基于 NTRU 与中国剩余定理的密文域可逆数据隐藏

张馨悦，赖昆义，唐鑫
国际关系学院网络空间安全学院，中国北京市，100091

摘要：基于同态加密的密文域可逆数据隐藏（RDH-ED）为隐私保护场景下的数据共享提供了极具前景的技术方案。然而，现有基于*N*次截断多项式环单元（NTRU）的方法面临嵌入容量与可逆性之间的根本冲突，通常需要对明文进行预处理，降低所获密文的随机性。针对上述问题，本文提出一种结合NTRU密码体制与中国剩余定理（CRT）的新型RDH-ED方案。该方案无需对明文进行预处理，并通过在密文域中构建多通道冗余，完整保留明文原始多项式结构。通过引入基于CRT的编码机制，单个多项式系数可承载多比特信息，在中等规模参数下，实现每多项式503比特的嵌入容量。同时，利用预先协商的互素参数，可在解密前完成嵌入信息的提取，从而提供更大的操作灵活性。严格的数学约束设计确保在解密过程中冗余项被自动消除，从而保证原始数据的无损恢复。实验结果表明，与现有基于NTRU、Paillier和ElGamal密码体制的主流RDH-ED算法相比，本文所提方案在不牺牲安全性或运行效率的前提下，显著提升了嵌入容量。

关键词：可逆数据隐藏；NTRU 密码体制；中国剩余定理；多通道冗余
https://doi.org/10.1631/ENG.ITEE.2025.0138