doi:10.1631/FITEE.1601054

题目：低计算复杂度的无证书混合签密方案

概要：混合签密是一种可以签密任意长度消息的重要技术。本文将无证书混合签密技术应用于椭圆曲线密码系统，构造了一个低计算复杂度的无证书混合签密方案。随机预言模型下，该方案在 ECCDH（elliptic-curve computation diffie-Hellman）被证明具有 IND-CCA2 （indistinguishability against adaptive chosen-ciphertext attacks）安全性，而且在 ECDL （elliptic-curve discrete logarithm）假设下具有 sUF-CMA （strong existential unforgeability against adaptive chosen-message attacks）安全性。分析表明该密码算法没有双线性对操作，比其他算法更高效。此外，它适合于资源受限的环境，比如无线传感器网络和 ad hoc 网络。

关键词：混合签密；标量乘；无证书密码系统；可证安全性