一种用于 RSA 和 ECC 的高能效可重构非对称密码模运算单元

别梦妮[1]，李伟[1]，陈韬[1]，南龙梅[2]，杨丹阳[1]
[1]信息工程大学，中国郑州市，450001
[2]复旦大学专用集成电路与系统国家重点实验室，中国上海市，200000

摘要：RSA和椭圆曲线密码（ECC）)算法广泛应用于身份验证、数据安全和访问控制。本文分析了ECC和RSA算法基本操作并对模乘和模逆算法进行优化。提出一个具有混合内存单元和双乘加结构的可重构模运算单元，实现了非对称密码算法在运算单元层次的统一。采用55 nm CMOS标准工艺对模运算单元进行综合，该单元占用硬件资源437 801 μm^2，最高时钟频率可达588 MHz。所提模运算单元完成2048位RSA模乘和模逆功耗分别为21.92和23.36 mW，完成512位ECC双域模乘和模逆功耗分别为16.16 和15.88 mW。它比现有单一算法单元更高效、更灵活。与现有多算法单元相比，所提单元表现出更好性能。将所提模运算单元嵌入64位RISC-V处理器，可实现RSA和ECC的密钥生成、加解密以及数字签名功能。实验结果表明，所提设计在$G(p)$和$G(2^m)$上实现256位ECC点乘分别需要0.224和0.153 ms，实现1024位RSA求幂需要0.96 ms，满足高能效需求。

关键词：模运算单元；可重构；高能效
https://doi.org/10.1631/FITEE.2000325