

量子计算与量子密码的原理及研究进展综述

王永利¹ 徐秋亮²

¹(山东大学数学学院 济南 250100)

²(山东大学软件学院 济南 250101)

(wyl@mail.sdu.edu.cn)

Principle and Research Progress of Quantum Computation and Quantum Cryptography

Wang Yongli¹ and Xu Qiuliang²

¹(School of Mathematics, Shandong University, Jinan 250100)

²(School of Software, Shandong University, Jinan 250101)

Abstract Quantum computation and quantum cryptography are based on principles of quantum mechanics. In 1984, Bennett and Brassard proposed the first quantum key distribution protocol called BB84, which started the study of quantum cryptography. Since then, a great deal of work has been carried out in various fields such as quantum encryption and quantum signature. In 1994, Shor designed the first practical quantum algorithm which can factor large integers in polynomial time. Shor's algorithm used Quantum Fourier Transform, which is the kernel of most quantum algorithms. In 1996, Grover designed a new algorithm which can search the unstructured data to get the required result in the time of approximately the square root of the total account of the data. Shor's algorithm and Grover's algorithm not only embody the advantages of quantum computing, but also pose a threat to the traditional cryptography based on mathematical difficulties such as RSA. After half a century's development, quantum computing and quantum cryptography have achieved fruitful results in theory and practice. In this paper, we summarize the contents from the perspectives of the mathematical framework of quantum mechanics, basic concepts and principles, basic ideas of quantum computing, research progress and main ideas of quantum cryptography, etc.

Key words quantum computation; quantum cryptography; Shor's algorithm; Grover's algorithm; quantum key distribution

摘 要 量子计算与量子密码是基于量子效应的计算技术和密码技术.1984 年 Bennett 和 Brassard 提出了第一个量子密钥分发协议,开启了量子密码学的研究,此后相继在量子加密、量子签名等领域进行了大量研究.1994 年,Shor 利用量子 Fourier 变换,设计了第一个实用的量子算法,在多项式时间内对大整数进行因子分解.1996 年,Grover 提出了量子搜索算法,能够对无结构数据进行二次加速.Shor 算法和 Grover 算法的提出不仅体现了量子计算的优越性,还对传统基于数学困难问题的密码学体制造成威胁.经过半个世纪的发展,量子计算与量子密码在理论与实践的研究上都取得了丰硕的成果.从量子力学的数学框架、基本概念和原理、量子计算基本思想、量子密码研究进展及主要思想等方面进行总结梳理.

收稿日期:2020-08-14;修回日期:2020-09-04

基金项目:国家自然科学基金项目(61632020)

This work was supported by the National Natural Science Foundation of China (61632020).

通信作者:徐秋亮(xql@sdu.edu.cn)

关键词 量子计算;量子密码;Shor 算法;Grover 算法;量子密钥分发

中图法分类号 TP309

量子计算与量子密码是基于量子力学机制的信息处理技术,被认为是下一代计算与信息安全的核心,已成为时代发展的需要,被世界各国寄予厚望.

其实,将量子效应应用到信息技术领域的思想,早在 20 世纪 60 年代末就开始出现了.1969 年,哥伦比亚大学的 Wiesner^[1] 在他的论文“Conjugate Coding”中提出了利用量子力学的不确定性原理制造不可伪造的量子钞票的思想.由于当时技术的限制,该思想没有被人们接受.10 年后,Wiesner 又与 IBM 公司的研究人员 Bennett 提及了这一思想,引起了 Bennett 的注意.在 1982 年的美密会上发表的论文中,Bennett 和加拿大 Montreal 大学的 Brassard 利用量子比特的储存来实现量子密码并提出量子公钥密码算法.此后不久,他们意识到量子比特的传输比量子比特的储存更便于实现和利用,基于该出发点,1984 年他们提出了著名的量子密钥分发的概念^[2],并构造了现在被称为 BB84 协议的密钥分发协议.BB84 协议的提出标志着量子密码学研究的真正开始.

1994 年,Shor^[3] 提出了著名的量子整数分解算法,该算法使用量子计算机可以在多项式时间内找到大整数的因子.Shor 算法的核心是利用量子 Fourier 变换求函数周期,这一算法不仅对大整数分解有效,对求解离散对数也有同样的效果.Shor 算法的出现,让人们们量子计算的优越性有了新的认识,具有里程碑意义.后来,Grover^[4] 提出了一种量子搜索算法,可以对无结构数据的搜索加速,它虽然不像 Shor 算法那样具有指数级加速效果,但也大大提升了搜索速度.这些量子算法的出现,不仅展现了量子计算的威力,同时也对现有基于大整数分解和离散对数等数学困难问题的密码体制造成很大的威胁,使得人们意识到后量子密码学研究的必要性.

经过近半个世纪的研究与发展,量子计算与量子密码不但在理论上形成了自身的框架体系,在技术上也取得了突破性进展.国际上许多大学和科研单位纷纷成立了从事量子计算和量子密码研究的机构.除了这些研究机构外,国际上也开始出现了专门从事研发量子密码技术产品、量子通信技术产品和量子计算机的公司,如早期瑞士的 ID Quantique 公司、美国的 MagiQ 公司,后来加拿大的 D-Wave,现在的 IBM 公司、Google 公司等.特别是在量子计算机研发方面,2019 年 1 月,IBM 在消费电子展

(CES)上展示了世界首款商业化量子计算机 IBM Q System One,同年 10 月 Google 制造的一台“Sycamore”量子计算机声称超越了传统计算机实现量子霸权,2020 年 6 月,Honeywell 公司发布了声称是世界最强的量子计算机,量子体积(quantum volume)达到 64.虽然这些产品更多的是只有实验研究价值,距离真正的量子计算还有很大的距离,但这已经迈出了向量子时代前进关键的一步,正如莱特兄弟第一架飞机的意义,因此很有必要对量子计算和量子密码的发展进行梳理.

本文对量子力学的数学框架、基本概念和原理、量子计算基本思想、量子密码研究进展及主要思想等方面作了总结.

1 量子力学的数学框架^[5]

量子力学理论给出了研究物理系统规律的数学框架,通过这个框架,物理世界和量子力学的数学描述得以联系起来.量子力学所描述的微观世界,与人们熟悉的宏观世界有很大的不同,从而显得奇妙而神秘,但如果将其放在量子力学的数学视角下,则不过是普通的 Hilbert 空间向量的运算与变换.本节对量子力学的基本数学框架进行简要介绍.

一个孤立的物理系统对应一个复 Hilbert 空间,该空间称为系统的状态空间,系统的状态由 Hilbert 空间中的向量描述,为了描述和运算方便,一般用英国理论物理学家狄拉克引入的狄拉克符号表示,如 $|\varphi\rangle$.这里需要注意的是,该数学描述并没有给出 Hilbert 空间的具体形式.

孤立物理系统的状态随时间的变化由 Hilbert 空间中的酉变换描述,如果系统在 t_1 时的状态为 $|\varphi_1\rangle$, t_2 时变为 $|\varphi_2\rangle$,则存在一个仅与 t_1 和 t_2 有关的酉变换 U ,使得 $|\varphi_2\rangle=U|\varphi_1\rangle$.同样需要注意的是这一数学描述没有给出酉变换的具体形式.

复合物理系统使用张量积描述,即复合系统的状态空间表示为各分系统状态空间的张量积.这一描述也提供了用分系统构造复合系统的方法.

