量子密码与量子同态加密

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。量子同态加密中没有执行数据解密操作，保护了数据的私密性，实现了用户的委托计算。

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。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。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。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。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 1 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。

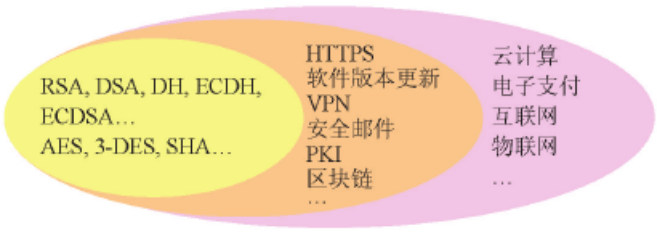

图 1　量子安全问题的影响范围

4．后量子公钥密码学与量子密钥分发

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 后量子密码学（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。

后量子密码是能够抵抗量子计算机对现有密码算法攻击的 新一代密码算法。所谓“后”，是因为量子计算机的出现，现有的绝大多数公钥密码算法（RSA、Diffie-Hellman、椭圆曲线等）能被足够大和稳定的量子计算机攻破，所以可以抵抗这种攻击的密码算法可以在量子计算和其之后时代存活下来，所以被称为“后”量子密码。

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。

4.2 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。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。

量子加密最著名的例子莫过于 BB84 协议，之所以叫这个名字，是因为该协议由 Charles Bennett 和 Gilles Brassard 于 1984 年提出的。这个协议可以实现量子密钥分发(Quantum key distribution, QKD)，也就是利用量子通信完成通信双方的密码交换。根据这个协议的想法，通信的发送方，通过发送不同偏振方向的光子完成加密。

发送方称为 Alice，接收方称为 Bob 量子密码分发过程如下所示：

（1）Alice 随机生成一段序列，比如 011010101，然后为序列的每个值随机选择 A、B 方案中的一个发送光子，即量子比特(Qubits)。Alice 只要记住这串随机序列，以及发送每个数值时使用的方案就可以了。

（2）Bob 随机使用 A、B 两套方案检测光子，并记录光信息到底是 0 还是 1。

（3）待所有量子比特传送完之后，Alice 和 Bob 通过公开的方式进行通话，Bob 依次告诉 Alice 每一个量子比特的测量方式，不需要说明具体的测量值，Alice 则只需要告诉 Bob 哪些量子比特测量的方法是正确的就可以了。

（4）最后 Bob 自然就知道哪些量子比特测对了，Alice 也知道 Bob 测对了哪些量子比特，于是两个人就可以使用这些测对的信息作为双方的密码了。

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。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。

5．量子同态加密框架

5.1 框架描述

一个量子同态加密(quantum homomorphic encryption，QHE)方案由四部分构成：密钥产生算法、加密算法、解密算法和评估算法。和一般的量子加密算法相比，QHE 多了一个评估算法。该算法的作用是构造相应的量子同态算子，并在加密数据上执行这些同态算子。当用户对其输出执行解密操作时，将得到相应操作在明文态上执行的结果。

假定 ρc 和 σm 是密文和明文的量子态表示形式，KeyGenA 是密钥产生算法，EncryptA 是加密算法， DecryptA 是解密算法，EualuateA 是评估算法，UΔ 是 一组可允许执行的量子操作集合，存在一个 U∈UΔ ，密 钥 k ∈{KeyGenΔ}，则 有 ρc = EncryptA(σm,k) 和 σm = DecryptA(ρc,k) 。EvaluateA 的描述如下:根据用户指定 的酉变换 U 和密钥 k ，评估函数计算出一个在用户加密数据上可执行的同态算子 U′ ，在这个计算过程 中没有执行 DecryptA 算法，而且假定了 EvaluateA 的 执行方(也叫代理)是诚信的。

在量子逻辑线路中，所有的逻辑门都是可逆的， 这一点不同于经典逻辑门。因此，对于评估函数的 输出结果，结合对称加密和量子逻辑门可逆性的特 点，将 QHE 方案表述为:

$$U'\rho_c = Encrypt_A(U\sigma_m, k) \tag{1}$$

该式说明，同态算子 U′ 作用在量子密文态 ρc 上 的结果(记为 U′ ρc)，等价于对原始操作 U 作用在量 子明文态 σm 上的结果(记为 Uσm)进行加密。所以说，用户只要对评估函数的输出进行解密，即可得到原始操作 U 作用在量子明文态 σm 上的结果，即:

$$U\sigma_m = Decrypt_A(U'\rho_c, k) \tag{2}$$

而且从式(1)还可以推导出关于同态算子 U′ 的公式，即：

$$U' = \frac{Encrypt_A(U\sigma_m, k)}{Encrypt_A(\sigma_m, k)} \tag{3}$$

对于式(3)，在同态算子 U′ 的计算过程中，有如下几点说明：(1)代理方需要知道用户的加密密钥;(2)没有调用解密过程 DecryptA ;(3)假定代理方是诚信的;(4)加密算子都是酉矩阵,注意矩阵运算规则。基于前三点，在量子同态算子的构造过程中，用户数据的私密性得到了很好的保护，而且代理方会 正确执行用户的委托计算，满足 QHE 的定义。

