2007 年中科大潘建伟教授领导的团队，在国际上首次利用光量子计算机实现了 Shor 量子分解算法，该研究成果发表在美国权威物理学期刊《Physical Review Letters》上[65]，标志着我国光学量子计算研究达到了国际先进水平；2010 年他们与清华大学组成的联合小组成功实现世界上最远距离（16 千米）的量子隐形传态，比此前的世界纪录提高了 20 多倍；2010 年 6 月 1 日出版的《自然·光子学》杂志以封面论文形式发表了这一研究成果，该实验结果首次证实了在自由空间进行远距离量子隐形传态的可行性，向全球化量子通信网络的最终实现迈出了重要一步。

这些研究成果充分表明，量子计算机进入实用化阶段只是时间早晚而已，经典密码算法面临的危机是客观存在的。面对量子计算机的潜在威胁，如何设计能够抵御量

子计算攻击的密码算法值得我们深入研究。国外为应对量子计算机的挑战，提出了“抗量子密码学”（Post-Quantum Cryptography）的新学科方向[1]，并于 2006 年成功举办了抗量子计算密码学的国际学术会议 PQCrypto2006，目前，抗量子计算密码学的国际学术会议已成功举行三届，对该领域的理论研究起到了很好的推动作用。近年来，大量相关文献不断涌现，国际上掀起了抗量子计算密码的研究热潮。

## 2 量子计算与经典密码学

20 世纪后期，量子计算作为量子力学和计算机科学相结合的产物，受到人们的广泛关注。1985 年 Deutsch 做了开拓性的工作，提出了第一个量子计算机的设计模型、定义了量子图灵机[27]。特别是 Shor 算法和 Grover 算法的提出，引起量子计算理论技术的研究高潮。本节将简要介绍这些量子算法基本原理及其经典密码体制（包括 RSA、ElGamal 和 ECC）所构成的威胁。

### 2.1 经典密码的量子破译算法

目前针对密码破译的量子计算机算法主要有两种：Shor 算法和 Grover 算法。1994 年 Shor 提出了大整数因子分解的 Shor 量子算法[91]，具体的分解过程如算法 1 所示。

算法 1：因子分解的量子算法（Shor 算法）

Input：大整数 $N$。

Output：$N$ 的因子。

Step1：如果 $N$ 为偶数，则输出因子 2；

Step2：随机选取 $a$（$1 < a < N-1$），若最大公因子 $\gcd(a,N) > 1$，则输出 $\gcd(a,N)$；

Step3：利用量子算法求出函数 $f(x) = a^x \bmod N$ 的周期，记为 $r$；

Step4：若 $r$ 为偶数且 $a^{r/2} \neq -1 \bmod N$，则计算 $\gcd(a^{r/2}-1,N)$ 和 $\gcd(a^{r/2}+1,N)$，二者至少有一个必为 $N$ 的因子。

[1]注：国内一些学者将“Post-Quantum Cryptography”翻译成“后量子密码学”，我们认为将其翻译为“抗量子密码学”更加贴切。同时，本文将所有能抵御量子计算机攻击的公钥密码体制(见2.2节)，称之为“抗量子公钥密码体制”

Shor 算法的基本思想就是将整数因子分解问题转化为求模指数函数 $f(x) = a^x \bmod N$ 的周期问题。随机选取 $a(1 < a < N-1)$，采用 Euclid 扩展算法计算整数 $a$ 和 $N$ 的最大公因子 $\gcd(a,N)$（算法 1 中第 2 步），如果 $\gcd(a,N) > 1$，则成功找到 $N$ 的因子。但绝大部分 $a$ 与 $N$ 是互素的，根据 Euler 定理，此时必存在正整数 $r$ 使得

$$a^r = 1 \bmod N \tag{1}$$

假如 $r$ 已经求出（由后面将要介绍的量子计算得到）且 $r$ 为偶数，则(1)式可写成

$$(a^{r/2}-1)(a^{r/2}+1) = 0 \bmod N \tag{2}$$

只要 $(a^{r/2}-1)$ 和 $(a^{r/2}+1)$ 不都是 $N$ 的倍数，则可通过算法 1 中第 4 步得到 $N$ 的因子。需要说明的是，Shor 算法是一个概率算法，这是因为(2)式中 $(a^{r/2}\pm1)$ 可能是 $N$ 的倍数，从而导致分解失败。但通过重复执行 Shor 算法 $k$ 次，可以将分解成功的概率至少提高到 $1-1/2^k$。

