**doi:**10.1631/FITEE.1601849

**题目：**抗泄露的 CCA2 安全的无证书公钥加密机制

**概要：**近年来，存在密钥泄露环境下密码学机制的安全性成为该领域研究热点，一些能够抵抗泄露攻击的密码学原语相继被提出。由于现有相关构造中，抗泄露密码学原语无法保证其输出对于任意多项式时间敌手完全随机，因此敌手能够从相应抗泄露密码学原语的输出中获知密钥部分信息。为获得更佳性能，提出一个抗泄露的 CCA2 安全的无证书公钥加密机制，基于经典的判定性 Diffie-Hellman 假设证明了该方案的安全性。分析显示，对于任意敌手，该方案输出均完全随机，使得敌手无法从给出的密文中获知密钥相关信息；此外，该方案具有较高泄露率。由于这些良好特性，该方案在实际应用中具有广泛应用前景。

**关键词：**无证书公钥加密；泄露容忍；可证安全性；CCA2 安全性；判定性 Diffie-Hellman 假设