量子密码的发展现状及其安全挑战

李凯轩 1901210424
张津婵 1901210582
张文默 1901210590

1.引言

量子技术与信息技术深度融合，促进了以量子通信、量子计算和量子测量为代表的第二次量子革命蓬勃兴起。量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式，提供超强的计算能力，不仅能够快速破解经典密码，还在生物制药、优化问题、数据检索等方面拥有广泛的应用前景。随着产业界持续加大力度投入，量子计算机的发展已呈加速之势，这将对基于计算复杂度的经典密码学带来严峻的挑战。量子通信是利用量子态作为信息载体进行传递的新型通信技术，在保密通信、量子云计算、分布式量子测量、未来量子互联网的构建等方面发挥重要作用。量子密钥分发是量子通信的典型应用，有望为信息安全领域带来可实现的长期安全性保障。

2.从经典密码到量子密码

密码学的终极目标是开发出“绝对安全”的密码方案，即假使敌手拥有无限强的计算能力，仍然无法破译这种密码，也就是所谓的无条件安全性。1917 年，Gilbert Vernam 发明一次性密码本（OTP）时就已实现了该目标。为一种加密算法，OTP 类似于其他现代密码系统，同样使用密钥来进行加密和解密，加密算法本身是公开的，其安全性由密钥的安全性来保证。OTP 算法的实现需要满足 3 个条件，分别是“密钥必须完全随机”“密钥不能重复使用”“密钥需与明文等长”。其无条件安全性并不难以理解，因为与明文等长的同一密钥加密的密文只出现一次，这使得在无法获知明文的情况下，任何算法即使穷举也无法破译出该密钥；另外，密钥使用一次即丢弃，因此即便破译者得到了部分密钥也无法用于破译其他密文。传统 OTP 加密美中不足之处是需要印刷大量的密码本，且实际分发操作难度很大。

众所周知的密钥分发难题，它涉及到经典物理中两个不可实现的任务：一是如何生成真正完全随机的密钥；二是如何在不安全的公共信道上无条件安全地分发密钥。随着量子信息技术的发展，人们发现基于量子物理学可以为这些问题提供答案：真正的随机数可以通过基本的量子物理过程生成，通过量子通信技术则可实现在公共信道上也无法窃听的密钥分发。在现代密码系统中，人们采用更简单易行的、基于数学算法的方法来解决密钥分发的问题。这些方法将信息理论安全要求放松为基于计算复杂度的安全性，即假设敌手拥有的计算能力有限的条件下无法破解即可。为了减少随机密钥量的消耗以简化密钥分发过程，大多数现代加密系统中使用短密钥来加密很长的消息，如 DES、AES 等算法，对称密码虽然大大减少了随机密钥的消耗，但没有解决密钥分发问题。

为了充分解决密钥分发问题，1977 年 Ron Rivest、Adi Shamir 和 LeonardAdleman 发明了著名的 RSA 方案（以发明者首字母命名）。RSA 是一种非对称的密钥算法，即加密和解密采用两个密钥，使用其中一个密钥加密的信息，仅能通过唯一对应的另一个密钥进行解密。这两个密钥由特殊的数学问题产生，

已知其中一个密钥很难计算出另一个密钥，例如 RSA 算法建立在两个大质数的积易于得到而难于分解的问题之上。这样消息接收者 Bob 可将其中一个密钥作为“私钥”保存起来，将另一个密钥作为“公钥”通过公共信道广播给消息发送者 Alice。Alice 即可用 Bob 的公钥对消息加密发送，然后 Bob 通过其私钥解密。公钥密码算法克服了密钥分发问题，但由于其运算量大，加密效率较低，通常用于加密传递（或称分发）对称密码的密钥。这种“利用公钥算法分发对称密钥，然后基于对称密钥进行加解密”的混合方案在当今的密码系统中得到广泛应用。公钥密码学的安全性依赖于一定的数学假设，例如 RSA 的安全性基于当时很难找到对大整数的素数因子进行分解的有效方法。然而，无法排除未来有人能找到这样的方法。1994 年，Peter Shor 即证明了通过量子计算机可高效求解质因子分解问题和离散对数问题。因此，只要第一台大型量子计算机开机，当前大多数密码系统就可能在一夜之间崩溃。