算法 1 中除了第 3 步外，其他的在经典密码学中已有成熟的理论方法。Shor 算法的核心是算法 1 中的第 3 步，即求解函数 $f(x)$ 的周期 $r$，这在经典计算机上需要指数级时间。这里“周期”的含义是指对于所有的正整数 $x$，满足 $f(x+r)=f(x)$ 的最小正整数 $r$。下面我们我们详细介绍量子计算机求解函数周期 $r$ 的详细过程：

假设量子计算机包括两个量子寄存器。$x$ 寄存器为 $m$ 个量子位，其中 $m$ 满足 $N^2 \leqslant 2^m < 2N^2$，寄存器的基态可理解为整数 $0, 1, \cdots, 2^m-1$ 的二进制表示，如基态 $|111\cdots1\rangle$ 表示整数 $2^m-1$，因此寄存器 $x$ 至少可存储 $N^2-1$ 个 $x$ 的取值。$y$ 寄存器用于存储函数 $f(x) = a^x \bmod N$ 的值，其长度大约需 $\log_2 N$ 量子比特。并且我们用 $|x,y\rangle$ 表示两个寄存器的基态，其中整数 $x$ 二进制展开表示 $x$ 寄存器的一个基态，$y$ 寄存器也一样。下面我们简要介绍怎样利用量子计算的方法求函数 $f(x) = a^x \bmod N$ 的周期 $r$，也称 $a$ 模 $N$ 的阶。

步骤 1：将两个寄存器初始化为状态 $|\phi_0\rangle = |0,0\rangle$，即将两个寄存器中的每个量子比特都置为状态 $|0\rangle$。

步骤 2：先对 $x$ 寄存器上的每一个量子比特执行 Hadamard 变换。由于 $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 所以当前 $x$ 寄存器的存储值为所有可能取值的叠加态。于是可以将两个寄存器的状态写成：

$$|\phi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x,0\rangle$$

步骤 3：定义幺正变换 $U_f$，$U_f|x,y\rangle = |x,y \otimes f(x)\rangle$，其中“$\otimes$”表示异或运算符，函

数 $f(x)=a^x \bmod N$。显然，$U_f|x,0\rangle=|x,f(x)\rangle$ 。对两个寄存器的状态 $\phi_1$ 做幺正变换 $U_f$ 后，两个寄存器的状态变为：

$$|\phi_2\rangle=U_f|\phi_1\rangle=\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,f(x)\rangle \tag{3}$$

由于寄存器 $x$ 中的存储是自变量 $x$ 所有可能值的叠加态，因此通过(3)式可同时求出所有可能的函数值 $f(x)$，这体现了量子计算的并行性。

步骤 4：对 $y$ 寄存器进行测量（具体测量方法见文献[73]），使每个量子比特处于状态$|0\rangle$或$|1\rangle$，由此得到一个 $m$ 位比特串，而这个比特串对应于整数 $\mu\in 2[0,N-1]$。测量操作后两个寄存器的状态变为：

$$|\phi_3\rangle=U_f|\phi_1\rangle=\frac{1}{\sqrt{t}}\sum_{x=0}^{2^m-1}\eta(x)|x,\mu\rangle \tag{4}$$

其中，$t$ 为满足 $f(x)=\mu$ 的所有可能取值 $x$ 的个数，函数 $g(x)$表示：

$$\mu(x)=\begin{cases}1, & \text{若 } f(x)=\mu\\ 0, & \text{若 } f(x)\neq\mu\end{cases}$$

