后量子对称密码的研究现状与发展趋势

眭 晗*①② 吴文玲①

①(中国科学院软件研究所计算机科学国家重点实验室可信计算与信息保障实验室 北京 100190)

②(密码科学技术国家重点实验室 北京 100878)

摘 要：经典对称密码算法的安全性在量子环境下面临严峻的挑战，促使研究者们开始探寻在经典和量子环境下均具有安全性的密码算法，后量子对称密码研究应运而生。该领域的研究目前仍处于初级阶段，尚未形成完整的体系。该文对现有的研究成果进行归类，从量子算法、密码分析方法、安全性分析、可证明安全4个方面对后量子对称密码领域的研究现状进行介绍。在分析研究现状的基础上，对后量子对称密码的发展趋势进行预测，为对称密码在量子环境下的分析和设计提供参考。

关键词：对称密码；量子算法；后量子；密码分析；可证明安全

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2020)02-0287-08

DOI: 10.11999/JEIT190667

Research Status and Development Trend of Post-quantum Symmetric Cryptography

SUI Han①② WU Wenling①

①(*TCA Laboratory, SKLCS, Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*)

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

Abstract: The security of classical symmetric cryptography is facing severe challenges in quantum environment, which has prompted researchers to explore cryptography algorithms that are secure in both classical and quantum environments. Post-quantum symmetric cryptography research emerges. Research in this field is still at its primary stage and has not formed a complete system. This paper categorizes the existing research results, and introduces the research status from four aspects, including quantum algorithm, cryptographic analysis method, security analysis, provable security. Based on the analysis of the research status, the development trend of post-quantum symmetric cryptography is predicted, which provides reference for the analysis and design of symmetric cryptography in quantum environment.

Key words: Symmetric cryptography; Quantum algorithm; Post-quantum; Cryptanalysis; Provable security

1 引言

近年来，后量子密码(post-quantum cryptography)成为密码学的热点研究问题，旨在研究密码算法在量子环境下的安全性，并设计在经典和量子环境下均具有安全性的密码系统。

量子计算技术，基于叠加、纠缠、隧穿等量子力学基本原理，是继电子计算机出现之后人类计算能力的又一次革命性进步。Feynman[1]于1982年首次提出了量子力学与计算机相结合的设想；Deutsch[2]于1985年进一步阐述了量子计算机的概念，并证明量子计算机比经典图灵计算机具有更强大的功能。正如电子计算机的出现彻底破解了古典密码学并催生了现代密码学，量子计算机的出现也将促使现代密码学产生重大变革。

Shor[3,4]于1994年提出了可以在多项式时间内求解因子分解问题和离散对数问题的量子算法，即Shor算法，攻破了目前广泛使用的RSA 和Diffie-Hellman公钥密码系统。这一发现不仅令量子计算成为了研究热点，同时震撼了公钥密码领域，催生出后量子密码研究，并促使NIST于2016年开始公开征集后量子公钥密码算法。

由于对称密码算法通常不具有明显的代数结构，在一段时间内，密码学界普遍认为针对对称密码，没有明显有效的量子攻击手段(如多项式时间

收稿日期：2019-09-02；改回日期：2019-10-18；网络出版：2019-11-18

*通信作者： 眭晗 suihan@tca.iscas.ac.cn

基金项目：国家自然科学基金(61672509)

Foundation Item: The National Natural Science Foundation of China(61672509)

量子算法)。面对利用Grover算法[5]进行加速搜索的威胁，密码学界广泛认为，只需要将现有分组密码的密钥量加倍，即可获得同样的安全强度。直到近几年，Kuwakado等人[6–8]指出利用量子周期发现算法Simon[9]可以将许多经典对称密码算法的攻击复杂度由生日界降至多项式级别，刷新了密码学界对于对称密码抗量子计算攻击的认知，促进后量子对称密码成为研究的热点问题。

由于后量子对称密码的发展起步时间较晚，相关的研究出现不过10年左右的时间，现有的研究尚未形成系统、完备的研究体系，呈现整体分散、局部集中的特点。后量子对称密码将对称密码置于量子环境中，其研究体系建立在量子计算与经典对称密码的研究体系之上。

以量子算法为切入点，将对称密码的特点融入量子算法的研究之中，依据量子算法自身的发展方向和特性，研究主要包含对量子算法进行优化、融合、创新，并对现有量子算法的资源需求进行估计和优化。

