基于现场可编程门阵列的不同数据路径架构ANU轻量级密码的设计与实现

Vijay DAHIPHALE[1], Gaurav BANSOD[1], Ankur ZAMBARE[1], Narayan PISHAROTY[2]
[1]浦那计算机技术学院，印度浦那，411043
[2]Iziel医疗私人有限公司，印度浦那，411028

摘要：自物联网（IoT）诞生以来，数据与系统安全一直是开发者关注的重点。由于大多数物联网设备在8位控制器上运行，其容量和计算力有限，因此需要使用轻量级密码在发送端和接收端分别进行加密和解密。提出用于ANU密码硬件实现的新架构，并给出每一架构的相关结果。在相同实施条件下，在4种不同现场可编程门阵列（FPGA）上分别以4位、8位、16位和32位的数据路径尺寸实现ANU密码，并比较每一性能指标。与以往ANU密码架构不同，新架构具有用于高吞吐量和硬件优化的并行替换盒（S盒）。通过不同数据路径设计，在资源极其有限的系统中，ANU密码被证明是实现安全性的最佳选择。

关键词：轻量级密码；物联网（IoT）；嵌入式系统安全；加密；现场可编程门阵列；数据路径设计
https://doi.org/10.1631/FITEE.1800681