得到(4)式的基本原理如下：测量使得寄存器 $y$ 的存储值坍塌到一个特定值 $\mu$，而此时寄存器 $x$ 的存储值却仍为叠加态，因此对于自变量 $x$ 的所有可能值均有 $f(x)=\mu$。又因为函数 $f(x)$为周期函数，且周期 $r\leqslant N$，注意到，周期函数只有在完成一个完整周期后才重复，故寄存器 $x$ 的存储值中至少有 $N$ 个不同的取值 $x$ 满足 $f(x)=\mu$。很明显，$|\varphi_3\rangle$ 中函数 $\eta(x)$与 $f(x)$具有相同的周期。于是后面我们转化为求 $\eta(x)$的周期 $r$。需要说明是，根据量子不可重复测量的性质，后续操作不再对 $y$ 寄存器进行任何操作，且不再写出 $y$ 寄存器的状态$|\mu\rangle$ 。

步骤 5：对 $x$ 寄存器进行量子 Fourier 变换，将量子 Fourier 变换作用到$|\phi_3\rangle$ 的变量 $x$ 上。于是 $x$ 寄存器的状态变为：

$$|\phi_4\rangle=\frac{1}{\sqrt{t}}\sum_{v=0}^{2^n-1}S(v)|v\rangle$$

其中，$S(v)$为$\eta(x)$的Fourier 变换，即：

$$S(v)=\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}\eta(x)e^{2\pi ivx/2^m}$$

由于函数 $\eta(x)$是一个简单的二值函数，因此其离散 Fourier 变换函数 $S(v)$也较为简单。函数 $S(v)$的峰值可提供其周期的相关信息。

步骤 6：采用与步骤 4 相同的测量方法对 $x$ 寄存器进行测量，得到坍塌值 $v$，概率为$||S(v)||^2/t$。如果测量值 $v$ 满足：

$$\left|\frac{v}{2^m}-\frac{j}{r}\right|\leqslant\frac{1}{2^{m+1}}$$

则称测量值 $v$ 是良性的。这里 $j$ 为整数，此时我们可以采用连分式渐进的方法[73] 估算出周期 $r$。同时，文献[73]中还详细分析了上述求解过程的成功概率。至此，我们介绍了 Shor 算法分解大整数因子的全过程。有兴趣的读者可参阅文献[91, 73]以得到关于 Shor 算法的更为详细介绍。

对于经典计算机而言，大整数因子分解问题是一个 NP 问题。目前最好的破译算法是数域筛法（NFS），分解一个 $n$ 比特大整数的复杂度为：

$$O\left(\exp(c(\log n)^{1/3}(\log\log n)^{2/3}\right)$$

而对于 Shor 算法，其复杂度仅需：

$$O\left((\log n)^2(\log\log n)(\log\log\log n)\right) \tag{5}$$

显然，式(5)中的复杂度是多项式时间。这表明 RSA 密码系统在量子计算机环境下是不安全的。自从 Shor 算法提出以来，引起了人们的广泛关注和研究推广。近年来，Shor 算法的研究还在纵向发展[47, 66]，已由量子傅里叶变换推广到一般情况下的 HSP 问题（Hidden Subgroup Problem），绝大数安全性能归结到 HSP 问题的公钥密码方案均不能抵抗量子计算机的攻击，包括 RSA、ElGamal 和 ECC。这意味着一旦量子计算机走向实用，那么目前这些广泛应用的经典公钥密码体制将不再安全。

另外一种量子破译算法是 Grover 在 1996 年提出的一种通用的量子搜索算法[51]，通常称为 Grover 算法。它将遍历搜索的复杂度从经典算法的 $O(N)$缩小到 $O(\sqrt{N})$。显然该算法对经典搜索算法起到了二次加速作用，从而显著地提高了搜索效率。对于密码破译而言，这相当于将密码算法的密钥长度 $n$（$N=2^n$）减少到原来的一半。这对现有密码还未构成本质的威胁，我们可以通过增加密钥长度来抵御这种量子搜索算法的攻击。

