量子密码发展现状及其安全挑战

张文默、张津婵、李凯轩

目录》
CONTENTS

01
PART

引言

背景意义

- 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。

02
PART

从经典密码到量子密码

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。

一次性密码本（OTP）

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。

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。

2、在现代密码系统中，人们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 ，发明了RSA 方案，一种非对称的密钥算法，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。公钥密码学的安全性依赖于一定的数学假设，例如大整数的素数因子分解难。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。

3、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。

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。

03
PART

量子安全问题及重要性

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。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。

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

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：
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，
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。

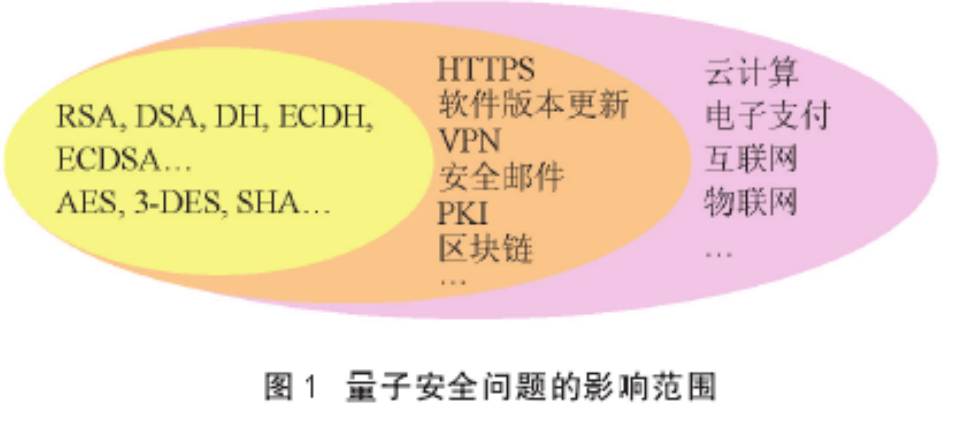

图 1　量子安全问题的影响范围

04
PART

量子安全问题应对措施

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。

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。

现有密码的加强

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

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。

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。

量子密钥分发（QKD）

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。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。

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。

05
PART

量子密码的应用

后量子密码技术在区块链中的应用

（1）抗量子数字签名方案

（2）共识算法的量子安全性

量子密码在电子支付中的应用

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。

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。

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。

06
PART

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。

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。

07
PART

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。

Thanks !