量子密码与量子同态加密

李凯轩 张津婵 张文默

北京大学
PEKING UNIVERSITY

前言
Introduction

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。

目录

CONTENTS

01 从经典密码到量子密码

02 量子安全问题及其重要性

03 后量子密码学与量子密钥分发

04 量子同态加密框架

01 从经典密码到量子密码

一次性密码本

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。

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。

密钥分发难题与公钥密码

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

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。公钥密码学的安全性依赖于一定的数学假设，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。

量子密码的提出

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。

02 量子安全问题及其重要性

量子计算机对经典密码的影响

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

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。

量子安全问题的影响范围

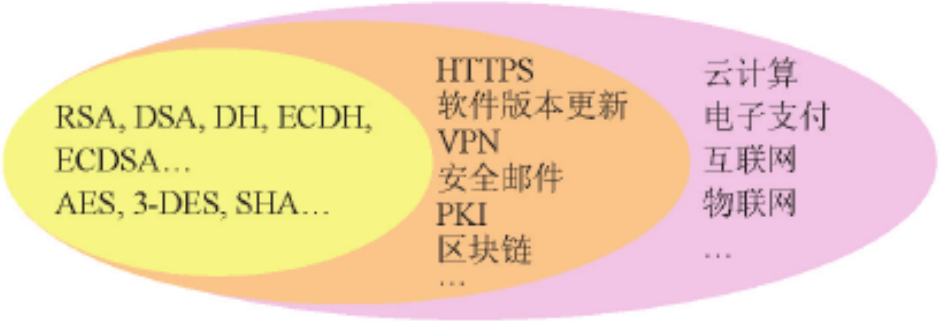

图 1　量子安全问题的影响范围

03 后量子密码学与量子密钥分发

后量子密码学（PQC）

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。也有人称之为“抗量子密码”，说的都是一个意思。英文中的表述是："Post-quantum Cryptography (PQC)"，或者 "Quantum-resistant cryptography"。

量子密钥分发（QKD）

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。

04 量子同态加密框架

框架介绍

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。

北京大学 PEKING UNIVERSITY

框架介绍

$$U'\rho_c = Encrypt_A(U\sigma_m, k) \quad (1)$$

ρc 和 σm -----密文和明文的量子态表示形式
KeyGenA -----密钥产生算法
EncryptA -----加密算法
DecryptA -----解密算法
EualuateA ----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) 。

北京大学 PEKING UNIVERSITY

框架介绍

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

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。

北京大学 PEKING UNIVERSITY

框架介绍

$$U'Encrypt_A(\sigma_m, pk) = Encrypt_A(U\sigma_m, pk) \quad (4)$$

$$U\sigma_m = Decrypt_A(U'\rho_c, sk) \quad (5)$$

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

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。

安全性

（1）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。

（2）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。

（3）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。

结束语

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。

汇报完毕 感谢您的聆听

北京大学
PEKING UNIVERSITY