对量子系统的测量与经典测量有很大的不同,量子测量由一组满足完备性的测量算子 $\{M_m\}$ 描述,其中, m 表示可能的结果.如果测量前系统为 $|\varphi\rangle$,则测量后以概率 $\langle\varphi|M_m^\dagger M_m|\varphi\rangle$ 得到结果 m ,且系统变为 $M_m|\varphi\rangle/\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}$.

2 基本概念和原理^[5]

2.1 量子比特

量子比特是二维 Hilbert 空间中的一个单位向量.在取定 2 个正交的基态 $|0\rangle$ 和 $|1\rangle$ 后,量子比特可表示为 $\alpha|0\rangle+\beta|1\rangle$,其中 α 和 β 是复数,且满足 $|\alpha|^2+|\beta|^2=1$.多个量子比特可以复合,如果每个量子比特取定基 $|0\rangle$ 和 $|1\rangle$,则 n 个量子比特复合后的系统可表示为 $\sum_{i=0}^{2^n-1} \alpha_i |i\rangle$,其中 α_i 为复数,且 $\sum_{i=0}^{2^n-1} |\alpha_i|^2=1$, $|i\rangle$ 为复合系统的基,称为计算基.复合量子比特是量子计算的基础.

在复合量子比特中,如果其状态向量不能表示为各量子比特状态向量的直积形式,则称该系统处于纠缠态.通俗来讲,处于纠缠态的系统,各子系统状态不能分开.纠缠态在量子计算与量子信息中起着重要作用,常用的纠缠态有两粒子纠缠的 Bell 态、三粒子纠缠的 GHZ 态等.

2.2 态叠加原理

如果 $|\varphi_i\rangle (i=0,1,2,\dots,n)$ 是系统的可能状态,则其线性叠加 $\sum_{i=0}^n \alpha_i |\varphi_i\rangle$ 也是系统的可能状态.从数学的观点看,因为系统状态是 Hilbert 空间中的向量,而 Hilbert 空间是线性空间,所以线性叠加性成立.

在量子计算中,一般会使用计算基的叠加态,由于酉算子是线性算子,酉算子在叠加态上的作用,相当于在各计算基上作用的叠加,从而获得真正意义上的并行计算能力.

2.3 不确定性原理

不确定性原理是量子系统的内在属性,与测量设备的精度以及测量设备对系统的扰动无关.原理指出:如果 2 个力学量所对应的算符不对易,则不能同时确定这 2 个力学量.如在测量光子偏振状态的过程中,线偏振状态和圆偏振状态不能同时确定,这也是 BB84 协议工作的理论基础.

更一般地,测量一个量子态时,能否获得精确测量结果依赖于该量子态是否为测量算符对应的本征态,如果该状态是测量算符对应的本征态,则可得到精确测量结果,否则,无法得到精确测量结果.

2.4 未知量子态不可克隆

1982 年 Wootters 和 Zurek^[6]首次提出了著名的量子不可克隆定理:在量子力学中,不存在一个对未知量子态精确复制的物理过程,即未知量子态不

可能精确复制,使得每个复制比特和初始量子比特完全相同.1986 年, Yuen^[7]推广了量子不可克隆定理,指出表示克隆过程的酉变换使得 2 个量子态被克隆,当且仅当它们相互正交,即非正交态不可克隆.

未知量子态的不可克隆性,虽然对量子计算中比特复制造成一定困难,但对量子密码学中安全体制的设计提供了重要保障.

2.5 非正交量子态不可区分

对于 2 个非正交量子态,没有一个物理过程可对其进行完美区分.这是由未知量子态的不可克隆性决定的.例如,对于 2 个量子比特,如果它们是非正交的,则任何操作或测量都不能将它们完美区分开来,总是会产生一些错误的结果.

同不可克隆性一样,非正交量子态的不可区分性给量子计算带来了很多困难,但在量子密码学中的应用,有着举足轻重的价值.

3 量子计算基本思想^[5]

量子计算通过量子逻辑门和连线构造量子线路实现.量子逻辑门在数学上由复 Hilbert 空间的酉变换描述.1985 年, Deutsch^[8]引入了量子线路模型.1995 年, Barenco, Bennett 和 Cleve 等人^[9]证明了单量子比特门和受控非门(controlled-NOT, CNOT)的通用性,为量子线路模型提供了完善的理论保证.

酉变换是可逆的,即量子逻辑门是可逆的,然而经典逻辑门大多不可逆,这些不可逆的经典逻辑门没有对应的量子逻辑门,所以不能用量子线路直接模拟经典线路.幸运的是我们可以用可逆的 Toffoli 门实现经典逻辑门,从而等价地构造经典线路. Tofooli 门是可逆门,可以用量子逻辑门实现,从而使得量子线路可以间接模拟经典线路,在量子线路上实现任何经典计算.

量子计算中,常用的量子逻辑门有 Pauli-X 门、Pauli-Y 门、Pauli-Z 门、Hadamard 门、相位门、受控门、交换门等.

量子态的叠加性决定量子计算具有并行性的特征,它可以同时计算一个函数在许多点处的函数值,使得量子计算的能力从本质上超越经典计算的能力.然而由于量子测量的特点,无法直接从叠加态中直接抽取信息,大大限制了量子计算的能力.虽然如此,还是可以通过巧妙的设计,有效利用量子计算的优越性,为计算问题加速,这也是量子算法设计的一个重要特点.从早期的 Deutsch-Jozsa 算法^[10]和 Simon

算法^[11]开始,出现了许多量子算法,其中最具有里程碑意义的是 Shor 算法^[3]和 Grover 算法^[4],它们分别使用了量子 Fourier 变换和量子搜索,本节对其思想进行简要介绍.

3.1 量子 Fourier 变换

量子 Fourier 变换是定义在标准正交基 $|0\rangle, |1\rangle, \dots, |2^n-1\rangle$ 上的一个酉变换,在这些基态上的作用为: $|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle$,通过代数计算,变换后的结果可以表示为

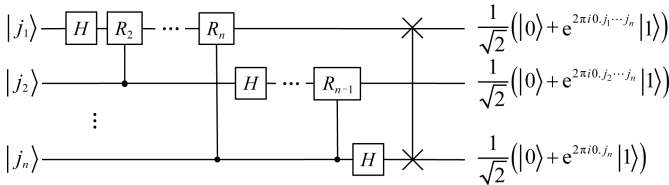


Fig. 1 The circuit of quantum Fourier transform
图 1 量子 Fourier 变换线路

通过量子 Fourier 变换可以实现相位估计,设 $|u\rangle$ 是酉算子 U 的特征值为 $e^{2\pi i \varphi}$ 的一个本征态,则可大概率得到 φ 的指定精度的近似值.相位估计是众多量子算法的关键部分,结合经典算法,可以有效解决求阶、求周期问题,更一般地,可有效解决隐含子群问题. Deutsch-Jozsa 算法、Shor 大整数分解算法、求离散对数等都是隐含子群问题的特例.目前大整数分解和求离散对数在经典计算机上还没有有效的求解方法,通过量子 Fourier 变换,在量子计算机上可有效求解,这也体现了量子计算较之经典计算的优越性.

3.2 量子搜索

量子搜索对无结构数据的搜索提供了二次加速.设在一个大小为 N 的无结构数据空间中有 M 个解,量子搜索通过大约 \sqrt{N} 次操作,可以找到一个解.虽然没有基于量子 Fourier 算法的指数加速效果,但由于搜索问题的普遍性,量子搜索算法仍具有很大的意义.