以对称密码为切入点，对应于经典对称密码研究体系中的对称密码分析方法、安全性分析、可证明安全理论这3个类别，量子环境下的对称密码的研究包括：基于量子计算的对称密码分析方法、对称密码算法的安全性分析、量子可证明安全理论。其中，对称密码分析方法是分析评估各类对称密码算法安全性的主要手段，利用量子算法的高速和并行性提升分析方法的实现效果的研究起步较早，主要集中于对分组密码等对称密码算法的安全性分析；对于算法结构及工作模式类的算法(如消息鉴别码、认证加密算法等)的分析，通常从寻找算法的代数结构或特殊性质为途径，量子周期发现算法Simon的引入带动了这一研究方向的发展，利用量子算法解决特定问题的优势，可以迅速提升具有相应特性的算法的攻击结果；而相对于发现具体的攻击，量子可证明安全理论则旨在基于合理的假设论证算法抵抗未知攻击的安全性，是算法安全性评估的重要依据，现有的理论多移植自经典的可证明安全理论。

本文将从量子算法的优化设计，基于量子计算的对称密码分析方法，对称密码算法的量子安全性分析，后量子对称密码的可证明安全理论这4个方面介绍后量子对称密码的研究现状，分析后量子对称密码领域的研究趋势。

2 量子算法的优化设计

量子算法利用量子的相干性和叠加性来加速运算，实现并行计算。作为量子计算机的程序语言，量子算法基于量子计算机提供优越的并行计算能力，可以解决经典计算机难于或不能解决的问题。

目前应用较广的量子算法大致分为3类：第1类为代数和数论相关的量子算法，以Simon和Shor算法为代表，基于量子Fourier变换方法等解决寻找函数周期性等数学性质，例如Shor算法可以将大数质因子分解问题由NP问题转化为P问题；第2类为基于黑盒的量子算法，以Grover算法为代表，基于振幅放大等方法，可以加速解决(超)多项式问题，例如Grover算法可以将搜索复杂度由$O(N)$降至$O(N^{1/2})$；第3类为近似和模拟算法，以Feynman算法为代表，模拟或解决量子物理问题。

目前对密码学领域产生较广影响的主要是Simon, Shor, Grover算法以及它们的优化和衍生算法。Shor算法对公钥密码领域产生了巨大的影响；而对称密码领域中则以Grover算法和Simon算法的研究为主。

2.1 量子算法及其优化和衍生

Grover于1996年提出一种在无序数据库中搜索目标条目的量子算法，即Grover算法[5]。假设数据库总条目数为N，目标条目个数为1, Grover算法可将该问题的查询复杂度从经典的$O(N)$降到$O(N^{1/2})$，即实现平方加速(quadratic speedup)。采用Grover算法对分组密码算法进行密钥穷举攻击时，其效果相当于将分组密码的密钥长度降低一半。通过提高密钥长度可以抵抗Grover算法对分组密码的威胁。

Simon于1994年提出Simon量子周期发现算法[9]，主要解决求特殊函数的周期问题。对于一个存在周期s的$\{0,1\}^n$上的特殊布尔函数f。在经典算法下求解s，需要对f进行$O(2^{n/2})$次查询；Simon量子算法仅需要对f进行$O(n)$次量子查询。

近年来，研究者进一步发展了上述算法。Brassard和 Høyer[10]说明了Simon算法能够解决的问题可以通过确定的多项式时间内的量子算法实现。对于函数存在形似周期的高概率碰撞(称为多余碰撞，unwanted collision)时Simon算法成功率可能降低的问题，Kaplan等人[8]分析证明了碰撞存在概率与算法成功率之间的关系。

Long等人[11]给出了量子搜索算法的3维表示，并利用这一表示给出了Long算法，这一算法可以解决Grover算法具有一定的失败概率的问题。这一工作得到了Grover的认可，并被Toyama等人[12]证明是迄今为止最简单、最有效和参数最优的量子搜索算法。

对于特定的应用场景，嵌套或融合不同的算法

可以带来良好的效果。例如，Leander和May[13]将Simon算法嵌套在Grover搜索迭代中，提出一种攻击FX结构的量子算法。该算法的查询复杂度为$O((s+m)2^{s/2})$，相比于仅使用Grover算法的复杂度$O((s+m)2^{(s+m)/2})$有明显降低(其中s和m分别表示初始密钥长度和扩展的密钥长度)。类似地，将该算法用于攻击基于白化密钥(whitening keys)扩展技术的加密算法，可有效地降低查询复杂度。

