

附件

提名项目情况表

项目名称		ZUC-256 算法国际化中的性能瓶颈技术突破研究	
提名等级		二等	
主要完成单位		兴唐通信科技有限公司、清华大学、国家密码管理局商用密码检测中心、中国科学院软件研究所	
主要创新点		1. 提出代流密码并行计算架构，提升 ZUC-256 算法的并行度。 2. 提出 MAC 生成算法按字操作等效计算的数学机理，结合指令特性完成并行化实现，突破 MAC 生成算法逐比特执行的效率瓶颈，性能提升 20 倍。 3. 提出算法特征驱动、路径延时感知的密码计算电路结构，实现不同运算负载与输入数据的计算均衡，提升 ZUC-256 算法的处理性能。	
完成人姓名	主要完成人贡献		主要排序
	1.提出项目总体研究方案，对项目整体创新也有贡献。		

4	白 亮	1.负责算法软件优化实现总体工作，对创新点 1、2 均有贡献； 2.研究非线性层并行实现方法，创新点 2 的主要贡献者； 3.在本项目投入工作量占本人总工作量的 40%。
---	-----	---

负责算法软件优化实现总体工作

- 主要成果：1.研究非线性层并行实现方法，创新点 2 的主要贡献者；
 2.在本项目投入工作量占本人总工作量的 40%。

负责算法软件优化实现总体工作

- 主要成果：1.研究非线性层并行实现方法，创新点 2 的主要贡献者；
 2.在本项目投入工作量占本人总工作量的 40%。

负责算法软件优化实现总体工作

1.负责算法软件优化实现总体工作，对创新点 1、2 均有贡献；

2.研究非线性层并行实现方法，创新点 2 的主要贡献者；

3.在本项目投入工作量占本人总工作量的 40%。

负责算法软件优化实现总体工作

1.研究非线性层并行实现方法，创新点 2 的主要贡献者；

2.在本项目投入工作量占本人总工作量的 40%。