量子计算密码攻击进展

王 潮[1),2),3)] 姚皓南[1),2)] 王宝楠[1),2),5)] 胡 风[1),2)] 张焕国[6)] 纪祥敏[4),6)]

[1)](特种光纤与光接入网重点实验室, 特种光纤与先进通信国际合作联合实验室 上海大学 上海 200444)

[2)](密码科学技术国家重点实验室 北京 100878)

[3)](鹏城实验室量子计算中心 广东 深圳 518000)

[4)](福建农林大学计算机与信息学院 福州 350002)

[5)](上海电力大学计算机科学与技术学院 上海 200090)

[6)](武汉大学国家网络安全学院 武汉 430072)

摘 要 通用量子计算机器件进展缓慢，对实用化 1024-bit 的 RSA 密码破译尚不能构成威胁，现代密码依旧是安全的. 量子计算密码攻击需要探索新的途径：一是，量子计算能否协助/加速传统密码攻击模式，拓展已有量子计算的攻击能力；二是，需要寻找 Shor 算法之外的量子计算算法探索密码攻击. 对已有的各类量子计算整数分解算法进行综述，分析量子计算密码攻击时面对的挑战，以及扩展至更大规模整数分解存在的问题. 结合 Shor 算法改进过程，分析 Shor 算法对现代加密体系造成实质性威胁前遇到的困难并给出 Shor 破译 2048 位 RSA 需要的资源. 分析基于 D-Wave 量子退火原理的 RSA 破译，这是一种新的量子计算公钥密码攻击算法，与 Shor 算法原理上有本质性不同. 将破译 RSA 问题转换为组合优化问题，利用量子退火算法独特的量子隧穿效应跳出局部最优解逼近全局最优解，和经典算法相比有指数级加速的潜力. 进一步阐述 Grover 量子搜索算法应用于椭圆曲线侧信道攻击，拓展其攻击能力. 探讨量子人工智能算法对 NTRU 等后量子密码攻击的可能性.

关键词 量子计算；量子退火；量子计算密码；量子攻击

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2020.01691

Progress in Quantum Computing Cryptography Attacks

WANG Chao[1),2),3)] YAO Hao-Nan[1),2)] WANG Bao-Nan[1),2),5)] HU Feng[1),2)]
ZHANG Huan-Guo[6)] JI Xiang-Min[4),6)]

[1)](*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai* 200444)

[2)](*State Key Laboratory of Cryptology, Beijing* 100878)

[3)](*Center for Quantum Computing, Peng Cheng Laboratory, Guangdong Shenzhen* 518000)

[4)](*College of Computer Information Science, Fujian Agriculture and Forestry University, Fuzhou* 350002)

[5)](*College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai* 200090)

[6)](*School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072)

Abstract Due to the limitations of hardware, the development of universal quantum computer devices is slow. At present, the maximum integer factorization by general Shor's algorithm is 85 (using the characteristics of Fermat numbers to factor the integer 85 with 8 qubits), which is not a threat to the practical 1024-bit RSA by Shor's algorithm. Since the universal quantum computer cannot be practical in a

收稿日期：2019-08-27；在线出版日期：2020-02-07. 本课题得到“国防创新特区项目”、国家自然科学基金项目（61572304，61272096）、国家自然科学基金重点项目（61332019）、密码科学技术国家重点实验室开放课题基金资助. **王 潮**，博士，教授，中国计算机学会(CCF)会员(E200008909S)，主要研究领域为人工智能、网络信息安全、量子密码学等.E-mail: wangchao@shu.edu.cn. **姚皓南**，硕士研究生，主要研究领域为信息安全、量子密码学. **王宝楠**，博士研究生，主要研究领域为信息安全、量子密码学. **胡 风**，博士研究生，主要研究领域为信息安全、量子密码学. **张焕国**，博士，教授，主要研究领域为密码学、密码协议、可信计算等. **纪祥敏**(通信作者)，博士研究生，副教授，中国计算机学会(CCF)会员(30663M)，主要研究领域为信息安全、密码学、可信计算.E-mail: jixm168@126.com

short time, the modern cryptography is still secure enough now. Quantum computing cryptography attack needs to explore new ways to enhance its quantum attacking ability: Firstly, whether quantum computing can assist/accelerate traditional cryptography attack mode and expand its more powerful quantum attacking ability on the basis of the existing quantum computing. Secondly, it is necessary to find quantum computing algorithms other than Shor's algorithm to explore quantum computing cryptographic attack. In this paper, various existing algorithms for integer factorization algorithms of quantum computing are studied and show optimistic potentials of quantum annealing algorithm and D-Wave quantum computer for deciphering the RSA cryptosystem. Such as Shor's algorithm (factor up to 85) via different platforms (like Hua-Wei quantum computing platform), quantum adiabatic computation via NMR (291311), D-Wave (purchased by Lockheed Martin and Google etc., has been initially used for image processing, machine learning, combinatorial optimization, and software verification etc.) quantum computer (factored up to 376289), quantum computing software environment provided by D-Wave (factor the integer 1001677 with 87 qubits) to obtain a higher success rate and extend it to a larger factorization scale. Actually, D-Wave using quantum annealing may be closer to cracking practical RSA codes than a general-purpose quantum computer (IBM) using Shor's algorithm. In addition, the model limitations and precision problems existing in the expansion of integer factorization to a larger scale are discussed. Majorities of scholars think Shor's algorithm as the unique and powerful quantum algorithm for cryptanalysis of RSA. Therefore, the current state of post-quantum cryptography research exclusively referred to potential threatens of Shor's algorithm. This paper analyzes the RSA deciphering method based on D-Wave quantum annealing principle, which is a new public key cryptography attack algorithm for quantum computing, and it is fundamentally different from Shor's algorithm in principle. It is the second effective quantum attack method (RSA deciphering) in addition to Shor's algorithm. Thus, the post-quantum cryptography research should further consider the potentials of D-Wave quantum computer for deciphering the RSA cryptosystem in future. Furthermore, Grover's quantum searching algorithm is applied to the elliptic curve side channel attack to expand its attack capability. It is a new effective public key cryptosystem attack method, which is helpful to expand the attack of quantum computing on other public key cryptosystem constitutions. Finally, the possibility of quantum artificial intelligence algorithm attacking NTRU and other post-quantum cryptography is discussed. It is necessary to explore a new cryptographic scheme that can resist the attack of quantum computing, and combine evolutionary cryptography with quantum artificial intelligence, which is expected to be applied to the design and analysis of cryptography algorithms in the post-quantum cryptography.

Keywords traditional cryptography; quantum computing; quantum annealing; quantum computing cryptography; quantum attack

1 引 言

现在的量子计算机可以分成两类. 一是通用量子计算机[1,2], 由于硬件平台发展缓慢, 对现在实用化 1024-bit RSA 密码破译尚不能构成威胁, 现代密码依旧安全. 二是 D-Wave 专用量子计算机,其商业化进展迅猛. 基于通用量子计算机的 Shor 算法受限于量子硬件发展缓慢, 对现在广泛使用的 RSA 公钥密码体系没有实质上的威胁. 但是人们容易将硬件发展较快、无法运行 Shor 算法的专用量子计算机与通用量子计算机混淆, 对现代密码体系的安全性做出错误的判断, 错误地以为现代密码体系即将受到 Shor 算法的攻击进而不再安全[3].

量子计算[4,5]将有助于推动密码攻击领域的诸多课题. 量子攻击提供了一种新的、不同于传统密码的计算模式, 在密码设计和破译领域实现对传统密码的进一步拓展.

2014 年, Nature 资深评论员 Matthias Troyer 在报道中指出, 包括 Shor 算法在内的量子密码破译无法实用化[6]. 2018 年, Google 量子人工智能实验室

主任 John Martinis 在 Science 报道中指出通用量子实用化任重道远，认为破译公钥密码距离实用化“be years”，美国能源部 DOE 也赞同这个观点[7,8].

2018 年，荣获 2012 年物理诺贝尔奖的 Serge Haroche 教授在报告“The Nobel Prize Series India 2018”中指出，短期内量子计算机有望应用于量子模拟、量子通信、量子测试等研究领域.

2019 年《Nature》上发表了 Google 最新一代量子处理器 Sycamore[9]，包含 53 个量子比特. 对量子处理器的输出进行重复性采样，并与经典计算机模拟的结果进行比较. Sycamore 完成同样的任务只需要 200 秒，而 Google 估计使用目前世界上最强大的超级计算机 Summit 需要 1 万年. 以此证明该量子处理器实现了量子优越性(Quantum Supremacy). IBM 提出使用二级存储[10]可以模拟 54-bit 量子计算机，并且通过优化将经典计算机执行任务的时间从 1 万年降低到 2.55 天. IBM 研究中心主任 Dario Gil 表示，量子计算机不会凌驾于经典计算机之上，两种计算机会是协同工作的方式. 量子计算机对硬件的要求较高，而将其与经典计算机进行混合架构共同执行任务，可以在达到量子加速的同时降低对量子硬件的需求.

尽管现在量子计算在一个任务上已经实现了量子优越性，但是由于量子纠错和容错量子计算技术远超当前技术水平[11-13]，通用量子计算机进展缓慢，量子算法达到实用化阶段尚需时日，以破译 RSA 公钥密码为例，目前分解 n 位大整数需要 $2n$ 位逻辑量子比特[14]. 基于 Shor 算法实现破译 1024 位 RSA 密码实际需 2000 多位通用逻辑量子比特，远非当下的通用量子计算机所能达到. 而专用量子计算机 D-Wave 硬件平台发展较快并且与洛克希德马丁、谷歌、美国国家航空航天局、美国国家实验室等多家机构进行合作，在量子计算机商用化的道路上处于领跑地位. 因此，有必要探索专用量子计算机(D-Wave)在密码设计与密码分析领域的潜力.

从密码学家的角度来看[15]，通用量子计算存在的两个问题可能构成了量子密码分析的主要障碍：增加容错量子位的数量. 第一个是所谓的量子比特的数量. 技术的进步使可用量子位的数量经常翻倍，这与经典计算机的摩尔定律相似，但是通用量子计算机受硬件限制，发展难度较大. 第二个就是容错. 在量子计算中，错误通常是由于量子比特与其环境之间不受控制的相互作用而产生的. 2019 年，最多量子比特的量子计算机拥有 72 个容错量子位，已经可以解决以前无法解决的组合、优化等问题，但目前还不能解决密码问题. 所以在通用量子计算机的进展缓慢、对实际运行的公钥密码不能构成安全威胁背景下，未来抗量子密码的研究有必要探索专用量子计算机(D-Wave)在密码设计与密码分析领域的潜力.

本篇综述主要归纳与总结传统密码与量子计算密码攻击的国内外研究进展，分析量子计算在公钥密码攻击和椭圆曲线侧信道攻击现状，并展望量子人工智能算法对 NTRU 等后量子密码攻击的可能性. 为量子计算在信息科学领域的工作提供思路. 根据《Nature》[6]和《Science》[7][8]报道，通用量子计算机进展缓慢，它的几个典型应用都无法成功，破译公钥密码距离实用化“be years”，因此，量子计算密码攻击需要探索新的途径：一是，量子计算能否加速传统密码攻击模式；二是，需要寻找 Shor 算法之外的量子计算算法探索密码攻击.

