量子时代的网络安全挑战及其应对研究

马彰超

摘要：量子信息技术的迅速发展对信息通信技术及网络安全将产生深远的影响。量子计算对传统密码学提出新的挑战，也为基于量子物理的新型量子密码技术的发展提供了契机。本文首先从密码学的历史演进出发，介绍从经典密码到量子密码的基本概念；然后对量子计算引发的安全问题、影响范围、紧迫性进行分析，并进一步探讨其应对措施和方案。

关键词：量子安全；量子密钥分发；后量子密码学

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。

密码是网络安全的基石。量子计算与量子通信的发展为密码安全带来新一轮矛与盾的碰撞和演进。本文拟针对量子安全问题是什么、何时应对、如何应对等问题进行剖析。首先，从经典密码到量子密码的演进历程出发，引出密码学面临的量子安全挑战以及量子密码的由来；然后，从量子计算机及量子算法的发展来说明其对经典密码带来的安全威胁，进而分析量子安全问题所带来的影响以及问题的紧迫性；最后，将针对应对量子安全问题的3种策略举措分别进行介绍。

2　从经典密码到量子密码

密码学拥有数千年的历史，在数字时代之前，密码学主要用于保护军事、政务、外交等具有高度保密性要求的通信，在人类历史中扮演着重要的角色。在信息化高度发达的今天，密码学技术的使用几乎无处不在，特别是在互联网中应用极广，对于保护日益数字化的世界至关重要。

密码学是在密码设计者和破解者的智慧较量中形成的一门艺术。每当现有密码被攻破，密码设计者们就会重新开发出更强大的密码来保证通信安全，这又会引发密码破译者们不断尝试新的攻击方式（见表1）。

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。这样的终极密码是否存在呢？令人惊讶的是，早在1917年，Gilbert Vernam发明一次性密码本（OTP）时就已实现了该目标。信息论的创立者香农（Claude Shannon，1916—2001年）1949年理论上证明了OTP密码具有的无条件安全性，或称信息理论安全性（Information-Theoretic Security，ITS）。

作为一种加密算法，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。

表1 密码学的演进历史

密码技术演进	发明时间	是否被攻破
单表替代密码	约公元前 50 年由 J. Caesar 发明	约 850 年由 Al-Kindi 提出破译方法
命名密码法	约 1400—约 1800 年	已可破译
多表代换密码(维吉尼亚密码)	1553—约 1900 年	1863 年由 F. W. Kasiski 提出破译方法
……		
一次性密码本	1918 年发明（G.Vernam）	1949 年由 C. Shannon 证明其理论无条件安全性
机电式多表代换加密机	1920—1970 年	已可破译
……		
数据加密标准	1977—2005 年	1998 年在 EFF 基金会资助下实现 56h 内破解
公钥密码学	1977 年发明基于大数分解问题的 RSA 算法 1985 年发明 ECC 算法	1994 年由 P. Shor 证明量子计算机可快速求解大数分解和椭圆曲线离散对数问题
高级加密标准	2001 年至今	尚未破解
量子密码学	1984 年发明，正在发展中	可证明理论无条件安全性
后量子公钥密码学	正在发展中	尚未破解

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。原则上牢不可破的OTP，一旦发送方Alice和接收方Bob用尽了预先共享的安全密钥，其安全通信将不得不中断，直到再次获取新的密钥。这就是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。

但在现代密码系统中，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。一种典型的应用场景是在手机SIM卡中预置长期不变的128位根密钥，用于控制SIM卡整个生命周期中的数据加解密。这种方案要求信息的发送方用于加密和接收方用于解密的密钥完全相同，通常称为对称密钥密码学。

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。在公钥密码学出现之前，仅能通过人工预置的方式分发密钥。为了充分解决密钥分发问题，1977年Ron Rivest、Adi Shamir和Leonard Adleman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。

有趣的是，当人们意识到可以使用量子计算机破

解公钥密码体制的10年前，就已经找到了可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。

另外，量子算法带来的冲击也促进了经典密码学的进一步演进。现有的量子算法相对于传统密码算法的“指数”加速性并不是对所有数学问题都成立。紧随Shor算法的出现，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）。

可以看到，量子信息科学的发展对密码学带来的深远影响正在逐步显现，围绕量子计算机这超越经典运算能力的超强攻击手段，密码学领域又掀起了新一轮矛与盾的对抗。

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。

Grover算法则能够加速数据搜索过程，其将在数据量大小为N的数据库中搜索一个指定数据的计算复杂度降低为O()，从而降低了对称密钥算法的安全性。例如，对于AES-128算法，其128位长度的密钥具有2128种可能性，采用Grover算法则仅需搜索264种可能性，相当于将AES-128的破解复杂度降低为AES-64的级别。

