后量子密码——格密码

1901210635 龚彦韬 1901210593 张宇驰

一、 量子计算对当前密码学体制的威胁

经典密码体制基本被分为两种，分别是对称密钥密码体制和非对称密钥密码体制，其中非对称密钥密码体系又可被称为公钥密码体制，其安全性基于计算复杂性的难题，例如 Diffie-Hellman 密钥交换协议基于离散对数问题，ECCDA 基于椭圆曲线离散对数问题，RSA 源于整数因数分解问题。然而早在上世纪九十年代，Shor 就提出了一种量子算法，可以在多项式时间内解决大整数分解问题，Shor 算法的核心就是利用量子计算的性质来求出函数的周期，这种思想对于求解离散对数问题仍然有效。因此，Shor 的工作表明，一旦量子计算机被真正制造出来，基于大整数分解问题，以及离散对数问题的密码体制，包括 RSA，ECC 等将不再安全。

而如今量子计算技术日新月异，制造量子计算机也不再是天方夜谭。即使目前还未能建立一个具有数千个稳定量子位的计算机，但是该领域已经有了显著进展。例如，有研究估计，到 2031 年，RSA 和 ECC 算法被破解的概率大约为 50%。而破解公钥加密系统会带来巨大的安全影响，甚至会给公钥密码体制带来灭顶之灾。面对这种崭新的挑战，必须要去构建新的密码体制。目前可以将对抗量子冲击的研究分为两大部分，一方面有人利用量子力学原理设计量子密码学以对抗量子计算机强大的计算能力，另一方面有人研究新的不存在有效量子算法的数学难题，以设计新的公钥密码算法。

二、 量子密码学

量子密码学是量子力学和经典密码学结合的产物，是利用量子力学特性：不确定性原理和不可克隆定理，来保证通信的安全性，即依靠微观粒子的量子属性来实现对信息的保护，研究的主要目标是抵抗量子计算攻击的密码算法和协议，是密码学的一个重要分支。量子密码的一个最独特，也是最重要的性质是，如果存在第三方试图窃听，则通信双方就会发现。根据量子力学的基本原理，任何对量子系统的测量，都会对系统产生扰动，而该扰动必定会被发现。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。

三、 后量子密码和格密码

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。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。

美国国家标准技术研究所(NIST)于 2012 年启动后量子密码方向的研究，2016 年正式启动了了全球范围内的后量子公钥密码算法标准征集工作，在 2017 年 11 月 30 日截止。在进行初步筛选后，NIST 公布了 69 个草案，主要包括以下 4 种数学方法构造的后量子密码算法：格(Lattice-based)、编码(Code-based)、多变量(Multivariate-based)和哈希(Hash-based)。

1)基于哈希(Hash-based)：最早出现于 1979 年，主要用于构造数字签名。代表算法：Merkle 哈希树签名、XMSS、Lamport 签名等。

2)基于编码(Code-based)：最早出现于 1978 年，主要用于构造加密算法。代表算法：McEliece。

3)基于多变量(Multivariate-based)：最早出现于 1988 年，主要用于构造数字签名、加密、密钥交换等。代表方法/算法：HFE(Hidden Field Equations)、Rainbow(Unbalanced Oil and Vinegar (UOV) 方法)、HFEv-等。

4)基于格(Lattice-based)：最早出现于 1996 年，主要用于构造加密、数字签名、密钥交换，以及众多高级密码学应用，如：属性加密(Attribute-based encryption)、陷门函数(Trapdoor functions)、伪随机函数(Pseudorandom functions)、同态加密(Homomorphic Encryption)等。代表算法：NTRU 系列、NewHope(Google 测试过的)、一系列同态加密算法(BGV、GSW、FV 等)。由于其计算速度快、通信开销较小，且能被用于构造各类密码学算法和应用，因此被认为是最有希望的后量子密码技术。

格密码其中最早出现于1996年，主要用于构造加密、数字签名、密钥交换，以及众多高级密码学应用。与基于数论问题的密码算法构造相比，基于格的算法可以实现明显提升的计算速度、更高的安全强度和略微增加的通信开销。与其他几种实现后量子密码的方式相比，格密码的公私钥尺寸更小，并且安全性和计算速度等指标更优。近年来，基于LWE(Learning with Errors)问题的格密码学构造发展迅速，被认为是最有希望被标准化的技术路线之一。下面将依次介绍格的基本知识和基于格的加密方案。