2　Shor 算法对公钥密码的攻击

三种公钥密码包括离散对数难题(Discrete Logarithm Problem, DLP)，大整数分解难题(Integer Factorization Problem, IFP)和椭圆曲线离散对数难题(Elliptic Curve Discrete Logarithm Problem, ECDLP). 对于 IFP 和 ECDLP，传统算法中最有效的方法是 1991 年由 Pollard 等人提出的通用数域筛选算法(GNFS)[16]. 通用数域筛选法(GNFS)求解大数质因子和椭圆曲线离散对数的时间复杂度分别是 $O(\mathrm{e}^{[(\log N)^{1/3}(\log(\log N))^{2/3}]})$ [17] 和 $O(\exp(c\sqrt{\log_2 k \log\log k})M(P))$ [18]，这里的 N 是指要分解的大数，k 就是我们要求的椭圆曲线的离散对数，P 是有限域的素域范围.

本章节主要介绍 Shor 算法对 RSA 的攻击研究和 Shor 算法求解椭圆曲线离散对数的研究.

2.1　Shor算法分解整数的研究

公钥密码系统的安全性随着 Shor 算法的提出和量子计算的发展受到了威胁. 众所周知，RSA 密码系统的安全性在于整数分解问题的难度. 它所依赖的数论问题不能在有效的多项式时间内求解. 破译 RSA 的核心问题即整数分解问题[19].

Shor 算法通过将因式分解问题简化为求阶的问题来发挥效用. 关于量子计算机的仿真[20]及 Shor 算法对整数 N 的分解的研究一直受到国内外学者的广泛关注.

1996 年，阿根廷科学家 Cesar Miquel 等人[21]分析了损耗和退相干对量子分解电路性能的影响，

并且展示分解整数 N=15，这项工作为实践中实施 Shor 量子算法提供了很好的参考.

2000 年英国伦敦帝国学院布莱克特实验室的 Parker 等人[22]给出了一个单一的纯量子比特与 log2N 量子比特在任意混合态下的集合都足以有效地实现 Shor 分解算法.

2001 年，IBM 研究实验室的 Vandersypen 等人[23]使用室温液态核磁共振技术实现了整数 N=15 的 Shor 算法演示性实验. 该实验主要目的是演示量子计算机的控制和建模，没有针对 Shor 算法的扩展性进行研究，无法应用到更大的整数.

2004 年，美国赫尔辛基理工大学的 Vartiainen[24]基于约瑟夫森电荷量子位寄存器实现整数 N=21 的 Shor 算法实验. 由于实验对退相干时间有严格要求，通过使用特别设计的量子位门和数值优化的方法完成了物理实现，因此难以扩展到大规模整数分解.

2007 年，文献[25]基于 Quantware 库使用 30 个量子比特完成整数 N=943 的分解，并研究残余耦合引起的缺陷对 Shor 算的影响. 同年，基于光量子计算机的 Shor 算法整数分解由 Lu 等人[26]首次完成，通过操控四个光量子实现了 N=15 的整数分解，通过实验证明该平台可以执行 Shor 算法，并完成整数分解.

2011 年，布里斯托大学的 M.G.Thompson 等人使用可控相位门和哈达门展示执行 Shor 算法的基本过程[27]，并成功完成整数 N=15 的分解.

2012 年，Lucero 等人[28]基于约瑟夫森电荷量子电路成功使用 3 个量子比特分解整数 N=15，和前文中 Vartiainen 的实验一样，对退相干时间严格要求，物理实现的要求较高.

2012 年，Enrique Martin Lopez 等人实验实现了 Shor 量子分解 21 的过程，通过使用一个迭代协议将量子比特重复利用，使得所需的所有的量子比特的数量是标准协议中要求的三分之一[29].

2013 年，佐治亚大学的 Geller 等人[30]使用 8 量子比特完成整数 N=51 和 N=85 的分解，由于利用了费马数的特殊性质，不能作为通用方法.

2013 年，文献[31]提出量子电路执行整数分解任务时第二寄存器的优化方法. 通过寻找 2 阶元素来实现整数的分解. 因此第二寄存器的量子比特数可以大大减小，有效降低总量子比特数.

2016 年，Thomas 等人[32]提出基于 Kitaev 的 Shor 算法的实现. 通过有效地使用和控制七个量子位和四个“高速缓存量子位”分解整数 15. 与传统算法相比，减少了近 3/4 的量子比特数.

2017 年，上海大学王宝楠等人[33]提出了针对 RSA 的小 Qubit 量子攻击算法设计，降低了算法的复杂度和成功率，提高了原算法中模幂计算的运算速率. 实验表明，该方法可以用 11、10、9 量子比特成功分解整数 119 的量子电路.

2018 年 Google 公司 Craig Gidney[14]提出引入 $n-1$ 个辅助量子比特(Dirty Ancillae Qubits)将 Shor 算法执行所需的量子比特数(Clean Qubits)从 Zalka[34] $1.5n+O(1)$ 缩减到了 $n-2$，并且没有增加电路的渐进规模和深度. Dirty Qubits 以一种未知状态存在不需要精确的初始化，但在电路执行结束之前需转为已知状态. Clean Qubits 用于具体的电路构造，需要初始化为已知的计算基态，Shor 算法发展如表 1. 表中 $M(n)$ 是乘法的经典时间复杂度，其极限是 $n\cdot(\lg n)\cdot 2^{O(\lg n)}$ [35]. ε 是通用门的最大误差.

表 1 Shor 量子算法改进过程

	Year	Depth	Gates	Clean Qubits	Total Qubits
Shor[36]	1994	$\Theta(nM(n))$	$\Theta(nM(n))$	$\Theta(n)$	$\Theta(n)$
Bechman[37]	1996	$\Theta(n^3)$	$\Theta(n^3)$	$5n+1$	$5n+1$
Veldral[38]	1996	$\Theta(n^3)$	$\Theta(n^3)$	$4n+3$	$4n+3$
Beauregard[39]	2003	$\Theta(n^3\lg\frac{1}{\varepsilon})$	$\Theta(n^3\lg\frac{n}{\varepsilon}\lg\frac{1}{\varepsilon})$	$2n+3$	$2n+3$
Takahashi[40]	2006	$\Theta(n^3\lg\frac{1}{\varepsilon})$	$\Theta(n^3\lg\frac{n}{\varepsilon}\lg\frac{1}{\varepsilon})$	$2n+2$	$2n+2$
Zalka[41]	2006	$\Theta(n^3\lg\frac{1}{\varepsilon})$	$\Theta(n^3\lg\frac{n}{\varepsilon}\lg\frac{1}{\varepsilon})$	$1.5n+O(1)$	$1.5n+O(1)$
Häner[42]	2016	$\Theta(n^3)$	$\Theta(n^3\lg n)$	$2n+2$	$2n+2$
Craig Gidney[14]	2017	$\Theta(n^3)$	$\Theta(n^3\lg n)$	$n+2$	$2n+1$

2019 年，Google 公司 Craig Gidney[43]假设物理门错误率为 10^{-3}，surface code 周期 1 微秒反应时间 10 微秒，同时考虑到噪声的影响等条件，使用窗口算法进行优化. 评估破解 2048 位 RSA 需要的物理

量子比特数为 22325184，需要的时间为 8 小时，所需的物理量比特数以及量子比特精度远远超出当前硬件水平，对实际运行的公钥密码不能构成安全威胁.

Microsoft 和 Google 量子研究组的研究人员 Matthias Troyer 和 John Martinis 均表示由于通用量子计算机硬件的限制短期内无法实现 Shor 算法破译现在实际使用的 RSA 加密体系，寻找通用量子计算机的杀手级应用仍是一大挑战. 因此，在量子计算攻击密码方面需要探索不同于 Shor 算法的量子计算密码破译之路.

2.2　Shor算法求解椭圆曲线离散对数的研究

目前，与 Shor 算法攻击 RSA 的研究相比，针对 ECC 的 Shor 算法的研究比较少. 原因大致有两个：一是因为 ECC 算法相对于 RSA 算法的数学理论较为复杂，在工程应用中实现较为困难；二是因为 Shor 算法本是设计用来解决大数分解和求解离散对数的，如果要想利用 Shor 算法求解椭圆曲线离散对数，理论上是不能直接完成的，而且因为椭圆曲线上的运算都是点的运算，很难进行量子电路的设计. 从而导致 Shor 算法求解椭圆曲线离散对数问题成为了一个科研上的难题.

1994 年，Shor[44]提出 Shor 算法，作为量子计算机最著名的应用之一，在大素数分解问题上比非量子计算算法有指数级别的优势，同时 Shor 算法还可以应用在离散对数问题上.

1997 年，里奇蒙大学的 Jodie Eicher 和 Yaw Opoku[45]在理论上设计了使用 Shor 算法解决与离散对数问题类似的椭圆曲线问题的具体步骤. 证明在 Shor 算法的基础上进行修改可以解决椭圆曲线问题. 和 Shor 算法一样，想真正物理实现这种算法需要解决量子器件的诸多挑战.

2003 年，滑铁卢大学 John Proos 研究了基于 Shor 算法的椭圆曲线问题[46]. John Proos 从 Shor 算法和数学分析进行研究：不同椭圆曲线在有限域下具有不同的性质，选择其中适当的一条特殊的椭圆曲线进行分析. 在 Shor 算法基础上针对模幂运算与量子傅里叶变换进行优化. 以此分析椭圆曲线问题上的优化方案和算法步骤. 根据计算结果，在 Shor 算法的基础上求解 ECDLP 时，对于给定的 n 位整数，需要 $6n$ 量子比特. 但是没有就实验模拟的过程进行研究. 同时该文献给出了另一种观点：求解椭圆曲线离散对数问题可以看作是求解二维的大数分解问题.

2014 年，美国微软研究院 Martin Roetteler 等人[47]给出了一个类似于 Shor 量子分解算法的概要量子电路，该量子电路设计了三个量子寄存器，由于椭圆曲线上点的表示及点的运算的复杂性，用量子电路来体现是极其困难的. 一般说的实现 Shor 算法的量子电路需要三个量子寄存器：第一个和第二个为控制量子寄存器，第三个为工作寄存器，事实上第三个量子寄存器只是一个代称，其可能需要多个量子寄存器来协同完成“工作寄存器”的功能. 即便可以，构造量子电路实现对 ECC 的攻击也将会是非常复杂的.

2017 年，美国微软研究院 Martin Roetteler 等人[48]对使用 Shor 算法求解椭圆曲线的离散对数问题时需要的量子资源进行了估算. 这些估算来自用于受控椭圆曲线点加法的 Toffoli 门网络的仿真，在量子计算软件工具套件 $LIQU_i|\rangle$ 的框架内实现. 确定可逆模块化运算的电路实现，包括模加法、模乘法和模逆运算，以及可逆椭圆曲线点加法. 得出结论：在 n 比特素数域上定义的椭圆曲线上的椭圆曲线离散对数，可以在量子计算机上用至多 $448n^3\log_2(n)+4090n^3$ Toffoli 门的量子电路计算，其量子比特数最多为 $9n+2\lceil\log_2(n)\rceil+10$. 虽然提出通过量子电路来实现 Shor 算法解决 ECDLP(Elliptic Curve Discrete Logarithm Problem)，并分析了实现这些电路所需的资源，但没有通过实验完全证明.