以Grover算法作为工具，Brassard等人[14]提出在2-to-1函数(即每个函数值对应2个原像)中搜索碰撞的量子算法，即BHT算法，该算法可以以高概率通过$O(2^{n/3})$次询问寻找到一组碰撞(其中函数定义域大小为2^n)。Ambainis[15]将研究范围扩展到任意的函数，提出可以通过$O(M^{2/3})$量子询问，找到碰撞(其中M为函数定义域大小)。Ambainis的算法同时解决了元素区分问题(element distinctness problem)，即区分单射函数和包含一个碰撞的函数。随后，Aaronson和Shi[16], Ambainis[17], Kutin[18]分别证明了$\Omega(M^{1/3})$是 2-to-1函数(可扩展到r-to-1函数)的下界；$O(M^{2/3})$是元素区分问题的下界。Yuen[19]降低了算法的成功率要求，指出当定义域与值域大小相同时，对于r-to-1函数，以最低界仅需要通过$\Omega(N^{1/5}/\lg N)$次量子询问既可以找到碰撞。Zhandry[20]进一步分析了降低成功率要求时寻找随机函数中的碰撞的问题，指出：对于随机函数f(函数定义域大小为M，对应域(co-domain)大小为N)，当$M=\Omega(N^{1/2})$时，通过$\Theta(N^{1/3})$次询问，能以常数概率找到碰撞；对于随机函数f，仅能以至多$O(q^3/N)$的概率找到一个碰撞；并给出了区分两个单射的区分概率与数据复杂度。Hosoyamada等人[21]研究了量子环境下的多碰撞的问题，指出当常数l较小时，寻找到l-碰撞仅需$O(N^{1/2})$次量子询问；当$M\geq l\times N$时，可以证明所需的询问次数的期望可以降低到$O(N^{(3^{l-1}-1)/(2\times 3^{l-1})})$。Liu和Zhandry[22]随后分析了压缩函数的l-碰撞问题，给出了以常数概率寻找到l-碰撞所需的充分必要的量子询问次数为$\Theta(N^{1/2\times(1-1/(2^l-1))})$。

2.2　量子计算资源估计与优化实现

量子计算资源估计，即对具体多大规模量子计算机才能对现有的密码算法产生影响，且产生多大影响等进行量化分析。Grassl等人[23]于2016年分析了Grover算法在AES密钥搜索中的资源消耗，指出破解128 bit的AES算法需要的逻辑量子比特数为2953，量子Toffoli门个数为1.19×2^{86}，线路深度为1.06×2^{80}。

在量子算法资源估计的基础上，人们希望通过改进量子算法或优化量子线路的方法来实现降低所需资源(比如所需的量子比特数、基本门个数、量子存储规模)的目的，使其易于在低规模量子计算机上运行。实际上，采用不同的通用量子门集合(来构造线路)、不同的容错方法、不同的量子态蒸馏方式[24]和不同的紧致化技术(来降低线路规模)[25]，实现量子算法所需要的量子比特数目和量子线路深度可能会大不相同[26]。

实现量子算法所需的量子存储空间，也是影响实现难度的重要因素。因此，降低所需的量子存储空间，也是资源优化的一种重要方式，如降低实现碰撞搜索算法时的量子存储复杂度。例如，BHT算法、Ambainis的算法等解决碰撞问题的量子存储复杂度均为$O(2^{n/3})$, Chailloux等人[27]于2017年基于振幅放大技术提出一个新的量子碰撞搜索算法，可将量子存储复杂度由$O(2^{n/3})$降低至$O(n)$。采用类似的方法。

3　基于量子计算的对称密码分析方法

对称密码的安全性分析是算法的设计与评估中不可或缺的重要组成。对称密码分析方法，是从攻击者的视角寻找算法中可能存在的弱点和漏洞，为算法的设计与完善提供安全性方面的参考与保障。现有的分析方法大体可分为统计类和代数类。统计类分析方法利用对称密码的统计特性与随机函数之间的偏差，结合统计学原理达到恢复密钥的目的。其中，差分类和线性类分析方法是最重要的两类统计类分析方法。差分类分析方法包含了经典的差分分析、截断差分分析、不可能差分分析，以及高阶差分分析等多个变种。线性类分析方法包含了线性分析、多重线性分析等变种。代数类分析方法试图通过分组密码算法输入、输出以及密钥之间的制约关系恢复密钥。这类分析方法包括代数攻击、猜测确定攻击、中间相遇攻击等。自2010年以来，密码学者开始尝试利用量子算法来改进对称密码的分析方法。