算法中使用了称为 Grover 迭代的算子, Grover 迭代可表示为 $(2|\psi\rangle\langle\psi| - I)O$, 其中 $|\psi\rangle = H^{\otimes n} |0\rangle$, O 为识别搜索问题解的 Oracle. 直观上看, Grover 迭代实现了由初始量子态和搜索问题解组成的均匀叠加态张成的二维空间中的一个旋转,如图 2 所示.

其中 $|\alpha\rangle = \sum_x |x\rangle / \sqrt{N-M}$ 为归一化的非搜索问题解的叠加态, $|\beta\rangle = \sum_y |y\rangle / \sqrt{M}$ 为归一化

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle = \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i 0.j_n} |1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n} |1\rangle),$$

其中 $j_1 j_2 \cdots j_n$ 是 j 的二进制表示, $0.j_1 \cdots j_n$ 为二进制小数.

上述变换可通过图 1 所示量子线路实现.

线路中使用了 Hadamard 门 H 、相位门 R_k 和交换门 \times , 其中 R_k 的矩阵表示为 $\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{pmatrix}$.

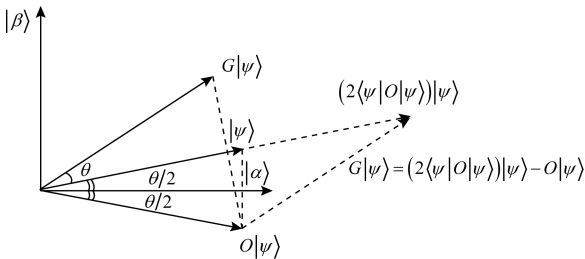


Fig. 2 The geometric intuitive of a Grover iterative
图 2 Grover 迭代几何直观

的搜索问题解的叠加态, G 为 Grover 迭代算子, θ 满足 $\cos(\theta/2) = \sqrt{(N-M)/N}$, 每经过一次 Grover 迭代, 初态 $|\psi\rangle$ 向 $|\beta\rangle$ 方向靠近 θ . 经过 $O(\sqrt{N})$ 次迭代, $|\psi\rangle$ 接近 $|\beta\rangle$, 在计算基中测量将以很高的概率输出搜索问题的一个解.

4 量子密码研究进展及主要思想

BB84 协议提出后,量子密码学正式登上历史的舞台.量子密码学以量子密钥分发为核心,对应于经典密码学领域的其他研究分支也得到了广泛关注,并形成各个不同的研究分支.本文对量子密钥分发、量子加密、量子签名和其他研究领域这 4 个方面的主要思想及进展情况进行介绍.

4.1 量子密钥分发

密钥分发用来在通信双方 (Alice 和 Bob) 安全

分发一个密钥,后续可以用该密钥安全通信.BB84 协议是第一个量子密钥分发协议,被研究的最多,也最具代表性,在量子密码研究中占有重要地位,我们在此以 Bennett 和 Brassard 提出的原始协议为基础对其进行介绍.

BB84 协议使用光子作为量子态的载体,使用 2 组偏振基编码数据.一种为线偏振基(记为“+”),水平偏振状态记为 $|\leftrightarrow\rangle$,垂直偏振状态记为 $|\updownarrow\rangle$;另一种为圆偏振基(记为“○”),左旋偏振状态记为 $|\curvearrowleft\rangle$,右旋偏振状态记为 $|\curvearrowright\rangle$.在这 2 组基下,比特“0”分别被编码为 $|\leftrightarrow\rangle$ 和 $|\curvearrowleft\rangle$,比特“1”分别被编码为 $|\updownarrow\rangle$ 和 $|\curvearrowright\rangle$.描述光子线偏振和圆偏振的力学量算符不可对易,由 Heisenberg 不确定性原理,这 2 种偏振状态无法被同时确定.

BB84 协议需要一条量子信道和一条经典信道.量子信道可以是光纤或自由空间,经典信道为普通的公共信道,安全性不需考虑.这 2 种信道都允许第三方(Eve)监听.

BB84 协议工作的过程如下:

- 1) Alice 对于某个安全参数 n ,随机选择稍多于 $4n$ 个比特,对每个比特随机选取线偏振基或圆偏振基进行编码,并将编码后的光子序列通过量子信道发送给 Bob;
- 2) Bob 收到光子序列后,随机选取线偏振基和圆偏振基对光子序列进行测量;
- 3) Bob 与 Alice 通过经典信道联系,对比他们所选择的基序列,舍弃选择不同基的比特,一般而言,他们将得到稍多于 $2n$ 个比特;
- 4) Alice 选择 n 个比特与 Bob 对比检查是否有第三方监听,如果错误率超过某一个阈值,则放弃本次协议(监听会造成对量子态的干扰,从而显著增大错误率);
- 5) Alice 和 Bob 对剩下的 n 个比特执行密钥纠错和安全性增强,得到最终的密钥.

BB84 协议的工作过程可用图 3 所示的例子直观描述:

Alice chooses random bits	0	0	1	0	1	1	0	1	0	1	1	0
Alice chooses encoding basis randomly	+	○	○	+	○	+	○	+	+	○	+	○
Alice sends quantum bits	$ \leftrightarrow\rangle$	$ \curvearrowleft\rangle$	$ \curvearrowright\rangle$	$ \leftrightarrow\rangle$	$ \curvearrowright\rangle$	$ \updownarrow\rangle$	$ \curvearrowleft\rangle$	$ \updownarrow\rangle$	$ \leftrightarrow\rangle$	$ \curvearrowleft\rangle$	$ \updownarrow\rangle$	$ \curvearrowright\rangle$
Bob chooses measuring basis randomly	+	+	○	+	○	○	+	+	○	+	○	○
Bob's measuring result ^①	$ \leftrightarrow\rangle$	$ \leftrightarrow\rangle$	$ \curvearrowright\rangle$	$ \leftrightarrow\rangle$	$ \curvearrowright\rangle$	$ \curvearrowleft\rangle$	$ \updownarrow\rangle$	$ \updownarrow\rangle$	$ \curvearrowright\rangle$	$ \leftrightarrow\rangle$	$ \curvearrowright\rangle$	$ \curvearrowleft\rangle$
Alice and Bob compare their basis	✓	×	✓	✓	✓	×	×	✓	×	×	×	✓
Alice and Bob keep the bits from the same basis	0		1	0	1			1				0
Comparison	Half of the reserved bits are compared, and the protocol is aborted when the error rate exceeds the threshold											
Error correction	Alice and Bob perform error correction on the remaining bits											
Security enhancement	Alice and Bob enhance the security of the corrected bits to get the final key											

① If Bob chooses the same base as Alice, he will obtain the correct results; otherwise, he will get one of the two states with uniform probability.

Fig. 3 The process of BB84 protocol
图 3 BB84 协议的工作过程

在 BB84 协议工作的过程中,Bob 收到 Alice 发送的光子序列后,并不知道 Alice 编码这些光子所用的基,他在随机选择测量基时,有 1/2 的概率和 Alice 使用的基相同,因此在作基比对后,他们能得到大概原始比特数一半的比特形成的序列,在这个比特序列中,由于设备、环境等因素的影响,会出现一定的错误,记错误率为 ξ_0 .如果协议过程中存在 Eve 监听,Eve 截获 Alice 发送的光子序列后,受未知量子态不可克隆原理的限制,他无法对光子序列

进行复制,为了获取信息,Eve 必须在原始光子序列上测量.然而,Eve 也不知道 Alice 编码光子所用的基,他只能随机选择测量基,在测量的过程中必然会对光子产生扰动,使得在 Alice 和 Bob 作比特比对时,得到的错误率超过 ξ_0 ,由此可以发现监听.

