DOI 10.15302/J-SSCAE-2022.04.015

量子密码协议研究现状与未来发展

张雪，高飞*，秦素娟，张平

（网络与交换技术国家重点实验室（北京邮电大学），北京 100876）

摘要：量子计算具有并行计算能力，在解决某些特定问题上展现出超越经典计算的能力；一旦大型量子计算机研制成功，基于计算复杂性假设的经典密码算法和协议，其安全性将受到严重挑战。量子密码是一种新型密码体制，相应安全性基于量子力学原理，因能对抗量子计算的攻击而受到广泛关注。本文聚焦量子密码近40年的发展历程，梳理了量子密钥分配、量子安全直接通信、量子秘密共享、量子身份认证、量子两方安全计算、量子保密查询等量子密码协议的研究进展和发展趋势，凝练发展过程中面临的技术与应用问题。分析表明，当前量子密码协议研究处于“量子密钥分配协议遥遥领先、其他协议有待突破”的不平衡状态，也是“其他协议难以突破”的瓶颈状态。着眼未来应用，针对数字签名、两方安全计算问题的实用化量子协议是亟需解决的核心问题。为此建议，量子密码与后量子密码研究应同步开展，加强“量子科技”“密码学”学科的交叉研究和人才培养，优化对相关基础研究的考核评价机制。

关键词：量子密码；协议；量子密钥分配；量子数字签名；量子保密查询

中图分类号：TN918.1；TP309.7　　**文献标识码：**A

Current Status and Future Development of Quantum Cryptographic Protocols

Zhang Xue, Gao Fei*, Qin Sujuan, Zhang Ping

(State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing 100876, China)

Abstract: Quantum computing has the capability of parallel computing and is superior to classical computing in solving some specific problems. Once a large-scale quantum computer is developed, the security of classical cryptographic algorithms and protocols, which is based on the assumption of computational complexity, will be severely challenged. Quantum cryptography is a new cryptosystem; its security is based on the principles of quantum mechanics, and can resist the attack of quantum computing. This paper focuses on the nearly 40 years development of quantum cryptographic protocols, including quantum key distribution (QKD), quantum secure direct communication, quantum secret sharing, quantum identity authentication, two-party secure computation, and quantum private query, and summarizes the problems in the process of development. The analysis shows that the quantum cryptographic protocols are in an unbalanced state: QKD is far ahead of other protocols and other protocols are difficult to achieve breakthroughs. In the future, practical quantum protocols for digital signature and two-party secure computation are core issues that needs to be addressed urgently. Therefore, research on quantum and post-quantum cryptography should be conducted synchronously, cross-over study and talent cultivation for the quantum science and cryptography disciplines should be strengthened, and the examination and evaluation mechanism of relevant basic research needs to be optimized.

收稿日期：2022-05-11；**修回日期：**2022-06-20

通讯作者：*高飞，北京邮电大学网络空间安全学院教授，研究方向为量子密码和量子算法；E-mail: gaof@bupt.edu.cn

资助项目：中国工程院咨询项目“量子信息技术工程化应用发展战略研究”(2021-HYZD-01)；国家自然科学基金项目(61972048, 61976024)

本刊网址：www.engineering.org.cn/ch/journal/sscae

Keywords: quantum cryptography; protocols; quantum key distribution; quantum digital signature; quantum private query

一、前言

自古以来，信息交流便是人们日常生活中不可或缺的一部分。信息传递的安全性是很多通信场景下的基本需求，在外交、军事、经济等保密性较高的领域中更显重要。密码学是保障网络与信息安全的理论基础，各类密码算法和协议在确保消息的机密性、完整性、不可否认性以及身份认证等方面发挥着重要作用。经典密码（指基于数学复杂性理论的数学密码，与量子密码相对应）算法可大致分为对称密码、公钥密码两类，各有优点且应用广泛。然而在20世纪90年代Shor算法、Grover算法提出后，量子算法对当前的密码体制形成了严重的安全性威胁。如果有了通用的量子计算机，Shor算法可以轻松攻破基于整数分解、离散对数问题的多种公钥密码；Grover算法也将挑战对称密码的安全性。因此，研究可以抵抗量子计算攻击的新型密码体制已经成为密码学领域的重大任务。

有趣的是，量子科技在对密码学的安全性形成威胁之际，也为抗量子计算攻击提供了一种潜在方法（即量子密码）。量子密码是量子力学和密码学相融合的产物，它采用量子态作为信息载体在用户之间传送信息。根据量子态的特性，在一个安全的量子密码协议中通信双方可以发现所有有效的窃听/攻击行为。可见，量子密码的安全性不再基于数学问题的困难性，而是由量子力学基本原理所保证。一个设计精巧的量子密码协议可以达到信息论安全。近年来，随着量子信息技术的逐渐丰富与成熟，人们已经提出了各类独具特色的量子密码协议。需要说明的是，经典密码通常在密码算法的基础上构建可完成各种密码学任务的协议，而量子密码往往直接利用量子性质来设计类似协议。因此，相比于算法，协议是量子密码中的主要研究内容。

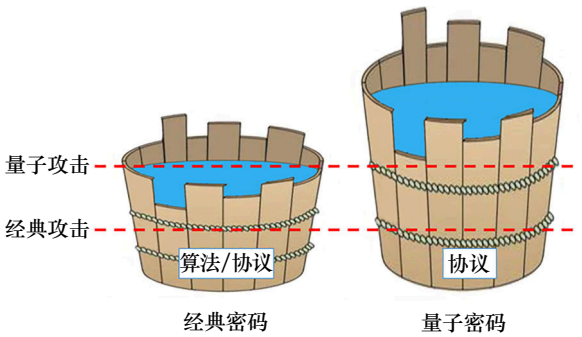

图1　量子密码协议的研究意义

注：木桶的容水量代表信息系统的安全性强度。

量子密码协议的研究意义可以参照木桶理论（见图1）来表述。在经典密码中，组成木桶的木板代表各类经典密码算法和协议；而在量子密码中，木板代表各类量子密码协议。一方面，协议对量子密码来说至关重要，所有密码学任务都是通过相关协议来完成；另一方面，与经典密码算法和协议相比，量子密码协议的安全性大大提高，可以对抗未来量子计算的攻击。人们希望利用量子性质能够实现各类密码协议功能，进而全面提升信息系统的安全性。

