轻量级分组密码 PRESENT

1 PRESENT

1.1 加密算法

1.2 解密算法

1.3 密钥扩展算法

2 软件实现

2.1 基本实现

2.2 一个分组并行实现

2.3 64 分组并行

代码

[1] 基本实现：https://github.com/michaelkitson/Present-8bit
[2] 分组内部并行：https://github.com/bozhu/PRESENT-C
[3] 分组之间并行：https://github.com/pfasante/present
[4] https://github.com/pfasante/present 给出了几种实现方式