基于 FPGA 的资源节约型结构 PRINCE 的实现

李浪[1,2,3]，冯景亚[1,2]，刘波涛[1,3]，郭影[1,3]，李秋萍[1,3]
[1]衡阳师范学院智能信息处理与应用湖南省重点实验室，中国衡阳市，421002
[2]湖南师范大学信息科学与工程学院，中国长沙市，410081
[3]衡阳师范学院计算机科学与技术学院，中国衡阳市，421002

摘要：在当今普适计算时代，低资源设备已广泛部署在各个领域。PRINCE是一种专为低延迟设计的轻量级分组密码，适用于普适计算应用程序。本文通过共享和简化逻辑电路为PRINCE组件提出新的电路结构，以达到使用较少逻辑门获得相同效果的目标。基于组件新的电路结构和组件之间的最佳共享，提出3种新的PRINCE硬件架构，并在不同可编程门阵列设备上对3种硬件架构进行仿真和综合。基于Virtex-6平台的实验结果表明，与现有架构相比，展开、低成本和两周期架构的资源消耗分别减少73、119和380个可编程逻辑单元。低成本架构仅需137个可编程逻辑单元。展开架构需409个可编程逻辑单元，其吞吐量为5.34 Gb/s。据我们所知，对于PRINCE的硬件实现，所提低成本架构具有更低资源消耗，且所提展开架构具有更高吞吐量。因此，所提架构具有更高资源效率，适用于低资源、低延迟的应用程序。

关键词：轻量级分组密码；现场可编程门阵列（FPGA）；低成本；PRINCE；嵌入式安全
https://doi.org/10.1631/FITEE.2000688