2018 年，上海大学陈宇航等人[49]提出能够使用小量子比特数来破解椭圆曲线加密的 Shor 量子攻击方法，对当前安全曲线有较大威胁，它的通用性更强. 该方法的步骤为：选取一条二进制素域上的椭圆曲线，然后输出该椭圆曲线上的所有点；任意选取椭圆曲线上两点 P 和 Q，满足 $P=kQ$，k 为离散对数，输出与椭圆曲线上各点 (x_t,y_t) 对应的 x_tP+y_tQ 和 x_tP 的点；构造以 k 为周期的周期函数；创建两个量子寄存器并设置其初始状态；对第一量子寄存器 $|\varphi_1\rangle$ 执行 Hadamard 变换；将 $\mathrm{U}_{x,a}$ 算符应用于第二量子寄存器 $|\varphi_2\rangle$；对第一量子寄存器进行量子傅立叶逆变换：测量第一量子寄存器的本征态概率，求使其达到最大值的阶 k；如果阶 k 是满足 $P=kQ$，则攻击私钥为 k.

图 1 是基于 Shor 算法求解椭圆曲线离散对数 k 问题的流程图.

目前，Shor 算法对公钥密码的攻击还需要更深入的研究，通用量子计算机分解大数和求解 ECC 离散对数的能力还很有限. 当前的物理实现只能控制运行 Shor 算法的小规模的量子比特，尚不能对现今使用的 1024 位 RSA 和 163 位的 ECC 构成威胁. 如果真正部署 Shor 算法在多项式时间内攻击现在的加

密算法，必须使用千位以上的通用量子计算机.

据《Nature》和《Science》[6]-[8]等报道，破译现有的163位ECC密码所需要的千位量子比特的通用量子计算机,在未来5到10年内仍难实现. 目前，在通用量子计算机的器件条件限制的情况下，对公钥密码ECC的小Qubit量子计算攻击问题仍没有得到较好解决. 未来，探索小比特破译椭圆曲线 ECC 是一大挑战.

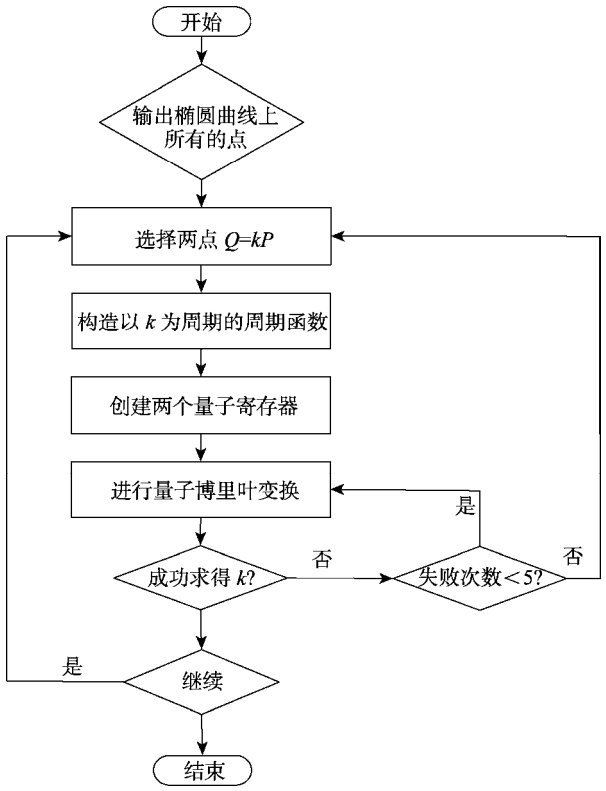

图 1 Shor 算法求解椭圆曲线离散对数 k 的流程图

3 基于量子绝热理论的整数分解方法

目前，通过量子计算实现整数分解主要有两个研究方向：一种为上面介绍的Shor算法的电路模型算法，另一种为绝热量子计算[50](Adiabatic Quantum Computation，AQC). 量子绝热计算已经应用于诸多组合优化问题，比如旅行商、图着色、蛋白质折叠、整数分解等问题[51-54]. 此外，AQC对由相位差、环境噪声和酉运算的不完善引起的误差具有更好的鲁棒性[55,56]. 因此，它很快发展成为量子计算中极具吸引力的一个领域.

2001年，Burges[57]首次提出将整数分解问题转化为优化问题，为绝热量子计算应用到整数分解做出了基础性工作,并于2010年由Schaller和Schutzhold[58]改进该方法.

3.1 基于绝热量子理论的NMR的整数分解的研究现状

2008年，彭新华等人[59]首次提出了基于绝热量子计算的因子分解算法，并成功地在 NMR 量子处理器上实现了21的分解.

2012年，徐南阳等人[60]在文献[59]的基础上提出了一个改进的绝热量子算法，并通过核磁共振量子处理器实现了对整数143的分解.

2014年，Nikesh S. Dattani等人[61]利用两个质因子的特殊性质实现 4 比特分解整数 56153，但是该数两个因子的二进制形式仅有两位不同，因此该方法不具有通用性与可扩展性.

2016年，Soham Pal等人[62]提出经典和量子计算混合方案通过500 MHz核磁共振谱仪(NMR)实现对整数551的分解.

2017年，李兆凯，彭新华，杜江峰等人[63]使用核磁共振谱仪(Nuclear Magnetic Resonance，NMR)在高于室温下使用3个量子比特实现整数291311的分解. 该方法是使用大数两个素因子的特殊性质实现的，不具有通用性和可扩展性.

2017年，杜江峰等人在室温下的固态单自旋系统上完成绝热量子算法整数分解实验[64]，系统将金刚石中的自旋作为量子处理器,通过分解整数N=35作为系统的基准测试，证明实验结果具有高保真度.

基于绝热量子理论的 NMR 的整数分解的研究由于量子比特数的限制，无法扩展到大规模整数分解的情况. 该研究仅可作为理论验证性的探索性的实验. 在通用量子计算机的进展缓慢和 NMR 的量子比特数受限的情况下,D-Wave量子计算机和基于D-Wave量子退火原理的整数分解的研究突飞猛进.

3.2 基于D-Wave量子退火原理的整数分解的研究

使用量子计算方法攻击RSA公钥体系问题上，Shor算法作为量子计算机最著名的应用之一，学界普遍性认为在不考虑硬件平台限制的情况下，严重威胁现在的公钥密码体系，从而忽略其他量子计算攻击RSA公钥体系的算法. 实际上学界众多学者均认为实际部署Shor算法攻击现有的加密体系仍然遥遥无期.

受限于相干时间、噪声、量子纠错等技术限制，近期难以研制出对现在使用的公钥密码具有威胁的通用量子计算机. 因此需要寻找不依赖通用量子计算机的量子算法攻击公钥密码. 实现原理不同的专用量子计算机D-Wave可以执行与Shor量子算法不同的绝热量子算法，对攻击公钥密码有重要的扩展

作用. D-Wave 量子计算机核心原理量子退火(Quantum Annealing，QA)利用量子领域重要的物理性质量子隧穿效应,在组合优化容易陷入局部最优问题上比传统优化算法更具优势,指数级搜索问题中有望逼近甚至达到全局最优解. 这也是考虑将 D-Wave 量子计算机用于密码设计及密码分析的基础.

2018 年 ETSI 会议专家分析 D-Wave 专用量子计算机在攻击加密体系受到忽视的原因. 因为 D-Wave 最初商业化的应用主要是的应用包括 Lockheed Martin 用于公司里飞机控制软件的测试，Google 将其用于图像识别问题等. 早期应用中不包括攻击加密体系，同时将整数分解问题转换为组合优化问题一直以来并没有被重点关注，从而忽视了利用 D-Wave 的量子隧穿效应在组合优化问题上的独特优势攻击 RSA 加密体系的应用. 因此，未来抗量子密码领域的研究还需要考虑基于量子退火原理的专用量子计算机攻击的威胁.

3.2.1　D-Wave 量子计算机的背景

2011 年 5 月，加拿大 D-Wave 公司推出全球首款 128 个量子位的商用量子计算机 D-Wave One 系统. 随后以 1000 万美元卖给著名的 Lockheed Martin（洛克希德马丁）公司用于 F35 战机等先进武器的设计，它标志着量子计算机正式进入商用阶段[65].

2012 年，Geordie Rose 提出了 D-Wave 量子计算机发展趋势图，预示 D-Wave 量子计算机的量子比特规模大约每两年增加一倍，达到了经典计算机中摩尔定律的增长速度，如图 2 所示.

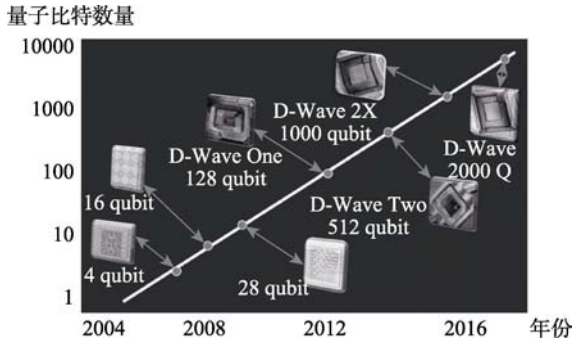

图 2　D-Wave 量子计算机发展路线（引自 D-Wave 官网）

D-Wave 量子计算机发展迅猛,完全不同于通用量子计算机的量子门电路构造思路，旨在多学科路线发展以及实用型商业化目标，目前正处于从纯科学向工程学的转型阶段. D-Wave 自 2011 年开始发布商用型 D-Wave 量子计算机，相继与美国军火商 Lockheed Martin、Google、美国 Los Alamos 国家实验室(LANL)、美国橡树岭国家实验室(Oak Ridge National Laboratory，ORNL)等建立合作. 2019 年德国 Forschungszentrum Jülich 超级计算中心购买了 D-Wave 公司最新的 Advantage 量子计算机，配备超过 5000 个量子比特,是 D-Wave 2000Q 的两倍以上. 符合 Geordie Rose 提出的发展趋势，与经典计算机领域的摩尔定律提出的发展速度相当.

3.2.2　基于 D-Wave 量子退火原理的整数分解国内外研究现状

量子退火算法最早是由 A.B.Finnila[66]提出来的,主要是用来解决多元函数的最小值问题. D-Wave 的量子退火算法旨在组合优化、机器学习[67]、采样等问题的研究，包括地球物理反演[68]、蛋白质折叠问题[53]、旅行商问题(Travelling salesman problem)[69]、图像着色问题(GCP)[52]、城市交通问题[70]、整数分解问题[71]、希格斯玻色子优化问题[72]、量子模拟问题[73-74]等.

量子退火(Quantum Annealing，QA)算法基本思想是利用量子涨落来构造优化算法，即量子隧穿效应(Quantum Tunneling Effect). 与传统经典计算机模拟热波动的模拟退火不同，量子退火算法独特的量子隧穿效应更容易跳出局部最优解，有望逼近全局最优解.

如图 3 所示，模拟退火算法在陷入局部最优点 P 后只能以“翻山越岭”的方式越过能量势垒到达全局最优点 P'，而量子退火算法独特的量子隧穿效应不用暂时接受较差的当前解就可以直接从 P 点穿透能量势垒到达 P'，这是与经典模拟退火及其他众多计算搜索算法相比的一个独特优势.

