Simon Speck for Triathlon

		Simon	Speck
CBC	RAM(bytes)	320 = 128 + 176 + 8 + 8	264 = 128 + 108 + 8 + 8 + 12
	Flash(bytes)	556 = 8 + 548	512
	Time(cycles)	64929	44126
CTR	RAM(bytes)	24 = 16 + 8	24 = 16 + 8
	Flash(bytes)	492 = 176 + 316	420 = 108 + 312
	Time(cycles)	4171	2553

1) CBC mode
   a) RAM：明文，轮密钥，初始向量 vector，解密保存临时密文，密钥扩展辅助数据 L(Speck 用到)；
   b) Flash：
      - 数据：**不包括明文，主密钥，初始向量 vector，直接对 RAM 中的数据进行初始化**；包括常量(Simon 中的 Z)；
      - 代码：密钥扩展，加密，解密代码总量；
   c) Time：密钥扩展，加密，解密时间之和；

2) CTR mode(没有 nonce，没有密钥扩展、解密部分)
   a) RAM：明文，计数器 counter
   b) Flash：
      - 数据：**只包括轮密钥，直接对 RAM 中明文和计数器进行初始化**；
      - 代码：加密的代码；
   c) Time：加密的时间；

Triathlon 和设计者评价指标比较

1) 设计者只对一个 block 进行加密；
2) 设计者的方法不包括解密；
3) **设计者方法中明文和密文是分开保存在 RAM 中；Triathlon 的加密后密文覆盖明文，解密后明文覆盖密文；**
4) **设计密钥扩展时，设计者的主密钥存放在 Flash 中，初始化时加载到 RAM；Triathlon 直接在初始化代码中将主密钥写入 RAM；**
5) Triathlon 的 RAM 中存在主密钥 masterKey 和轮密钥 keys（包括主密钥），masterKey 初始化完成，轮密钥在扩展时先进行主密钥的复制，再扩展。实际上就是 masterKey 存了两次，这样可以更好地保证 masterKey 不会被修改，但是多消耗了 RAM。