以应对这种攻击的解决方案，即量子密钥分发（Quantum Key Distribution，QKD）。基于量子物理的基本原理，QKD 提供了一种理论上无条件安全的密钥分发方式，即使通过不安全的信道分发密钥也无法被窃听。QKD 生成的安全密钥可以进一步应用于 OTP 方案或其他加密算法中，以提高信息安全性。国内外密码学家已对基于格、编码、多元多项式等新问题的密码方案开展了大量研究，期望设计出可对抗量子计算攻击的新型公钥算法，这些研究称为后量子密码学（Post-Quantum Cryptography，PQC）。

3．量子安全问题及其重要性

3.1 量子计算机带来的密码安全威胁

量子计算机能够以特定的计算方式有效解决一些经典计算机无法解决的数学问题。这种用于量子计算机的运算操作方法，就是所谓的“量子算法”。目前，最

著名的量子算法是 Shor 算法和 Grover 算法，已经能够威胁到当前广泛应用的密码体系。由于现有商用密码系统均是基于算法复杂度与当前计算能力的不匹配来保证其安全性，而 Shor 算法可以将对于经典计算机难以解决的大整数分解问题和离散对数问题，转换为可在多项式时间求解的问题。这使得量子计算机可利用公钥高效地计算得到私钥，从而对现有的大部分公钥算法构成实质性威胁。

表 2　量子计算机对经典密码的影响

密码学算法	类型	目　的	受到量子计算机的影响
AES	对称密钥	加密	需增加密钥长度
SHA-2, SHA-3	-	哈希散列函数	需增加输出长度
RSA	公钥	数字签名，密钥分发	不再安全
ECDSA, ECDH(Elliptic Curve Cryptography)	公钥	数字签名，密钥分发	不再安全
DSA (Finite Field Cryptography)	公钥	数字签名，密钥分发	不再安全

3.2 量子安全问题的影响范围

目前，已知对于量子计算机攻击处于高危状态的安全协议或密码系统包括：
（1）建立在大整数因子分解和离散对数问题计算复杂度之上的公钥密码算法，包括 RSA、DSA、Diffie-Hellman、ECDH、ECDSA 及其他变种。需要指出的是，目前几乎所有重要的安全产品和协议在公钥密码学部分都在使用这几类算法。
（2）基于上述公钥密码算法的任何安全协议。
（3）基于上述安全协议的任何产品或安全系统。

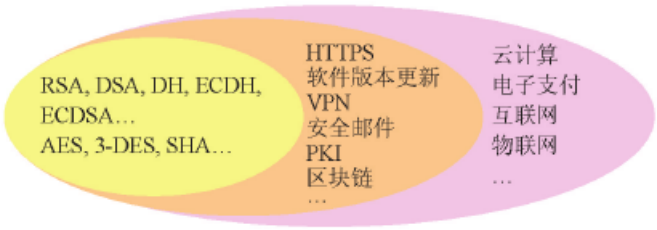

图 1　量子安全问题的影响范围

目前，可用于破解密码的实用化量子计算机仍未出现，且距离该目标仍有相当长的距离。那么在这之前，是否可以忽视量子安全问题所带来的风险呢？

4. 量子安全问题的应对措施

量子计算带来的潜在安全威胁已经引起了全球性的广泛重视。如何应对“量子安全”问题，设计能够抵御量子计算攻击的量子安全密码，已成为下一代信息通信系统必须考虑的问题。目前，业界考虑的应对措施主要包括基于现有密码的加强、研发新型的后量子公钥密码和基于量子物理的量子密钥分发技术。