Alice 和 Bob 在比特比对后,需要对剩下的比特序列纠错,其基本思想是将这些比特序列分为若干区,对每个区进行奇偶校验,如果校验通过,则放弃一个比特后保留该区,如果校验不通过,则放弃整个区,

经过若干次重复,可确保他们有非常高的概率持有相同的比特序列.纠错后,Alice 和 Bob 对共享比特序列进行安全性增强,如随机选择 Hash 函数对其进行压缩,得到最终的共享密钥.

不同于经典密码学的安全性基于数学困难问题,BB84 的安全性基于量子不可克隆和不确定性原理等物理学定律,它提供了无条件安全性,Shor 和 Preskill^[12]于 2000 年对其进行了证明,确认了这是一个可证安全的密钥分配方案,符合现代密码学设计的基本要求.

BB84 协议提出后,人们对这一领域的研究产生了极大热情.1991 年,Ekert^[13]提出了利用纠缠光子对实现密钥分发的协议,称为 E91 协议,该协议也是目前最具代表性的 QKD 协议之一.协议执行开始时,Alice 和 Bob 共享一组量子比特纠缠对 $(|01\rangle - |10\rangle)/\sqrt{2}$,其中 $|0\rangle, |1\rangle$ 为 Pauli-Z 算符的本征态.随后 Alice 从 Bloch 球 x - y 平面上方位角分别为 $0, \pi/4, \pi/2$ 的 3 个基矢中随机选择测量基,Bob 从 Bloch 球 x - y 平面上方位角分别为 $\pi/4, \pi/2, 3\pi/4$ 的 3 个基矢中随机选择测量基,分别对自己持有的量子比特进行测量.接下来,他们在公开信道上比对测量基,得到 2 组结果:一组是使用不同测量基得到的结果,利用这组结果通过 Bell 不等式检验^[14]来确定是否存在第三方监听,如果发现监听则终止协议;另一组是使用相同测量基得到的结果,Alice 和 Bob 的测量结果具有反关联性,他们中的任一人翻转持有的比特就得到一致的共享比特序列.最后同 BB84 协议一样通过密钥纠错和隐私增强,得到最终的共享密钥.

1992 年,Bennett^[15]独立提出一个量子密码分发协议,称为 B92 协议.其工作原理与 BB84 协议类似,但不同于 BB84 使用了 4 种量子态,B92 只使用了 $|\uparrow\rangle$ 和 $|\varphi\rangle$ 这 2 种量子态.Bob 随机选择线偏振基或圆偏振基进行测量,如果测得 $|\leftrightarrow\rangle$ 或 $|\curvearrowright\rangle$,则可以肯定 Alice 发送的是 $|\varphi\rangle$ 或 $|\uparrow\rangle$,否则 Bob 不能确定 Alice 发送的量子比特.随后 Bob 告诉 Alice 在哪些量子比特上得到确定的结果,并对相应的测量基进行编码(如线偏振基编为“0”,圆偏振基编为“1”),得到共享密钥.同年,Bennett 等人^[16]结合纠缠态和 BB84 的思想,提出了 BBM92 协议,该协议也使用纠缠量子比特对,但与 E91 协议使用 Bell 不等式检验判断监听的方法不同,BBM92 协议使用和 BB84 协议类似的方法确定监听是否存在.此外他们还证明了 BBM92 协议与 BB84 协议本质上的等价性.

BB84 协议中使用单光子作为量子比特,然而在实际系统中,理想的单光子很难制备,一般通过对光

源发出的激光进行衰减,产生弱相干光代替单光子,这就会产生多光子脉冲,使协议容易受到光子数分离攻击^[17].鉴于此,2003 年,Hwang^[18]提出了诱骗态思想,2005 年,Lo 等人^[19]和 Wang^[20]分别独立地提出了诱骗态协议,通过在光信号中混入诱骗态,Bob 可以通过测量统计结果的异常发现第三方监听.诱骗态协议的提出,有力地推进了量子密钥分发由理论到实际应用的进程.

在实际应用过程中,上述量子密钥分发协议还有很多问题,它们一般依赖于理想状态的设备,这在现实中很难实现,因此人们开始考虑在协议层面避免对理想设备的过度依赖.2007 年,Acín 等人^[21]提出了设备独立的 QKD 协议(DI-QKD),它通过检测 Bell 不等式不成立来保证协议的安全,不依赖于设备细节,甚至在敌手提供设备的情况下也可以安全执行协议.然而,DI-QKD 协议对探测设备的效率要求很高,大大降低了协议的实用性.2012 年,Lo 等人^[22]提出了测量设备独立的 QKD 协议(MDI-QKD),不仅可以彻底抵御探测器端的攻击,还大大提高了协议执行的效率,此后人们对 MDI-QKD 又做了许多研究^[23-26].2014 年,Lim 等人^[27]提出了探测设备独立的 QKD 协议(DDI-QKD),进一步提高了效率,该协议不是完全的测量设备无关协议,但可天然抵抗时移攻击^[28].2016 年,Boaron^[29]对 DDI-QKD 的安全性作了理论分析,解释了其依赖的安全假设,并说明了与 MDI-QKD 协议不等价.2018 年,Lucamarini 等人^[30]提出了双场量子密钥分发协议(TF-QKD),在保证密钥安全的前提下突破了成码率和传输距离极限,引起很大轰动.

除了在理论研究方面取得引人瞩目成果外,量子密钥分发协议在具体实现方面也取得了许多成果,如基于光纤的长距离传输方案^[31-32]和基于自由空间的传输方案^[33-34]等.可以说,在量子密码学领域,量子密钥分发是被研究的最广泛、最深刻的一个方向,但仍存在许多问题与挑战,尤其是在具体的实现过程中,在密钥生成效率、传输距离、抗噪声、抗设备缺陷等方面,还有很多的工作要做.

4.2 量子加密

1) 量子一次一密

1917 年,Vernam^[35]提出了一种完善保密的加密方法,称为“一次一密”(one-time pad).与之对应,量子密码学也有量子“一次一密”算法.根据明文、密钥和密文分别是经典比特还是量子比特,量子“一次一密”算法主要有 3 种类型.

① 使用 2 位经典比特加密一位量子比特明文,

得到一位量子比特密文.该算法由 Boykin 和 Roychowdhury^[36]提出.算法中加密过程为: $|c\rangle = X^\alpha Z^\beta |m\rangle$,其中 $|m\rangle$ 为明文文比特, $|c\rangle$ 为密文比特, $\alpha, \beta \in \{0, 1\}$ 是两比特密钥, X 为 Pauli-X 门, Z 为 Pauli-Z 门.解密是加密的逆过程: $|m\rangle = Z^\beta X^\alpha |c\rangle$.

② 超密编码.由 Bennett 和 Wiesner^[37]首先提出.超密编码开始需要通信双方 Alice 和 Bob 共享一对处于纠缠态的量子比特,如 Bell 态. Alice 对自己手中的量子比特作 Pauli 门操作或不作任何操作后,将其发送给 Bob, Bob 通过对这一对纠缠比特作合适测量,可得到 Alice 想要发送的 2 位经典比特明文.超密编码可以看作是使用一位量子比特作为密钥,加密 2 位经典比特明文,得到一位量子比特密文.

