附件

提名项目情况表

项目名称	ZUC-256 算法国际标准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. 提出代数特性分解方法和并行交错执行技术，实现数据操作与指令特性的高效融合，解决 ZUC-256 算法非线性层在通用处理器上的并行实现难题。 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。	
主要完成人		主要完成人贡献
排序	姓名	
1	刘雷波	1.提出项目总体研究方案，对项目整体创新均有贡献； 2.提出算法硬件优化实现的整体架构，创新点 3 的主要贡献者； 3.在本项目投入工作量占本人总工作量的 80%。
2	冯　程	1.负责跟进 3GPP 标准化动态和算法实现需求，细化算法实现要求，把控项目进度，对项目整体创新均有贡献； 2.研究通用处理器指令集，研究 S1 盒优化实现技术，创新点 1 的主要贡献者； 3.在本项目投入工作量占本人总工作量的 60%。
3	罗　鹏	1.负责研究算法特征，提出算法性能仿真评估方法，对项目整体创新均有贡献； 2.研究架构与电路性能评估方法，对创新点 3 有贡献； 3.在本项目投入工作量占本人总工作量的 40%。

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%。
5	朱　敏	1.负责算法硬件优化实现总体工作； 2.研究平衡数据通路关键路径的方法，对创新点 3 有贡献； 3.在本项目投入工作量占本人总工作量的 30%。
6	贾文义	1.参与算法软件实现优化工作； 2.研究 MAC 并行实现方法，对创新点 2 有贡献； 3.在本项目投入工作量占本人总工作量的 30%。
7	张　斌	1.作为 ZUC-256 算法主要设计人员，指导优化实现工作； 2.参与软硬件优化实现的方法设计，对创新点 1、2、3 均有贡献； 3.在本项目投入工作量占本人总工作量的 30%。
8	杨锦江	1.参与算法硬件优化设计具体实现； 2.研究模加法器设计及运算路径优化，对创新点 3 有贡献； 3.在本项目投入工作量占本人总工作量的 20%。
9	李　冬	1.参与算法性能评估方案设计，对创新点 2、3 有贡献； 2.在本项目投入工作量占本人总工作量的 20%。
10	徐　晖	1.作为算法标准化推进工作的主要参与者，对所有创新点均有贡献； 2.研究通用指令集的特性，对创新点 1 有贡献； 3.在本项目投入工作量占本人总工作量的 20%。