4.1 现有密码的加强

由于目前可用于破解对称密钥算法的 Grover 量子算法，在搜索密钥空间时相比经典搜索算法仅能提供平方加速能力。这意味着一旦量子计算机强大到可以破解 N 位密钥长度的对称密码时，只需要将密钥的长度扩大到原来的两倍，量子计算机的破解难度就会上升至与经典计算机类似水平。例如，AES-128 对于当前的经典计算机来说难以破解，而 AES-256 对于量子计算机来说同样也很难破解。在美国国家安全局（NSA）2016 年发布的“关于量子计算攻击的答疑以及新的政府密码使用指南”中，明确指出未来量子计算机的实现将威胁当前所有广泛使用的密码算法，并重新定义了其国家商用安全算法集合。在对称密码方面，弃用了原有的 AES-128 和 SHA-256 算法，使用更长密钥的 AES- 256 和更长输出的 SHA- 384 算法，以应对将来可能出现的量子计算攻击。在公钥密码方面，由于目前还没有很好的量子安全解决方案，其仅是增加了原有 RSA 和 ECC 算法的密钥长度，并提请美国国家技术标准研究所（NIST）尽快建立后量子时代的公钥算法密码标准（PQC）。

4.2 后量子公钥密码学（PQC）

Shor 算法能够破解公钥密码主要是针对两个特定的计算问题——即整数因子分解和离散对数问题，找到了远超越经典计算机的量子计算方案。事实上对于某些数学问题，Shor 量子算法相对于传统算法并没有明显的优势。目前，认为可抵抗量子算法攻击的数学问题主要来源于格理论、编码理论、多元多项式理论等数学领域的研究。但是，以这些新方法为基础构建量子安全的公钥密码也还面临一些新的挑战，例如与传统公钥算法相比，它们往往需要更长的密钥和数字签名。

当前的互联网及很多其他系统所使用的安全协议及产品，对于公钥密码学的依赖程度很高。采用基于新的数学问题的公钥算法来应对量子安全问题，无疑是一种对现行密码体制影响较小、易于现有网络安全基础实施迁移的解决方案。目前，国际上 PQC 技术仍处于研究及标准化初期。美国 NIST 于 2015 年起针对后量子时代的密码技术开展了大量预研工作，并于 2016 年年底正式启动 PQC 项目，目标制定可抵抗已知量子算法攻击的新型公钥算法标准，其工作计划如下：

（1）2016 年 12 月：面向公众征集 PQC 提案（量子安全的公钥加密、密钥协商、数字签名方案）。

（2）2017 年 11 月 30 日：PQC 提案征集截止。

（3）历时 3~5 年的方案评估期。

（4）评估完成的 2 年后发布标准草案（即 2023—2025 年）。

NIST 首轮征集到来自全球密码学家提出的 69 种算法，正在开展紧锣密鼓的安全性评估工作。但可以看到，用于破解密码的量子算法也在不断演进，如何保证可抵御现有 Shor 算法的 PQC 不被随时可能出现的新型量子算法攻破，亦成为密码学界面临的难题。

4.3 量子密钥分发（QKD）

量子密码学的研究源于 Bennett 和 Brassard 的开创性工作。不同于经典密码学，量子密码学的安全性保障并不来自于数学算法的计算复杂度，而是建立在量子物理学的基本定律之上。这些物理定律可以认为是永久有效的，使得 QKD 能够提供独特的长期安全性保障，这是量子密码学的重要特征和优势。所谓的长期安全性理念，来自信息论的鼻祖香农（C. Shannon）1949 年提出的信息理论安全模型，其证明在一次性密码本（OTP）的加密下，即使敌手的算力无限强，也无法从密文中窃取任何信息，这使得窃听者的存在毫无意义。通过 OTP 加密与信息理论安全密钥交换的组合，即构成了可实现长期安全性的密码方案，而这正是量子密钥分发（QKD）发挥其独特优势的地方。无论从理论还是实践来看，QKD 都是迄今为止实现长期安全性密钥交换的最佳选择。从实践上来看，基于 QKD 的保密通信技术已经在美国、奥地利、中国、日本、瑞士、英国等国家得到了广泛的试验部署和应用验证。基于 OTP+QKD 的长期安全性保密通信方案距离广泛应用仍然还有很长的路要走。首先，OTP 加密要求密钥与明文数据等长且只能使用一次，这要求 QKD 产生的密钥速率必须与经典通信的信息速率相当，显然目前 QKD 的成码率无法满足除语音之外的大多数业务进行 OTP 加密的需求。但是可以看到，QKD 技术仍然在快速发展，未来点对点 QKD 可以达到更高的速率、更远的传输距离；另外，基于量子纠缠实现量子态存储和转发的量子中继器也正在加速研制，已经不存在理论上的瓶颈。

