浅谈量子计算与后量子密码

郁昱，张江

最近有一些新闻媒体报道了量子信息/量子计算将对传统密码技术（也称为现代密码或经典密码）构成严峻挑战甚至将是彻底的颠覆。作为密码学的研究人员，我们抛砖引玉谈谈对“量子计算 VS 密码技术”这一问题的看法，同时简单介绍一下我们正在开展的后量子密码方面的研究工作。

1. 生活中的“密码”

随着信息技术的发展和互联网的普及，密码技术被广泛用于网络和信息系统安全的各个方面，保护着信息的秘密性、完整性、不可抵赖性等信息安全的重要属性，也是网络空间安全学科的一个重要组成部分[1]。由于翻译和使用习惯的原因，绝大多数民众理解的密码仅限于登陆各种应用账号（如邮箱、支付宝、微信等）需要输入的若干数字和字母组合，即所谓的口令（英文为 password/passphrase）。通常来说，口令只是用于实现服务器对用户的身份认证，然而密码学（Cryptology）的意义则广泛得多，生活中常用的手机 SIM 卡、银行 U 盾、比特币、网络证书，TLS/SSL 等协议甚至包括公交卡、二代身份证等都需要不同密码技术的支持。

2. 量子密码技术对传统密码技术的“威胁”

相对于现代密码技术，目前量子密码的应用相对较少，主要包括量子密钥分发和量子比特承诺等，其中量子密钥分发可用于实现信息的安全传输，是目前最受关注的量子密码应用。接下来，我们围绕安全的信息传输，简要介绍一下传统的密码系统。经典的密码系统主要由密钥和密码算法两部分组成，密码算法通常是公开的，而密码系统的安全性只决定于密钥的保密性。如下图所示，在一个加密系统中，加密算法 Enc 和解密算法 Dec 都是公开的，而加密者 Alice 和解密者 Bob 则分别拥有加密密钥 k1 和解密密钥 k2，Eve 是传输信道上的攻击者。当 Alice 想要发送数据 m 给 Bob 时，Alice 将加密密钥 k1 和数据 m 作为加密算法 Enc 的输入，计算得到密文 c=Enc(k1,m)并发送给解密者 Bob。当接收到密文 c 后，Bob 将解密密钥 k2 和密文 c 作为解密算法 Dec 的输入，计算得到明文 m=Dec(k2,c)。

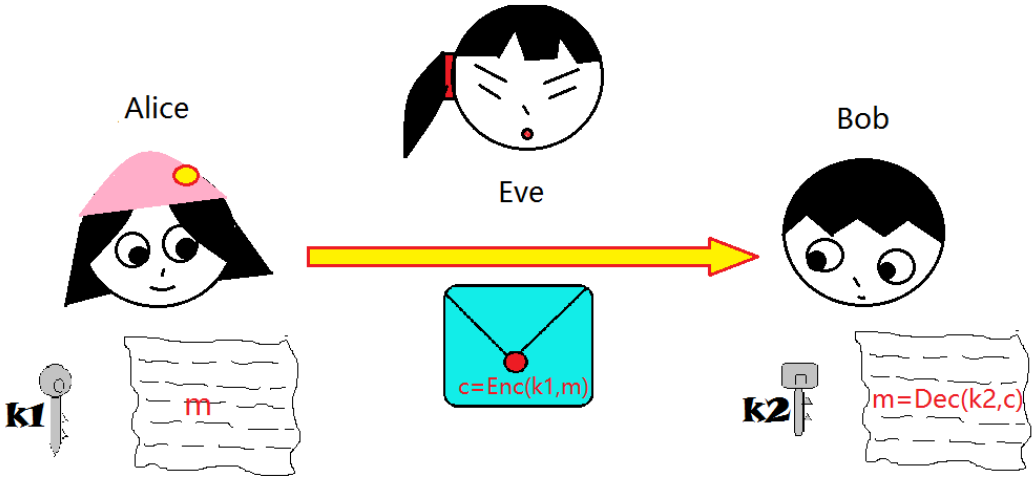

图 1. 现代加密系统的工作原理图（由黄晨歌绘制）。

根据密钥使用方式的不同，加密系统又分为对称加密系统和公钥加密系统。在对称加密系统中，加密和解密是用同一个密钥，即 k1=k2，该密钥是对外保密的。对称加密系统主要包括流密码和分组密码，其中分组密码较为常用，我们熟知的美国的分组加密标准 DES、AES 以及我国的商用分组加密标准 SM1、SM4 等。这类算法通常是密码学家在一些现有的设计原则和分析方法上设计出来的，而不是基于已知的数学和计算复杂性理论方面的困难问题。据我们所知，在量子计算模型下，目前针对对称密码系统最高效的 Grover 算法，也只是将密钥的有效长度减少为原来的一半。换句话说，真正意义上的量子计算机，即使能够实现，其破解 AES-256 仍然需要 2^{128} 量级的计算代价。