本文针对量子密码协议的发展动态和趋势进行研究。按照协议的不同功能，梳理6类主流量子密码协议（见图2）的发展现状并分别分析实用化潜力及局限性；统筹考虑量子密码整体的实际应用需求，凝练领域未来亟待解决的关键科学问题并预判潜在的技术途径，提出我国在本领域的技术发展建议，以期为量子密码协议的深化研究提供基础性参考。

二、量子密钥分配协议

量子密钥分配（QKD）是一种通信双方通过传

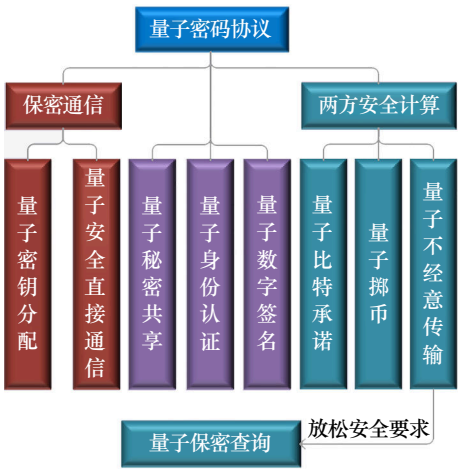

图2　几类具有代表性的量子密码协议

输量子态来建立密钥的协议，其目的是使通信双方获得一串只有他们两个知道的密钥（由经典的随机比特构成，但由于是用量子方式建立的，因此也被称为“量子密钥”）。由于QKD和一次一密（OTP）加密算法均具有信息论安全性，将两者结合使用就可以实现完美安全的保密通信。

根据光源编码空间的维度不同，QKD可以分为离散变量（DV）和连续变量（CV）两类。QKD系统由发送端、接收端以及信道组成。QKD信道包括量子信道和经典信道，分别用于传输量子和经典消息。在量子密码协议中，一般假设经典通信是不可篡改的，这一点可以利用具有信息论安全性的经典消息认证码来实现。此外，为了在有噪声的现实情况下获得信息论安全性，QKD一般包含纠错和隐私放大的过程，前者用于纠正噪声引起的密钥错误，后者用于压缩窃听者在噪声掩护下可能获得的密钥信息。

1984 年，IBM 的 Bennett 和 Montreal 大学的 Brassard 首次提出量子密码的概念，并给出第一个QKD协议——BB84协议 [1]。经过近四十年的发展历程，人们基于不同量子力学特性提出了多种QKD协议，一些典型QKD协议的安全性也得到了严格证明，但实际上QKD系统中因为器件的不完美仍然存在一些安全性漏洞。设备无关（DI）QKD协议可从根本上消除这些漏洞 [2,3]。该类协议不需要假设QKD设备是完美的，它们甚至可以是不可信的。DI-QKD的安全性基于如下事实：量子过程和经典过程对贝尔不等式的违背程度是不同的。通信双方通过观测输入和输出的经典比特信息间的关联关系，计算贝尔不等式的违背值，即可判断设备的可信程度，并估计出窃听者所能获取的最大信息量。只要实验中观测到的违背值足够大，则说明设备足够可信，通信双方进而可以获得信息论安全的密钥。DI-QKD协议过程相当于对其设备的可信性进行了一次“自测试”，只有可信的设备才能通过测试，进而让通信双方成功建立密钥。此后，人们又提出了测量设备无关（MDI）QKD协议，它可以在测量设备不可信的情况下实现安全的密钥分配 [4,5]，且实现难度较DI-QKD更低。

QKD实用化研究也进展快速。2021年，中国科学技术大学潘建伟团队演示了一个集成的空对地量子通信网络。基于“墨子号”量子卫星，通过集成光纤和自由空间QKD链路，该QKD网络中的任何用户都可以与其他任何用户进行通信，总距离可达4600 km [6]。同年，中国科学技术大学封召等演示了10 m水下信道基于偏振编码的QKD实验，安全密钥生成率超过700 kpbs [7]。2022年，中国科学技术大学郭光灿团队实现833 km光纤QKD，将无中继QKD安全传输距离世界纪录提升了200余 km，向实现1000 km陆基量子保密通信迈出重要一步 [8]。

综上所述，QKD作为量子密码领域研究最早、理论最成熟的部分。目前已有多个国家建立了基于QKD的通信网络，如美国的DARPA、欧洲的SECOQC、日本的Tokyo QKD Network、中国的京沪干线等。随着“墨子号”量子卫星的发射，京沪干线、沪杭干线的相继落成，QKD已经在一定程度上具备了走向实用化的条件。尽管如此，受技术条件限制，当前的QKD系统在传输速率、传输距离两个方面还不能满足大规模应用的需求。在具体应用中，人们往往会选择一些折衷方案。比如，针对密钥生成速率低的问题，人们也常将QKD密钥用于高级加密标准（AES）等加密算法中，这样的保密通信就不再具有信息论安全性。再比如，针对传输距离近的问题，QKD网络往往需要“可信中继”（见图3），即假设中继是可信的（如果中继节点不可信，它将轻易获得用户所分配的密钥，进而获得后续用该密钥加密的秘密消息），这也会在一定程度上损害QKD的安全性，并限制QKD的大规模应用。

中继节点分别与通信双方执行QKD，并利用其与Bob的密钥将其与Alice的密钥加密传输给Bob，使得Alice和Bob可以远距离建立密钥。当然，除了这种可信中继之外，人们也在研究“量子中继”[9]，它通过量子存储、纠缠交换等技术来提高纠缠态分发的距离，进而可以提升QKD的传输距离。这种中继不会损害QKD的安全性，具有更好的应用潜力，但相关技术还不够成熟，目前还达