③ 量子隐形传态^[38].开始时 Alice 和 Bob 共享一个 EPR 对,每人拥有 EPR 对的一个量子比特. Alice 将待发送的量子态 $|\varphi\rangle$ 与自己手中的一半 EPR 对作联合测量,得到两比特的经典信息,然后其发给 Bob, Bob 可以根据这两比特信息对自己的一半 EPR 对作相应测量,得到 $|\varphi\rangle$. Gisin 等人^[39]将其视为明文、密钥和密文都是量子比特的一次一密.

量子一次一密在构造量子签名等其他密码学应用时,有着广泛的应用.

2) 量子公钥加密

2000 年, Okamoto 等人^[40]在美密会上首先提出了量子公钥加密方案.方案中,消息的发送方、接收方以及敌手都被抽象成量子多项式时间图灵机,并且在量子计算模型下构造了量子单向陷门函数.在这之后,多种多样的量子公钥密码方案被提出. 2003 年, Yang^[41]提出了一个基于经典 NP 完全问题的量子公钥加密方案. 2008 年, Nikolopoulos^[42]基于量子比特旋转变换提出了一个公钥加密方案. 2009 年, Gao 等人^[43]使用对称密钥构造了量子公钥加密方案. 2012 年, Liang 等人^[44]提出了一个信息论安全的加密方案. 2014 年, Zheng 等人^[45]提出了面向比特的概率型量子公钥加密方案. 2015 年, Vlachou 等人^[46]提出了基于量子随机游走的方案. 2017 年, Wu 等人^[47]提出了基于 Bell 态的公钥加密方案.

下面基于 Nikolopoulos 的方案,以加密一个比特为例,简要说明量子公钥加密的原理.

① 密钥生成.随机选取正整数 $n \gg 1$, 随机选取 $s \in \mathbb{Z}_{2^n}$, 将 $|0\rangle$ 绕 y 轴旋转 $s\theta_n$ 后得到 $|\varphi_s\rangle = R_y(s\theta_n)|0\rangle$, 其中 $\theta_n = 2\pi/2^n$, y 轴垂直纸面向外, 如图 4 所示. 私钥为 (n, s) , 公钥为 $|\varphi_s\rangle$.

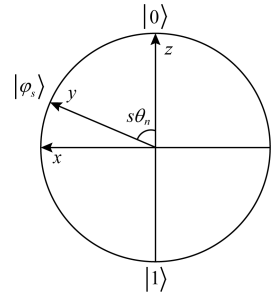


Fig. 4 $|0\rangle$ rotates $s\theta_n$ around y -axis

图 4 $|0\rangle$ 绕 y 轴旋转 $s\theta_n$

② 加密.设 $m \in \{0, 1\}$ 为明文, 将 $|\varphi_s\rangle$ 绕 y 轴转 $m\pi$ 得密文 $|c\rangle = R_y(m\pi)|\varphi_s\rangle = R_y(s\theta_n + m\pi \bmod 2\pi)|0\rangle$.

③ 解密.将 $|c\rangle$ 绕 y 轴旋转 $-s\theta_n$ 得到状态

$$R_y(-s\theta_n)|c\rangle = R_y(m\pi)|0\rangle = \begin{cases} |0\rangle, & m=0 \\ |1\rangle, & m=1 \end{cases}$$

在基 $\{|0\rangle, |1\rangle\}$ 下进行测量, 然后根据测量结果恢复明文 m .

在该公钥加密方案中, 私钥为经典数据, 公钥为量子数据, 方案通过量子比特旋转变换, 将经典比特加密为量子比特.

3) 量子同态加密

2012 年, Rohde 等人^[48]使用玻色子采样和量子行走模型实现了有限的量子同态加密. 2015 年, Liang^[49]基于通用量子线路, 构造了量子全同态加密方案, 该方案中可以对加密数据执行任意量子变换. 2015 美密会上, Broadbent 和 Jeffery^[50]基于经典 FHE 的存在提出了 2 种 QHE 方案. 他们提供了 2 种不同的方法来完成具有有限数量的非 Clifford 门线路的同态加密, 还提出了 QFHE 及其安全性的正式定义. 2016 年, Dulek 等人^[51]扩展了这项工作, 以便有效地评估任意多项式大小的线路, 并提供了一种新的紧凑型 QHE 方案. 2017 年, Ouyang 等人^[52]提出了一种 (n, n) 阈值秘密共享方案, 该方案允许对共享秘密上的量子线路进行评估而无需对其进行解码. 此外还有一些其他的量子同态加密方案^[53-55].

4.3 量子签名

量子签名是量子密码学的一个重要分支, 在 2001 年由 Gottesman 等人^[56]首次提出, 它通过量子力学原理保证数据签名的安全性. 同经典签名一样, 其安全性需要满足 3 个属性:

- 1) 不可伪造. 没有人能伪造一个合法的签名.
- 2) 不可否认. 签名者不能对自己的签名否认.

3) 可公开验证.接收到消息的任何人均可通过公钥验证消息签名的合法性.

人们最开始研究的量子签名是依赖于仲裁的,第一个具体方案由 Zeng 等人^[57]在 2002 年提出,此后 Curty 等人^[58]、Zou 等人^[59]、Gao 等人^[60]利用经典签名协议的分析方法,给出了该方案的一些安全漏洞.2009 年,Li 等人^[61]提出了基于 Bell 态的仲裁量子签名.2015 年,Li 和 Shi^[62]提出了基于 CNOT 链加密的仲裁量子签名.2018 年,Feng 等人^[63]提出了基于连续变量量子态的仲裁量子签名.

以签名一个量子比特为例,简要介绍基于 Bell 态的仲裁量子签名的思想.

1) 初始化.Alice 和 Bob 与仲裁分别共享密钥 k_A 和 k_B ,仲裁制备 Bell 态 $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,并分发给 Alice 和 Bob 各一个粒子.

2) 签名.Alice 制备 3 份待签名消息 $|p\rangle = \alpha|0\rangle + \beta|1\rangle (\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$,然后用 k_A 将一份 $|p\rangle$ 加密得 $|r\rangle = Enc_{k_A}(|p\rangle)$,接下来将另一份 $|p\rangle$ 与自己持有的 Bell 态粒子联合作 Bell 测量,

$$|p\rangle \otimes |\psi^+\rangle = \frac{1}{2} \{ |\psi^+\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) + |\psi^-\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) + |\varphi^+\rangle_A (\alpha|1\rangle_B + \beta|0\rangle_B) + |\varphi^-\rangle_A (\alpha|1\rangle_B - \beta|0\rangle_B) \},$$

其中, $|\psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\psi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, $|\varphi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ 和 $|\varphi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ 为 Bell 基,下标 A,B 分别代表 Alice 和 Bob.记结果为 M_A .最后 Alice 用 k_A 加密 $|r\rangle$ 和 M_A 得签名 $s = Enc_{k_A}(|r\rangle, M_A)$,并将第 3 份 $|p\rangle$ 和 s 发给 Bob.