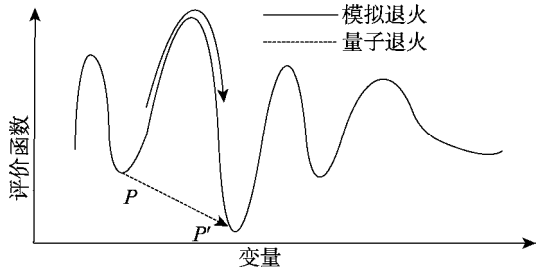

图 3　量子退火与模拟退火示意图

2012 年，上海大学王潮等人首先提出将组合优化问题映射到 D-Wave 机器的理论模型[65]，并且分析了量子计算在密码破译方面的应用.

2017 年，Dridi 等人[54]首次提出将代数几何应用于量子退火相关问题. 将代数几何与量子退火算法结合通过 D-Wave 2X 分解整数 200099,该模型存在量子连接限制，需要的比特数多.

2018 年，Shuxian Jiang 等人[71]通过 D-Wave

2000Q，使用具有 Ising 模型的乘法表来分解整数 376289. 通过对乘法表进行分栏，有效地平衡分解整数时使用量子比特数和 D-Wave 输入参数的范围. 在 D-Wave 硬件受限的情况下，降低对其精度的需求. 由于 D-Wave 中存在量子比特连接约束，受到硬件架构的可扩展性的限制，因此不能直接应用于大规模问题.

2019 年，洛克希德马丁公司的 RICHARD H. WARREN[75]提出可遍历分解 1000 以内所有整数的链式模型. 为了使量子退火算法可以分解某一个区间内所有的数，将输入参数固定为区间上限. 同时为了降低算法复杂度，排除所有包含 2、3、5 因子的数. 为了证明算法有效性，RICHARD H. WARREN 遍历分解 1000 以内所有的数. 但该算法在分解较小的数时会有很多冗余的量子比特并且 Ising 模型参数范围较大，因此难以具有实际意义.

2018 年，上海大学王潮教授等人[76]在整数分解的二进制乘法表的基础上，提出通用的量子退火整数分解框架. 通过根据目标值限制高栏进位变量个数的方式有效减少了构造成本函数的冗余变量，增加专用量子计算机量子比特的利用率. 同时在 D-Wave 公司提供的量子计算软件环境中成功分解整数 1005973(20-bit). 最大分解的整数超过文献[71]的 376289 和文献[75]的 7781 达到目前公开文献的最大规模. 并且对于任意分解的整数量子比特数、局部场系数和耦合项系数均优于二者.

对于通用量子计算机里说，由于受限于量子纠错(surface code)等技术的限制，无论是目前量子比特规模最大的 72 量子比特 Bristlecone（“狐尾松”）还是实现了量子优越性的 Sycamore 都远达不到.

美国科学促进会、科学网和 IEEE 对该研究进行报道，在 EurekAlert 上点击次数超过 13399 次. 王新梅教授在肯定该研究成果的同时认为可以考虑基于量子退火算法攻击其他加密算法[77].

现有两类量子计算机，一是通用量子计算机，二是 2011 年加拿大 D-Wave 公司推出的商业化专用量子计算机. 通过量子计算实现整数分解主要有两个研究方向：一种为基于通用的 Shor 算法的电路模型算法，另一种量子绝热计算(QAC)，也可实现整数分解. 与通用量子计算机不同的是 D-Wave 量子计算机的原理量子退火是基于绝热量子理论. 但是理想绝热的环境无法在现实中完美达到，比如 D-Wave 在 80 mK 以下进入热退火阶段，15 mK 以下进入量子退火阶段，最终稳定在 5 mK. D-Wave 量子计算机无法达到绝对零度，量子演化过程中微弱的热交换使其有一定概率发生跃迁，导致实际量子退火无法达到理想绝热水平.

因此，基于 D-Wave 原理的量子退火实际上可以看成一种高度逼近理想绝热退火的算法，这也是 D-Wave 量子计算机可用于寻找最优解及亚优解的原因.

图 4 为整数分解的几种方法的比较. Shor 算法由于通用量子器件的进展缓慢，目前仅能物理实现整数 85 的分解，对实际运行的公钥密码不能构成安全威胁. 因此，在不具备突破性的量子纠错码等技术之前，安全领域构成巨大潜在威胁的应用仍旧还有一段距离. 这也说明在抗量子密码研究领域需考虑来自于 Shor 算法之外的 D-Wave 量子退火的攻击可行性.

基于绝热量子理论的 NMR 的整数分解的研究由于 NMR 的量子比特数的限制，无法扩展到大规模整数分解的情况，且该方法不具有通用性与可扩展性，当前最大可实现以 3 比特分解整数 291311.

基于 D-Wave 原理量子退火算法分解的最大整数为 376289. 专用型量子计算机 D-Wave 商用化进展迅猛，已实现 100 多个应用，覆盖人工智能、密码学、生物化学等重点学科领域. 然而密码学方面的应用由于 Shor 算法而被人们忽视，最大分解整数规模大于通用量子计算机的同时，硬件平台的扩展速度较快，比 Shor 算法更具现实威胁性[78].

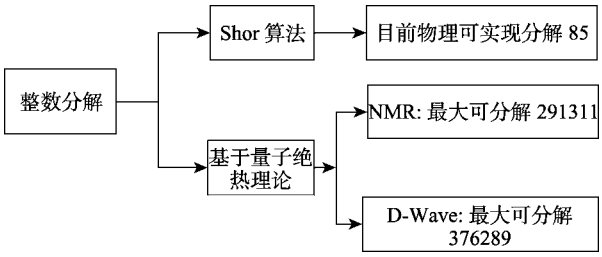

图 4 整数分解方法比较

3.3 D-Wave量子计算机后量子密码时代攻击潜力分析

前文介绍了 D-Wave 量子计算机的商业化进展和发展速度. 如果能保持比肩摩尔定律的发展速度，经过多次迭代则有望制造出大规模专用型量子计算机，影响范围包括人工智能、密码学、生物化学等领域. 在后量子密码时代，将 RSA 加密算法转化为组合优化问题[57]后利用 D-Wave 量子计算机的量子隧穿效应搜索全局最优解完成密码破译.

在密码破译领域，D-Wave 量子计算机破译 RSA 在通用性和可扩展性上受其自身硬件的量子

互连限制制约，对量子设备本身以及理论模型构造也是一大挑战. 现在的量子算法需要从整数分解时使用的量子比特和 Ising 模型参数 h,J 进行优化，量子硬件可以从拓扑连接结构和量子比特耦合精度等方面进行优化. 在密码设计领域，RSA 加密体系对基于量子退火原理的攻击方式还没有针对性的防御手段，在后量子密码时代有被破译的可能性，可以考虑来自 D-Wave 量子计算机的攻击.

4　量子计算加速传统密码攻击模式，拓展已有量子计算的攻击能力

4.1　椭圆曲线密码的侧信道攻击背景

椭圆曲线密码(Elliptic Curve Cryptography, ECC)是 1985 年由 N.Koblitz 和 V.Miller 提出的一种公钥密码体制[79,80]，其安全性建立在椭圆曲线离散对数问题(ECDLP)的指数级求解困难性之上的,已经被广泛应用到保护信息系统数据的私密性. 椭圆曲线密码在单位安全强度、密钥长度、抗攻击能力等方面优于 RSA 公钥密码.

ECC 的安全性主要依靠椭圆曲线离散对数问题(ECDLP)，针对椭圆曲线算法的攻击方法有：穷举搜索、大步小步算法(Baby-Step giant-step algorIthm)[81]、Pollard's rho 算法[82]、Pohlig-Hellman 算法[83]、Multiple Logarithms 算法[84]、Index Calaulus 算法[85]、MOV 约化[86]、FR 约化[87]、SSSA 算法(Semaev-Smart-Satoh-Araki)[88-90]、Weil Descent 攻击[91].

安全强度高的加密算法不能唯一确定密码系统的安全性，分析密码系统的安全性时需要考虑来自攻击加密算法以外的破译模式. 任何部署加密算法的软硬件平台在工作期间不可避免地向系统外界泄露物理信息. 攻击者通过不同手段获取这些信息后可以绕开加密算法攻击加密保护的系统，利用这种信息攻击的方式称为侧信道攻击.

侧信道攻击（Side Channel Attack—SCA,又叫旁路攻击或边信道攻击）成为密码学应用研究中的热点[92]，常见的攻击方式如图 5 所示. 这些攻击方式都不针对加密算法本身进行攻击而是通过各种方式从密码系统泄露出的信息中进行分析，攻击成本较低、效果较好，严重影响密码系统的安全程度.

对椭圆曲线密码的侧信道攻击研究可以被认为是一种安全测试方法，即通过测试密码芯片泄露信息识别和修复安全漏洞来提高密码系统的安全性.

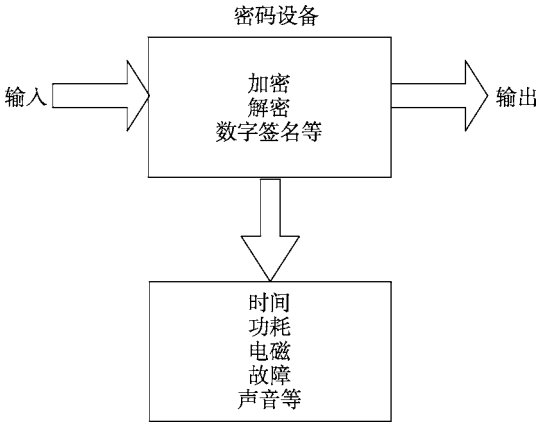

图 5　侧信道攻击模型

4.2　椭圆曲线密码的侧信道攻击的国内外研究现状

1999 年，法国学者 Jean-S´ebastien Coron[93]提出将差分能量分析(Differential Power Analysis，DPA)攻击推广到椭圆曲线(ECC)密码系统，描述了关于 EC Diffie-Hellman 密钥交换和 EC El-Gamal 类型加密的 DPA，并提出了相应的防御措施.

2000 年美密会上，Ingrid Biehl 等人把对 RSA 地差分故障攻击(Differential Fault Attack，DFA)成功地应用于椭圆曲线上[94]，提出了三种不同类型的攻击，如果将误码插入到防篡改设备的椭圆曲线计算中，则可以使用这些攻击来获得关于密钥的信息，并通过实验证明了攻击的有效性.

2003 年，Toru Akishita 等人[95]基于 Louis Goubin 的思想提出了一种新颖的攻击方式—零值点攻击(Zero-Value Point Attacks)，并详细地介绍了此攻击方式的原理，为 ECC 的安全实现提供了新的安全标准. 最后强调应该关注允许执行 DPA 的计算环境下的零值点攻击.

2006 年，国内清华大学的赵彦光、白国强等人[96]简单功耗分析(Simple Power Analysis, SPA)对 ECC 专用密码芯片进行抗攻击和功耗攻击研究，实验表明要恢复出密码芯片中长度大于 192-bit 的密钥，仅需采集一条功耗曲线.

2007 年，国内浙江大学的赵岚[97]通过利用 Simplepower 功耗分析工具对 Montgomery 标量乘法进行功耗分析(SPA)和差分功耗分析(DPA)的研究，实验结果表明 Montgomery 标量乘法虽然具有较好的抵抗简单功耗攻击(SPA)的能力，但无法抗差分功耗攻击(DPA).