利用Bernstein-Vazirani(BV)算法[28]可以将求解内积中隐藏变量的复杂度进行指数级降低，Li和Yang等人[29–31]于2017年先后提出了量子差分分析方法，包括：量子差分分析、量子小概率差分分析、量子不可能差分分析和量子截断差分分析。这些方法以改善差分分析第1阶段(即寻找差分)的搜索效率为主要途径，可以在$O(\mathrm{poly}(w))$时间内找到一条期望的差分(其中w是轮密钥的长度)。而对于差分分析第2阶段，根据已知的差分寻找密钥，Zhou等人[32]基于量子搜索和计数算法提出了相应的量子版本，达到了平方加速效果。Kaplan等人[33]于2017年

指出，在量子查询下，差分分析和线性分析第2阶段通常能获得相对于经典分析方法的平方加速效果，而截断差分分析在量子查询下提供的加速较小。

Chen和Gao[34]于2017年提出量子代数攻击，当等式系统的条件个数较小时，该方法实现了对稀疏布尔方程求解的指数级加速。Kaplan等人[8]于2016年提出量子滑动攻击，运用Simon算法给出经典滑动攻击的量子加速模型，使得攻击复杂度可获得指数级降低。Bonnetain等人[35]和Dong等人[36]分别给出了高级滑动攻击的量子计算模型，攻击复杂度获得指数级降低，以量子多项式时间复杂度破解了2K/4K-Feistel等算法。

此外，量子算法在侧信道攻击中也有潜在应用。Montanaro[37]于2010年提出一个改进的Grover算法，可应用于搜索由不同先验概率权重的元素构成的数据库。Martin等人[38]于2017年在侧信道攻击中用该算法对所获得的不同权重的密钥进行搜索，使得该方法相对经典算法实现了平方加速。

4 对称密码算法的量子安全性分析

利用Grover算法的搜索加速和Simon算法寻找函数周期的特性，针对对称密码算法产生了一系列的攻击结果。其中，由于Simon算法可以将特定函数求解周期的复杂度有效地降到多项式级别，针对分组密码算法结构、加密模式、消息鉴别码算法、认证加密算法等的设计特点，构造周期函数并利用Simon算法求解，进一步构造区分攻击、伪造攻击或密钥恢复攻击，是目前主要的研究思路。

Kuwakado与Morii[6]于2010年提出利用Simon算法可以有效地区分3轮Feistel密码结构和随机置换。与经典方法的查询复杂度$\Theta(2^{n/4})$相比，该算法的复杂度降为$O(n/2)$(其中n为分组长度)。2012年，Kuwakado与Morii[7]用类似的方法攻击了Even-Mansour密码结构，将攻击复杂度从$O(n^3)$次经典查询降为$O(n2^{n/6})$次经典查询和$O(2^{n/6})$次量子查询。

2016年，Kaplan等人[8]提炼出利用Simon算法构造攻击的基本思路，将其划分为构造周期函数，利用Simon算法求解周期，构造攻击3个步骤，并总结出采用给定函数构造周期函数的两种方法，将对称密码算法的分析与Simon算法的实现拆分开，简化了攻击过程。运用这一思路，可以有效求解出LRW结构(以及XEX, XE结构)中的白化密钥。在此基础上，Kaplan等人攻击了部分标准密码算法(包括CBC-MAC, PMAC, GMAC, GCM和OCB)以及部分CAESAR竞赛候选算法(包括CLOC, AEZ, COPA, Minalpher, OMD和POET等)。

