有限域上非线性方程求解与优化的量子算法研究取得进展

2018-04-30 | 编辑：文/先进制造部

按照信息论与密码学先驱Shannon的观点，密码学的大多数问题可以转化为有限域上代数方程组的求解问题。多变量多项式方程求解的困难性是很多密码体系，包括流密码、分组密码、多变元公钥密码，其安全性的数学保证。有限域上非线性多变量方程求解的量子算法研究，是密码设计与分析的关键问题。

先进制造部的科研人员在有限域上非线性方程求解与优化的量子算法方面取得重要进展。

他们根据布尔环上的量子算法, 设计了有限域上方程求解与优化的量子算法, 对于有限域Fq , $q=p^m$上的多项式方程组$F\subset F_q[x_1,\ldots x_n]$其计算复杂度为$O((T^{3.5}n^{3.5}m^{15}(\log\ p)^{16})k^2)$, 其中T为输入多项式的稀疏度, k为多项式系统对应的扩展矩阵的条件数。这一算法在方程组对应的矩阵条件数不高的情况下, 量子算法能达到指数级加速。

进一步地, 将有限域上方程组求解问题更一般化, 扩充为包含有限域上变元以及含有界整数变元的含非线性约束的优化问题。这一问题包含了很多应用, 比如含噪声的多项式系统求解(polynomial systems with noise), 小整数解问题(short integer solution problem), Number Theory Research Unit (NTRU), 背包问题等。他们 首先通过引入新变元将这一问题转化为0-1规划问题, 其次将0-1规划问题转化为布尔变量的方程组求解问题。利用去年陈俣翱和高小山的结果, 给出了这一优化问题的量子算法. 这一算法的复杂度也是关于输入规模的多项式复杂度, 类似于有限域上的方程求解, 复杂度中也包含了k^2这一因子. 也就是说, 在优化问题所对应的矩阵条件数不高的前提下, 量子算法可以对优化问题进行指数级加速。

上述这些算法的提出, 揭示了在量子计算模型下, 基于有限域上方程组求解与优化的相应密码体制的安全度依赖于其所对应的扩展矩阵的条件数。