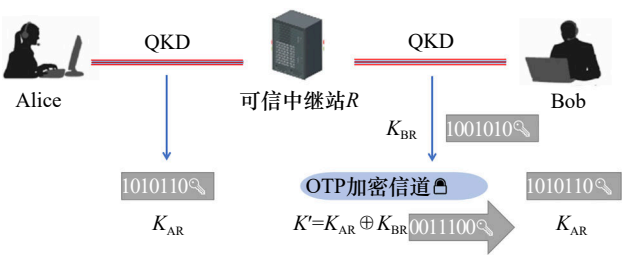

图3 QKD的可信中继方案

不到实用化的程度。

三、量子安全直接通信协议

量子安全直接通信（QSDC）是一种收发双方不需要建立密钥而直接利用量子信道传输机密信息的保密通信技术。与传输随机密钥不同，由于要确保消息的完整性，利用量子态直接传输秘密消息将不利于协议过程中的窃听检测、纠错、隐私放大等步骤的实施。QSDC 协议通过分块传输、量子隐私放大等技术来解决该问题，进而可以实现直接传输秘密消息的功能。

2000 年，清华大学龙桂鲁和刘晓曙利用纠缠态的块传输技术首次提出了一种量子保密通信模型用于传输机密信息 [10]。2004 年，清华大学邓富国和龙桂鲁等将非正交量子态块传输和经典 OTP 结合起来，提出了基于单光子的 QSDC 方案 [11]。与基于纠缠态的方案相比，单光子态的操控更容易实现。此后，QSDC 这一通信模式成为国际量子保密通信的研究热点 [12]。

近年来，人们在 QSDC 的实现方面也取得了可喜的进展。2016 年，山西大学肖连团队和清华大学龙桂鲁团队联合实验演示了基于单光子的 QSDC [13]。2021 年，上海交通大学陈险峰、江西师范大学李渊华等利用 QSDC 原理，首次实现了网络中 15 个用户之间的安全通信，传输距离达 40 km [14]。

从目前的研究现状来看，QSDC 在技术上已经接近实用化的程度。从功能上讲，QSDC 与 QKD & OTP 相同，都属于保密通信的范畴。

四、量子秘密共享协议

秘密共享的基本思想是将秘密以适当的方式拆分，拆分后的每一个份额由不同的参与者管理，使得单个参与者无法恢复秘密信息，而只有若干个参与者相互协作才能恢复。秘密共享的目的是防止秘密过于集中以实现分散风险。最常见的秘密共享协议为 (k,n) 门限方案，即分发者把秘密消息加密成 n 份，分别发送给 n 个接收者，要求接收者中任意 k 个人合作都可以重构出这条消息，而任何少于 k 个人的组合都得不到这条消息的任何信息。经典密码中，常见的秘密共享协议有基于多项式拉格朗日插值公式的 Shamir 门限方案、基于中国剩余定理的门限方案等。随着量子密码学的不断发展，量子秘密共享（QSS）协议也引起了学者们的广泛研究。

1999 年，Hillery、Buzek 和 Berthiaume 三人利用 GHZ 态的纠缠特性提出了第一个 QSS 协议 [15]。后续学者们又利用不同的量子特性提出了多种 QSS 协议 [16]。

在实验实现方面，2014 年，Bell 等在线性光学装置中利用光子实现了基于图态的经典信息和量子信息的秘密共享 [17]；2018 年，周瑶瑶等实现了一种利用光场的多体束缚纠缠的 QSS 协议，可实现四个参与者之间的秘密共享 [18]。2021 年，Liao 等提出一种基于离散调制相干态的 CV-QSS 协议，该方案最大传输距离达到 100 km 以上 [19]。

从理论上看，QSS 具有广阔的研究前景，如对 (k,n) 门限方案的研究、对多方 – 多方秘密共享方案的研究、对理性秘密共享方案的研究等。然而，目前 QSS 协议仍不具有实际应用价值。一是由于对 QSS 协议的研究大多着重于研究 (n,n) 门限方案，很难做到 (k,n) 门限秘密共享，使得 QSS 的应用场景受限；二是 QSS 协议中纠错与隐私放大方案匮乏，难以真正实现信息论安全。实际上，将 QKD 协议与经典门限方案相结合就可实现信息论安全的秘密共享，更具有实际应用价值。因此，QSS 可以看作是 QKD 的一个直接应用。

五、量子身份认证协议

量子身份认证（QIA）指在量子密码协议中对参与者的身份进行验证，以防止攻击者假冒参与者身份窃取信息。为了在 QKD 过程中实现信息论安全的身份认证，人们提出了一系列的 QIA 协议。QIA 协议大致可以分为两类：共享经典密钥型、共享纠缠态型。

在共享经典密钥型 QIA 协议中，通信双方事先共享一个预定好的字符串，以此表明双方身份。1999 年，Dušek 等首次提出用经典的消息认证协议来认证 QKD 中所传递的经典信息 [20]。此后，也有方案利用该经典密钥来代表窃听检测粒子的位置和测量基，同样也可以达到认证双方身份的功能。

共享纠缠态型 QIA 协议指通信双方共享一组纠缠态粒子，双方各自拥有每对纠缠态粒子中的一个，

对纠缠对进行相应的操作来互相表明身份。这种方法需要长时间存储大量纠缠态粒子，不易实现。

为了达到信息论安全，QIA 协议中用户事先共享的密钥或纠缠态要确保在使用过程中不会被窃听者所获得，而且一般不能重复使用。此外，身份认证一般应与 QKD 等协议同时进行，防止窃听者跳过认证阶段直接进行密钥分发。

不难看出，QIA 的实现思路与经典身份认证是类似的，都是在不泄露身份密钥的前提下向对方证明自己拥有该身份密钥。区别在于，前者的身份密钥既可以是经典的，也可以是量子的，而后者是经典的。然而从目前来看，QIA 协议的实际应用并不多。原因如下：QIA 一般与实现其他密码功能的量子密码协议（如 QKD）配套使用。而在绝大多数量子密码协议中，经典信道往往采用信息论安全的消息认证码（MAC）来确保消息的完整性。该技术不但可以保证经典消息不被篡改，同时也可实现相互认证身份的功能。因此，在量子密码协议中通常不需要额外做身份认证。