使用对称加密有个前提，即加密者和解密者必须事先共享一个较短(例如 128 比特)的密钥，这在一些应用场景下是不现实的。公钥加密系统的出现，解决了这个问题。最具开创性的 Diffie-Hellman 密钥交换协议可以确保了通讯双方在不共享任何保密信息的前提下建立共享的密钥，之后又出现了 RSA 和 ElGamal 公钥加密，我国也有相应的公钥密码标准 SM2。由于公钥类的加密效率相对较低，现实应用中，在通讯双方建立共享密钥之后，一般都会使用更为高效的对称加密算法对大量数据进行加密。公钥加密的特点是，它们的安全性都是建立在一些著名的计算困难问题之上，如 RSA 大数分解，离散对

数等等，目前研究学者没有找到在图灵机模型下高效求解大整数分解和离散对数问题的经典算法，但美国科学家 Peter Shor 在 1995 年却给出了能够在多项式时间内高效求解大整数分解和离散对数的量子算法。即借助于量子计算机，攻击者可以高效的破解基于大整数分解和离散对数问题的 RSA 和 Diffie-Hellman 等公钥密码方案。虽然目前量子计算机还局限在几个量子比特的原型阶段，在其上面运行 Shor 算法也仅能分解两位的合数，科学家们都在为迎接“后量子时代”做准备。量子信息技术对以上问题给出的解决方案是通过量子密钥分发技术在传输双方建立共享密钥，然后再通过香农一次一密或类似的方法对称地加密实现无条件的安全性。然而目前量子密钥分发的速率仍是实现高速率信息传输的瓶颈。而且，与传统的密码技术一样，理论上可论证的安全性并不等同于实际系统的安全性，密码系统在实现时硬件和系统的非理想性也可成为能被攻击者利用的漏洞。

3. 后量子密码技术

量子算法对于传统密码系统的冲击是由于量子算法相对于经典算法在一些问题上具有一定的加速性（可以简单理解为量子算法具有高度的并行计算能力）。例如，在传统计算机上需要亚指数计算时间的大整数分解问题，在量子计算机上多项式时间内就可求解。然而，量子算法相对于传统算法的“指数”加速性并不是对所有数学问题都成立。事实上，对于某些问题（如 NP 完全问题、基于格、基于编码和基于多变元方程的数学问题），量子算法相对于传统算法并没有明显的优势。紧跟着 Shor 算法的出现，国内外密码学家已对基于格、基于编码和基于多变元方程密码方案展开了大量的研究，力图设计可以对抗量子计算机的经典密码算法，并统称这些研究为后量子密码学。以下我们对后量子密码中的一两个基本困难问题做一个简单的介绍。这里攻击者的目标是求解以下的 n 元一次方程组，其中系数 $a_{11}, \dots, a_{qn}$，未知数 $x_1, \dots, x_n$ 都是 GF(2)上随机选取的（即 0 或 1 的随机比特），$e_1, \dots, e_q$ 都各自独立的服从参数为 0<u<1/2 的 Bernoulli 分布（即每个 e_i 等于 1 的概率为 u，否则 e_i 等于 0）。

$$
\begin{aligned}
&a_{11}x_1 + a_{12}x_2 + \mathrm{L} \ + a_{1n}x_n + e_1 = y_1 \ (\mathrm{mod}\ 2)\\
&a_{21}x_1 + a_{22}x_2 + \mathrm{L} \ + a_{2n}x_n + e_2 = y_2 \ (\mathrm{mod}\ 2)\\
&\ \ \mathrm{M}\\
&a_{q1}x_1 + a_{q2}x_2 + \mathrm{L} \ + a_{qn}x_n + e_q = y_q \ (\mathrm{mod}\ 2)
\end{aligned}
$$

