Faster Algorithm for Solving Hard Knapsacks for Moderate Message Length

L. Jiang

2021 年 1 月 15 日

目录

1 介绍

本文我们将介绍多种加密算法：McEliee 加密算法 [1] ，RSA 加密算法 [2] ，ElGamal 加密算法 [3] ，ECC 加密算法 [4] 。

2 RSA 公钥加密算法

RSA 公钥加密算法 [2] 是 Rivest, Shamir, Adleman 三人于 1983 年设计的一种加密算法，此算法被证明能够在透明的通信信道中传输保密信息，也就是说允许通信双方在可能存在中间人窃听的非安全信道中通过 RSA 加密算法构建一个安全的通信信道。

3 McEliece 加密算法

McEliece 加密算法 [1] 是 McEliece 于 1978 年设计的。目前正在使用的主流公钥加密算法：RSA 和 ECC 均被证明可以通过 Shor 于 1994 年提出的 Shor 量子计算机算法 [5] 进行攻击。而 McEliece 加密算法具有抵抗量子计算机的能力。

参考文献

[1] R. J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory,” pp. 114–116, 1978. [Online]. Available: http://ipnpr.jpl.nasa.gov/progress{_}report2/42-44/44title.htm

[2] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 26, no. 1, pp. 96–99, 1983.

[3] T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 196 LNCS, no. 4, pp. 10–18, 1985.

[4] B. N. Koblitz, “Elliptic Curve Cryptosystems,” vol. 4, no. 177, pp. 203–209, 1987.

[5] P. W. Shor, T. B. Labs, M. Ave, and M. Hill, “Algorithms for Quantum Computation : Discrete Log and Factoring,” *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, p. 124, 1994.