现代密码学

第五十五讲 后量子密码学

信息与软件工程学院

第五十七讲 后量子密码学

- 量子计算对密码学的影响
- 后量子密码学的研究方向

量子计算对密码学的威胁

- 贝尔实验室，Grove算法，1996年
  - 针对所有密码（包括对称密码）的通用的搜索破译算法
  - 所有密码的安全参数要相应增大
- 贝尔实验室，Shor算法，1994年
  - 多项式时间求解数论困难问题如大整数分解问题、求解离散对数问题等
  - RSA、ElGamal、ECC、DSS等公钥密码体制都不再安全

量子计算对密码学的威胁（续）

密码算法	类型	目的	受大规模量子计算机的影响
AES	对称密钥	加密	密钥规模增大
SHA-2, SHA-3	**Hash函数**	完整性	输出长度增加
RSA	公钥密码	加密，签名，密钥建立	不再安全
ECDSA，ECDH	公钥密码	签名，密钥交换	不再安全
DSA	公钥密码	签名	不再安全

量子计算机的研究进展

- 2001年，科学家在具有15个量子位的核磁共振量子计算机上成功利用Shor算法对15进行因式分解。
- 2007年2月，加拿大D-Wave系统公司宣布研制成功16位量子比特的超导量子计算机，但其作用仅限于解决一些最优化问题，与科学界公认的能运行各种量子算法的量子计算机仍有较大区别。
- 2009年11月15日，世界首台可编程的通用量子计算机正式在美国诞生。同年，英国布里斯托尔大学的科学家研制出基于量子光学的量子计算机芯片，可运行Shor算法。
- 2010年3月31日，德国于利希研究中心发表公报：德国超级计算机成功模拟42位量子计算机。
- 2011年5月11日，加拿大的D-Wave System Inc. 发布了一款号称 “全球第一款商用型量子计算机”的计算设备“D-Wave One”。

量子计算机的研究进展（续）

- 2011年9月，科学家证明量子计算机可以用冯·诺依曼架构来实现。同年11月，科学家使用4个量子位成功对143进行因式分解。
- 2012年2月，IBM声称在超导集成电路实现的量子计算方面取得数项突破性进展。同年4月，一个多国合作的科研团队研发出基于金刚石的具有两个量子位的量子计算机，可运行Grover算法，在95%的数据库搜索测试中，一次搜索即得到正确答案。该研究成果为小体积、室温下可正常工作的量子计算机的实现提供可能。
- 2013年5月D-Wave System Inc宣称NASA和Google共同预定了一台采用512量子位的D-Wave Two量子计算机。
- 2017年，中科大和浙江大学联合宣布基于超导量子计算方案实现了10位量子比特的纠缠操控。这一成果打破了美国之前保持的9个量子比特操纵的记录，形成了一个完整的超导计算机的系统，使我国在超导体系量子计算机研究领域也进入世界一流水平行列。

全球在抗量子密码方面的行动

- 2006年开始至今召开了9届后量子密码学国际学术研讨会。
- 各国资助机构对后量子密码的支持
  - 欧洲联盟（欧盟）项目pqcrypto和safecrypto
  - 日本的CREST密码数学项目
- 行业标准组织的活动：
  - 自2013年以来，欧洲电信标准协会（ETSI）组织了三个“量子安全密码”研讨会
  - 2015年NIST举行题为“后量子世界的网络安全”研讨会
  - 2016 年 2 月美国国家标准与技术研究院正式面向全球公开了后量子密码标准化的路线图，并在同年秋正式公布征集后量子密码系统建议的计划，其中包括公钥密码、数字签名以及密钥交换算法
  - 2017年11月30日，第一轮算法征集截止，并公布了69个候选算法

第五十九讲 后量子密码学

- 量子计算对密码学的威胁
- 后量子密码学的研究方向

后量子密码学的研究方向

- 基于Hash的签名体制
- 基于纠错码的公钥密码学
- 基于格的公钥密码学
- 多变量公钥密码学

基于Hash的签名体制

- 安全性：**Hash函数的安全性**
- 典型方案：**Merkle, R.C.: A certified digital signature. CRYPTO 1989**
- 优点：签名和验证签名效率较高
- 缺点：签名和密钥较长，产生密钥的代价较大
- 改进方案：
  - **Buchmann, J., Dahmen, E., Hulsing, A.: XMSS - a practical forward secure signature scheme based on minimal security assumptions. PQCrypto 2011**
- 挑战：有状态性和参数优化

基于纠错码的公钥密码学

- 安全性：任意线性码的译码问题是NP-完全问题
- 典型方案：
  - McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. DeepSpace Network Progress Report (1978)
  - Landais, G., Sendrier, N.: Implementing CFS. INDOCRYPT 2012.
  - Persichetti, E.: Secure and anonymous hybrid encryption from coding theory. PQCrypto 2013
- 优点：加解密效率高（McEliece），签名长度短(CFS)
- 缺点：密钥量大，签名效率较低（CFS）
- 挑战：降低密钥量，提高效率

基于格的公钥密码学

- 安全性：格中困难问题如最短向量问题(SVP)、最近向量问题(CVP)、learning with errors problem (LWE)和最小整数解问题 (SIS)
- 典型方案：
  - Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal gaussians. CRYPTO 2013
  - Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. ANTS 1998
  - Gentry, C.: Fully homomorphic encryption using ideal lattices. STOC 2009
- 优点：强安全性（允许最坏情形困难性规约到一般情形困难性）
- 缺点：参数较大
- 挑战：参数优化，效率提升

多变量公钥密码学

- 安全性：求解有限域上随机生成的多变量非线性多项式方程组是NP-困难的
- 典型方案：
  - Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. ACNS 2005.
  - Petzoldt, A., Chen, M.-S., Yang, B.-Y., Tao, C., Ding, J.: Design principles for HFEv- based multivariate signature schemes. ASIACRYPT 2015
- 优点：效率较高
- 缺点：公钥量大，安全性不确定
- 挑战：可证明安全的密码体制，降低密钥量

感 谢 聆 听!

xynie@uestc.edu.cn