3) 验证.Bob 在收到 Alice 的消息 $|p\rangle$ 和签名 s 后,用 k_B 将其加密得 $y_B = Enc_{k_B}(|p\rangle, s)$,并发送给仲裁.仲裁收到 y_B 后,用 k_B 解密得 $|p\rangle$ 和 s ,再用 k_A 解密 s 得 $|r'\rangle$ 和 M_A ,然后比较 $|r'\rangle$ 和 $|r\rangle = Enc_{k_A}(|p\rangle)$ 得

$$\gamma = \begin{cases} 0, & |r'\rangle \neq |r\rangle = Enc_{k_A}(|p\rangle) \\ 1, & |r'\rangle = |r\rangle = Enc_{k_A}(|p\rangle) \end{cases}$$

仲裁用 k_B 加密 $M_A, |p\rangle, s$ 和 γ 得 $y'_B = Enc_{k_B}(M_A, |p\rangle, s, \gamma)$ 并发给 Bob. Bob 收到 y'_B 并解密,如果 $\gamma = 0$,则拒绝签名,如果 $\gamma = 1$,则作进一步验证. Bob 首先根据 M_A 按规则 $|\psi^+\rangle \rightarrow I, |\psi^-\rangle \rightarrow \sigma_z, |\varphi^+\rangle \rightarrow \sigma_x, |\varphi^-\rangle \rightarrow \sigma_z \sigma_x$ (其中, I 为单位变换, σ_x 为 Pauli-X 变换, σ_z 为 Pauli-Z 变换)对自己持有 Bell 态粒子做

酉变换,然后将结果与 $|p\rangle$ 比较,如果相等则接受签名,如果不相等则拒绝签名.

近年来,除了普通量子签名外,人们还对量子盲签名、量子群签名、量子代理签名等分支进行了大量研究,取得了丰硕成果.

量子盲签名是一种特殊的签名,签名前先将消息盲化,签名者对盲化的消息进行签名,最后消息拥有者对签字除去盲因子,得到签名者关于原消息的签名.盲签名要求签名有可验证性、不可伪造性、不可否认性和盲性,即可验证去掉盲化因子的原消息签名,盲签名不能被伪造,签名者不能否认签名和签名者不知道所签署消息的内容.量子盲签名的研究成果主要有文献[64-70].

量子群签名允许群体中任意一个成员可以以匿名的方式代表整个群体对消息进行签名,并可以被公开验证.群签名要求可验证性、匿名性、不可伪造性、不可否认性和可追踪性,即消息接收者可以验证签名的有效性,但不能确定是哪个成员签署了消息,签名不能被伪造,签名者不能否认签名,有争议时管理员可揭示签名者的身份.量子群签名的研究成果主要有文献[71-75].

量子代理签名允许原始签名人将其签名权委托给代理签名人,代理签名人可以代表原始签名人进行签名.代理签名要求可验证性、不可伪造性、不可否认性、可区分性和可注销性,即签名的有效性可被验证,代理签名人和原始签名人都不能冒充对方伪造签名,也不能否认代签和委托,代理签名中包含代理签名人和原始签名人的信息,与普通签名可区分,原始签名人可注销代理签名人的签名权.量子代理签名的研究成果主要有文献[76-80].

4.4 其他研究领域

目前,量子密码以量子密钥分发为主要研究方向,加密、签名等也有不同程度的研究,而在其他密码学领域也有着一定的研究,形成了不同的研究分支.主要有量子秘密共享^[81-85]、量子比特承诺^[86-90]、量子不经意传输^[91-95]、量子安全直接通信^[96-100]、量子隐私查询^[101-105]、量子身份认证^[106-110]等,但总体来说还处于起步阶段.

5 面临的问题与挑战

量子计算由于其真正意义上的并行计算机制,可以进行指数级加速,大大超越经典计算的能力.然而,由于量子态制备、从量子态中提取信息等受客观

规律的限制,量子计算的广泛应用受到很大影响.想要有效发挥量子计算的威力,需要非常巧妙的设计硬件和软件.量子世界遵循的规律与经典世界有很大的不同,由于人们在日常生活中对经典世界的习惯,在利用量子规律时思维容易受到限制,这也是在量子计算研究中普遍存在的困难,是真正能体现量子计算优越性的算法少之又少的原因之一.如何设计好的硬件和软件,充分利用量子计算的能力,是广大科研工作者面临的重要挑战之一.

基于量子力学机制,量子密码学有着先天的优势.从理论上讲,量子密码学有着无条件安全性的特点,这是信息安全领域理想的目标之一.然而在实际应用时,由于设备缺陷、噪声影响等因素,还存在许多安全问题,需要人们从理论和实践 2 个层面去解决.此外在效率、易用性、健壮性等方面也存在诸多问题有待解决.在量子密码学安全方案设计方面,同经典密码一样,由于很难穷举所有攻击方式,仅进行启发式分析是远远不够的,必须考虑可证安全理论.量子力学有其独特的机制,如量子纠缠、未知量子态不可克隆等,利用这些特有的机制设计与经典密码学中没有显式对应的安全应用,也是一个重要的方向.同量子计算一样,由于受经典思维方式的影响,这一方面的工作也面临重要挑战.

6 结束语

本文简单介绍了量子计算及其主要算法的基本数学思想,并对基于量子力学机制的量子密码学的发展状况做了简要介绍.量子密钥分发是被研究的最深入的一个领域,无论是从理论上还是实践上,都取得了丰硕的研究成果,并开始进入商用阶段.其他量子密码学研究领域也取得了许多成果.未来的时代也许是属于量子的,量子计算及量子密码学的研究是为人们进入量子时代的必要准备,虽面临重重挑战,但已指明了方向.

参 考 文 献

- [1] Wiesner S. Conjugate coding [J]. ACM Sigact News, 1983, 15(1): 78-88
- [2] Brassard C, Bennett C H. Quantum cryptography: Public key distribution and coin tossing [C] //Proc of Int Conf on Computers, Systems and Signal Processing. Piscataway, NJ: IEEE, 1984: 175-179
- [3] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring [C] //Proc of the 35th Annual Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1994: 124-134
- [4] Grover L K. A fast quantum mechanical algorithm for database search [C] //Proc of the 28th Annual ACM Symp on Theory of Computing. New York: ACM, 1996: 212-219
- [5] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information [M]. Cambridge, UK: Cambridge University Press, 2010
- [6] Wootters W K, Zurek W H. A single quantum cannot be cloned [J]. Nature, 1982, 299(5886): 802-803
- [7] Yuen H P. Amplification of quantum states and noiseless photon amplifiers [J]. Physics Letters A, 1986, 113(8): 405-407
- [8] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer [J]. Proceedings of the Royal Society of London. A: Mathematical and Physical Sciences, 1985, 400(1818): 97-117
- [9] Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation [J]. Physical Review A, 1995, 52(5): 3457-3467
- [10] Deutsch D, Jozsa R. Rapid solution of problems by quantum computation [J]. Proceedings of the Royal Society of London. A: Mathematical and Physical Sciences, 1992, 439(1907): 553-558
- [11] Simon D R. On the power of quantum computation [J]. SIAM Journal on Computing, 1997, 26(5): 1474-1483
- [12] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441-444
- [13] Ekert A K. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters, 1991, 67(6): 661-663
- [14] Bell J S. On the Einstein Podolsky Rosen paradox [J]. Physics Physique Fizika, 1964, 1(3): 195-200
- [15] Bennett C H. Quantum cryptography using any two nonorthogonal states [J]. Physical Review Letters, 1992, 68(21): 3121-3124
- [16] Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem [J]. Physical Review Letters, 1992, 68(5): 557-559
- [17] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330-1333
- [18] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication [J]. Physical Review Letters, 2003, 91(5): No.057901
- [19] Lo H K, Ma Xiongfang, Chen Kai. Decoy state quantum key distribution [J]. Physical Review Letters, 2005, 94(23): No.230504
- [20] Wang Xiangbin. Beating the photon-number-splitting attack in practical quantum cryptography [J]. Physical Review Letters, 2005, 94(23): No.230503
- [21] Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks [J]. Physical Review Letters, 2007, 98(23): No.230501

