量子电子商务——量子数字签名实用化之路

尹华磊[1,2,†]　曹啸宇[2]　李炳宏[2]　陈增兵[2,††]
（1　中国人民大学物理学系　北京　100872）
（2　南京大学物理学院　南京　210093）

2024－01－26收到
†　email：hlyin@ruc.edu.cn
††　email：zbchen@nju.edu.cn
DOI：10.7693/wl20240206

近期，我们提出了首个量子电子商务方案，并在国际上首次实现了五用户的量子电子商务应用场景演示[1]。这一进展引起了国内外极大的兴趣和关注。本文试图通俗、准确地简述该研究方向的进展，客观、科学地分析该方向未来的前景和挑战，以供读者参考。

1　量子通信背景介绍

在现代信息技术所衍生的各种活动中，大量的信息数据被采集、加工、传输和存储，与此同时也面临被窃听、篡改、伪装和否认的安全威胁。现代密码学发展了完备的体系来保障信息安全的四个基本要素：机密性、完整性、真实性和不可抵赖性，分别对应这四种攻击。然而，目前广泛应用的密码学技术的安全性大多都基于计算复杂度的假设，未来会受到如量子计算机等先进算力的严重威胁。比如，著名的RSA公钥算法在经典计算机上需要上万年才能破解[2]，但攻击者如果拥有了量子计算机，利用Shor算法便可以在1秒钟时间内快速完成破解[3]。基于量子力学基本原理的量子信息科学被认为是解决这一问题的理想途径。量子原理决定了没有任何方法去复制一个未知量子态，即产生它的完美副本，这个结果被称为“不可克隆定理”，是量子信息相对于经典信息的基本优势之一。该定理与密码学密切相关，因为经典密码学的暴力攻击往往假设了截获、复制和重发，而复制这一关键步骤不能应用于携带未知信息的量子信道。以此为基础，美国IBM公司的C. H. Bennett与加拿大蒙特利尔大学的G. Brassard于1984年提出第一个量子密钥分发协议，即分隔遥远的两个用户通过制备、分发、测量量子态从而实现共享随机的隐私密钥[4]。结合量子密钥分发和一次一密加密方式，在特定的安全性假设下，可以实现无条件安全的保密通信，为信息处理提供机密性保护。以量子保密通信为主要研究内容的量子通信在近二十年得到了前所未有的发展。例如，我国科学家基于墨子号量子试验卫星和京沪量子保密通信干线率先实现了空地一体化的广域量子通信网络[5]。然而，量子通信的实际服务能力也不断地受到美国国家安全局的质疑，其主要关注点在于目前主要的研究集中于量子密钥分发，即只能为信息处理提供机密性来阻止窃听攻击，而不能提供一个完整的解决方案[6]。事实上，提供信息安全其他三个要素的技术在现实中有着更为广泛的应用，如提供真实性、完整性、不可抵赖性的数字签名技术等。如何为这些技术提供实用化的量子解决方案是量子通信研究亟需解决的问题。

2　量子数字签名发展历史

量子数字签名是基于量子力学基本原理为信息处理提供数据的完整性、真实性和不可抵赖性的无条件安全保护的技术。量子数字签名的概念早在2001年便被美国麻省理工学院和加州大学伯克利分校的研究人员提出，其思想起源于经典密码学中基于单向函数的数字签名，并且可以通过量子指纹态构造“量子单向函数”[7]。这个方案只是一个理论上的模型，在实验和可操作性方面存在着巨大的挑战，但是它奠定了后续量子数字签名研究的理论基础。此后，欧美国家众多研究单位都在相关领域进行了深入研究。2012年，Clarke等人给出了基于相位编码的量子签名方案，借助相干态和线性光学避开了非破坏态比较[8]；2014年，Dunjko等人和Collins等人分别给出了去