## 2.2 经典密码应对量子计算挑战的对策

众所周知，现代密码学是建立在计算复杂性理论基础之上的。例如，RSA 公钥密码体制的安全性就是建立在大整数因子分解是 NP 困难性问题这一论断之上的，然而，Shor 算法却表明大整数因子分解难题在量子图灵机环境下是可解问题。因此，我们要设计能抵御量子计算攻击的密码算法，就需要对量子复杂性理论有所了解。与经典图灵机中的 P 问题、NP 问题相对应，我们记量子计算中的可解问题为 QP 问题，难解问题为 QNP 问题。另外，我们说 BPP 问题是指经典概率图灵机可通过多项式时间求解的一类确定性问题，且对所有输入的差错概率上界为 1/3；而 BQP 问题是指量子图灵机可通过多项式时间求解的一类确定性问题，且对所有输入的差错概率上界为 1/3。量子复杂性类中最重要的结果之一是 1992 年 Deutsch 等[28] 证明发现：$P \subseteq QP$ 和 $BPP \subseteq BQP$。这一结论表明量子图灵机的计算能力确实比经典图灵机强大，但同时 Bennett 等[11] 给出了另外一个重要结论：$NP \not\subseteq BQP$，这说明量子图灵机的计算能力也存在极限。不过，目前我们对量子计算复杂性问题和量子图灵机的计算能力问题研究还不十分清楚。

从前面的分析易知，量子计算攻击现代密码学的实质是依赖于量子计算机的高度并行计算能力、将相应的 NP 问题化解为 QP 问题，这对于基于 NP 困难数学问题设计的现代公钥密码而言，其潜在的威胁是致命的。而对于私钥密码（如 AES）、Hash 函数等密码算法来说，由于它们的设计不依赖任何困难性问题，目前尚未发现量子计算的有效攻击方法。因此，目前量子计算对现代密码学的威胁主要体现在公钥密码方面。于是，本文我们侧重探讨如何设计能抵御量子计算攻击的公钥密码体制，并将这些具有量子计算安全的公钥密码体制统称为“抗量子公钥密码体制（Post-quantum Public Key Cryprography）”。结合现代密码学的观点，以量子计算复杂度为基础设计的密码系统必然具有抗量子计算的性质，换言之，要求我们采用 QNP 问题来设计公钥密码算法。目前只知道能转化为 HSP 问题的 NP 问题属于 QP 问题。根据 Bennett 的结论，并非所有的 NP 问题（尤其 NPC 问题）都能转化为 QP 问题，但要证明哪些 NP 问题仍属 QNP 问题是一个极具挑战性的工作，对于密码设计者而言更显急迫。另外，抗量子公钥密码算法的设计还要遵循一个基本原则，即首先它在经典图灵机上必须是计算安全的。综合这些因素的考虑，目前，基于格问题、MQ 问题、一般线性码的译码问题等设计公钥密码算法被认为是具有抗量子计算能力的而备受关注，但这些相应的 NP 问题是否属于 QNP 问题有待我们深入研究。

# 3 抗量子计算公钥密码体制

下面我们简要介绍目前国际密码学界公认的，并且热点关注的几种抗量子计算公钥密码体制。它们分别是基于 Hash 函数的 Merkle 树签名方案、基于纠错码的公钥密码体制、基于格问题的公钥密码体制及基于有限域上非线性方程组难解性问题的公钥密码体制。

## 3.1 基于 Hash 函数的数字签名

基于 Hash 的数字签名（主要指 Merkle 签名方案）源于一次签名方案（One Time Signature，OTS）。1978 年 Rabin 首次提出了一次签名方案[88]，该方案验证签名需要与签名者交互。次年，Lamport 提出了一个更为有效的一次签名方案[62]，它不要求与签名者交互；Diffie 将其推广[32]，建议用 Hash 函数替代基于数学难题的单向函数以提高该机制的效率，因此，常称之为 Lamport-Diffie 一次签名方案（LD-OTS）。随后，又相继出现了一些改进方案，如 Bos-Chaum 方案、Winternitz 方案等[7]。大多数一次签名方案具有签名生成和验证高效的优点。一次签名方案可应用在某些特殊环境比如芯片卡中，它们具有较低的计算复杂度。

