doi:10.1631/FITEE.1800434

题目：高效构造基于有限域上莫德尔椭圆曲线的密码置换盒

概要：椭圆曲线密码体制与其他密码体制相比有密钥小、安全性高等优点，被广泛应用于各种安全系统。在许多著名安全系统中，仅置换盒是非线性结构。最近研究表明，用动态置换盒代替静态置换盒可提高密码系统安全性，因此需构造新的安全置换盒。提出一种高效构造置换盒方法，该方法基于素数域上的一类莫德尔椭圆曲线，并通过定义不同总阶数实现。对于每个输入，该方法在线性时间与恒定空间内输出一个置换盒。因此，与现有基于椭圆曲线的置换盒生成方法相比，所提方法占用更少时间和空间。计算结果表明，所提方法能生成加密性强的置换盒，且其安全性与现有基于其他数学结构的置换盒相当。

关键词：密码置换盒；有限域；莫德尔椭圆曲线；总阶数；计算复杂度