摘要

量子技术的进步正在威胁我们日常的网络安全。为迎接量子时代，很多国家都启动了抵抗量子计算机攻击的公钥加密方案和数字签名方案的征集工作。在征集到的方案中，基于编码的密码方案在其中占有重要地位。在报告中，我们将对基于编码的后量子密码方案的设计与安全性分析作简要介绍。