在一次数字签名方案中，每个密钥对仅能签署一条消息，否则签名将以很高的概率暴露更多的私钥信息，因此很容易伪造针对新消息的签名。每次签署消息都需更新公钥，这相当于“一次一密”，虽然具有较高的安全性，但却缺乏实用性。当一次签名与认证技术结合时，多次签名就成为了可能。

1989 年 Merkle 提出了 Merkle 认证树签名方案（MSS）[76]。该方案描述如下，令 $H$: $\{0,1\}^{*}\rightarrow\{0,1\}^{n}$是一个密码学上的 Hash 函数，且一次签名方案已经给定。

**MSS 密钥对产生**：签名者选取 $h\in Z^{+}$且 $h\geqslant 2$，产生 $2^{h}$个一次签名密钥对$(X_i,Y_i)$，$i=1,\cdots,2^{h}$，其中 $X_i$, $Y_i$ 分别是签名密钥和验证密钥。MSS 的私钥是一次签名密钥序列。为确定 MSS 的公钥，构造一颗二叉认证树，叶子节点是验证密钥的 Hash 值 $H(Y_i)$，内部节点（包括根节点）是它左右孩子节点级联的 Hash 值，则 MSS 的公钥是认证树的根节点。更准确地表示，记 Merkle 认证树的节点为 $v_s[i]$，$0\leqslant s<2^{h-s}$，其中 $s\in[0,h]$该节点的高度，则 $v_s[i]=H(v_{s-1}[2i]||v_{s-1}[2i+1])$，$1\leqslant s\leqslant h$，$0\leqslant i<2^{h-s}$. MSS 密钥产生过程中需要计算 $2^{h}$个一次签名密钥对和 $2^{h+1}$-1 个 Hash 值。

**MSS 签名过程**：假设用第 $i$ 个密钥对$(X_i,Y_i)$ 签名消息摘要 $d$，则签名为$(i,Y_i,\sigma,A_i)$，

其中，$\sigma$ 由一次签名算法产生，$A_i$ 为序列号 $i$ 所对应的认证路径，令 $A_i=(a_0,\cdots,a_{h-1})$，则：

$$a_j=\begin{cases} v_j[i/2^j-1], & \lceil i=2^j \rceil \equiv 1 \bmod 2 \\ v_j[i/2^j+1], & \lceil i=2^j \rceil \equiv 0 \bmod 2 \end{cases}$$

其中，$j=0,\cdots,h-1$。图 1 给出 $h=3$ 的一个实例，当用第 4 个密钥对$(X_4,Y_4)$ 签名消息摘要时，认证路径为 $A_4=(v_0[5], v_1[3], v_2[0])$，即图中的虚线圆圈；图中箭头表示从叶节点 $v_0[4]=H(Y_4)$到根节点的路径。

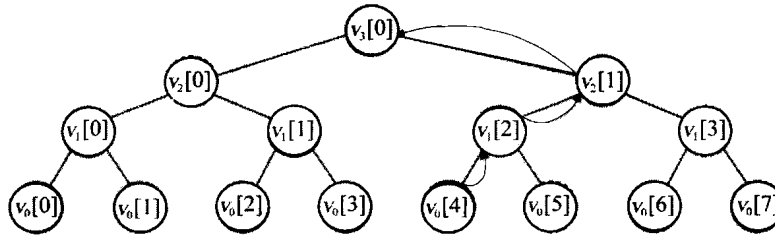


图 1：叶节点数为 8 的 Merkle 树及当 $i$=4 时 Merkle 签名的产生过程

**验证签名过程：**为验证一个 MSS 签名$(I,Y_i,\sigma,A_i)$，首先用验证密钥 $Y_i$ 检验一次签名 $\sigma$ 的正确性，然后用认证路径 $A_i$ 验证 $Y_i$ 的正确性，若二者均通过验证则接受签名，否则拒绝签名。

