**doi:** 10.1631/FITEE.1500415

**题目：**BORON：面向普适计算的超轻量低功耗加密设计

**概要：**我们提出一种超轻量，紧凑且低功耗的分组密码：BORON。BORON 是一种替换、互换网络，运行于 64 位纯文本上，支持 128 位或 80 位密钥长度。针对 128 位密钥和 80 位密钥，BORON 的紧凑结构分别需要 1939 个和 1626 个等效门（gate equivalents, GE）。BORON 包含移位、循环移位和异或操作。其的独特设计有助于在较少的回合内产生大量的活动 S-box，从而挫败针对加密的线性或差分攻击。BORON 在硬、软件平台上均具有较好的性能。与轻量加密 LED 相比，BORON 具有更低的功耗水平；与现有 SP 网络加密相比，BORON 具有更高的吞吐量。本文还展示了 BORON 的安全性分析及其作为超轻量紧凑型加密的性能。BORON 可适用于将引脚面积和功率耗散作为关键参数的应用。

**关键词：**轻量密码；SP 网络；分组密码；物联网；加密；嵌入式安全