在 QKD 的性能瓶颈真正解决之前，人们还可以采用 QKD 与对称密钥算法混

合使用的过渡方案，实际上这种混合方案已经在 QKD 试验及商用系统中广泛使用。通过 QKD 代替公钥算法来保证对称密钥的安全分发，然后再通过对称密钥算法来保护大量信息传输的机密性，即可同时兼顾传输性能和安全需求。这种混合解决方案也是当前对抗量子计算攻击的可选方案之一。

5．量子密码的应用

5.1 后量子密码技术在区块链中的应用

区块链的安全性基于密码算法，如 Hash 函数、椭圆曲线 密码算法，而在量子计算机出现后，由于量子计算机可以高效 求解离散对数问题。所以基于离散对数问题困难性的数字签名算法在量子计算机出现后将不再安全。

（1）抗量子数字签名方案

在 Random Oracle 模型下构造签名方案(相比与标准模型下)较为高效，目前高效的后量子数字签名方案均是在 Random Oracle 模型下构造的。其构造方法主要通过两种范式----Fiat- Shamir 变换与 Hash-and-Sign 签名。我们将区块链中的数字签名算法应用后量子数字签名算法替换。以保证区块链系统的后量子安全性。

（2）共识算法的量子安全性

共识算法是区块链的关键组成部分。它用于在分布式系 统中实现各节点数据的一致性。竞争共识和协作共识算法是共识算法的两种主要类型。对于量子计算机而言，相对于非对称密码系统，散列函数比较难以破解。然而，还有一种量子算法可能会使找到 Hash 函数的碰撞变得相对容易，即降低破解密码学散列函数的安全级别。这种量子算法就是 Grover 的算法，Grover 的算法允许用户在无序列表中搜索特定项。Grover 的算法是概率算法:它衡量系统各种潜在状态的概率。给出了一定数量元素的无序列表，并要求找到满足某个条件的元素。可以使用经典计算 机遍历每个元素以找到满足条件的元素。

然而，量子计算使用叠加来同时测试多个输入。量子计算机将使用 Grover 算法进行几轮计算。通过每轮计算，某些项具有所需条件的概率增加。该算法随着进展而缩小选择范围，并在结束时输出一个高概率结果。

假设在经典计算机上我们需要进行 N 次运算来找到一个 Hash 函数的碰撞，那么应用 Grover 算法，在量子计算机上，需要大致 N/2 次操作，我们就能以一个很高的概率输出一个碰撞。所以对于区块链的共识机制，在量子计算机出现后，由于 Grover 算法,我们需要增加 hash 函数的安全强度，应用安全强度在 SHA-256 以上的 Hash 函数来保证共识机制的安全。

5.2 量子密码在电子支付中的应用

通常电子商务的安全控制是借助密码技术来实现的。即互联网世界的商务通信加密和传输安全，依赖于复杂的加密算法。传统的电子商务技术有两个关键的

缺陷:其一是，当有一台拥有足够计算能力的设备时，保密程序将会被破解。量子计算机就是现代密码技术的克星，在量子计算机面前，再复杂的加密算法，顷刻之间就被完全破译;其二则是当数据传输信道被“窃听”，就会造成信息的丢失被盗。所以传统通信，即便是再高级的保密通信，只要通过当前的电话线、无线电、光纤等通信设施，都会面临被破译和窃听的可能。