该问题要求在已知给定的系数 $a_{11}, \ldots, a_{qn}$ 和结果 $y_1, \ldots, y_q$ 的条件下，求解未知数 $x_1, \ldots, x_n$ (如果 $x_1, \ldots, x_n$ 求解出来，$e_1, \ldots, e_q$ 也立即可以得到)。以上问题就是著名的 Learning Parity with Noise (LPN)问题。当 q 远大于 n，并且 u 是小于 1/2 的常数的情况下，未知数 $x_1, \ldots, x_n$ 是几乎可以唯一确定的。该问题被证明在最坏情况下是 NP 完全的，即使在平均情况下，人们至今没有找到解决该问题的有效算法，目前渐进意义上最好的 BKW 算法需要亚指数的时间复杂度，更重要的是，量子算法解决该问题也不具有任何优势。我国学者在利用 LPN 设计后量子对称密码算法[2]和针对 LPN 在具体参数设定下的密码分析[3,4]上取得了较为领先的成果，我们也有一项进行中的工作是基于标准 LPN 问题的困难性设计公钥密码算法和不经意传输协议。Oded Regev 进一步将以上的 LPN 问题推广到更大的素数域上，即以上方程组中所有的系数和未知数都是 GF(p)上的元素，且相关的加法和乘法都在 GF(p)上运算，其中 p 是一个较大的素数，$e_1, \ldots, e_q$ 都独立地服从 GF(p)上的离散高斯分布。以上推广后的问题就是著名的 Learning with Errors (LWE)问题。目前已知 LWE 在一定的参数设定下可以归约到 GapSVP，SIVP 等格上的困难问题（即求解 LWE 问题并不比求解格上困难问题容易），因此也是后量子安全的。虽然 LWE 相对于 LPN 在效率上有一定降低，但其具有更广泛的密码应用，除了公钥加密，LWE 还可以用来设计抗碰撞哈希函数、全同态加密等。我国学者在这方面也有一些工作，如张江等人基于 Ring-LWE 设计的可用于 TLS 协议的后量子安全的高效密钥交换协议[5]。

综上，现代密码学并不等同于基于 RSA、离散对数等少数几个数论困难

问题的密码系统，量子计算机的到来也并不是现代密码学的末日，安全信息传输只是传统密码学诸多应用中的一个，因此量子密码不可能完全取代传统密码。经过近 20 年的发展，后量子密码学的研究已经取得了丰硕的成果，同时也为抵抗量子计算机攻击储备了大量了的密码技术，一些标准制定机构即将甚至已经在开展后量子密码算法的标准化工作，相信在不久的将来量子安全的（但仍是在传统计算机上运行）密码系统即可以部署到我们日常使用的系统和网络中，更好地保护我们的信息安全。

参考文献

[1] 张焕国，韩文报，来学嘉，林东岱，马建峰，李建华. “网络空间安全综述” 中国科学，第 46 卷，第 2 期：125-164，2016.

[2] **Yu Yu** and John Steinberger. “Pseudorandom Functions in Almost Constant Depth from Low-Noise LPN”, in Advances in Cryptology - EUROCRYPT 2016.

[3] Qian Guo, Thomas Johansson, Carl Löndah., “Solving LPN Using Covering Codes”. In Advances in Cryptology - ASIACRYPT 2014.

[4] Bin Zhang, Lin Jiao, Mingsheng Wang. “Faster Algorithms for Solving LPN”. In Advances in Cryptology – EUROCRYPT 2016.

[5] **Jiang Zhang**, Zhenfeng Zhang, Jintai Ding, Michael Snook, Özgür Dagdelen. “Authenticated Key Exchange from Ideal Lattices”, In Advances in Cryptology – EUROCRYPT 2015.

作者简介：

郁昱，上海交通大学特别研究员，博士生导师。主要从事密码学基础理论的研究工作，2010 年回国后曾分别在华东师范大学和清华大学任教，多项研究成果发表在密码三大会(CRYPTO/EUROCRYPT/ASIACRYPT)和 CCS, TCC, CHES, CT-RSA, ESORICS 等密码与信息安全的代表性会议上。目前服务于国际密码学会理事会（IACR board）担任观察员并负责学会官网 www.iacr.org 的日常管理事务，2015 年获得中国密码学会优秀青年奖。

张江，信息安全博士，主要关注于可证明安全、公钥加密和密码协议的研究，现为密码科学技术国家重点实验室助理研究员，在国际重要密码会议和期刊 EUROCRYPT、ASIACRYPT、PKC、DCC、TCS 等发表了多项研究成果。个人主页：jiangzhang.net