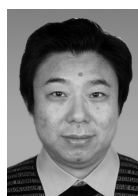
- [22] Lo H K, Curty M, Qi Bing. Measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2012, 108(13): No.130503
- [23] Zhao Yijia, Zhang Yichen, Xu Bingjie, et al. Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction [J]. Physical Review A, 2018, 97(4): No.042328
- [24] Ma Hongxin, Huang Peng, Bai Dongyun, et al. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction [J]. Physical Review A, 2018, 97(4): No.042329
- [25] Li Chunyan. Fault-tolerant measurement-device-independent quantum key distribution in a decoherence-free subspace [J]. Quantum Information Processing, 2018, 17(10): No.287
- [26] Hu Xiaolong, Yu Zongwen, Wang Xiangbin. Efficient measurement-device-independent quantum key distribution without vacuum sources [J]. Physical Review A, 2018, 98(3): No.032303
- [27] Lim C C W, Korzh B, Martin A, et al. Detector-device-independent quantum key distribution [J]. Applied Physics Letters, 2014, 105(22): No.221112
- [28] Qi Bing, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems [J]. Quantum Information & Computation, 2007, 7(1): 73-82
- [29] Boaron A, Korzh B, Houlmann R, et al. Detector-device-independent quantum key distribution: Security analysis and fast implementation [J]. Journal of Applied Physics, 2016, 120(6): No.063101
- [30] Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters [J]. Nature, 2018, 557(7705): 400-403
- [31] Diamanti E, Takesue H, Langrock C, et al. 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors [J]. Optics Express, 2006, 14(26): 13073-13082
- [32] Stucki D, Walenta N, Vannel F, et al. High rate, long-distance quantum key distribution over 250km of ultra low loss fibres [J]. New Journal of Physics, 2009, 11(7): No. 075003
- [33] Liao Shengkai, Cai Wenqi, Liu Weiyue, et al. Satellite-to-ground quantum key distribution [J]. Nature, 2017, 549(7670): 43-47
- [34] Liao Shengkai, Yong Hailin, Liu Chang, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication [J]. Nature Photonics, 2017, 11(8): 509-513
- [35] Vernam G S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications [J]. Journal of the AIEE, 1926, 45(2): 109-115
- [36] Boykin P O, Roychowdhury V. Optimal encryption of quantum bits [J]. Physical Review A, 2003, 67(4): No. 042317
- [37] Bennett C H, Wiesner S J. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states [J]. Physical Review Letters, 1992, 69(20): 2881-2884
- [38] Bennett C H, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Physical Review Letters, 1993, 70(13): 1895-1899
- [39] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography [J]. Reviews of Modern Physics, 2002, 74(1): 145-195
- [40] Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2000: 147-165
- [41] Yang Li. Quantum public-key cryptosystem based on classical NP-complete problem [J]. arXiv preprint, arXiv: quant-ph/0310076, 2003
- [42] Nikolopoulos G M. Applications of single-qubit rotations in quantum public-key cryptography [J]. Physical Review A, 2008, 77(3): No.032348
- [43] Gao Fei, Wen Qiaoyan, Qin Sujuan, et al. Quantum asymmetric cryptography with symmetric keys [J]. Science in China Series G: Physics, Mechanics and Astronomy, 2009, 52(12): 1925-1931
- [44] Liang Min, Yang Li. Public-key encryption and authentication of quantum information [J]. Science China Physics, Mechanics and Astronomy, 2012, 55(9): 1618-1629
- [45] Zheng Shihui, Gu Lize, Xiao Da. Bit-oriented quantum public key probabilistic encryption schemes [J]. International Journal of Theoretical Physics, 2014, 53(1): 116-124
- [46] Vlachou C, Rodrigues J, Mateus P, et al. Quantum walk public-key cryptographic system [J]. International Journal of Quantum Information, 2015, 13(7): No.1550050
- [47] Wu Wanqing, Cai Qingyu, Zhang Huanguo, et al. Quantum public key cryptosystem based on Bell states [J]. International Journal of Theoretical Physics, 2017, 56(11): 3431-3440
- [48] Rohde P P, Fitzsimons J F, Gilchrist A. Quantum walks with encrypted data [J]. Physical Review Letters, 2012, 109(15): No.150501
- [49] Liang Min. Quantum fully homomorphic encryption scheme based on universal quantum circuit [J]. Quantum Information Processing, 2015, 14(8): 2749-2759
- [50] Broadbent A, Jeffery S. Quantum homomorphic encryption for circuits of low T-gate complexity [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2015: 609-629
- [51] Dulek Y, Schaffner C, Speelman F. Quantum homomorphic encryption for polynomial-sized circuits [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 2016: 3-32
- [52] Ouyang Yingkai, Tan Sihui, Zhao Liming, et al. Computing on quantum shared secrets [J]. Physical Review A, 2017, 96(5): No.052333
- [53] Lai Chingyi, Chung Kaimin. On statistically-secure quantum homomorphic encryption [J]. Quantum Information & Computation, 2018, 8(9/10): 785-794