Merkle 数字签名方案中，没有太多的理论假设，它的安全性仅仅依赖于 Hash 函数的安全性，目前在量子计算机模型下还没有一般 Hash 函数的有效攻击方法，因此，Merkle 签名方案具有抗量子计算性质。与基于数学困难性问题的公钥密码相比，Merkle 签名方案不需要构造单向陷门函数，给定一个单向函数（通常采用 Hash 函数）便能构造一个 Merkle 签名方案，我们知道在密码学上构造一个单向函数要比构造一个单向陷门函数要容易得多，因为设计单向函数不必考虑隐藏求逆的思路，从而可以不受限制地运用置换、迭代、循环、反馈等简单编码技巧的巧妙组合，以简单的计算机指令或廉价的逻辑电路实现高度复杂的数学效果。新的 Hash 标准 SHA-3[80]的征集过程中，涌现出了许多新的安全的 Hash 函数，利用这些新的 Hash 算法可以构造出一批新的实用 Merkle 签名算法。

Merkle 数字签名方案的优点是签名和验证签名效率较高；缺点是签名和密钥较长，产生密钥的代价较大。在最初的 Merkle 签名方案中，需要签名的数量与需要构造

的二叉树紧密相关，能够签名的数量越大，所需要构造的二叉树越大，同时消耗的时间和空间代价也就越大。因此该方案的签名数量是受限制的。近年来，许多学者对此做了广泛的研究，提了一些修改方案，大大地增加了签名的数量，如 CMSS 方案[8]、GMSS 方案[9]、DMSS 方案等[22]。Buchmann、Dahmen 等提出了 XOR 树算法[8,34]，只需要采用抗原像攻击和抗第二原像攻击的 Hash 函数，便能构造出安全的签名方案。而在以往的Merkle树签名方案中，要求Hash 函数必须是抗强碰撞的。这是对原始Merkle签名方案的有益改进。上述这些成果，在理论上已基本成熟，在技术上已基本满足工程应用要求，一些成果已经应用到了 Microsoft OutLook 及移动代理路由协议中[64]。

目前，基于 Hash 函数的数字签名的理论和技术都还需要深入研究，仍有许多开放性课题。如增加签名的次数、减小签名和密钥的尺寸、优化认证树的遍历方案及实现相比其他公钥体制所不具备的功能（如基于身份的认证）等均值得我们进一步研究探讨。

## 3.2 基于纠错码的公钥密码体制

纠错编码公钥密码体制可理解为：把纠错的方法作为私钥，加密时对明文进行纠错编码并主动加入一定数量的错误，解密时运用私钥纠正错误，恢复出明文。McEliece 利用 Goppa 码有快速译码算法的特点，提出了第一个基于纠错编码的 McEliece 公钥密码体制[75]。该体制描述如下，设 $G$ 是二元 Goppa 码$[n,k,d]$ 的生成矩阵，其中 $n=2^h$，$d=2t+1$，$k=n-ht$，明密文集合分别为 $GF(2)^k$ 和 $GF(2)^n$。随机选取有限域 $GF(2)$ 上的 $k$ 阶可逆矩阵 $S$ 和 $n$ 阶置换矩阵 $P$，并设 $G'=SGP$，则系统私钥为 $S$、$G$、$P$，公钥为 $G'$。如果要加密一个明文 $m\in GF(2)^k$，则计算 $c=mG'+z$，这里 $z\in GF(2)^n$ 是重量为 $t$ 的随机向量。要解密密文 $c$，首先计算 $cP^{-1}=mSGPP^{-1}+zP^{-1}=mSG+zP^{-1}$，由于 $P$ 是置换矩阵，显然 $z,zP^{-1}$ 的重量相等且为 $t$，于是可利用 Goppa 的快速译码算法将 $cP^{-1}$ 译码成 $m'=mS$，则相应明文 $m=m'S^{-1}$。

