密码学和复杂性理论

cryptology and complexity theories

G. Ruggiu

翻译：李晓峰 (cy_lxf@163.com)[*†]

V1.0

2023 年 10 月 24 日

摘要

复杂性理论最近被用来做为密码机性能评估的基础，与香农模型相比，在随机性概念上有新的亮点，但需要强调的是，统计学的观点仍然更加可靠。

复杂性理论最近被提出作为评估密码系统性能的基础。我们将在这个简短的调查中介绍用于连接这两个概念的不同方法。

复杂性理论是相当新的理论，其动机是分析算法的效率。它们的主要特点是它们是处理非常通用的算法的非常通用的理论：它们最具体的结果给出了关于算法的渐近行为的一些信息。

密码学的核心问题是对保密系统的安全性进行评估，即系统如何对密码分析免疫。当这种密码分析成为可能时，这种评估必须衡量破解方案所需的时间和信息。

I 香农模型

参考文献

1.C. SHANNON - Communication Theory of Secrecy Systems B.S.T.J. V o l . 28, October, 1949, p. 656.

[*]译者目前为北京联合大学智慧城市学院信息安全老师。

[†]译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT, 欢迎大家加入经典翻译项目，为更多的人能够获取这些经典文献所传递信息做一点贡献。

2.M. MACHTEY, P. YOUNG - An introductlon to the general Theory of algorrthms - North-Holland, 1978.

3.G. BRASSARD - A note on the complexlty of cryptography - I E E E Trans. on 1.". , Vol. IT-25,n0 2 , hrch 1979, p. 232.

4.W. DIFFIE, M. HELLEMAN - New directions in cryptography, I E E E TrdnS. on I.T.. V o l . IT-22, no 6, Sovember 1976, p. 644.

5.A . LEMPEL - Cryptoloqy in tr3nsition. Computinq Surveys, V o l . 11, n o 4, mcember 1979, p. 285 (Example. p. 300).

6.A . KOLMCGOROV - Thrre dppronchrs t o tht-. qudntitativr drfinition of information. Problemy Pecedaci Informacii 1 , 4-7, 1965.

7.G. CHAITIN - Alqorrthmlc Information Throry - IBM J. RPS. Drv. Vol. 21, July 1977， p.350.

8.T. FINE - Theories of Probability. Academic Press, 1973 (Chapter V) .

9.A. LEMPEL, J. ZIV - On the complexity o€ sequences - I E E E Trans. on I.T., Vol. IT-22, no 1. January 1976, p. 75.

10.E. FISHER - Measuring Cryptoqrahic performance with production Processes. Cryptologia, V o l . 5, no 3, July 1981, p. 158