除量子存储的签名方案[9, 10]；2016年，尹华磊等人和Amiri等人分别独立地提出新的签名方案，移除了对量子安全信道的要求，至此实现了量子数字签名完备的安全性要求和实验可行性，为后续的量子数字签名研究提供了框架[11, 12]。其原理可以概括为，通过签名方分别于接收方和验证方之间制备、分发和测量未知量子态，从而实现签名方—接收方和签名方—验证方之间共享关联的量子态而对应的量子密钥。关联性需要满足“对称性”和“非对称性”两个效果，即在签名方的视角中，接收方和验证方的密钥是对称的，以此来防止否认；在接收方的视角中，他自己的密钥和验证方的密钥是非对称的，即他不能获得接收方的全部密钥，以此来防止篡改和伪造。其中对称性由共享量子态产生，非对称性由基矢选择或交换部分密钥产生。之后，量子数字签名及其应用的研究迎来了蓬勃发展。例如，德国和英国研究人员于2021年合作展示了一个20 km的量子数字签名[13]；英国、西班牙和克罗地亚等国研究人员于2022年演示了一个基于量子纠缠光源的量子数字签名网络[14]。

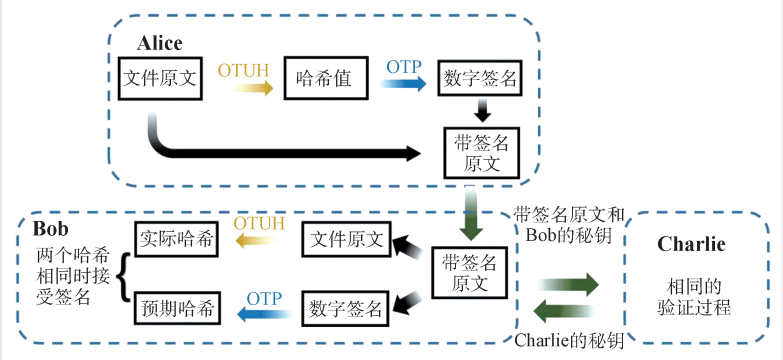

图1 一次性全域哈希量子数字签名框架。其中，Alice是签名方，Bob是接收方，Charlie是验证方，OTUH表示一次性全域哈希，OTP表示一次性密码

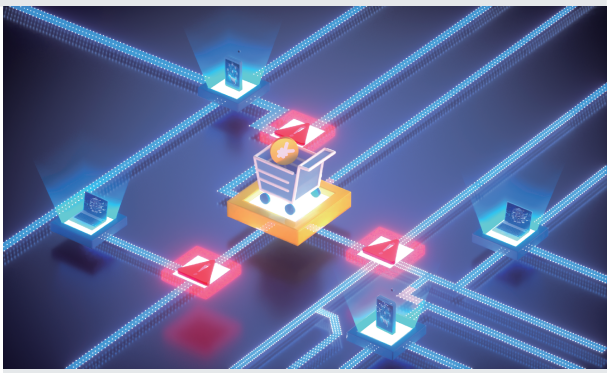

图2 五用户量子电子商务网络，包括一个商家(中间节点)，两个购买者(上下两个节点)和两个第三方平台(左右两个节点)，商家可以和购买者建立合同实现线上交易

然而，以上量子数字签名的工作都延续了2001年提出的框架，即通过构造“量子单向函数”对单比特的文件进行签名，我们称其为单比特方案。单比特方案需要消耗大量的量子态(对应的量子密钥一般为几万比特)对一个比特的文件进行签名，因此效率极低，远远无法满足实用需求。针对这个问题，我们在2021年提出了一种新的量子数字签名框架——一次性全域哈希量子数字签名，如图1所示[15, 16]。这个框架跳出了单比特方案的范式，通过巧妙地构造签名发送方、接收方和验证方之间的非对称量子密钥关系和信息交换顺序，我们将“一次一哈希”的单向特性、秘密共享的非对称特性和“一次一密”的隐私特性有机地结合起来，从而同时提供了“对称性”和“非对称性”。此方案直接利用全域哈希函数作用在待签名的多比特文件上，将其映射成数百比特的摘要。量子态对应的量子密钥被用于哈希函数的选择和摘要的加密。因此只需要数百个量子密钥就可以一次性对整个文件进行签名，极大地提升了签名效率。相比于单比特方案，如果假设签名的文件大小为兆比特量级，此方案在签名效率上会有八至九个数量级的提升。