2008 年，以色列学者 Eli Biham, Adi Shamir 等人[98]在美密会上提出了一种新的利用计算机指令的硬件实现中的漏洞来进行攻击的方案——漏洞攻击

(Bug Attack),对 Pohlig-Hellman 和 RSA 密码体制展示这种攻击，并讨论该攻击对椭圆曲线密码系统和对称密码的适用性.

2009 年，滑铁卢大学的 Agustin Dominguez Oviedo 等人[99]针对椭圆曲线中的标量乘法(ECSM)算法提出新的攻击方法：基于故障攻击(Fault-Based Attack)，给出了对一般椭圆曲线和对 NIST 公布的标准安全曲线攻击的原理、实现算法以及成功的概率，使用该方法攻击 NIST 公布的多条安全曲线成功率达到了 99%，威胁到除了 K-283 曲线以外的所有曲线. 这种攻击对现有椭圆曲线的安全性具有相当大的威胁，针对这种攻击，他们也给出了一些有效防御措施.

2010 年，西安电子科技大学的马博等人[100]在智能卡中椭圆曲线密码(ECC)抗功耗攻击基础上提出一种改进方案. 该方案的核心是选取坐标系的最优组合，并将密钥分解为多组相同长度的短密钥. 实验结果表明,智能卡中的 ECC 抗功耗攻击方案执行效率提高了 1/4 以上.

2011 年,中国科技大学的邓秋成等人[101]对 ECC 中的 ML(Montgomery Ladder)点乘算法进行了差分功耗分析攻击. 实验结果表明,ML 算法不能抗零指数多数据(Zero-Exponent Multiple-Data, ZEMD)差分功耗分析攻击. 证明该算法不安全，在实际应用中应采取一些保护措施.

2012 年，军械工程学院的张金中等人[102]基于符号变换故障攻击原理，针对采用滑动窗口算法实现点乘运算的椭圆曲线密码对故障位于不同运算（倍点运算和加法运算）提出解决方案. 当故障位于倍点运算时，提出一种改进的故障分析方法，可以解决“零块失效”问题. 实验结果表明，通过 15 次故障注入可以恢复 192 位完整密钥. 当故障位于加法运算时，给出一种新的故障分析方法. 实验结果表明,1 次故障注入可将密钥搜索空间降低 2^7~2^{15}. 该研究对使用滑动窗口算法的其他加密算法故障攻击具有一定的参考意义.

2016 年梁芳和华中科技大学沈济南[103]针对密码芯片资源受限，抵抗功耗攻击和加密效率相互矛盾的问题，利用奇系数梳妆算法对标量编码可以抵抗 SPA 攻击. 同时利用掩码技术将标量乘运算的基点随机化，使其可以抵抗 RPA、DPA、ZPA 攻击. 该算法与 BR、WBRIP 抗功耗攻击算法相比较，可以同时兼顾到安全性和运算效率.

2018 年南京航空航天大学刘哲[104]使用 Four$\mathbb{Q}$ 软件在嵌入式设备节能、高效和高安全性地实现椭圆曲线密码，可以有效抵抗多种侧信道攻击. Four$\mathbb{Q}$ 首先在 128 位安全级别为基于常量时间曲线的标量乘法、DH 密钥交换和数字签名设置了新的速度记录，实现目标为 8、16 和 32 位微控制器. 其次，利用 Four$\mathbb{Q}$ 算法设计了一套侧信道对策，并提出了一种安全的实现方案，提供针对各种复杂的侧信道攻击的保护，包括差分功耗分析(DPA). 定时攻击实验结果表明，Four$\mathbb{Q}$ 有效性超过了 Curve25519，有在遵循物联网协议的低功耗设备上部署的潜力.

4.3 基于量子算法的椭圆曲线密码的侧信道攻击方法

ECC 的安全性较高，几乎不可能通过传统的数学分析和穷举攻击来解决. 根据现在计算机的运算能力，攻击 160 位 ECC 安全曲线需要大约 1012 年. 对于 NIST 公布的安全曲线中最小的 163-bit 位曲线来说，攻击所耗费的人力、物力、时间等都是不可估量的. ECC 因其破译难度高，占用通信资源少，通信安全性高等优势得到了广泛的应用.

虽然相对于数学攻击，侧信道攻击利用系统内部无意间泄露的信息进行攻击，相比数学分析更快速有效，但某些侧信道攻击方法仍存在计算复杂度较高、资源浪费等问题. 因此，需要探索新的攻击方法来解决椭圆曲线密码的侧信道攻击问题.

随着量子时代的来临，量子计算对现代密码学的攻击引起广泛关注. 受限于量子计算机硬件发展不充分的限制，纯量子算法难以对现代密码体系造成实质上的威胁，还停留在概念层面.

通过量子计算与经典计算混合架构的方式，可以降低密码攻击时对量子硬件的需求. 混合架构兼具量子力学和经典计算机的特性，具有强大的计算和存储能力. 将量子计算独有的特性与经典算法相结合，可以加速传统密码攻击模式. 椭圆曲线破译中，侧信道密码攻击模式和量子计算的结合取得了进展. 它作为一种新颖的密码系统攻击思路，对量子计算攻击各种公钥密码体系起到了引导作用.

4.3.1 基于量子退火的差分功耗分析

基于量子绝热理论的量子退火算法将量子隧穿效应跳出局部最优解的能力应用于侧信道攻击防御系统中，可能实现对密码系统安全性的进一步优化.

为了应对侧信道攻击中的基于功耗的攻击模式，文献[105,106]提出波动动态差分逻辑(Wave Dynamic Differential Logic, WDDL). 虽然消除了差

分功耗，但需要额外的电路面积和功耗，密钥依然有可能被破译. 2010 年 Kazuyuki Tanimura[107]提出基于传统模拟退火算法的 ExCCel(Exploration of Complementary Cells)优化算法，对 WDDL 进行优化. 该算法利用标准单元自动生成和探索互补单元的组合，有效降低在 AES S-Box 电路中需要的额外面积和功耗，并且对差分功耗分析的抵抗能力较强.

2016 年，仲明等人[108]提出基于量子退火算法的差分功耗分析(DPA)防御系统的优化，利用量子退火算法对 WDDL 进行优化，减少不必要的附加单元，相对于 ExCCel 优化算法，利用量子隧穿特性有概率穿透能量更高的势垒而不必暂时接受较差的当前解，可以以更高的概率更快地得到最优解. 使得电路额外面积和功耗进一步降低，提高抵抗差分功耗分析的能力.

量子退火与模拟退火相比有着独一无二的特性，如何利用该特性来替换实际场景中的模拟退火算法起到量子计算加速优化目的，是量子计算的一个应用方向.

4.3.2　基于 Grover 算法的 ECC 侧信道攻击

在密码破译方面，某些量子算法，如 Grover 算法，只是将密钥长度降为一半的穷举搜索，对密码算法构不成致命威胁. 因此考虑将量子算法与经典算法中的侧信道攻击结合，对 ECC 加密算法进行攻击.

如何利用量子计算的优势对经典密码的分析过程进行加速是密码学中的重要问题. 2009 年，钟普查[109]等人将量子计算领域的 Grover 搜索算法和经典密码学中的中间相遇攻击方法相结合，三个密钥的三重 DES 攻击可以在 $O(56\times2^{56})$步骤完成，相对已有的攻击算法，该算法降低了算法的计算复杂度.

2010 年 NARA[110]使用扫描式攻击方式破译 ECC 加密算法. 通过检测中间值特定的 1-bit 序列，判断 ECC 点乘运算的寄存器位置，从而判断该中间值是否由目标电路计算出来. 对于给定的 n-bit 的密钥，使用该算法可以将计算复杂度从 2^m 降低到 $2m^2$.

2016 年，陈宇航等人[111]对 NARA 的扫描式攻击方法进行改进，首次将量子 Grover 搜索算法与侧信道攻击相结合. 扫描式攻击方法需要对采集到中间值建立一个数据库，使用清华大学龙桂鲁[112]提出的 Grover 改进算法可以将数据库搜索的复杂度从 $O(n)$ 降低到 $O(\sqrt{n})$，并且在数据库不是很大的时候成功率也能达到 100%. 完成了 ECC 扫描式攻击方法中间值数据库大小有限的情况下的量子计算加速，将计算复杂度从 2^N 降低到 $2N^{3/2}$，提高算法的搜索效率.

中间相遇攻击牺牲存储空间降低破译密码时的计算复杂度，通过将明文和密文处理到中间值状态，并且对比二者的中间值来推测正确的密钥. 对于 ECDSA 签名来说，每次使用的临时密钥都是不同的，需要在一次数据采集的时间内完成. 而破译时外界环境具有不确定性，受到内存、CPU 等因素影响，可能会导致破译的密钥出现部分 bit 的错误，降低破译成功率. 2016 年，贾徽徽等人[113]提出了一种新的 Grover 量子中间相遇搜索算法，将 Grover 量子搜索算法和中间相遇攻击相结合，并将其应用于纠正 ECC 侧信道攻击中出现的错误密钥位. 对于长度为 N 的临时密钥，当受到外界影响出现 M 个错误 bit 时，改进的方法进行破译时计算复杂度和中间相遇算法相比大幅降低. 实验结果表明攻击 ECC 时可以保证破译的结果正确率为 100%.

2017 年，王潮等人[114]在 ECC 受到故障攻击时使用固定相位的 Grover 算法进行优化，发现不同的旋转相位攻击成功率不同，当旋转相位固定为 0.1π 时最高. 作为量子攻击算法，在攻击公钥密码时计算复杂度以指数级下降，是一种新的有效攻击方法. 电压毛刺攻击的临时密钥后建立数据库，并且将错误密钥经过点乘运算后与数据库中的密钥进行对比，此时使用基于固定旋转相位改进的 Grover 量子算法可以加速完成数据库搜索. 根据实验结果，使用该方法攻击 NIST 发布的 Kob1itz 安全曲线 K-163 能以 100%的概率完成，有助于拓展量子计算对其他公钥密码体制的攻击.

Grover 量子搜索算法在 ECC 侧信道攻击中的部分攻击方式有一定进展，包括电压毛刺攻击、中间相遇攻击、扫描式攻击，采用量子算法和经典算法混合架构的方式可以有效地利用量子计算机的特性对现代密码体系的破译起到加速功能.

量子算法为不同于传统的椭圆曲线的侧信道攻击方法，它的成功应用于椭圆曲线的侧信道攻击的威胁性要大于传统方法. 将量子计算作为子系统加速传统侧信道攻击方法，结合了二者优势的情况下对公钥密码体系的安全性造成了更大的挑战. 同时，也为密码分析提供一种新的参考方法. 随着越来越多的学者加入到侧信道分析研究中，相信在不久的将来，侧信道分析会在密码系统的安全性测试中发挥重要作用.

5　NTRU 破译及后量子分析

NTRU 公钥密码体制是目前少有的受到量子计

算攻击时有抵抗能力的加密算法，是后量子密码的研究热点之一，可有效抗击 Shor 等量子计算攻击.