1978 年 Berlekamp 等人证明了任意线性码的译码问题是 NP 完全问题[15]. McEliece 密码方案的原始版本经受了 30 多年来的广泛密码分析，被认为是目前安全性最高的公钥密码体制之一。文献[21,48,63,92]对其安全性做了深入的研究，其中 Gibson 证明了加密变换中存在多个等价陷门，任何一个陷门都可用于解密，但要找到其中一个在计算上是不可行的。虽然 McEliece 公钥密码的安全性高且加解密运算比较快，但该方案也有它的弱点，其一是它的公钥尺寸太大，其二是信息扩展了 $n/k$ 倍。以最初推荐参数 $n=1024$，$k=644$，$t=38$ 为例，公钥大小为 $2^{19}$ 比特，信息扩展了 1.6

倍。由于这些原因，该方案一直以来并没有引起人们太多的关注。

1986年Niederreiter 提出了另一个基于纠错码的公钥密码体制[79]。与McEliece 公钥不同的是，它隐藏的是Goppa 码的校验矩阵。该系统的私钥包括二元Goppa 码$[n,k,d]$的校验矩阵 $H$ 及 $GF(2)$上的可逆矩阵 $M$ 和置换矩阵 $P$。公钥为错误图样的重量 $t$ 和矩阵 $H'= MHP$。假如明文为重量为 $t$ 的 $n$ 维向量 $m$，则密文为 $c = mH'^{T}$ 。解密时，首先根据加密表达式可推导出 $z(M^T)^{-1}= mP^TH^T$ ，然后通过 Goppa 码的快速译码算法得到 $mP^T$，从而可求出明文 $m$。1994 年李元兴、王新梅等[67]证明了 Niederreiter 公钥与 McEliece 公钥密码体制在安全性上是等价的。当然，也可采用其他具有快速译码算法的线性分组码如 BCH 码、RS 码等来构造公钥密码体制，但其安全性要比采用 Goppa 码低，主要原因是同一参数$[n, k, t]$ 的其他码的数量要比 Goppa 码少得多。2009 年 Misoczki 等针对 McEliece 体制密钥量大弱点，提出了一种改进方案[74]，但该方案将被 Faugere 等利用代数攻击攻破[44]。

与其他公钥密码体制（如 RSA 等）不同，McEliece 公钥及 Niederreiter 公钥密码方案只能用于加密，但却不具备数字签名功能。1990 年我国学者王新梅提出了第一个基于纠错编码的数字签名方案——Xinmei 方案[99]。1992 年 Harn 等[57] 对 Xinmei 方案进行了攻击和改进。Alabhadi 和 Wieker 于 1992 年提出了另一种攻击方法[5]，其选择明文的攻击的复杂度仅为 $O(n^3)$，这种攻击方法对 Harn 的改进方案同样有效，为了抵抗这种攻击，他们于 1993 年有提出了 AW 方案。2000 年王新梅对原始 Xinmei 方案进行了修正，得到了比 AW 方案更为简单的修正 Xinmei 方案[101]。除此之外，1991 年李元兴等[98]构造了一类同时具有签名、加密和纠错能力的公钥体制。张振峰、冯登国和戴宗铎于 2003 年对 AW 方案进行有效的分析[106]，仅利用公钥便能构造出等价的私钥，并指出利用大矩阵分解的困难性很难构造出安全较高的纠错码数字签名体制。

目前，国际上公认安全的纠错码签名方案是 2001 年 Courtois 等[19] 提出的 CFS 签名方案。McEliece 公钥及 Niederreiter 公钥密码方案不能用于签名的主要原由是，用Hash算法所提取的待签消息摘要向量能正确解码的概率极低。对于Goppa 码$[n,k,d]$，可以正确解码的数目为：

$$N_1 = \sum_{i=1}^{t} \binom{n}{i} \approx \binom{n}{t} \approx \frac{n^t}{t!}$$

而 Goppa 码$[n,k,d]$ 的总数为 $N^2 = 2^{n-k} = n^t$，因此，随机给定消息待签向量，可正