此后有关研究者提出的对称密码结构的分析延续了上述思路，部分分析通过结合Grover算法等对结果进行了改进。

对于经典Feistel结构，Kuwakado与Morii[6]于2010年给出3轮Feistel的选择明文区分攻击；Dong和Wang[39]于2018年结合Simon和Grover算法给出了r轮Feistel结构的密钥恢复攻击；Ito等人[40]于2019年采用选择密文方式构造了4轮Feistel结构的区分攻击。对于具有特定轮函数构造方式的Feistel结构，Hosoyamada和Sasaki[41]将量子算法与Demiric-Selçuk中间相遇攻击结合，将6轮Feistel结构的区分攻击的复杂度由$O(2^{3n/4})$降至$\tilde{O}(2^{n/2})$。

对于广义Feistel结构，Dong等人[42]于2019年给出了$2d-1$轮的(d分支)Type-1型GFS的量子区分器，以及$2d+1$轮的($2d$分支)Type-2型的GFS的量子区分器。

对于Even-Mansour结构，Kuwakado和Moriiu[8]于2012年给出了1轮EM结构的恢复密钥攻击。Hosoyamada和Aoki[43]于2017年结合相关密钥给出了2轮EM结构的恢复密钥攻击。

对于FX结构，Leander和May[13]于2017年利用Grover算法和Simon算法的组合构造了恢复密钥攻击，该方法用Simon算法作为内部判定函数，用Grover算法作为外部搜索算法。该结果同时表明，在量子环境下，FX结构的前后白化密钥并没有提高算法的安全强度。

此外，延续Kaplan等人[8]对AEZ的分析，Bonnetain[44]对认证加密算法AEZv4和AEZv5构造了密钥恢复攻击，并应用于构造AEZ10的伪造攻击，其数据复杂度约为2^{10}个分组，远低于设计者提出的2^{44}个分组。

5 后量子对称密码的可证明安全理论

可证明安全理论旨在论证密码算法抵抗未知的可能攻击的能力，是评估算法的安全性具有重要依据。与经典的可证明安全理论的发展脉络相似，量子环境下的对称密码的安全理论的研究也晚于公钥密码，现有的研究主要集中在将经典环境下的安全性概念及安全模型如何移植到量子环境下，并围绕基本的迭代型密码结构的安全性规约展开。

Boneh等人[45]于2011年提出量子随机谕言模型(quantum(-accessible) random oracle model)，指出量子环境下的随机谕言机应允许量子访问(quantum-accessible)，并定义了攻击者可以提交形如$|\varphi\rangle=\Sigma\alpha_x|x\rangle$的量子询问。由此出现了后量子安全(post-quantum security)的两个层级：

标准安全(standard security)：攻击者具有量子计算能力，但仅能对谕言机进行经典询问；

量子安全(quantum security)：攻击者具有量子计算能力，且可以对谕言机进行量子叠加态询问。

为了区分攻击者是否拥有量子访问能力的差异，Boneh等人给出了一个在仅允许经典访问时安全而在允许量子访问时不安全的方案。

Zhandry[46]将GGM(Goldreich-Goldwasser-Micali)结构推广到量子环境中，证明这种迭代PRG构造PRF的方法在量子环境下也是可行的，如果底层PRG针对多项式量子攻击者是安全的，那么GGM结构是量子安全的(quantum-secure)。Zhandry定义了量子区分优势，扩展了经典的真实与随机区分模型，并将问题转化为区分函数集合上的两个概率分布。

延续Zhandry的思路，Song和Yun[47]引入了带有随机泄露的伪随机函数(PRFs under random leakage)，并相应地提出带随机泄露的谕言安全性(oracle security under random leakage)，证明了NMAC, ACSC(与NMAC的差别在于最外层有一次不含密钥的函数变换)的量子安全性。Hosoyamada和Yasuda[48]延续了文献[46]中量子区分优势的定义，进一步将估算概率分布的区分优势转化为估算两个分布之间的迹距离(trace distance)，或总变差距离(total variation distance)。同时，正式提出量子环境下的理想密码模型(ideal cipher model)，即均匀随机选自Ciph(m,n)，允许攻击者进行逆向询问。其中Ciph(m,n)表示密钥长度为m、分组长度为n的令$E(k,\cdot)$为置换的函数集合。

值得注意的是，在这些安全理论中，“量子”主要体现在对攻击者的询问的刻画，而安全模型与区分优势的定义与经典环境下基本相同。Zhandry[49]于2018年以不可区别性(indifferentiability)的模型为研究对象，指出以往的定义并不能适应这一场景。在与攻击者进行交互的过程中，模拟器需要对以往的询问进行查询以模拟真实算法的行为。由于量子环境的特点，记录(recording a query)等同于测量；而真实的谕言机无须进行测量，可以据此对两个谕言机进行区分。为解决这一问题，Zhandry提出了一种新的压缩谕言技术(compressed oracle technique)，可以用攻击者无法侦测的方式记录攻击者的询问。