演化密码已经在 NTRU 后量子密码领域取得了实际成果[115]：2005 年，解放军理工大学的赵小龙等人[116]将攻击 NTRU 问题进行转换,使用遗传算法进行求解. 和传统的强力攻击相比，算力的需求降低 3 个数量级. 作为组合优化问题，如果可以利用量子隧穿效应进行加速可以进一步优化.

2009 年，解放军理工大学的唐元刚等人[117]提出基于格理论的 NTRU 遗传算法攻击，把对 NTRU 的攻击问题转化为遗传算法能解决的问题空间，讨论了初始种群、变异率等参数对算法的影响. 实验表明，与一般搜索算法相比，该算法虽然有一定优势但是仍然属于经典计算机的范畴，当标准格维数增加时，受限于计算机算力，难以对 NTRU 造成实质性威胁. 并且初始参数不同对计算结果和稳定性影响较大，

2016 年 3 月,印度学者 Himani Agrawal 和 Monisha Sharma 比较了基于进化的算法对 NTRU 的优化效果[118]. 对比了蚁群优化算法和粒子群优化算法的效果. 根据实验结果，两种算法优化后的 NTRU 仿真速度有了不同程度的改进. 优化后速度分别可以增加 34.65%和 41.31%. 加密同样比特数的信息时,粒子群优化后的 NTRU 加密速度和 RSA 相比从 1.74 倍增加到了 4.59 倍,使得 NTRU 的优势进一步扩大，证明了优化算法在改进 NTRU 加密算法的有效性. 同年，两位学者使用组合优化方法对 NTRU 进一步优化[119]. 优化后的计算复杂度接近 RSA 加密算法，并且具有速度快、占用内存小的优点. 实验结果表明，使用粒子群算法优化 NTRU 可提供高于遗传算法和蚁群算法的安全性.

在后量子密码时代有望利用量子计算并行计算加速能力和量子隧穿效应在优化 NTRU 时进行加速.

碰撞问题是在保证存在碰撞的前提下，在函数 $F:X\to Y$ 中寻找两个不同的元素映射后结果相同. 碰撞问题对于密码学来说特别有意义，因为在各种加密协议中使用了一些称为哈希函数的函数. 这些协议的安全性主要取决于在这些函数中查找冲突的假定难度.

哈希函数[120]最有效的量子攻击称作 Grover 算法，它成功扩展到在一对函数中找到所谓的 *claws*，大大降低哈希运算的安全性. 同时，这对经典签名和比特承诺方案的安全性产生了影响.

2016 年法国研究者 Marc Kaplan 等人[121]使用量子资源攻击经典密码系统，研究了一种攻击算法——Simon 量子算法，以此来攻击该模型下的对称密码学系统，利用 Simon 算法，许多寻找冲突的经典攻击算法能得到显著提速. 例如，在经典设定中，寻找一个冲突需要 $\Omega(2n/2)$ 次查询；当冲突伴随一些隐藏的周期性时，利用量子模型只需要 $O(n)$ 次查询即可找到冲突.

以对称密码为例，对称密码的安全性取决于对原语进行的密码分析的数量. 对于分析对称原语，密钥长度的加倍已经不足以恢复抵抗量子对手的安全性.

得益于多年来在经典世界中构建的大型且不断更新的密码分析工具箱，我们对原语抵抗经典对手的安全性可以进行可靠的评估. 然而，在后量子世界，也就是考虑量子对手时，情况就不同了. 因此，我们需要为量子对手建立一个完整的密码分析工具箱，就像为经典世界所做的那样. 这是正确评估现有密码的后量子安全性，为后量子世界设计新的安全密码的基础.

6 总结与展望

本文通过对量子计算在密码学应用的研究与分析，强调量子计算基础研究对跨学科应用可行性的重要性以及对基础学科领域突破的推动性. 在传统密码研究的基础上，拓展到量子计算环境下的密码学研究，并展望量子人工智能算法对 NTRU 等后量子密码攻击的可能性. 在基于量子算法的 ECC 侧信道攻击、Shor 算法对公钥密码的攻击、基于量子绝热理论的整数分解等方面均取得了丰硕的研究成果,为量子计算在信息科学领域的工作提供了思路,对未来量子计算环境下的密码学研究提供了一定的借鉴意义.

在密码破译领域，通用量子器件发展缓慢，离破译现今使用的 1024 比特的 RSA 和 163 比特的 ECC 很遥远. 所以亟需探索其他量子算法的攻击可行性. 2018 年国内首次提出使用专用量子计算机 D-Wave 攻击 RSA 加密体系，作为完全不同于 Shor 算法的量子退火整数分解算法，通过实验验证了在分解不同整数时的通用性和与其他量子退火算法相比的有效性. 最大分解整数 1005973(20-bit),达到目前整数分解的最大规模，大于普渡大学和洛克希德马丁公司的 376289 和 7781. 并且在量子退火整数分解算法的三项指标（量子比特数、局部场系数、耦合项系数）上均为最优.

量子攻击方法为不同于传统的侧信道分析方法,拓展了已有量子计算的攻击能力. Grover 量子搜索算法成功应用于 ECC 侧信道的中间相遇攻击，能

够以成功率 1 修正 ECC 攻击中出现的错误比特. 相比于传统模拟退火算法的 ExCCel 算法，量子退火算法应用于 ECC 侧信道攻击可以以更高的概率更快获得最优解，提高系统的抗差分功耗攻击能力.

图 6 为量子计算环境下的相关密码学的研究，包括椭圆曲线侧信道攻击，公钥密码及基于量子绝热理论的整数分解的研究.

量子攻击提供了一种新的、不同于传统密码的计算模式，在密码设计和破译领域实现对传统密码的进一步拓展. 量子环境下的密码学研究将成为已有的密码学研究方法的一种增强手段，协助/加速传统密码的攻击模式，拓展已有量子计算的攻击能力.

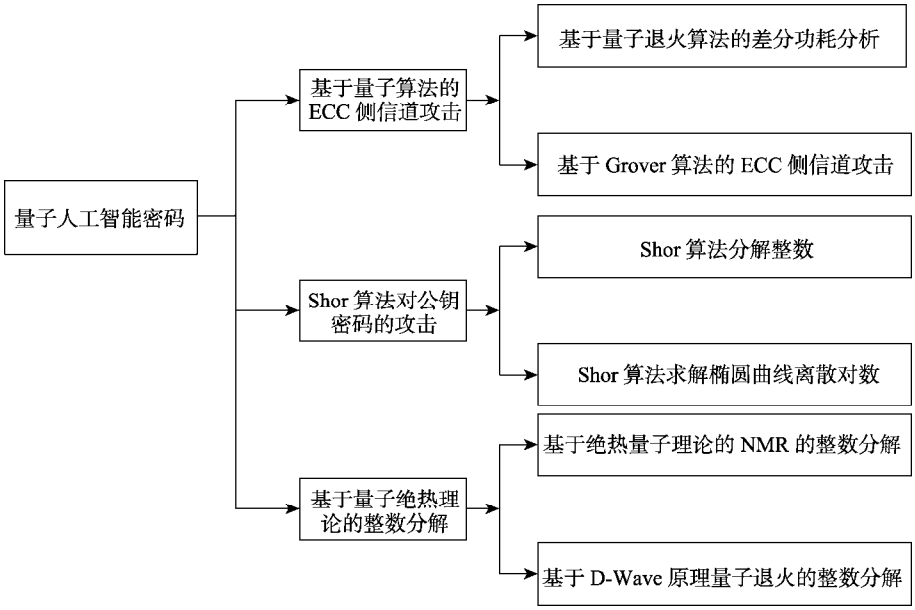

图 6　量子计算环境下的密码学研究

未来密码学针对量子计算的研究可以针对以下几个方面：

(1)量子计算著名的 Shor 算法在理论上威胁到现有密码体系的安全性，但是量子计算并非站在密码学的对立面. 无论在密码设计还是密码破译领域，量子计算都可以起到一定的辅助作用. 通过强大的并行计算能力、独特的组合优化求解能力等特性解决传统算法不擅长的问题，同时后量子密码的研究扩展了加密算法的演进道路.

(2)发展专用型量子计算用于其他密码部件设计及公钥密码分析的潜能及拓展. 量子设计密码是一个新的领域，不仅要考虑如何将传统密码部件与量子计算方式结合，还要考虑如何通过量子计算获得所需的密码学部件相关指标. 未来探索专用型量子计算机用于其他密码部件设计是一大挑战.

(3)探索量子经典混合计算架构在密码设计和密码分析领域的模块化分析及设计潜能. 基于已有的研究，探索量子经典混合计算架构在密码设计和密码分析领域模块化的潜在可行性研究，也可进一步提出 D-Wave 量子计算机结合类脑认知的混合计算思想，探索构建高效精确自主的量子人工智能计算架构.

(4)量子计算密码攻击有望对一些新型的密码体制攻击提供探索性研究.

量子计算的发展对经典公钥密码系统的安全性构成了极大威胁[122]，研究抵抗量子攻击方案时应该考虑来自 Shor 算法和量子退火算法攻击的可能性，同时演化密码结合量子退火算法扩展了密码设计思路.

结合量子计算的密码学研究可为传统密码设计、量子计算破译密码、抗量子密码研究提供新的角度和思路. 量子计算加速了传统密码攻击模式，拓展了已有量子计算的攻击能力.

参　考　文　献

[1] Feynman R P. Quantum mechanical computers. Optics News, 1985, 11(2): 11-20

[2] Feynman R P. Simulating physics with computers. International Journal of Theoretical Physics, 1982, 21(6): 467-488

[3] Wang Chao, Wang Yun-jiang, Hu Feng. Shaping the future of commercial quantum computer and the challenge for information security. Chinese Journal of Network and Information Security, 2016, 2(3): 17-27 (in Chinese)
(王潮, 王云江, 胡风. 量子计算机的商业化进展及对信息安全的挑战. 网络与信息安全学报, 2016, 2(3): 17-27)

[4] Bennett C H, Shor P W. Quantum information theory. IEEE Transactions on Information Theory, 1998, 44(6): 2724-2742