六、量子数字签名协议

2001 年，Gottesman 和 Chuang 首次提出了量子数字签名（QDS）的概念，并基于量子单向函数给出了第一个量子数字签名协议 [21]。尽管该协议需要量子存储、量子态交换比较测试和安全量子信道等较难实现的技术，但是由于其具有信息论安全的优势，引起了人们对 QDS 研究的浓厚兴趣。不幸的是 Barnum 等证明对量子消息进行数字签名不可行，即使计算安全也不可行 [22]。后续，人们尝试弱化对 QDS 的一些要求，提出了仲裁量子签名的概念。仲裁量子签名需要在仲裁的帮助下才能完成对数字签名的验证，这与实际应用的数字签名有差别，但是它不仅可以签名经典消息，还可以签名量子消息，引起了学者们的关注。

同其他量子密码协议一样，实际应用中攻击者也会利用物理设备的不完美性对 QDS 协议进行攻击。为克服实际安全问题，人们提出了设备无关 QDS 协议 [23]。最近，为了进一步提高 QDS 的实用性和安全性，人们提出了基于连续变量的 QDS 协议和基于诱骗态的 QDS [24,25]。同时，面向各种实际应用场景，学者们提出了多种 QDS 协议，如 Qiu 等提出了一种面向敏感数据访问控制的 QDS 协议 [26]，Singh 等利用 QDS 设计了一种安全区块链交易协议 [27]。

目前 QDS 主要集中在三方协议（即包括一个签名者，一个接收者和一个验证者）这种特殊情形，且验证者需要事先共享验证密钥，无法达到经典数字签名中任意用户都可验签的便利性需求。另外，QDS 在实验和实用化方面的成果还很少。总之，无论技术上还是理论上，QDS 距离真正的实用化还有很大的距离，还仍需要继续深入研究。

七、量子两方安全计算协议

（一）量子比特承诺

比特承诺最早由 1995 年图灵奖得主 Blum 提出，它可用于构建零知识证明、可验证秘密共享、掷币等协议，是安全多方计算中最重要的基础协议之一。人们期望通过量子途径，探索实现信息论安全比特承诺的可行性。

1997 年，Lo 和 Chau 构建了量子比特承诺协议的标准模型，并证明了无论在经典环境下还是量子计算环境下，标准模型下的比特承诺协议都不能达到信息论安全 [28]。同年，Mayers 也独立证明了该结论 [29]。这一结论被称为 no-go 定理，成为阻碍量子比特承诺甚至其他量子两方安全计算协议发展的一大障碍。后续，人们不断尝试放松条件的量子比特承诺（QBC）以规避 no-go 定理，比如有噪量子存储模型和狭义相对论模型。

在实验方面，2012 年，Ng 等完成了有噪量子存储模型下的 QBC 实验 [30]。2013 年和 2014 年，Lunghi 等和 Liu 等分别完成了狭义相对论模型下的 QBC 实验 [31,32]。

综上所述，目前 no-go 定理的正确性得到了绝大多数学者的认可，要想实现信息论安全的 QBC 还存在重要的理论障碍。而对于为了跨过 no-go 定理而提出的有噪量子存储模型和狭义相对论模型，前者不能达到信息论安全，后者缺乏实用潜力。

（二）量子掷币

掷币是使互不信任、不在一起的双方共同产生一个随机比特，这个比特不能被某一方决定。根据掷币协议的参与方对掷币结果是否有固定的喜好，

可将掷币协议分为强掷币协议和弱掷币协议。如果不诚实方的攻击不能使得任何一个掷币结果出现概率超过p=1/2+ε，称为强掷币。若两方的喜好结果不同，不诚实方的攻击不能使得他喜好的掷币结果出现概率超过p=1/2+ε，称为弱掷币。其中参数ε称为某一方（或协议）的偏。ε度量了协议的安全性，其值越小协议越安全。ε应该严格小于1/2以保证欺骗方不能完全控制掷币结果。当且仅当双方的偏相等时，称掷币协议是公平的。当双方的偏均为0时，称掷币协议是完美的。

1984年Bennett和Brassard首次提出了量子掷币协议[1]。但是10年后，Lo和Chau证明了完美量子掷币协议是不存在的，此后人们一直致力于研究具有更小偏的掷币协议。Kitaev证明任何强量子掷币协议的偏不可能小于0.207。2007年Mochon证明量子弱掷币的偏可以任意小[33]。2009年，Berlin等提出并定义了容忍损失的量子掷币协议并证明任意一方通过作弊获得的偏为0.4[34]。2010年Chailloux等证明容忍损失的量子掷币协议的任意一方通过作弊获得的偏最少为0.359[35]。

在实验方面，2010年，Chailloux等实验实现了偏为0.207的强量子掷币协议[36]；2020年，Bozzio等提出了一个只需要单光子和线性光学装置的实用弱掷币协议，其偏达到了0.207[37]。

目前，量子强掷币协议的偏不可能小于0.207（即双方欺骗成功概率可达到0.707），而且在有噪声和损失的情况下，偏至少为0.35[38]。此概率过大，导致量子掷币协议并不实用。

（三）量子不经意传输

不经意传输（OT）协议作为一种保护隐私的通信协议，被广泛应用于安全多方计算、认证协议等诸多隐私敏感的领域。类似于对其他密码协议的研究，人们也希望利用量子技术来实现信息论安全的OT协议，即量子不经意传输（QOT）。

1988年Crépeau等提出了第一个QOT协议，该协议假定Bob无法将量子测量过程延迟[39]。后续，学者们基于QBC提出了多种QOT协议，但随着QBC no-go定理的提出，所有基于QBC的QOT协议不再安全。

