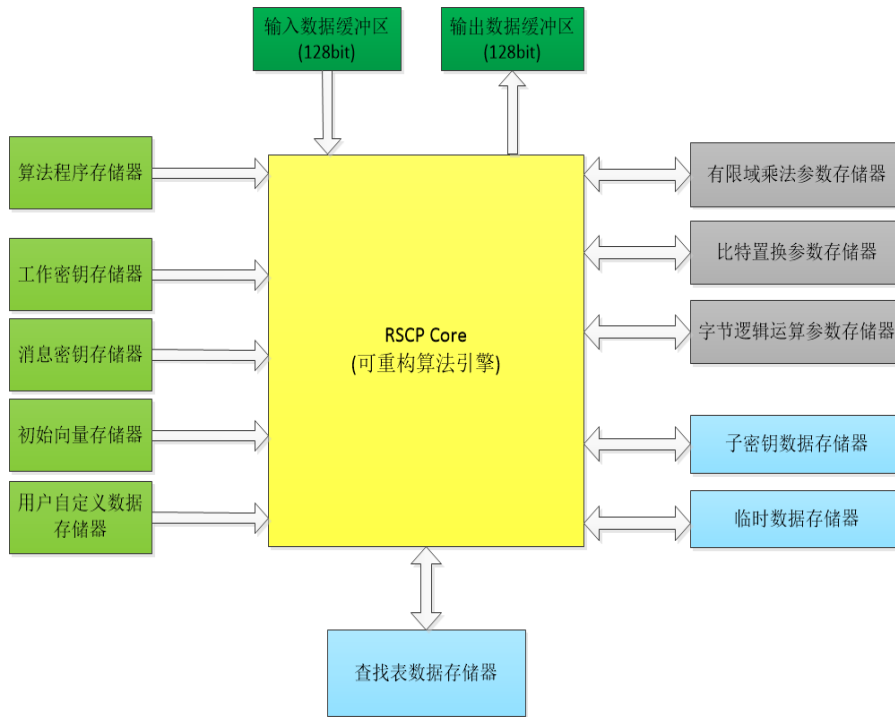


可重构算法引擎

概述

RSCP (Reconfigurable Symmetric Cryptography Processor) 是一种用于对称加密算法的专用指令集处理器。它具有哈佛架构，有独立的指令总线 and 数据总线。利用 C*Core 提供的对称密码指令集，RSCP 可以实现大多数分组密码算法、散列算法和流算法。



框架图

算法特征

- 集成对称算法专用 256 位指令集
- 哈佛体系结构，支持独立数据总线和指令总线。
- 通过编程，支持绝大多数非公钥算法：
- 分组密码算法
- 流密码算法
- 杂凑密码算法
- 支持 15 大类密码指令，并可根据应用需求快速定制或删减指令
- 可独立运行，或与 SEC 紧耦合
- 支持算法程序安全存储

算法性能

- 工艺：SMIC40LL
- 面积：1mm² 全功能（包含特殊加速支持）

- 基本功能: 0.5mm²
- 时钟频率: 400MHz
- 功耗: 120mW