6　存在问题和研究趋势

后量子对称密码是量子计算与对称密码构成的交叉方向，相关研究跨越不同学科，而且研究出现不过10年左右的时间，有许多问题尚待探索。

量子算法及其优化和衍生：量子算法的设计目标通常是解决一类特定的问题，例如Grover算法可用于提高搜索速度、Simon算法可以求解函数周期。利用量子算法分析对称密码时，可能局限于对密码算法相应特性的挖掘，而对于不具有相应特性的密码算法则显得束手无措。深入对称密码算法自身特点的挖掘，研究设计可以解决相应数学问题的量子算法，将对后量子对称密码的分析带来巨大的影响。与此同时，现有量子算法的优化同样具有重要的意义，算法优化包含两个方面：一是对理论的优化，包括降低假设条件、提高成功率等；二是对资源的优化，包括降低实现代价、提高实现效率等。

量子算法与密码分析方法的融合：对称密码分析方法具有丰富的研究成果，利用量子算法提高密码分析方法的有效性，包括对分析方法提出有效的量子算法结合，或者对已结合量子算法的分析方法提出优化。研究量子算法和对称密码分析方法的融合问题，包括提出对称密码分析方法的量子加速模型，利用量子计算能力有效提升对称密码算法的分析结果，优化方法以提高算法的可行性等。

密码算法量子安全性的分析评估：量子计算中的Simon和Grover等算法已被证实对很多的对称密码算法存在有效的理论攻击，然而是否所有经典的对称密码算法均存在类似的有效攻击还是未知的问题。同时，现有的许多量子算法尚未被应用于对称密码的分析之中，这些量子算法是否会影响对称密码算法的安全性，是目前亟待解决的问题。

量子可证明安全理论的研究：在后量子对称密码的研究领域中，仅有的若干研究成果均围绕基本的迭代型函数构造延伸开，缺乏对各类常见对称密码结构及经典对称密码算法的安全性论证，表现出明显的局限性。分析安全模型、发展证明技术，从可证明安全角度分析对称密码算法及其结构，是目前亟待拓展的研究方向。另一方面，现有的研究思路是用概率分布之间的差异描述密码算法与随机理想谕言机之间的区分性，将算法的量子安全性归约到迭代函数的量子安全性。可以注意到，现有的量子可证明安全理论与结合量子算法的算法攻击之间存在脱节。采用量子算法构造对称密码算法的攻击时，所考虑的是量子算法和对称密码算法的特性，而不是算法所对应的函数的概率分布。如何弥补这种差异性是解决对称密码分析与可证明安全理论有机结合的关键。

后量子对称密码算法的设计：现有对称密码算法在量子环境下是否安全可用一直是备受关注的问题，采用现有的工具是否可以设计出具有后量子安

全的对称密码算法是亟待解决的问题。由于目前量子分析方法与证明技术的研究均处于初级阶段，评估与论证对称密码算法在量子环境下安全尚属少见，在量子环境下设计提出新的安全的对称密码算法更是目前的研究空白。此外，考虑到量子算法对于对称密码算法的影响以及现有对称密码算法的应用情况，寻找通用的修改方法或框架，将经典环境下安全的对称密码算法转换为在量子环境下同样安全的算法，对于应用实现具有更广泛的意义。

参 考 文 献

[1] FEYNMAN R P. Simulating physics with computers[J]. *International Journal of Theoretical Physics*, 1982, 21(6/7): 467–488.

[2] DEUTSCH D. Quantum theory, the Church-Turing principle and the universal quantum computer[J]. *Proceedings of the Royal Society A Mathematical, Physical and Engineering Sciences*, 1985, 400(1818): 97–117. doi: 10.1098/rspa.1985.0070.

[3] SHOR P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]. The 35th Annual Symposium on Foundations of Computer Science, Santa Fe, USA, 1994: 124–134.

[4] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. *SIAM Journal on Computing*, 1997, 26(5): 1484–1509. doi: 10.1137/S0097539795293172.

[5] GROVER L K. A fast quantum mechanical algorithm for database search[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, 1996: 212–219.

