| Simon Speck Rectangle | | |
|---|---|---|
| 时间 | 作者 | 说明 |
| 2015.09.09 | 包珍珍<br>罗鹏 | ● Simon、Speck 在 CTR 下的计算方法都是将两个 block 展开 |
| 2015.09.18 | — | — |
| 2015.10.06 | 罗鹏 | ● 轮内循环控制从加密、加密中独立出来计算<br>● 细化 Simon、Speck 密钥编排、加密、解密指令 |
| 2015.11.13 | 包珍珍<br>罗鹏 | ● 09.09 日的版本中两个 block 是展开计算的，这次统一使用循环加密两个 block 的方法计算<br>● 包珍珍对 Rectangle 的密钥编排做了优化，在 Scenario1 中可以减少了 50 bytes 的 RAM |

**Simon Speck for Triathlon**

| | | Simon | Speck |
|---|---|---|---|
| CBC | RAM(bytes) | 320 = 128 + 160 + 16 + 8 + 8 | 280 = 128 + 108 + 16 + 8 + 12 + 8 |
| | Flash(bytes) | 558 = 8 + 550 | 560 |
| | Time(cycles) | 64880 | 44264 |
| CTR | RAM(bytes) | 24 = 16 + 8 | 24 = 16 + 8 |
| | Flash(bytes) | 364 = 176 + 188 | 294 = 108 + 186 |
| | Time(cycles) | 4181 | 2563 |

# Scenario1

- Simon
  - 320 = 128plaintext, 160extend round keys, 16master keys, 8init vector, 8temp data in decryption;
  - 558 = 8round constants, 550(EKS, ENC, DEC code)
  - 64880 = (4253-803) + (34722-4263) + (65703-34732)
- Speck
  - 280 = 128plaintext, 108extend round keys, 16master keys, 8init vector, 12L in key schedule, 8temp data in decryption;
  - 560 = (EKS, ENC, DEC code)
  - 44264 = (4300-792) + (22928-4310) + (45076-22938)

# Scenario2

- Simon
  - 24 = 16plaintext, 8counter;
  - 364 = 176round keys, 188(ENC code)
  - 4181 = (4331-150)
- Speck
  - 24 = 16plaintext, 8counter;
  - 294 = 108round keys, 186(ENC code)
  - 2563 = (2713-150)