此后，人们不断探索打破no-go定理的QOT。2002年Shimizu等提出以50%概率成功传输秘密消息的方案（称为全或无OT），协议中Bob无法以100%概率得到某个秘密消息，从而回避了no-go定理的限制[40]。2005年Damgard等考虑三种特殊场景来尝试跨过no-go定理，实现了基于BB84的全或无QOT和QBC协议[41]。2016年Pitalúa-García利用时空约束提出了一种2取1 QOT协议，随后在2018年进行了实验验证[42]。

目前2取1 QOT协议最优欺骗概率在参与方半诚实条件下可以达到2/3[43]。2021年，Amiri等提出了一种在参与方不诚实时达到欺骗概率2/3的2取1半随机QOT协议[44]。半随机QOT协议的功能如下：Alice有两个比特消息x_0、x_1，协议结束时Bob随机得到消息(b,x_b)，且不能得到$x_{\bar{b}}$，Alice不能得到Bob的输出消息(b,x_b)。

综上所述，2取1 QOT协议始终无法逾越no-go定理这座大山。而为了跨过no-go定理的限制，人们基于用户技术条件受限的假设提出了多种协议，但它们往往不再是信息论安全的。此外，如何解决容忍量子信道噪声的问题，也是QOT走向实际应用所面临的一大挑战。因此QOT协议离真正投入使用还有很长的路要走。

（四）量子保密查询

在很多场景下，人们不仅需要保护传递的信息不被外部攻击者窃取，还需要保护通信双方的隐私不被对方获取。对称私有信息检索（SPIR）就是这样一类密码任务。本质上，SPIR实现的是“多取一”的不经意传输。根据no-go定理，理想的SPIR在量子密码中不能实现。目前人们最为实际的做法是，将SPIR中的隐私要求放松到“欺骗敏感”的程度（即所有有效的欺骗行为都会有非零的概率被对方发现），这种协议通常被称作量子保密查询（QPQ）[45]。

QPQ对安全性要求如下：①数据库拥有者Bob试图获取用户Alice检索地址的欺骗行为以非零概率被Alice发现；②用户Alice除了获得检索的条目外，可以随机获得有限几个数据库条目。Alice额外得到的条目是随机的，一般不是她需要的，而Bob通常不敢冒着被发现欺骗的危险去攻击，因为一旦被发现将损害自己的声誉，甚至可能会面临十分严厉的惩罚。因此，这种安全性虽不理想但可以满足应用需求。

2008 年意大利学者 Giovannetti 等提出了第一个 QPQ 协议（GLM 协议）[46]。该协议中，Bob 将数据库信息编码到酉操作上，收到用户 Alice 的查询量子态后，他将该操作作用到查询态上然后返回给 Alice，Alice 通过测量获取想要的数据库条目。这类将数据库信息编码到酉操作上的 QPQ 协议在理论上意义非凡，但实际上并不实用。一方面，将整个数据库（尤其是当数据库规模较大时）编码到酉操作上，该酉操作必然维数很大，在现有条件下难以实现。另一方面，这类协议不能容忍信道损失，即一旦存在信道损失的情形，将威胁到双方的隐私。此外，在实际应用中不完美的信号源，信道噪声等也影响着协议的成功概率。为了解决这些问题，后续人们对 QPQ 协议做了大量研究。

2011 年，瑞士日内瓦大学 Jacobi 等基于 SARG QKD [47]提出了一个 QPQ 协议（J 协议）[48]。它借助现有的 QKD 技术来实现，实现难度与数据库规模无关，且能够容忍信道损失，因此成为 QKD 之外实用潜力较为突出的一类密码协议。协议中用户可获得的数据条目不能灵活调整，要么过多不利于保护数据库安全性，要么过少导致失败概率增大。2015 年，基于环回差分相移 QKD 协议，刘斌等设计了一种 QPQ 协议，实现诚实用户获得的数据库条目数始终是 1，这保证了理想的数据库安全性，并且方案失败概率为 0，意味着在忽略噪声的情况下，协议总能成功执行 [49]。

此后，学者们发现了 QPQ 在实用中面临的一些新问题，并逐一解决。魏春艳等提出窄移位叠加的技术，使得不仅能够用于大数据库查询，而且在不完美光源下依然保持了理想的数据库安全性和零失败概率 [50]。在对抗信道噪声方面，Gao 等[51]和 Chan 等 [52]分别提出利用纠错码和校验矩阵对 QPQ 原始密钥进行后处理。在应用研究方面，2019 年，陈秀波等提出了一种适用于量子无线网络的 QPQ 方案，通过让用户节点和服务器节点之间预先共享纠缠态和引入多个协助第三方的方法实现任意用户可向任意服务器进行检索的目标 [53]。

综上，由于 QPQ 协议只需要使用与 BB84 协议相同的光源和探测器就可以实现，纠错和隐私放大理论较完善，因而具有很好的实用化潜力。但是由于 QPQ 中两方可以互相欺骗，要兼顾两方利益，因此与 QKD 相比其具有更大的理论难度。一个具体表现就是，目前 QPQ 能容忍的错误率较低（典型参数下可容忍 4% 的错误率 [54]）。

八、未来研究方向

众所周知，量子计算对现代密码学的安全性形成了严峻挑战。随着 QKD 协议的提出并被证明具有信息论安全性，量子密码逐渐成为可对抗量子计算攻击的下一代密码技术中的一个重要选项。

在经典密码中，已经存在成熟的算法和协议体系，比如用对称或公钥加密算法来保证消息的机密性、用消息认证码来保证消息的完整性来源可靠性、用数字签名来保证消息的不可否认性等，这些具备多种功能的成熟算法和协议构成了一个完整的木桶（见图 1），可以确保一个信息系统在复杂网络环境下的安全运行。

鉴于 QKD 的巨大安全性优势，学者们希望借鉴其思想，通过引入量子技术来全面提升各类密码协议的安全性，并最终建成一个“信息论安全”的协议体系，也只有如此才能全面提升信息系统在未来量子计算时代的安全性。然而从较大规模的实验进展来看，目前达到实用化程度的量子密码协议主要是 QKD，也就是我们通常所说的“量子通信”。总体来说，量子密码协议目前处于“QKD 遥遥领先、其他协议有待突破”的不平衡状态，其实也是一个“其他协议难以突破”的瓶颈状态。因此，要想实现全面提升信息系统安全性的目标，量子密码协议研究还有很长的路要走。