[5] Castelvecchi D. Quantum computers ready to leap out of the lab in 2017. Nature, 2017, 514(7635): 9-10
[6] Gibney E. Physics: Quantum computer quest. Nature News, 2014, 516(7529): 24
[7] Brainard J. What's coming up in 2018. Science, 2018, 359(6371): 10-12
[8] Cho A. DOE pushes for useful quantum computing. Science, 2018, 359(6372): 141-142
[9] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574(7779): 505-510
[10] Pednault E, Gunnels J A, Nannicini G, et al. Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits. arXiv preprint arXiv: 1910.09534, 2019
[11] Li Ying, Sun Chang-Pu. Universal quantum computer and fault-tolerant quantum computation — concepts, status and prospects. Physics, 2019, 48(8): 477-487 (in Chinese)
(李颖, 孙昌璞. 通用量子计算机和容错量子计算——概念、现状和展望. 物理, 2019, 48(8): 477-487)
[12] Fowler A G, Devitt S J, Jones C. Surface code implementation of block code state distillation. Scientific Reports, 2013, 3(1): 1-6.
[13] Knill, E. Quantum computing with realistically noisy devices. Nature, 2005, 434(7029): 39-44
[14] Gidney C. Factoring with n+2 clean qubits and n-1 dirty qubits. arXiv: 1706.07884v2, 2018
[15] Deneuville J C. Post-quantum cryptography: tomorrow's security//Proceedings of the 3rd Envirorisk-Natural and technological risk management forum, Bourges, France, 2018: 1-6.
[16] Lenstra A K, Hendrik Jr W. The development of the number field sieve. Berlin, Germany: Springer, 1993
[17] Hamdi S M, Zuhori S T, Mahmud F. A Compare between Shor's quantum factoring algorithm and general number field sieve//Proceedings of the International Conference on Electrical Engineering and Information & Communication Technology. Dhaka, Bangladesh, 2014: 1-6
[18] Gaj K, Kwon S, Baier P. Area-time efficient implementation of theelliptic curve method of factoring in reconfigurable hardware for application in the number field sieve. IEEE Transactions on Computers, 2010, 59(9): 1264-1280
[19] Yan S Y. Quantum Computational Number Theory. Berlin, Germany: Springer, 2015
[20] Mahmud N, El-Araby E, Caliga D. Scaling reconfigurable emulation of quantum algorithms at high-precision and high-throughput. Quantum Engineering. 2019. 1(2): 1-21
[21] Miquel C, Paz J P, Perazzo R. Factoring in a dissipative quantum computer. Physical Review A, 1996, 54(4): 2605-2613
[22] Parker S, Plenio M B. Efficient factorization on with a single pure qubit and logN mixed qubits. Physical Review Letters, 2000, 85 (14): 3048-3052
[23] Vandersypen L M K, Steffen M, Breyta G. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 2001, 414(6866): 883-887
[24] Vartiainen J J, Niskanen A O, Nakahara M. Implementing Shor's algorithm on Josephson charge qubits, Physical Review A, 2004, 70 (1): 1-12
[25] García-Mata I, Frahm K M, Shepelyansky D L. Effects of imperfections for Shor's factorization algorithm. Physical Review A, 2007, 75(5): 1-10
[26] Lu C Y, Browne D E, Yang T. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. Physical Review Letters, 2007, 99(25): 1-4
[27] Thompson M G, Politi A, Matthews J C F. Integrated waveguide circuits for optical quantum computing. Institution of Engineering and Technology, 2011, 5 (2): 94-102
[28] Lucero E, Barends R, Chen Y. Computing prime factors with a josephson phase qubit quantum processor. Nature Physics, 2012, 8(10): 719-723
[29] Martín-López E, Laing A, Lawson T, et al. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature Photonics, 2012, 6(11): 773-776
[30] Geller M R, Zhou Z. Factoring 51 and 85 with 8 qubits. Scientific Reports, 2013, 3: 1-5
[31] Smolin J A, Smith G, Vargo A. Oversimplifying quantum factoring. Nature, 2013, 499(7457): 163-165
[32] Monz T, Nigg D, Martinez E A, et al. Realization of a scalable shor algorithm. Science, 2016, 351(6277): 1068-1070
[33] Wang B L, Chen Y H, Ying B, Hu F, Zhang H G, Wang C. Research of the small Qubit quantum computing attack to the RSA public key cryptography, Chinese Journal of Network and Information Security, 2017, 3(10): 25-34 (in Chinese)
(王宝楠, 陈宇航, 尹宝, 胡凤, 张焕国, 王潮. 第一寄存器小 Qubit 量子计算攻击 RSA 研究.网络与信息安全学报, 2017, 3(10): 25-34)
[34] Zalka C. Shor's algorithm with fewer (pure) qubits. arXiv preprint quant-ph/0601097, 2006
[35] Fürer M. Faster integer multiplication. SIAM Journal on Computing, 2009, 39(3): 979-1005
[36] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 1999, 41(2): 303-332
[37] Beckman D, Chari A N, Devabhaktuni S, et al. Efficient networks for quantum factoring. Physical Review A, 1996, 54(2): 1034-1063
[38] Vedral V, Barenco A, Ekert A. Quantum networks for elementary arithmetic operations. Physical Review A, 1996, 54(1): 147-153
[39] Beauregard S. Circuit for Shor's algorithm using 2n+ 3 qubits. arXiv preprint quant-ph/0205095, 2002
[40] Takahashi Y, Kunihiro N. A quantum circuit for shor's factoring algorithm using 2*n*+2 qubits. Quantum Information & Computation, 2006, 6(2): 184-192
[41] Zalka C. Shor's algorithm with fewer (pure) qubits. arXiv preprint quant-ph/0601097, 2006
[42] Häner T, Roetteler M, Svore K M. Factoring using 2n+ 2 qubits with Toffoli based modular multiplication. arXiv preprint arXiv: 1611.07995, 2016
[43] Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. arXiv preprint arXiv: 1905.09749, 2019
[44] Shor, P W. Algorithms for quantum computation: Discrete logarithms and factoring//Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, USA, 1994, 124–134
[45] Eicher J, Opoku Y. Using the Quantum Computer to Break

Elliptic Curve Cryptosystems, 1997

[46] Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv preprint quant-ph/0301141, 2003

[47] Rötteler M, Steinwandt R. A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth *O* (log 2 *n*). Quantum Information & Computation, 2014, 14 (9): 888-900

[48] Roetteler M, Naehrig M, Svore K M, et al. Quantum resource estimates for computing elliptic curve discrete logarithms// Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China, 2017: 241-270

[49] Chen Y H, Ying B, Hu F, Zhang H G, Wang C. A quantum attack method for Shor algorithm of public key cryptography ECC. ZL 201510392417.1[P].2018 (in Chinese)
(陈宇航, 尹宝, 胡风, 张焕国, 王潮. 一种针对公钥密码 ECC 的 Shor 量子攻击方法. 中国专利, ZL 201510392417. 1[P]. 2018)

[50] Farhi E, Goldstone J, Gutmann S, et al. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. Science, 2001, 292(5516): 472-475

[51] Martoňák R, Santoro G E, Tosatti E. Quantum annealing of the traveling salesman problem. Physical Review E, 2004, 70(5): 057701

[52] Titiloye O, Crispin A. Quantum annealing of the graph coloring problem. Discrete Optimization, 2001, 8(2): 376-384

[53] Perdomo-Ortiz A, Dickson N, Drew-Brook M, et al. Finding lowenergy conformations of lattice protein models by quantum annealing, Scientific Reports, 2012, 2: 571-1-7

[54] Dridi R, Alghassi H. Prime factorization using quantum annealing and computational algebraic geometry. Scientific Reports, 2017, 7: 43048-1-10.

[55] Childs A M, Farhi E, Preskill J. Robustness of adiabatic quantum computation. Physical Review A, 2001, 65(1): 012322-6144- 6155

[56] Roland J, Cerf N J. Noise resistance of adiabatic quantum computation using random matrix theory. Physical Review A, 2005, 71(3): 032330—309-315

[57] C. J. C. Burges. Factoring as optimization. Microsoft Research, 2002, 2002(83): 1-18

[58] G. Schaller, R. Schützhold. The role of symmetries in adiabatic quantum algorithms. Quantum Information & Computation, 2010, 10 (1): 109-140

[59] Xinhua Peng, Zeyang Liao, Nanyang Xu, et al. Quantum adiabatic algorithm for factorization and its experimental implementation. Physical Review Letters, 2008, 101(22): 220405-1-4

[60] Nanyang Xu, Jing Zhu, Dawei Lu, et al. Quantum factorization of 143 on a dipolarcoupling nuclear magnetic resonance system. Physical Review Letters, 2012,108(13): 130501-1-5

[61] Dattani, N. S. , Bryans, N. Quantum factorization of 56153 with only 4 qubits. 2014, arXiv: 1411.6758

[62] Pal, S., Moitra, S., Anjusha, V. S., et al. Hybrid scheme for factorization: factoring 551 using a 3-qubit NMR quantum adiabatic processor. 2016, arXiv: 1611.00998

[63] Li, Zhaokai. High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: application to the experimental factorization of 291311. 2017, arXiv: 1706.08061

[64] Kebiao Xu, Tianyu Xie, Zhaokai Li, et al. Experimental adiabatic quantum factorization under ambient conditions based on a solid-state single spin system. Physical Review Letters, 2017, 18(13): 130504-1-5

[65] Wang C, Zhang H G. The influence of Canadian commercial quantum computer in cryptography. China Information Security, 2012, 2(35): 31-32.(in Chinese)
(王潮, 张焕国. 加拿大商用量子计算机对密码学影响. 信息安全与通信保密，2012, 2(35): 31-32)

[66] Finnila A.B., Gomez M.A., Sebenik C., et al. Quantum annealing: A new method for minimizing multidimensional functions. Chemical Physics Letters, 1994, 219(5-6): 343-348

[67] Feng Hu, Baonan Wang, Ning Wang, et al. Quantum machine learning with D-wave quantum computer. Quantum Engineering, 2019, 1(2): 2-12

[68] Wei Chao, Li Xiao-fan, Zhang Mei-gen. Quantum annealing optimization and geophysical inverse method. Progress in Geophysics, 2007, 22(3): 785-789 (in Chinese)
(魏超, 李小凡, 张美根. 量子退火最优化与地球物理反演方法. 地球物理学进展, 2007, 22(3): 785-789)

[69] M Roman, GE Santoro, T Erio.Quantum annealing of the traveling-salesman problem. Physical Review E, 2004, 70(5): 057701-1-4

[70] F. Neukart, D. Von Dollen, G. Compostella, et al. Traffic flow optimization using a quantum annealer. Frontiers in ICT, 2017, 4(29): 1-6

[71] S Jiang, KA Britt, TS Humble, et al. Quantum annealing for prime factorization. Scientific Reports, 2018, 8(1): 17667-1-9

[72] Mott A., Job J., Vlimant J.R., et al. Solving a higgs optimization problem with quantum annealing for machine learning. Nature, 2017, 550(7676): 375-379

[73] Harris R., Sato Y., Berkley A.J., et al. Phase transitions in a programmable quantum spin glass simulator. Science, 2018, 361(6398): 162-165

[74] King A.D., Carrasquilla J., Raymond J., et al. Observation of topological phenomena in a programmable lattice of 1,800 qubits. Nature, 2018, 560 (7719): 456-460

[75] Warren R. Factoring on a quantum annealing computer. Quantum Information and Computation, 2019, 19(3&4): 252–261

[76] W. C. Peng, B. N. Wang, F. Hu, et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. Science China: Physics, Mechanics & Astronomy 2019, 62(6): 5-12

[77] X. M. Wang. Quest towards“factoring larger integers with commercial D-Wave quantum annealing machines”. Science China: Physics, Mechanics & Astronomy2018, 62(6): 060331-1

[78] Wang Baonan, Yao Haonan, Hu Feng, et al. Quantum annealing distributed integer decomposition study of local field coefficient h and coupling coefficient J with stability Ising model. Scientia Sinica: Physica, Mechanica & Astronomica. 2018, 50(3): 030301-11 (in Chinese).
(王宝楠, 姚皓南, 胡风,王潮. 具有稳定性 Ising 模型局部场系数 h 和耦合项系数 J 的量子退火分布式整数分解研究. 中国科学: 物理学 力学 天文学. 2018, 50(3): 030301-11

[79] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Compution American Mathematical Society, 1987,48(177):

203-309

[80] V. Miller. Use of elliptic curves in cryptography. Lecture Notes in Computer Science, 1986, 218: 417-426

[81] Shanks D. Class number, a theory of factorization and genera. Lewis, 1971,1971(20): 415-440

[82] J. Pollard. Monte Carlo methods for index computation. Mathematics of Computation, 1978, 32(143): 918-924

[83] S. Pohlig, M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory, 1978, 24(1): 106-110

[84] Chang K C, Leung C C, Yew W W, et al. Peak plasma rifampicin level in tuberculosis patients with slow culture conversion. European Journal of Clinical Microbiology & Infectious Diseases, 2008, 27(6): 467-472

[85] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Journal of Symbolic Computation, 2009, 44(12): 1690-1702

[86] A. Menezes, T. Okamoto, S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory, 1993, 39(5): 1639-1646

[87] G. Frey and H. Ruck. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of computation, 1994, 62(206): 865-874

[88] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Rikkyo Daigaku sugaku zasshi, 1998, 47(1): 81-92.