针对现有密码算法受到量子计算影响的程度，美国国家技术与标准研究院（NIST）、欧洲电信标准协会（ETSI）等组织已进行了一些评估，其结论参见表2。

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。

如图1所示，传统公钥算法（如RSA、ECC等）广泛用于各类安全协议和应用服务，因此量子安全问题的影响范围极广。

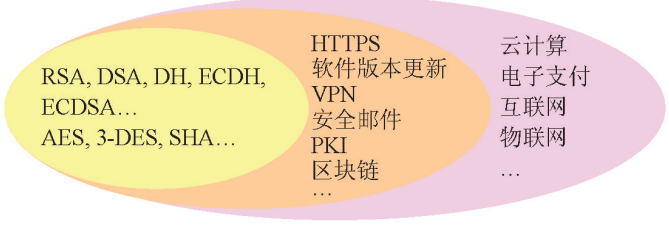

图1　量子安全问题的影响范围

3.3 量子安全问题的紧迫性

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？

如何应对量子安全问题，何时启动应对措施，这不仅仅涉及到需要多久来研发成功量子计算机，同时还需考虑具体应用的安全性要求，以及现有网络基础设施迁移到新的量子安全密码所需的代价和时间。这里引用一个简单的公式来分析量子安全问题的紧迫性，首先假设：X＝具体应用所要求的信息保密年限（年），Y＝当前信息安全设施迁移到新的量子安全密码方案所需的时间（年），Z＝建成可破解密码的大型量子计算机所需时间（年）。

如果“X+Y>Z”的话，意味着该应用有部分信息将无法达到其保密年限要求。在图2所示的MIN（X+Y-Z，Y）年内，攻击者完全可以通过监听在公共信道上传输的信息并存储下来，然后等若干年后量子计算机实现时提前解密这些信息。从技术上来看，当前飞速发展的大数据技术为海量网络数据的存储和分析提供了可行性。

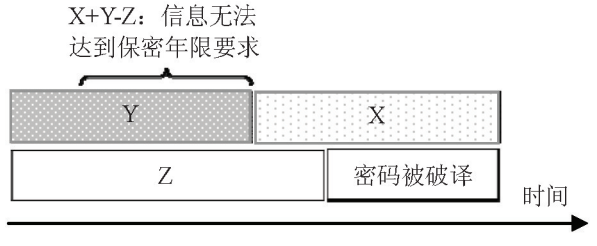

图2 量子安全威胁生效时间分析

X的取值取决于具体应用的安全性要求，例如信用卡通常要求X=5年。实际上，还有很多应用需要保障长期的机密性。例如，医疗数据的保密年限，通常要求大于患者的寿命时长；个人的基因组数据，则需要更长的保密时间；金融、政务、军事等高度机密的数据则往往要求更严格的保密期限，有些甚至需要无限期的保护。

关于大型量子计算机的构建时间Z，在2015年NIST关于后量子时代的网络空间安全研讨会上，有专家给出预测在2026年前实现的概率为1/7，在2031年前实现的概率为1/2。剑桥大学Simon Benjamin教授给出似乎更精确的预测，其认为构建可容错的量子计算机已不存在理论上的困难，但有效破解RSA算法需要约600万量子比特，在投资充足的情况下（约需300亿美元）需6~12年即可实现，否则在现有投资水平下则需15~25年；另外，其认为一旦非容错的量子计算机理论取得突破，则仅需数千量子比特即可破解RSA算法，粗略估计在投资充足情况下5~7年即可实现，否则需8~12年。

关于现有系统向量子安全方案升级所需的时间Y，需要针对不同的迁移路线分别考虑。NIST目标重新设计新型的后量子公钥算法（PQC），其标准发布的预计时间在2023—2025年。而新的密码算法标准推向市场，通常还需要多年的时间才能完成应用整体的迁移，这样Y将很可能在10年以上。另外，采用量子密钥分发替代基于公钥的密钥交换也是可选的方案之一，但其对网络和设备的特殊要求，使得目前仅能适用于一些特殊业务场景。

可见，目前ICT应用所面临的量子计算安全挑战已十分严峻。对于一些保密年限要求较长的信息系统，应该立即考虑启用抗量子计算机攻击的保密通信技术。

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　结束语

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。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。

参考文献

[1] 高树忠. 二战中的密码战[J]. 环球军事, 2015(4): 52-53.

[2] Singh, S. The code book: the science of secrecy from ancient egypt to quantum cryptography[M]. Anchor, 2000.

[3] Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications[M]. Transactions of the American Institute of Electrical Engineers, 1926, 45: 295-301.

[4] Shannon, C. E. Communication theory of secrecy systems[M]. Bell System Technical Journal, 1949,28(4): 656-715.

[5] Budiansky, S. Battle of wits: the complete story of codebreaking in World War II[M], Simon and Schuster, 2000.

[6] Jennewein, T., et al. A fast and compact quantum random number generator[M]. Review of Scientific Instruments, 2000,71 (4): 1675-1680.

[7] Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring[J]. Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, Ieee.

[8] Bennett Ch, H. and G. Brassard. Quantum cryptography: public key distribution and coin tossing Int. Conf. on Computers, Systems and Signal Processing . Bangalore, India, Dec. 1984.

[9] L. Chen, S. Jordan, etc. NIST: report on post-quantum cryptography[R]. NIST, 2016.

作者简介：

马彰超 国科量子通信网络有限公司标准总监，高级工程师

The cyber security challenge in the quantum era and its countermeasures

MA Zhangchao

Abstract: The rapid development of quantum information technology will have a profound impact on information and communication technology and cyber security. Quantum computing poses new challenges to traditional cryptography and also stimulates the development of quantum cryptography based on quantum physics. This paper begins with the historical evolution of cryptography and introduces the basic concepts from classical cryptography to quantum cryptography. Then it analyzes the quantum security problems and its urgency caused by quantum computing, and further explores its countermeasures and solutions.

Key words: quantum security; quantum key distribution; post-quantum cryptography

（收稿日期：2019-08-25）