显然，量子密码协议领域未来还有诸多科学问题需要解决。比如在微观层面，人们需要找到对抗信道噪声影响的新理论，并寻找立足于量子密码特点的新型密码学任务；在宏观层面，人们需要解决量子公钥密码难题；而在应用层面，需要建立量子 – 经典相结合的密码新体系。下面分别阐述这几个关键问题并讨论解决这些问题的潜在技术途径。

（1）处理信道噪声的新理论。在量子密码协议中，窃听或欺骗行为通常会给量子态带来难以控制的干扰。针对这一特点，量子密码协议都有检测窃听的步骤。它通常通过将量子态的测量结果与其预期状态相比较，得到错误率，进而判断是否存在窃听或欺骗行为。众所周知，信道噪声本身也会带来一定的错误率，而攻击者可以在噪声的掩饰下获得

部分非法的秘密信息。因此，为了对抗信道噪声，量子密码协议都需要有一个经典后处理的过程，目的是纠错和压缩攻击者非法所得的信息量。这种后处理过程是严格证明量子密码协议安全性的一个关键，也是相关研究的难点所在。针对不同协议的安全性要求，如何给出能够妥善处理信道噪声的新理论，是量子密码协议走向实用过程中急需解决的关键问题。

（2）立足于量子密码特点的新型密码学任务。在量子密码研究过程中，人们往往以经典密码协议的功能为目标来设计量子协议。然而量子密码和经典密码的安全性基础有着本质区别，量子密码适合做的密码学任务可能与经典密码有很大不同。这可能正是我们照搬经典密码协议目标来设计量子密码协议时遇到瓶颈的原因。因此，针对量子理论特点，尝试改变经典密码协议的安全目标（需确保仍有应用价值），或者发掘新型的密码学任务，是一种有望取得突破的研究思路。近年来取得成功的QPQ协议就是这方面的一个典型例子。它将经典“多取一”不经意传输的安全性目标修改为“欺骗敏感”类型，既迎合了量子协议的特点，又符合实际应用需求，已经具备了很好的实用化潜力。

（3）量子公钥密码模型。从应用角度来说，量子密码协议研究中急需解决两个重要问题：数字签名和两方安全计算。前者在日常通信网络中应用广泛、不可或缺，后者是构建其他复杂密码协议的基本组件，两者都在密码协议体系中占有重要地位。在经典密码中，数字签名和两方安全计算大多是借助公钥密码算法来实现。而目前人们还没有找到有实用价值的量子公钥密码。实际上，量子密码对“信息论安全”的追求与公钥密码“基于数学复杂性假设”的属性相互矛盾，直接对照经典公钥密码的设计方法来设计量子公钥密码很可能是行不通的。量子公钥密码，很可能是一种不同于经典公钥密码、但能实现经典公钥密码功能的全新模型。因此，如何独辟蹊径、用量子力学性质来实现公钥密码的类似功能，成为解决上述两个问题的重中之重。

如上所述，量子密码中不一定能像经典密码那样，可以找到公钥密码并在此基础上得到数字签名和两方安全计算方案。因此，分别设计具有实用化潜力的量子数字签名协议、能跨过no-go定理的两方安全计算协议也是一种解决思路。

（4）量子–经典相结合的密码新体系。目前来看，量子密码中一些典型协议发展遇到瓶颈，难以满足全面提升信息系统安全性的应用需求。涉及到相关功能的信息系统，只能用经典密码来保护其安全性。也就是说，系统整体使用量子–经典相结合的密码体制，比如密钥分配用量子的，而数字签名（因为没有实用化的量子协议）用经典的。此时如果简单地将（当前可用的）量子密码协议与经典密码协议相结合使用，有可能会导致量子密码的使用失去价值（比如对于上述具备了QKD功能的信息系统，具有量子计算能力的攻击者仍然可以通过攻破经典数字签名来非法登录系统、获得密钥或秘密消息）。针对这一现状，围绕当前可用的量子密码协议（如QKD和QPQ），专门设计与之相适配的经典密码协议，确保量子密码协议的使用能够带来切实的、即便只是一定程度上的安全性优势，是一种可行的研究思路。这里有研究价值的问题包括：①利用当前可用的量子密码功能，能否给某些经典密码带来本质上的安全性提升？②如果可以，这种新的安全性如何定义？③公钥密码出现之前各项密码学功能是如何实现的？这显然对尚无公钥密码的量子密码体制有重要的参考价值。④能否通过充分发掘可信第三方的功能，来协助解决数字签名、两方安全计算等量子密码协议中的瓶颈问题？总之，如果在可预见的未来，量子密码仍旧不能“独自扛大梁”，那么退而求其次，研究它能给经典密码带来什么提升和帮助是非常有现实意义的课题。

九、对我国相关研究的建议

如上所述，要想达到全面提升信息系统安全性的实用化目标，量子密码协议中还有诸多问题需要解决。尽管如此，量子密码的独特安全性令人着迷。在理论上，它将对密码算法和协议的发展带来全新的思想、有价值的启发以及安全性上的实质性提升；在应用中，它至少可以实现一个具有有限功能的、在某些场景下有显著优势的新体制，比如功能较少的专用网络（“功能多”往往意味着需要使用非信息论安全的经典密码，而这些密码的使用会限制信息系统整体的安全性，使之不能达到量子密码所追求的“超高安全性”）。量子密码本质上属

于抗量子计算攻击的密码学研究领域。关于我国在该领域的后续研究，我们给出以下几点建议。

（一）量子密码与后量子密码研究应同步开展

基于目前量子计算还无法有效解决的数学难题（比如格、多变量、Hash、编码等问题）可以设计公钥密码，这种密码被称作后量子密码（或抗量子密码）。尽管后量子密码达不到信息论安全，但其抗量子计算攻击的能力已经获得了广泛认可，并且具有兼容性好、易实现等优点。因此，量子密码和后量子密码各具优势，两者都是抵抗量子计算攻击的重要选项。鉴于目前人们对量子计算机的研制逐渐提速，应做好两方面准备并确保研究的同步开展。