通过式(3)可以根据用户指定的量子操作(也叫酉变换，该变换作用于量子明文态)，构造出作用于量子密文态的同态算子(也是一种酉变换)，使得 用户只需解压评估函数的输出态，就可以得到指定 操作在量子明文态上的结果。评估函数不仅实现了 用户委托的量子计算，而且完成了针对用户指定量子酉变换的 QHE 方案的设计。

综上所述，把式(3)称为构造量子同态操作的一 般性方法(即评估函数的设计)，进而建立起设计 QHE 方案的通用框架。当然，该框架可以推广至量 子公钥加密体系，如下列 3 个等式所示:

$$U'Encrypt_A(\sigma_m, pk) = Encrypt_A(U\sigma_m, pk) \tag{4}$$

$$U\sigma_m = Decrypt_A(U'\rho_c, sk) \tag{5}$$

$$U' = \frac{Encrypt_A(U\sigma_m, pk)}{Encrypt_A(\sigma_m, pk)} \tag{6}$$

其中，pk 和 sk 分别代表量子公钥加密体系中的公钥 和私钥。从式(6)可以得到，推广后的非对称的 QHE 框架中，计算量子同态算子的过程只需要加密密钥 而不需要解密密钥，而且是独立于解密过程的。它 不再需要假定代理方是诚信的，扩大了 QHE 方案的 适用范围。相比较于式(3)的对称 QHE 框架，式(6)的非对称 QHE 框架，具有更高的安全性和更广阔的适用范围。

5.2 安全性分析

对于一个 QHE 方案来说，它的安全性可以从两个方面进行分析。首先是加密算法的安全性。在该框架中，由于采用了对称加密算法，导致评估函数在计算相应的量子同态操作时，一个是要假定代理方 是诚信的，另外还需要加密密钥，这就导致数据有泄 密的可能性(因为加解密密钥是一样的)。就对称加密算法本身来说，二值情况下，有信息理论安全的量子一次一密方案。但是在三值情况下，目前还没有一个信息理论安全的对称量子加密方案。当该模型推广至量子公钥加密体系下时，代 理方是否诚信和可能的数据泄密就不存在了，这无疑会提高 QHE 方案的安全性和适用范围。

最后，分析该框架中的密钥安全性。首先，该框架中的加解密密钥都是只使用一次的，类似于一次一密方案。密钥串的获取可以基于重发机制的量子密钥分发协议得到，而且分发过程是无条件安全的。其次，基于量子测不准原理和量子不可克隆原理，任何强行测量未知量子态 的做法，都只能得到一些随机的量子比特串，而非私密信息。最后，只要密钥的拥有者不泄露密钥的任何私密信息的话，任何窃听者都将无法获得有效的私密信息。另外，由评估函数构造的量子同态算子 (只有代理方知道)作用于用户加密数据，相当于二次加密，这无疑增加了窃听者获取有效信息的难度。综上所述，QHE 框架在二值量子态下是信息理论安全的，但在三值量子态下，却是弱安全性的。主要原因是在三值情况下缺乏信息理论安 全的对称量子加密方案。但当将其推广至量子公钥加密体系下后，该框

架将能够获得信息理论安全的 QHE 方案。

6．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、后量子公钥密码学与量子秘钥分发。同时，介绍了量子同态加密框架及其安全性。

量子同态加密方案可以实现委托的量子计算，主要是指代理方可以构造出基于用户加密密钥和指定操作的 同态算子，使其作用在用户加密数据上。当用户对评估函数的输出结果进行解密时，用户将得到原始操作在明文态上执行的效果。这个过程中没有执行数据解密操作，保护了数据的私密性，实现了用户的委托计算。寻找量子公钥加密算法和优化评估函数，设计高效安全的 QHE 或 QFHE 方案，将是未来量子密码发展的一个方向。

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]陈智罡,王箭,宋新霞.全同态加密研究[J].计算机应用研究.2014(06)
[5]王育齐,佘堃.通用的量子同态加密框架[J].计算机科学与探索,2016,10(11)
[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