项目 \ 方法			Triathlon		Simon and Speck
			128 bytes CBC	128 bits CTR	1 byte(With Key Schedule)
初始化		明文	×	×	×
		轮密钥 keys	×	—	×
		Simon 常量 Z	×	—	×
		向量 vector	×	—	—
		计数器 counter	—	×	—
RAM		加密数据	√	√	√
		轮密钥 keys	√	—	√
		向量 vector	√	—	—
		保存密文 tempCipher	√	—	—
		计数器 counter	—	√	—
		辅助数据 L(Speck 密钥扩展)	√	—	√
Flash(data)		Simon 常量 Z	√	—	√
		初始密钥 masterKey	√	—	√
		随机数 nonce	—	√	—
		轮密钥 keys	—	√	—
Flash(code) Time	密钥扩展	密钥扩展	√	—	√
	加密	加载向量 vector	√	—	—
		明文异或向量 vector	√	—	—
		加载计数器 counter	—	√	—
		加载随机数 nonce	—	√	—
		异或随机数 nonce	—	√	—
		计数器 counter 自增	—	√	—
		加密计数器 counter	—	√	—
		明文异或 counter	—	√	—
		加载明文	√	√	√
		明文加密	√	—	√
		密文写回	√	√	√
		循环控制	√	√	√
	解密	加载向量 vector	√	—	—
		加载密文	√		
		保存密文	√		
		解密	√		
		异或向量 vector	√		
		更新 vector	√		
		写回明文	√		
		循环控制	√		

说明：

1) Simon Speck 设计者在 AVR 上的实现方法有多种，有的有密钥扩展有的则没有。为了统一，对 Simon 和 Speck 做下述约定：包含密钥扩展，只加密一个 block 但没有循环展开，不包含解密；
2) 符号说明

√表示方法包含指定的项目并且资源消耗计算在内；
×表示方法包含指定项目但资源消耗不计算在内，只存在于初始化的部分；
—表示方法不包含指定项目；