[6] KUWAKADO H and MORII M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C]. 2010 IEEE International Symposium on Information Theory, Austin, USA, 2010: 2682–2685.

[7] KUWAKADO H and MORII M. Security on the quantum-type Even-Mansour cipher[C]. 2012 International Symposium on Information Theory and Its Applications, Honolulu, USA, 2012: 312–316.

[8] KAPLAN M, LEURENT G, LEVERRIER A, *et al*. Breaking symmetric cryptosystems using quantum period finding[J]. arXiv: 1602.05973, 2016.

[9] SIMON D R. On the power of quantum computation[C]. The 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994: 116–123.

[10] BRASSARD G and HOYER P. An exact quantum polynomial-time algorithm for Simon's problem[C]. The Fifth Israeli Symposium on Theory of Computing and Systems, Ramat-Gan, Israel, 1997: 12–23.

[11] LONG Guilu. Grover algorithm with zero theoretical failure rate[J]. *Physical Review A*, 2001, 64(2): 022307. doi: 10.1103/PhysRevA.64.022307.

[12] TOYAMA F M, VAN DIJK W, and NOGAMI Y. Quantum search with certainty based on modified Grover algorithms: Optimum choice of parameters[J]. *Quantum Information Processing*, 2013, 12(5): 1897–1914. doi: 10.1007/s11128-012-0498-0.

[13] LEANDER G and MAY A. Grover meets Simon - Quantumly attacking the FX-construction[C]. Proceedings of the 23rd International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 2017: 161–178.

[14] BRASSARD G, HØYER P, and TAPP A. Quantum cryptanalysis of hash and claw-free functions[C]. Theoretical Informatics: Third Latin American Symposium, Campinas, Brazil, 1998: 163–169.

[15] AMBAINIS A. Quantum walk algorithm for element distinctness[J]. *SIAM Journal on Computing*, 2007, 37(1): 210–239. doi: 10.1137/S0097539705447311.

[16] AARONSON S and SHI Yaoyun. Quantum lower bounds for the collision and the element distinctness problems[J]. *Journal of the ACM*, 2004, 51(4): 595–605. doi: 10.1145/1008731.1008735.

[17] AMBAINIS A. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range[J]. *Theory of Computing-An Open Access Electronic Journal in Theoretical Computer Science*, 2005, 1(1): 37–46.

[18] KUTIN S. Quantum lower bound for the collision problem with small range[J]. *Theory of Computing-An Open Access Electronic Journal in Theoretical Computer Science*, 2005, 1(1): 29–36.

[19] YUEN H. A quantum lower bound for distinguishing random functions from random permutations[J]. *Quantum Information & Computation*, 2014, 14(13/14): 1089–1097.

[20] ZHANDRY M. A note on the quantum collision and set equality problems[J]. *Quantum Information & Computation*, 2015, 15(7/8): 557–567.

[21] HOSOYAMADA A, SASAKI Y, and XAGAWA K. Quantum multicollision-finding algorithm[C]. The 23rd International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 2017: 179–210.

[22] LIU Qipeng and ZHANDRY M. On finding quantum multi-collisions[C]. The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 2019: 189–218.

[23] GRASSL M, LANGENBERG B, ROETTELER M, *et al*. Applying Grover's algorithm to AES: Quantum resource estimates[J]. arXiv: 1512.04965, 2015.

[24] FOWLER A G, DEVITT S J, and JONES C. Surface code implementation of block code state distillation[J]. *Scientific Reports*, 2013, 3(1): 1939. doi: 10.1038/srep01939.

[25] FOWLER A G and DEVITT S J. A bridge to lower overhead quantum computation[J]. arXiv: 1209.0510, 2012.

[26] DEVITT S J, STEPHENS A M, MUNRO W J, *et al*. Requirements for fault-tolerant factoring on an atom-optics quantum computer[J]. *Nature Communications*, 2013, 4(1): 2524. doi: 10.1038/ncomms3524.

[27] CHAILLOUX A, NAYA-PLASENCIA M, SCHROTTENLOHER A, *et al*. An efficient quantum collision search algorithm and implications on symmetric cryptography[C]. The 23rd International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 2017: 211–240.

[28] BERNSTEIN E and VAZIRANI U. Quantum complexity theory[C]. The 28th Annual ACM Symposium on Theory of Computing, San Diego, USA, 1993: 11–20.