需要强调的是，尽管量子密码目前的实用性还不完善，但其对密码学理论发展的重要意义不容忽视。量子密码协议体系的研究是一个漫长的过程，不能因为技术成本高或者过分追求实用性的短视行为而荒废。一方面，随着技术的不断发展，量子密码设备的成本必然会下降，而且技术的发展也可能会催生理论的突破（比如量子信道噪声降低之后，协议后处理的难度也会随之大幅降低）。另一方面，即便后量子密码（因为其实用性）先走向应用，量子密码在未来仍可能有用武之地，毕竟后者对抗量子计算攻击的理论基础更加坚固。

（二）加强“量子科技”和“密码学”两个学科的交叉研究和相关的人才培养

在量子密码中，研究量子–经典相结合的密码新体系势在必行；在后量子密码中，研究可用于密码分析的量子计算算法也对评估其“量子安全性”至关重要。这两个重要研究方向均需要对上述两个学科都熟悉的专业人才。然而由于两个学科相互独立、专业性强，其交叉研究难度大、门槛高，符合上述要求的研究人员还很匮乏，使得我们的相关研究与国外相比还有不小的差距。因此，可以在政策上对相应的交叉研究和人才培养给予扶持。

（三）优化对相关基础研究的考核评价机制

抗量子计算攻击的密码学领域目前还处于难度很大的理论攻坚阶段，其突破需要相关学者具有敢啃“硬骨头”、甘坐“冷板凳”的精神。当前考核评价机制中的一些急功近利之风（如对短期成果、大项目等的追求）不利于该领域的研究。因此，在“反五唯”的基础上继续优化对相关研究的考核评价机制，营造适合“围绕一个问题长期潜心研究”的科研环境，对该领域的研究有很好的促进作用。

十、结语

本文调研分析了量子密钥分配、量子安全直接通信、量子秘密共享、量子身份认证、量子数字签名、量子两方安全计算等量子密码协议的研究现状，指出当前量子密码协议尚处于“QKD 遥遥领先、其他协议有待突破”的不平衡状态，距离建立起成熟、实用的协议体系还有大量工作要做。在此基础上，从微观、宏观和应用角度给出了未来量子密码领域需要解决的关键问题和相关研究建议。

量子密码是密码学的新方向，具备极高的安全性潜力，因此具有重要的研究价值。从应用角度来说，量子密码并不能“独挑大梁”，将它与经典密码融合使用几乎是必然的选择。如何给信息系统的整体安全性带来提升，在使用时需要重点考量。由于目前实用化的量子密码协议还很少，在应用中可以优先考虑功能较少的专用网络。以后随着实用量子密码协议和与之相适配的经典密码技术日趋完善，量子密码将可能有广阔的应用空间。

致谢

感谢李永梅、郭明超、蔡晓秋、李静、魏春艳、吴圣尧、魏东梅等课题组成员对本文撰写的大力协助。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: May 11, 2022; **Revised date:** June 20, 2022

Corresponding author: Gao Fei is a professor from the School of Cyberspace Security, Beijing University of Posts and Telecommunications. His major research fields include quantum cryptography and quantum algorithms. E-mail: gaof@bupt.edu.cn

Funding project: Chinese Academy of Engineering project “Research on the Development Strategy for the Engineering Application of Quantum Information Technology” (2021-HYZD-01); National Natural Science Foundation of China project (61972048, 61976024)

参考文献

[1] Bennett C H, Brassard G. WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing [C]. New York: Proceedings of the IEEE International Conference on Computers Sys-

tems and Signal Processing, 1984.

[2] Christandl M, Ferrara R, Horodecki K. Upper bounds on device-independent quantum key distribution [J]. Physical Review Letters, 2021, 126(16): 1–6.

[3] Schwonnek R, Goh K T, Primaatmaja I W, et al. Device-independent quantum key distribution with random key basis [J]. Nature Communications, 2021, 12(1): 2880.

[4] Woodward R I, Lo Y S, Pittaluga M, et al. Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers [J]. npj Quantum Information, 2021, 7: 58.

[5] Zeng P, Zhou H Y, Wu W J, et al. Quantum key distribution surpassing the repeaterless rate-transmittance bound without global phase locking [EB/OL]. (2022-01-22)[2022-05-10]. https: //arxiv.org/abs/2201.04300.

[6] Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4600 kilometres [J]. Nature, 2021, 589: 214–219.

[7] Feng Z, Li S B, Xu Z Y. Experimental underwater quantum key distribution [J]. Optics Express, 2021, 29(6): 8725–8736.

[8] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830 km fiber [J]. Nature Photonics, 2022, 16: 154–161.

[9] Liu X, Hu J, Li Z F, et al. Heralded entanglement distribution between two absorptive quantum memories [J]. Nature, 2021, 594: 41–45.

[10] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 1–10.

[11] Deng F G, Long G L. Secure direct communication with a quantum one-time pad [J]. Physical Review A, 2004, 69(5): 1–10.

[12] Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication [J]. Frontiers of Physics in China, 2007, 2(3): 251–272.

[13] Hu J Y, Yu B, Jing M Y, et al. Experimental quantum secure direct communication with single photons [J]. Light-Science & Applications, 2016, 5: 1–10.

[14] Qi Z T, Li Y H, Huang Y W, et al. A 15-user quantum secure direct communication network [J]. Light-Science & Applications, 2021, 10(1): 183.

[15] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829.

[16] Chou Y H, Zeng G J, Chen X Y, et al. Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information [J]. Scientific Reports, 2021, 11: 1–10.

[17] Bell B, Markham D, Herrera-Martí D, et al. Experimental demonstration of graph-state quantum secret sharing [J]. Nature Communications, 2014, 5(1): 1–12.