3 量子数字签名的应用——量子电子商务

以一次性哈希量子数字签名为底层技术，我们团队提出了量子电子商务方案，并在一个五用户的网络上实现了实验演示，如图2所示。我们演示了网上购物的场景，涉及商家、客户和第三方平台。该方案通过将含噪声量子态的隐私特性、一次性全域哈希函数的单向性和秘密共享的非对称特性结合起来，防止了商家对合同的反悔否认、

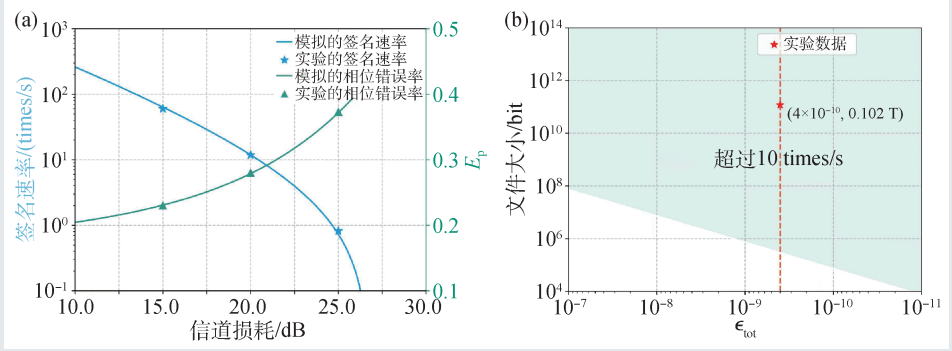

图3 五用户量子电子商务实验结果 (a)不同信道损耗下的签名速率和相位错误率，可以看到实验结果符合理论预期；(b)安全性参数和文件大小的关系

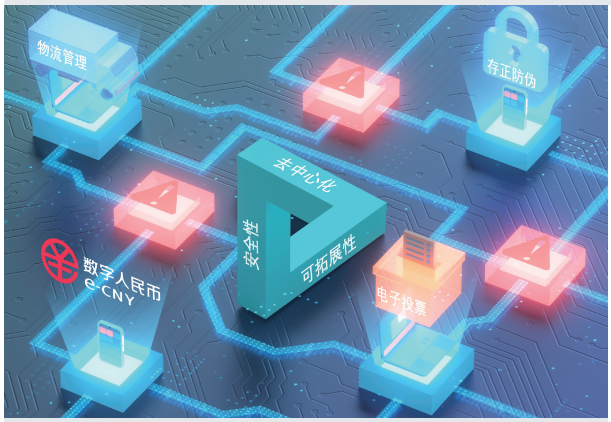

图4 容错量子区块链共识网络及其应用示意图

客户对合同的伪造或篡改以及第三方对交易金额的篡改等攻击。该量子电子商务协议可以容忍量子密钥的部分隐私泄露，因此在后处理阶段不需要进行复杂的隐私提纯操作，在大规模网络和大数据传输的情景下可以节省可观的计算资源、网络带宽和数据处理时间。该方案成功在25 dB (约150 km光纤衰减)的传输损耗下对大小为0.428 Mb的交易文件实现每秒0.82次的处理速率，如图3(a)所示。相较之前量子数字支付方案[17]，处理速度与传输距离均有了极大提升。此外，该方案在处理大文件时具有出色的性能，随着签名长度的增加，在相同的失败概率下，签名文件的大小呈指数级增长，在20 dB的传输衰减下对千兆大小的文件处理速度超过10次每秒，如图3(b)所示，为实现城域范围内的实时交易带来希望。同时，研究团队还证明了该方案对于设备不完美的鲁棒性，实验中通过量化量子态的制备缺陷、量子态的传输偏差，对包括光强波动、码型效应、偏振偏差、相位差异和特洛伊木马攻击等所造成的信息泄露量精确估计，从而给出了协议失败的最大概率。此外，该研究工作中建立的网络结构不需要事先指定可信第三方进行支付验证，因而不需要固定中心节点。总的来说，本次演示在城域距离下对兆比特交易文件实现秒量级的处理速率，展现出量子电子商务极大的应用潜力。