[29] LI Hongwei and YANG Li. Quantum differential cryptanalysis to the block ciphers[C]. The 6th International Conference on Applications and Techniques in Information Security, Beijing, China, 2015: 44–51.

[30] XIE Huiqin and YANG Li. Quantum impossible differential and truncated differential cryptanalysis[J]. arXiv: 1712.06997, 2017.

[31] XIE Huiqin and YANG Li. Using Bernstein-Vazirani algorithm to attack block ciphers[J]. *Designs, Codes and Cryptography*, 2019, 87(5): 1161–1182. doi: 10.1007/s10623-018-0510-5.

[32] ZHOU Qing, LU Songfeng, ZHANG Zhigang, *et al*. Quantum differential cryptanalysis[J]. *Quantum Information Processing*, 2015, 14(6): 2101–2109. doi: 10.1007/s11128-015-0983-3.

[33] KAPLAN M, LEURENT G, LEVERRIER A, *et al*. Quantum differential and linear cryptanalysis[J]. arXiv: 1510.05836, 2015.

[34] CHEN Yuao and GAO Xiaoshan. Quantum algorithms for Boolean equation solving and quantum algebraic attack on cryptosystems[J]. arXiv: 1712.06239, 2017.

[35] BONNETAIN X, NAYA-PLASENCIA M, SCHROTTENLOHER A, *et al*. On quantum slide attacks[R]. 2018/1067, 2018.

[36] DONG Xiaoyang, DONG Bingyou, WANG Xiaoyun, *et al*. Quantum attacks on some Feistel block ciphers[R]. 2018/504, 2018.

[37] MONTANARO A. Quantum search with advice[C]. The 5th Conference on Theory of Quantum Computation, Communication, and Cryptography, Leeds, UK, 2010: 77–93.

[38] MARTIN D, MONTANARO A, and OSWALD E. Quantum key search with side channel advice[C]. The 24th International Conference on Selected Areas in Cryptography, Ottawa, Canada, 2017: 407–422.

[39] DONG Xiaoyang and WANG Xiaoyun. Quantum key-recovery attack on Feistel structures[J]. *Science China Information Sciences*, 2018, 61(10): 102501. doi: 10.1007/s11432-017-9468-y.

[40] ITO G, HOSOYAMADA A, MATSUMOTO R, *et al*. Quantum chosen-ciphertext attacks against feistel ciphers[C]. The Cryptographers' Track at the RSA Conference, San Francisco, USA, 2019: 391–411.

[41] HOSOYAMADA A and SASAKI Y. Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic feistel constructions[C]. The 11th International Conference on Security and Cryptography, Amalfi, Italy, 2018: 386–403.

[42] DONG Xiaoyang, LI Zheng, WANG Xiaoyun, *et al*. Quantum cryptanalysis on some generalized Feistel schemes[J]. *Science China Information Sciences*, 2019, 62(2): 22501. doi: 10.1007/s11432-017-9436-7.

[43] HOSOYAMADA A and AOKI K. On quantum related-key attacks on iterated Even-Mansour ciphers[C]. The 12th International Workshop on Security, Hiroshima, Japan, 2017: 3–18.

[44] BONNETAIN X. Quantum key-recovery on full AEZ[C]. The 24th International Conference on Selected Areas in Cryptography, Ottawa, Canada, 2018: 394–406.

[45] BONEH D, DAGDELEN Ö, FISCHLIN M, *et al*. Random oracles in a quantum world[C]. The 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, 2011: 41–69.

[46] ZHANDRY M. How to construct quantum random functions[C]. The 53rd Annual Symposium on Foundations of Computer Science, New Brunswick, USA, 2012: 679–687.

[47] SONG Fang and YUN A. Quantum security of NMAC and related constructions[C]. The 37th International Cryptology Conference, Santa Barbara, USA, 2017: 283–309.

[48] HOSOYAMADA A and YASUDA K. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions[C]. The 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2018: 275–304.

[49] ZHANDRY M. How to record quantum queries, and applications to quantum indifferentiability[C]. The 39th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2019: 239–268.

眭 晗：女，1986年生，助理研究员，研究方向为可证明安全理论、认证加密算法的设计与分析.

吴文玲：女，1966年生，研究员，博士生导师，主要研究方向为对称密码的设计与分析.