- [54] Mahadev U. Classical homomorphic encryption for quantum circuits [C] //Proc of the 59th IEEE Annual Symp on Foundations of Computer Science (FOCS). Piscataway, NJ: IEEE, 2018; 332–338
- [55] Newman M, Shi Yaoyun. Limitations on transversal computation through quantum homomorphic encryption [J]. arXiv preprint arXiv:1704.07798, 2017
- [56] Gottesman D, Chuang I. Quantum digital signatures [J]. arXiv preprint quant-ph/0105032, 2001
- [57] Zeng Guihua, Keitel C H. Arbitrated quantum-signature scheme [J]. Physical Review A, 2002, 65(4): No.042312
- [58] Curty M, Lütkenhaus N. Comment on “Arbitrated quantum-signature scheme”[J]. Physical Review A, 2008, 77(4): No. 046301
- [59] Zou Xiangfu, Qiu Daowen. Security analysis and improvements of arbitrated quantum signature schemes [J]. Physical Review A, 2010, 82(4): No.042325
- [60] Gao Fei, Qin Sujuan, Guo Fenzhuo, et al. Cryptanalysis of the arbitrated quantum signature protocols [J]. Physical Review A, 2011, 84(2): No.022344
- [61] Li Qin, Chan W H, Long Dongyang. Arbitrated quantum signature scheme using Bell states [J]. Physical Review A, 2009, 79(5): No.054307
- [62] Li Fengguang, Shi Jianhong. An arbitrated quantum signature protocol based on the chained CNOT operations encryption [J]. Quantum Information Processing, 2015, 14 (6): 2171–2181
- [63] Feng Yanyan, Shi Ronghua, Guo Ying. Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states [J]. Chinese Physics B, 2018, 27(2): No.020302
- [64] Qi Su, Zheng Huang, Wen Qiaoyan, et al. Quantum blind signature based on two-state vector formalism [J]. Optics Communications, 2010, 283(21): 4408–4410
- [65] Wang Tianyin, Wen Qiaoyan. Fair quantum blind signatures [J]. Chinese Physics B, 2010, 19(6): No.060307
- [66] Shi Jinjing, Shi Ronghua, Guo Ying, et al. Batch proxy quantum blind signature scheme [J]. Science China Information Sciences, 2013, 56(5): 1–9
- [67] Li Wei, Shi Jinjing, Shi Ronghua, et al. Blind quantum signature with controlled Four-Particle cluster states [J]. International Journal of Theoretical Physics, 2017, 56(8): 2579–2587
- [68] Wen Xiaojun, Niu Xiamu, Ji Liping, et al. A weak blind signature scheme based on quantum cryptography [J]. Optics Communications, 2009, 282(4): 666–669
- [69] Wang Mingming, Chen Xiubo, Yang Yixian. A blind quantum signature protocol using the GHZ states [J]. Science China Physics, Mechanics and Astronomy, 2013, 56 (9): 1636–1641
- [70] Lou Xiaoping, Chen Zhigang, Guo Ying. A weak quantum blind signature with entanglement permutation [J]. International Journal of Theoretical Physics, 2015, 54(9): 3283–3292
- [71] Yang Yuguang, Wen Qiaoyan. Quantum threshold group signature [J]. Science in China Series G: Physics, Mechanics and Astronomy, 2008, 51(10): 1505–1514
- [72] Wen Xiaojun, Tian Yuan, Ji Liping, et al. A group signature scheme based on quantum teleportation [J]. Physica Scripta, 2010, 81(5): No.055001
- [73] Xu Rui, Huang Liusheng, Yang Wei, et al. Quantum group blind signature scheme without entanglement [J]. Optics Communications, 2011, 284(14): 3654–3658
- [74] Shi Jinjing, Shi Ronghua, Tang Ying, et al. A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform [J]. Quantum Information Processing, 2011, 10(5): 653–670
- [75] Xu Guangbao, Zhang Kejia. A novel quantum group signature scheme without using entangled states [J]. Quantum Information Processing, 2015, 14(7): 2577–2587
- [76] Yang Yugang, Wen Qiaoyan. Threshold proxy quantum signature scheme with threshold shared verification [J]. Science in China Series G: Physics, Mechanics and Astronomy, 2008, 51(8): 1079–1088
- [77] Yang Yuguang. Multi-proxy quantum group signature scheme with threshold shared verification [J]. Chinese Physics B, 2008, 17(2): 415–418
- [78] Shi Jinjing, Shi Ronghua, Tang Ying, et al. A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform [J]. Quantum Information Processing, 2011, 10(5): 653–670
- [79] Wang Tianyin, Wei Zongli. One-time proxy signature based on quantum cryptography [J]. Quantum Information Processing, 2012, 11(2): 455–463
- [80] Shi Jingjing, Shi Ronghua, Guo Ying, et al. Batch proxy quantum blind signature scheme [J]. Science China Information Sciences, 2013, 56(5): 1–9
- [81] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829–1834
- [82] Hsu L Y. Quantum secret-sharing protocol based on Grover’s algorithm [J]. Physical Review A, 2003, 68(2): No.022306
- [83] Yan Fengli, Gao Ting. Quantum secret sharing between multiparty and multiparty without entanglement [J]. Physical Review A, 2005, 72(1): No.012304
- [84] Karimipour V, Asoudeh M. Quantum secret sharing and random hopping: Using single states instead of entanglement [J]. Physical Review A, 2015, 92(3): No.030301
- [85] Wang Yu, Tian Caixing, Su Qi, et al. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state [J]. Science China Information Sciences, 2019, 62(7): No.72501
- [86] Brassard G, Crépeau C. Quantum bit commitment and coin tossing protocols [C] //Proc of Conf on the Theory and Application of Cryptography. Berlin: Springer, 1990: 49–61

- [87] Kent A. Quantum bit string commitment [J]. Physical Review Letters, 2003, 90(23): No.237901
- [88] Buhrman H, Christandl M, Hayden P, et al. Security of quantum bit string commitment depends on the information measure [J]. Physical Review Letters, 2006, 97(25): No. 250501
- [89] Lunghi T, Kaniewski J, Bussi eres F, et al. Experimental bit commitment based on quantum communication and special relativity [J]. Physical Review Letters, 2013, 111(18): No.180504
- [90] Song Yaqi, Yang Li. Semi-counterfactual Quantum Bit commitment protocol [J]. Scientific Reports, 2020, 10(1): 1-12
- [91] Mayers D. Quantum key distribution and string oblivious transfer in noisy channels [C] //Proc of Annual Int Cryptology Conf. Berlin: Springer, 1996: 343-357
- [92] Shimizu K, Imoto N. Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty [J]. Physical Review A, 2002, 66(5): No. 052316
- [93] He Guangping, Wang Z D. Oblivious transfer using quantum entanglement [J]. Physical Review A, 2006, 73(1): No.012331
- [94] Schaffner C. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model [J]. Physical Review A, 2010, 82(3): No.032308
- [95] Ribeiro J, Wehner S. On bit commitment and oblivious transfer in measurement-device independent settings [J]. arXiv preprint arXiv:2004.10515, 2020
- [96] Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key [J]. Acta Physica Polonica A, 2002, 3(101): 357-368
- [97] Deng Fuguo, Long Guilu. Secure direct communication with a quantum one-time pad [J]. Physical Review A, 2004, 69(5): No.052319
- [98] Lin Song, Wen Qiaoyan, Gao Fei, et al. Quantum secure direct communication with χ -type entangled states [J]. Physical Review A, 2008, 78(6): No.064304
- [99] Chen Shanshan, Zhou Lan, Zhong Wei, et al. Three-step three-party quantum secure direct communication [J]. Science China Physics, Mechanics & Astronomy, 2018, 61(9): No.90312
- [100] Zhou Zengrong, Sheng Yubo, Niu Penghao, et al. Measurement-device-independent quantum secure direct communication [J]. Science China Physics, Mechanics & Astronomy, 2020, 63(3): No.230362
- [101] Chor B, Goldreich O, Kushilevitz E, et al. Private information retrieval [C] //Proc of IEEE 36th Annual Foundations of Computer Science. Piscataway, NJ: IEEE, 1995: 41-50
- [102] Gertner Y, Ishai Y, Kushilevitz E, et al. Protecting data privacy in private information retrieval schemes [J]. Journal of Computer and System Sciences, 2000, 60(3): 592-629
- [103] Giovannetti V, Lloyd S, Maccone L. Quantum private queries [J]. Physical Review Letters, 2008, 100(23): No. 230502
- [104] Olejnik L. Secure quantum private information retrieval using phase-encoded queries [J]. Physical Review A, 2011, 84(2): No.022313
- [105] Gao Fei, Qin Sujuan, Huang Wei, et al. Quantum private query: A new kind of practical quantum cryptographic protocol [J]. Science China Physics, Mechanics & Astronomy, 2019, 62(7): No.70301
- [106] Du ek M, Haderka O, Hendrych M, et al. Quantum identification system [J]. Physical Review A, 1999, 60(1): 149-156
- [107] Curty M, Santos D J. Quantum authentication of classical messages [J]. Physical Review A, 2001, 64(6): No.062309
- [108] Yang Yuguang, Wen Qiaoyan, Zhang Xing. Multiparty simultaneous quantum identity authentication with secret sharing [J]. Science in China Series G: Physics, Mechanics and Astronomy, 2008, 51(3): 321-327
- [109] Bartkiewicz K,  ernoch A, Lemr K. Using quantum routers to implement quantum message authentication and Bell-state manipulation [J]. Physical Review A, 2014, 90(2): No. 022335
- [110] Kang M S, Choi Y H, Kim Y S, et al. Quantum message authentication scheme based on remote state preparation [J]. Physica Scripta, 2018, 93(11): No.115102



Wang Yongli, born in 1982. PhD candidate in Shandong University. His main research interest is quantum cryptography.



Xu Qiuliang, born in 1960. Professor and PhD supervisor in Shandong University. His main research interests include public key cryptography and multi-party secure computation.