4 未来展望

这次演示的量子电子商务方案，和现实中的应用场景相比，在用户数量、传输距离和功能多样性方面仍然有一定差距。为了进一步推动该技术的实用化，后续还需要在如下方面发力。

(1) 多并发用户

在实际应用中需要成千上万的用户在网络中进行并发的电子商务活动，而用户的增加会带来对量子密钥需求的增加。

(2) 更远距离

目前，国内外都已经部署了大规模的量子保密通信骨干网络，其中以北京到上海的“京沪量子保密通信干线”为代表。借助这些已经部署的网络可以实现更远距离的量子电子商务演示。

(3) 更高速率

在本次演示中，交易速率已经接近实用要求。未来，通过利用当前先进的量子密钥分发所使用的量子通信技术，可以进一步提升量子电子商务协议中量子态调制速率、制备精度和传输稳定度，使得在城域范围内保障的交易文件处理速率提升多个数量级。

(4) 更多功能。

除了电子商务以外，现代互联网还有很多其

他应用，未来的量子网络也应该是一个集成多功能的交互系统。构造和发展解决不同问题的量子通信技术也是未来极具潜力的一个研究方向。其中，本团队近期基于一次性全域哈希量子数字签名提出了一种为区块链共识提供无条件安全的量子拜占庭共识协议[18]，如图4所示。该协议打破了容忍恶意节点数的经典极限，体现了“量子优势”。相信未来会有更多的技术实现“无条件安全”。

总体来看，实用化的量子电子商务仍然受制于量子密码分发技术的发展。因此，一方面我们要继续发展量子密码技术；另一方面也可以考虑在实际应用层面放弃量子密钥的理论安全性，而只追求抗量子算力攻击下的安全性，这样有可能实现量子电子商务的快速、大规模应用。

参考文献

[1] Cao X Y, Li B H, Wang Y *et al*. Sci. Adv., 2024, 10: eadk3258
[2] Rivest R L, Shamir A, Adleman L. Commun. ACM, 1978, 21: 120
[3] Shor P W. SIAM Journal on Computing, 1999, 41: 303
[4] Bennett C H, Brassard G. Theor. Comput. Sci., 2014, 560: 7
[5] Chen Y A, Zhang Q, Chen T Y *et al*. Nature, 2021, 589: 214
[6] Gottesman D, Chuang I. 2021, arXiv preprint quant-ph/0105032
[7] Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
[8] Clarke P J, Collins R J, Dunjko V *et al*. Nat. Commun., 2012, 3: 1174
[9] Dunjko V, Wallden P, Andersson E. Phys. Rev. Lett., 2014, 112: 040502
[10] Collins R J, Donaldson R J, Dunjko V *et al*. Phys. Rev. Lett., 2014, 113: 040502
[11] Yin H L, Fu Y, Chen Z B. Phys. Rev. A, 2016, 93: 032316
[12] Amiri R, Wallden P, Kent A *et al*. Phys. Rev. A, 2016, 93: 032325
[13] Richter S, Thornton M, Khan I *et al*. Phys. Rev. X, 2021, 11: 011038
[14] Pelet Y, Puthoor I V, Venkatachalam N *et al*. New J. Phys., 2022, 24: 093038
[15] Yin H L, Fu Y, Li C L *et al*. Natl. Sci. Rev., 2023, 10: nwac228
[16] Li B H, Xie Y M, Cao X Y *et al*. Phys. Rev. Appl., 2023, 20: 044011
[17] Schiansky P, Kalb J, Sztatecsny E *et al*. Nat. Commun., 2023, 14: 3849
[18] Weng C X, Gao R Q, Bao Y *et al*. Research., 2023, 6: 0272

读者和编者