[18] Zhou Y, Yu J, Yan Z, et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field [J]. Physical Review Letters, 2018, 121(15): 1–6.

[19] Liao Q, Liu H, Zhu L, et al. Quantum secret sharing using discretely modulated coherent states [J]. Physical Review A, 2021, 103(3): 1–10.

[20] Dušek M, Haderka O, Hendrych M, et al. Quantum identification system [J]. Physical Review A, 1999, 60(1): 149.

[21] Gottesman D, Chuang I L. Quantum digital signatures [EB/OL]. (2001-05-08)[2022-05-01]. https: //arxiv.org/abs/quant-ph/0105032.

[22] Barnum H, Crépeau C, Gottesman D, et al. Authentication of quantum messages [C]. Vancouver: The 43th Annual IEEE Symposium on Foundations of Computer Science, 2002.

[23] Puthoor I V, Amiri R, Wallden P, et al. Measurement-device-independent quantum digital signatures [J]. Physical Review A, 2016, 94(2): 1–10.

[24] Thornton M, Scott H, Croal C, et al. Continuous-variable quantum digital signatures over insecure channels [J]. Physical Review A, 2019, 99(3): 1–10.

[25] Zhao W, Shi R, Ruan X. High-efficiency continuous-variable quantum digital signature protocol for signing multi-bit messages [J]. Laser Physics Letters, 2021, 18(3): 1–6.

[26] Qiu L, Cai F, Xu G. Quantum digital signature for the access control of sensitive data in the big data era [J]. Future Generation Computer Systems-The International Journal of eScience, 2018, 86: 372–379.

[27] Singh S, Rajput N K, Rathi V K, et al. Securing blockchain transactions using quantum teleportation and quantum digital signature [J]. Neural Processing Letters, 2020, 52: 1–10.

[28] Lo H K, Chau H F. Is Quantum bit commitment really possible? [J]. Physical Review Letters, 1997, 78(17): 3410–3413.

[29] Mayers D. Unconditionally secure quantum bit commitment is impossible [J]. Physical Review Letters, 1997, 78(17): 3414–3417.

[30] Ng N, Joshi S, Ming C, et al. Experimental implementation of bit commitment in the noisy-storage model [J]. Nature Communications, 2012, 3: 1326.

[31] Lunghi T, Kaniewski J, Bussières F, et al. Experimental bit commitment based on quantum communication and special relativity [J]. Physical Review Letters, 2013, 111: 1–10

[32] Liu Y, Cao Y, Curty M, et al. Experimental unconditionally secure bit commitment [J]. Physical Review Letters, 2014, 112: 1–10.

[33] Mochon C. Quantum weak coin flipping with arbitrarily small bias [EB/OL]. (2007-11-26)[2022-05-01]. https: //arxiv.org/abs/07711.4114.

[34] Berlín G, Brassard G, Bussières F, et al. Fair loss-tolerant quantum coin flipping [J]. Physical Review A, 2009, 80(6): 1–10.

[35] Chailloux A. Improved loss-tolerant quantum coin flipping [EB/OL]. (2022-01-22)[2022-05-10]. https: //arxiv.org/abs/1009.0044.

[36] Chailloux A, Kerenidis I. Optimal quantum strong coin flipping [C]. Atlanta: 2009 50th Annual IEEE Symposium on Foundations of Computer Science, 2010.

[37] Bozzio M, Chabaud U, Kerenidis I, et al. Quantum weak coin flipping with a single photon [J]. Physical Review A, 2020, 102(2): 1–10.

[38] Pappa A, Jouguet P, Lawson T, et al. Experimental plug and play quantum coin flipping [J]. Nature Communications, 2014, 5: 3717.

[39] Crépeau C, Kilian J. Achieving oblivious transfer using weakened security assumptions [C]. White Plains: 29th Annual Symposium on Foundations of Computer Science, 1988.

[40] 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): 1–10.

[41] Damgard I B, Fehr S, Salvail L, et al. Cryptography in the bounded quantum-storage model [C]. Pittsburgh: 46th Annual IEEE Symposium on Foundations of Computer Science, 2005.

[42] Pitalúa-García D. Spacetime-constrained oblivious transfer [J]. Physical Review A, 2016, 93(6): 1–10.

[43] Chailloux A, Gutoski G, Sikora J. Optimal bounds for semi-honest quantum oblivious transfer [J]. Chicago Journal of Theoretical Computer Science, 2016: 1–16.

[44] Amiri R, Stárek R, Reichmuth D, et al. Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation [J]. PRX Quantum, 2021, 2(1): 1–10.

[45] Gao F, Qin S, Huang W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol [J]. Science China Physics, Mechanics & Astronomy, 2019, 62(7): 1–10.

[46] Giovannetti V, Lloyd S, Maccone L. Quantum private queries [J]. Physical Review Letters, 2008, 100(23): 1–10.

[47] Scarani V, Acin A, Ribordy G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations [J]. Physical Review Letters, 2004, 92(5): 1–10.

[48] Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol [J]. Physical Review A, 2011, 83(2): 1–10.

[49] Liu B, Gao F, Huang W, et al. QKD-based quantum private query without a failure probability [J]. Science China-Physics Mechanics & Astronomy, 2015, 58(10): 1–10.

[50] Wei C, Cai X, Liu B, et al. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure [J]. IEEE Transactions on Computers, 2018, 67(1): 2–8.

[51] Gao F, Liu B, Huang W, et al. Postprocessing of the oblivious key in quantum private query [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2015, 21(3): 98–108.

[52] Chan P, Lucio-Martinez I, Mo X, et al. Performing private database queries in a real-world environment using a quantum protocol [J]. Scientific Reports, 2014, 4: 5233.

[53] Li N, Li J, Chen X B, et al. Quantum wireless network private query with multiple third parties [J]. IEEE Access, 2019, 7: 33964–33969.

[54] Wei C, Cai X, Wang T, et al. Error tolerance bound in qkd-based quantum private query [J]. IEEE Journal on Selected Areas in Communications, 2020, 38(3): 517–527.