概率加密*

作者：S Goldwasser，S Micali

译者：李晓峰, 北京联合大学智慧城市学院†

2022 年 9 月 8 日

摘要

介绍了一种新的数据加密概率模型。对于该模型，在适当的复杂度假设下，证明了对于具有多项式有界计算资源的对手来说，从密码文本中提取任何关于明文的信息平均来说是困难的。该证明适用于具有任何概率分布的任何消息空间。给出了该模型的第一个实现。在二次剩余模复合数因式分解是困难问题的假设下，证明了该实现的安全性。

*原文：Goldwasser S , Micali S . Probabilistic Encryption[J]. Journal of Computer & System Sciences, 1984, 28(2):270-299.

†译者 email：cy_lxf@163.com，译文来自于译者发起的“信息安全经典翻译”开源项目 https://gitee.com/uisu/InfSecClaT