从几何学角度来描述，格是n维空间中规则排列的离散的无限点集，其形式化定义为：格是由$\mathbb{R}^n$中的k个线性无关向量$b_1,b_2,\cdots,b_k$的整数线性组合构成的集合：$L(b_1,b_2,\cdots,b_k)=\{\sum_{i=1}^{k}x_ib_i:x_i\in\mathbb{Z}\}$。格上的困难问题包括最短向量问题SVP(Shortest Vector Problem)，最近向量问题CVP(Closest Vector Problem)，近似最短向量问题GapSVP和近似最短线性无关向量组问题SIVP。

AD方案：最早的基于格构建的公钥加密方案是由Ajtai和Dwork提出的，此方案的安全性建立在最差情况下的uSVP(uniqie Shortest Vector Problem)问题的困难性上的，但此类方案存在效率低的问题：设格的维数为n，公钥的长度就为$\bar{O}(n^4)$，每个加密比特将增加为$\bar{O}(n^2)$，因此还无法真正应用。

GGH方案：GGH公钥加密方案的安全性基于最近向量问题CVP(Closest Vector Problem)。CVP是格上的一个NP问题，但由于GGH的构造使用的是一类特殊的格，所以对解决GGH中使用的特殊格的近似CVP实例的难度小很多，该方案在1999年被成功破译。

NTRU方案:NTRU是由Hoffstein等提出的一种在环上构建的公钥密码方案，此方案也可以使用特殊结构的格来描述，这种特殊结构的格叫做回旋模格(convolutional modular lattice)。此类格的维数为偶数且曼珠两个特性：一是在将向量(x,y)映射到(Tx,Ty)的线性变换下的封闭性，此方案效率较高，具有实用价值。但NTRU也存在着两个不足之处：一是存在解密错误问题，二是其安全性一直没有在理论上被证明。

基于LWE问题的加密方案：目前基于格问题困难性构造的加密方案中，效率最高的是一类基于LWE(Learning With Error)问题而构造的加密方案。LWE问题

是根据奇偶性学习问题演化而来，经过一般化可以很好的应用于构造公钥密码协议中。Regev 提出的 LWE 搜索问题可表述如下：已知$n,m,q=q(n)>2$且均为正整数。(A,v)作为输入的数据对，其中$A\in\mathbb{Z}_q^{m\times n},v\in\mathbb{Z}_q^m$，误差$e\in\mathbb{Z}_q^m$服从$\mathbb{Z}_q^m$上的概率分布$\chi^m$，求$s\in\mathbb{Z}_q^n$使得$v=As+e$成立。该问题的困难性等同于最差情况下 GapSVP 问题的困难性，并给予 LWE 问题设计了第一个 LWE 加密方案。此方案中的公钥长度$\bar{O}(n^2)$，获取一个比特的密文需要$\bar{O}(n)$比特的操作，因此其效率和密钥长度相对 AD 方案有了很大提高。Regev 给出的公钥加密方案可描述如下。

令 n 为密码方案中的安全参数，方案中还使用了两个整数 m 和 p 以及$\mathbb{Z}_p$上的概率分布χ进行参数化，这些参数集合保证了方案的安全性和正确性。首先选择介于n^2和$2n^2$之间的素数$p\geq 2$，对于任意常数$\varepsilon>0$，令$m=(1+\varepsilon)(n+1)\log q$。概率分布$\chi$服从正态分布$\bar{\Psi}_{\alpha(n)}$，且满足$\alpha(n)=o(1/(\sqrt{n}\log n))$，也就是说，$\alpha(n)$满足$\lim_{n\to\infty}\alpha(n)\cdot\sqrt{n}\log n=0$，例如可以选择$\alpha(n)=1/(\sqrt{n}\log^2 n)$。

- 私钥生成算法：随即均匀选择$s\in\mathbb{Z}_p^n$，将 s 作为私钥。
- 公钥生成算法：对于$i=1,K,m$，在均匀分布中独立的选择 m 个向量$a_1,K,a_m\in\mathbb{Z}_p^n$，并根据概率分布$\chi$独立的选择元素$e_1,K,e_m\in\mathbb{Z}_p$，则公钥通过$(a_i,b_i)_{i=1}^m$给出，其中$b_i=\langle a_i,s\rangle+e_i$。
- 加密算法：为了加密一个比特，我们在$[m]$的2^m个子集中均匀的选取一个随即集合 S，若待加密的比特是 0，则加密结果为$(\sum_{i\in S}a_i,\sum_{i\in S}b_i)$，若待加密的比特为 1，则加密结果为$(\sum_{i\in S}a_i,\left\lfloor\frac{p}{2}\right\rfloor\sum_{i\in S}b_i)$。
- 解密算法：若$b-\langle a,s\rangle$接近 0 而不是$\left\lfloor\frac{p}{2}\right\rfloor \bmod p$，则加密结果为$(a,b)$，否则，解密结果为 1。