量子通信的关键要素是量子密钥，即以具有量子态的物质作为密码，信息被截获或被测量时，其自身形状立刻改变，所以，截获者只能得到无效信息。与现阶段成熟的通信技术相比，量子通信的工作机制，一次一密，完全可以实现，由此可见，量子通信极其安全，任何微小的干扰都可以被发现，双方共享的密钥被编码进极化的光子序列中，任何窃听活动都会留下其痕迹。因而可以利用量子通信技术，设计电子支付协议，保障交易过程中的信息安全。

6.未来发展

对于量子编码技术，除了最初利用光子的偏振特性进行编码外，还出现了一种新的编码方法——利用光子的相位进行编码。于偏振编码相比，相位编码的好处是对偏振态要求不那么苛刻。要使这项技术可以操作，大体上需要经过这样的程序：在地面发射量子信息——通过大气层发送量子信号——卫星接受信号并转发到散步在世界各地的接受目标。这项技术面对的挑战之一，就是大气层站的空气分子会把量子一个个弹射到四面八方，很难让它们被指定的卫星吸收。但是，这项技术需要面对“低温状态下加密且无法保证加密速度”的挑战。

量子密钥分发（QKD）作为人类首次利用量子物理手段来实现保密通信的创新实践，QKD 的发展面临着成本经济、商业模式等诸多挑战，但同时也得到了产业界和学术届的大力支持。在设备层面，QKD 的性能增强、小型化、甚至芯片化已在不断迭代升级；在组网层面，基于可信中继的 QKD 网络也在不断地扩展完善；在标准层面 ITU、ISO/IEC JTC1、ETSI、CCSA 等国内外标准组织正在加速制定相应的技术标准；在应用层面，QKD 在需要长期安全性保障的领域，例如金融、政务、医疗等方面的商业应用已在逐步成形。可以看到，量子保密通信技术呈现出蓬勃发展的势头，随着技术和产品的不断发展成熟，将来必然拥有广阔的应用前景。

7.结束语

本文简要介绍了量子密码的发展，并结合传统密码阐述了量子密码的优点。同时，介绍了量子密码量子安全问题及其重要性、量子安全问题的应对措施以及量子密码的应用和未来发展。

量子信息技术的发展必将为信息社会的演进注入新动力。然而，量子计算带来的密码安全威胁则不容忽视，特别是对于一些保密年限要求较长的场景，亟需立即采取应对措施。目前，一方面建议对于经典对称密钥密码体制进行加固，同时应加快抗量子攻击的公钥密码算法研发及标准化进程。另外，对于采用基于量子物理的 QKD 等新型量子密码方案，同样应予以足够重视。

参考文献：

[1]侯林林.量子密码通信原理及应用前景探究[J].科学之友(B 版)s,2009(4):143-144
[2]甘斌,周海刚,赵华.量子密码研究与进展[J].网络安全技术与应用,2010(3):54.
[3]陆炳旭.量子密码技术发展概述[J].计算机光盘软件与应用,2014,17(24):314-315.
[4]刘小平,李泽霞.基于共词分析的量息学前沿热点分析[J].科学观察,2014,9(05):13-22.
[5]吴振宇.区块链技术的特点以及应用方法分析[J].网络安全技术与应用,2017(4):121-121.
[6]张志强,陈云伟,陶诚,徐婧,田倩飞.基于文献计量的量子信息研究国际竞争态势分析[J].世界科技研究与发展,2018,40(1):37-49
[7]邓桄涛,毛向杰.后量子密码技术在区块链系统中的应用[J].信息通信,2018,(12):54-46
[8]马彰超.量子时代的网络安全挑战及其应用[J]信息通信技术与政策,2019(10):37-41