[89] Semaev I. Evaluation of discrete logarithms in a group of *p*-torsion points of an elliptic curve in characteristic *p*. Mathematics of computation, 1998, 67(221): 353-356

[90] N.P. Smart. The discrete logarithms problem on elliptic curves of trace one. Journal of Cryptology, 1999, 12(3): 193-196

[91] S. Glbraith and N. Smart. A cryptographic application of Weil descent. Codes and Cryptography. Lecture Notes in Computer Science, 1999,1746: 191-200

[92] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. Lecture Notes in Computer Science, 1996, 1109: 104-113

[93] J. Coron. Resistance against differential power analysis for elliptic curve cryptosystem. Lecture Notes in Computer Science, 1999, 1717: 292-302

[94] Ingrid Biehl, Bernd Meyer, Volker Muller. Differential fault attacks on elliptic curve cryptosystems. Lecture Notes in Computer Science, 2000, 1880: 131-146

[95] T. Akishita, T. Takagi. Zero-value point attacks on elliptic curve cryptosystem. Lecture Notes in Computer Science, 2003, 2851: 218-233

[96] Zhao Yanguang, Bai Guoqiang, Chen Hongyi, et al. Study of power analysis attack to ECC in ASIC chip. Computer Engineering and Applications, 2006, (16): 25-28 (in Chinese)
(赵彦光, 白国强, 陈弘毅等. ECC 专用密码芯片的功耗分析研究. 计算机工程与应用, 2006, (16): 25-28)

[97] Zhao Lan. Research of power-analysis to elliptic curve cryptography. Mechanical & Electrical Engineering Magazine, 2007, 24(8): 8-10 (in Chinese)
(赵岚. ECC 算法的功耗分析研究. 机电工程, 2007, 24(8): 8-10)

[98] Eli Biham, Yaniv Carmeli, Adi Shamir. Bug Attacks. Lecture Notes in Computer Science, 2008, 5157: 221-240

[99] Agustin Dominguez-Oviedo. Fault-Based Attack on montgomery's ladder ECSM algorithm. Journal of Cryptology, 2011, 24(2): 346-374

[100] Ma Bo, Bao Si gang, Dai Xian ying. Efficiency improvement of ECC Resisting power attack scheme in smart card. Computer Engineering, 2010, 36(16): 113-115 (in Chinese)
(马博, 包斯刚, 戴显英. 智能卡中 ECC 抗功耗攻击方案的效率改进. 计算机工程, 2010, 36(16): 113-115)

[101] Deng Qiucheng, Bai Xuefei, Guo Li, et al. Research on Differential Power Analysis Attack on ECC Algorithm. Microelectronics & Computer, 2011, 28(2): 149-152(in Chinese)
(邓秋成, 白雪飞, 郭立等. ECC 密码算法的差分功耗分析攻击研究. 微电子学与计算机, 2011, 28(2): 149-152)

[102] Zhang Jin zhong, Kou Ying zhan, Wang Tao, et al. Fault analysis on elliptic curve cryptosystems with sliding window method. Journal on Communications, 2012, 33(1): 71-78(in Chinese)
(张金中, 寇应展, 王韬等. 针对滑动窗口算法的椭圆曲线密码故障分析. 通信学报, 2012, 33(1): 71-78)

[103] Liang Fang, Shen Ji nan. Resisting power analysis attacks scheme for ellipse curve cryptography based on ODD-only comb method. Computer Applications and Software, 2016, 33(03): 288-293(in Chinese)
(梁芳, 沈济南. 基于奇系数 Comb 的椭圆曲线密码抗功耗攻击方案. 计算机应用与软件, 2016, 33(03): 288-293)

[104] Liu Z, Longa P, Pereira G, et al. Four Q on embedded devices with strong countermeasures against side-channel attacks. IEEE Transactions on Dependable and Secure Computing, 2018,1(2): 1-21

[105] Tiri K, Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation// Proceedings of the Design, Automation and Test in Europe Conference and Exhibition. Paris, France, 2004: 246-251

[106] Tiri K, Verbauwhede I. A digital design flow for secure integrated circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2006, 25(7): 1197-1208

[107] Tanimura K, Dutt N. ExCCel: Exploration of complementary cells for efficient DPA attack resistivity//Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). Anaheim, USA, 2010: 52-55

[108] Zhong Ming, Jia Huihui, Jing Liying, et al. The optimization of DPA defense system based on quantum annealing algorithm. Netinfo Security, 2016, 3: 28-33 (in Chinese)
(仲明, 贾徽徽, 姜丽莹, 王潮. 基于量子退火算法的 DPA 防御系统优化. 信息网络安全, 2016,3: 28-33)

[109] Zhong P C, Bao W S. Quantum mechanical meet-in-the-middle search algorithm for Triple-DES. Chinese Science Bulletin, 2009, 54(19): 3003-3007 (in Chinese)
(钟普查, 鲍皖苏. 三重 DES 的量子中间相遇搜索算法. 科学通报, 2009, 54(19): 3003-3007)

[110] Nara R, Togawa N, Yanagisawa M, et al. Scan-based attack against elliptic curve cryptosystems//Proceedings of the 15th Asia and South Pacific Design Automation Conference (ASP-DAC), Taipei, China, 2010: 407-412

[111] Chen Yuhang, Jia Huihui, Jang Liying, et al. ECC scanning attack based on Grover algorithm. Netinfo Security, 2016, 2:

28-32 (in Chinese)
(陈宇航, 贾徽徽, 姜丽莹, 王潮. 基于 Grover 算法的 ECC 扫描式攻击.信息网络安全, 2016, 2: 28-32)
[112] Long Guilu, Li Yan-song, Xiao Li, et al. Phase matching in quantum searching and the improved Grover algorithm. Nuclear Physics Review, 2004, 21(1): 114-116 (in Chinese)
(龙桂鲁, 李岩松, 肖丽等. Grover 量子搜索算法及改进. 原子 核物理评论, 2004, 21(1): 114-116)
[113] Jia Huihui, Wang Chao, Gu Jian, et al. Error bit correction of ecc attack based on grover quantum intermediate encounter search algorithm. Netinfo Security, 2016,16 (6): 28-34(in Chinese)
(贾徽徽, 王潮, 顾健, 陆臻. 基于 Grover 量子中间相遇搜索算法的 ECC 攻击错误 bit 的修正. 信息网络安全, 2016, 16(6): 28-34)
[114] Wang C, Cao L, Jia H H, et al. ECC fault attack algorithm based on Grover's quantum search algorithm with 0.1π phase rotation. Journal on Communications, 2017, 38(8): 1-8(in Chinese)
(王潮, 曹琳, 贾徽徽, 胡风. 基于 0.1π 旋转相位 Grover 算法的 ECC 电压毛刺攻击算法. 通信学报, 2017, 38(8): 1-8)
[115] Wang Baonan, Hu Feng, Zhang Huanguo, ea al. From evolutionary cryptography to quantum artificial intelligent cryptography. Journal of Computer Research and Development, 2019，56(10): 2112-2134 (in Chinese)
(王宝楠, 胡风, 张焕国等. 从演化密码到量子人工智能密码综述.计算机研究与发展, 2019, 56(10): 2112-2134)
[116] Zhao Xiaolong, Wang Yanbo, Li Bin, et al. Genetic algorithms attack on NTRU public-key cryptosystem. Journal of System Simulation, 2005, 17(10): 2455-2458 (in Chinese)
(赵小龙, 王衍波, 李彬等. NTRU 公钥密码体制的遗传算法攻击. 系统仿真学报, 2005, 17(10): 2455-2458)
[117] Tang Yuan-gang，CHEN Jia-qi.Genetic Algorithms attacks on NTRU cryptosystem based on lattice theoretic.Computer Engineering and Applications, 2009, 45(1): 134-136(in Chinese)
(唐元刚, 陈家琪. 基于格理论的 NTRU 遗传算法攻击. 计算机工程与应用, 2006, 45(1): 134-136)
[118] Agrawal H, Sharma M. Optimization of NTRU cryptosystem using ACO and PSO algorithm. Internaional Journal of Science, Engineering and Technology Research, 2016, 5(3): 617-621
[119] Agrawal H, Sharma M. Calculation of complexity of NTRU and optimized NTRU using GA, ACO, and PSO algorithm. Security and Communication Networks, 2016, 9(17): 4301-4318
[120] Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions//Proceedings of the 1998 Latin American Symposium on Theoretical Informatics, Berlin, Germany, 1998: 163-169
[121] Kaplan M, Leurent G, Leverrier A, et al. Breaking symmetric cryptosystems using quantum period finding//Proceedings of the 2016 International Cryptology Conference, Berlin, Germany, 2016: 207-237
[122] Wang Licheng, Wang Lihua, Cao Zhenfu, et al. Conjugate link problem on braid group and a new design of digital signature scheme based on braid group. Scientia Sinica (Informationis), 2010, 40(2): 258-271(in Chinese)
(王励成, 王立华, 曹珍富等. 辫群上的共轭链接问题及基于辫群的数字签名方案的新设计. 中国科学: 信息科学, 2010, 40(2): 258-271)

WANG Chao, Ph. D., professor. His research interests include AI, network information security, quantum computing cryptography.

YAO Hao-Nan, M.S. His main research interests include information security and quantum computing cryptography.

WANG Bao-Nan, Ph.D. Her main research interests include information security and quantum computing cryptography.

HU Feng, Ph.D. His main research interests include information security and quantum computing cryptography.

ZHANG Huan-Guo, Ph.D., professor. His main research interests include cryptography, cryptographic protocols, trusted computing.

JI Xiang-Min, Ph.D. candidate. associate professor, His research interests include information, cryptography, trusted computing.

Background

The project is a quantum computing cryptography attacks review, and provides certain reference for cryptography research in the future quantum computing environment. Many researchers have been worked about traditional cryptography and quantum computing cryptography, and these results are scattered in many papers. In this paper we make a summary of the traditional cryptography and quantum computing cryptography, introduces the traditional cryptography, and extends to the cryptography research in the quantum computing environment. The research of cryptography in quantum environment will be an enhancement method to the existing cryptography research. Finally, some important issues worth studying in the future and the design and analysis of cryptosystems under the quantum computing environment are outlooked.

This work is supported by Supported by the grant of "the Special Zone Project of National Defense Innovation", the National Natural Science Foundation of China (No.61572304, 61272096), and the Key Program of the National Natural Science Foundation of China (No. 61332019), Open Research Fund of State Key Laboratory of Cryptology.