近几年来，基于格的加密方案大致沿着 2 条线。首先是对 NTRU 加密系统的改造，Stehle 和 Steinfeld 在 2011 年首次对 NTRU 进行了成功改进，将方案的

语义安全规约到了 ring-LWE 问题的困难性假设。在 PKC2017 会议上，Yu 等人讨论了在素分圆环$\mathbb{Z}[X]/\langle X^{n-1}+\cdots+X+1\rangle$(其中 n 是奇素数)上的 NTRU 加密方案，得到一个标准模型下的 IND-CPA 安全方案，其安全性可规约到理想格上的最坏情况的困难问题。提出这种环的研究主要是因为它比 2011 年 Stehle 的环更容易控制而且能抵抗子域攻击，此外注意到素分圆环$\mathbb{Z}[X]/\langle X^{n-1}+\cdots+X+1\rangle$是 NTRU 环$\mathbb{Z}[X]/\langle X^{n}-1\rangle$的一个子环，因此基于素分圆环构造加密方案更接近于原始的 NTRU 加密系统。另外，格加密方案大多应用 LWE 和 ring-LWE 问题构建某些特殊加密方案如谓词加密(predicate encryption)、基于属性加密(attribute based encryption)和可验证加密等。例如有文献讨论了基于 LWE 的谓词加密，然而方案的构造借助于全同态加密(fully homomorphic encryption FHE)机制，在分层电路到所有电路中用到了自举(bootstrap)的方法，方案的效率比较低。对于现有方案的一些改进方向大多都是不改动方案本身，单独优化 FHE 效率从而提高谓词加密的效率。最后，2014 年亚洲密码年会 Benhamouda 等人提出的零知识证明能够改进基于 ring-LWE 的加密方案;2017 年欧洲密码年会 Lyubashebsky 等人利用明文知识证明构造了一个可验证加密方案等。总之，基于格构造各种特殊的加密方案是格加密的重要发展趋势，丰富了格密码的研究内容。

四、 发展趋势

受市场对更高效计算及解决先前不切实际问题能力的需求推动，量子计算从基础理论研究到现实应用之间的转换正在加速。10 年之前，很少有实用量子计算机的证据。然而仅仅到了 2019 年谷歌便宣称实现了“量子霸权”。量子计算技术飞速的发展使得密码学的更新换代显得更加必要。

后量子密码可以被应用于更高层次一些的协议应用，包括：HTTPS (TLS)、数字证书 (PKI)、SSH、VPN、IPsec、比特币等数字货币、U 盾、桌面/移动操作系统等各个领域和应用中。现在用到公钥密码算法的应用，基本可以使用后量子密码算法进行代替。虽然格困难问题在密码体制的设计和安全性方面有着很大的潜力，但仍有许多问题还不明朗，有待于密码学家进一步去研究、验证。

参考文献

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM review, 1999, 41(2): 303-332.

[2] Srednicki M . Quantum Field Theory[M]// Quantum field theory =. 世界图书出版公司, 2010.

[3] Ekert, Artur K . Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6):661-663.

[4] Lo H K , Curty M , Tamaki K . Secure quantum key distribution[J]. Nature Photonics, 2014, 8(8):595-604.

[5] Ajtai M. Generating hard instances of lattice problems[C]//Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996: 99-108.

[6] Ajtai M, Dwork C. A Public-Key Cryptosystem with Worst-Case[C]//Average-Case Equivalence Electronic Colloquium on Computer Complexity. 1996.

[7] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem[C]//International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 1998: 267-288.

[8] Chen L, Chen L, Jordan S, et al. Report on post-quantum cryptography[M]. US Department of Commerce, National Institute of Standards and Technology, 2016.

[9] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?", QCrypt, 2015.

[10] "The Quantum Countdown. Quantum Computing And The Future Of Smart Ledger Encryption", Long Finance, http://longfinance.net/DF/Quantum/Countdown.pdf, February 2018.

[11] Lyubashevsky V, Neven G. One-shot verifiable encryption from lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2017: 293-323.

[12] Benhamouda F, Camenisch J, Krenn S, et al. Better zero-knowledge proofs for lattice encryption and their application to group signatures[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2014: 551-572.

[13] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2011: 27-47.

[14] Yu Y, Xu G, Wang X. Provably secure NTRU instances over prime cyclotomic rings[C]//IACR International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2017: 409-434.

[15] Gorbunov S, Vaikuntanathan V, Wee H. Predicate encryption for circuits from LWE[C]//Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2015: 503-523.