life.augmented

STM32 生态系统 第十六期

信息安全 . Information Security

07. STM32的加解密硬件模块

2020.03

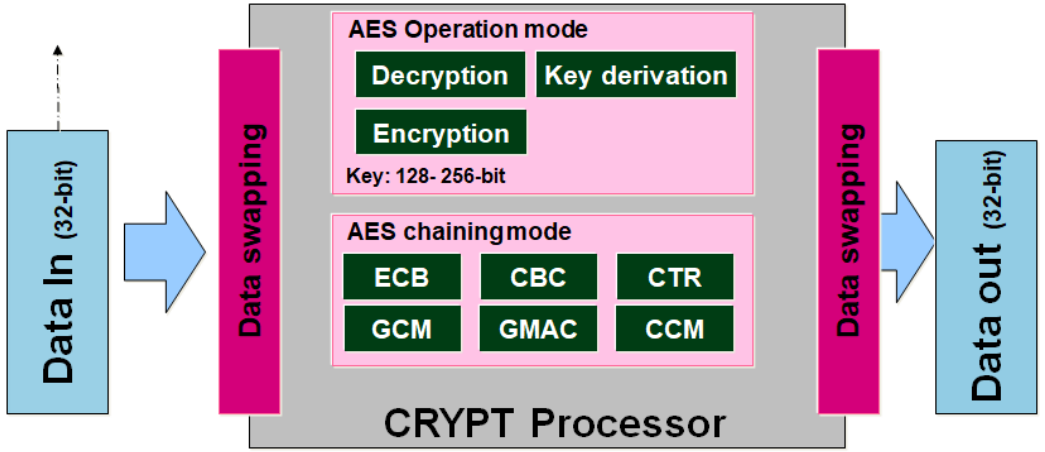
STM32的真随机数产生器 TRNG

- 基于物理噪声源的随机数产生器
- 生成32位随机数
- AHB 从设备，不使用时可关闭它以节省功耗
- 广泛运用于加解密算法和协议中
  - 密钥的生成
  - “Challenge- Acknowledge”认证模式中，充当Challenges（质询 ）
  - 初始向量（IV）
  - 随机数（Nonce）
  - …

life.augmented

STM32的对称加解密加速器 AES

- **支持的算法模式有**
  - AES – ECB、CBC、CTR
  - AES – GCM、CCM、GMAC
  - 密钥长度：128位，256位可选
- **支持DMA加载输入和读取输出**
- 该模块经过NIST FIPS认证
- **集成**该对称加解密硬件加速模块的**STM32系列有**

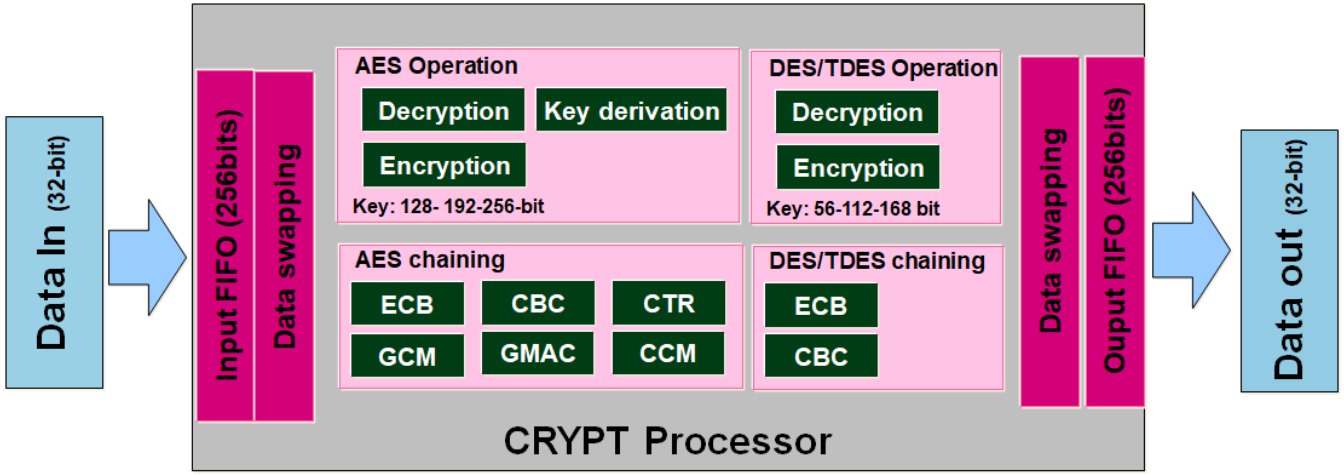


- STM32F423
- STM32F730-732-733
- STM32L021-041-062-063-081-082-083
- STM32L162
- STM32L422-442-443-462-485-486-4a6-4s5-4s7-4s9
- STM32L562
- STM32G041-081
- STM32G441-483-484
- STM32WB50-W55

life.augmented

STM32的对称加解密加速器 Crypto

- **支持的算法模式有**
  - DES/TDES – ECB、CBC
    - 密钥长度：标准56位 + 8位检验
  - AES - ECB、CBC、CTR
  - AES – GCM、CCM、GMAC
    - 密钥长度：128位，192位、256位可选



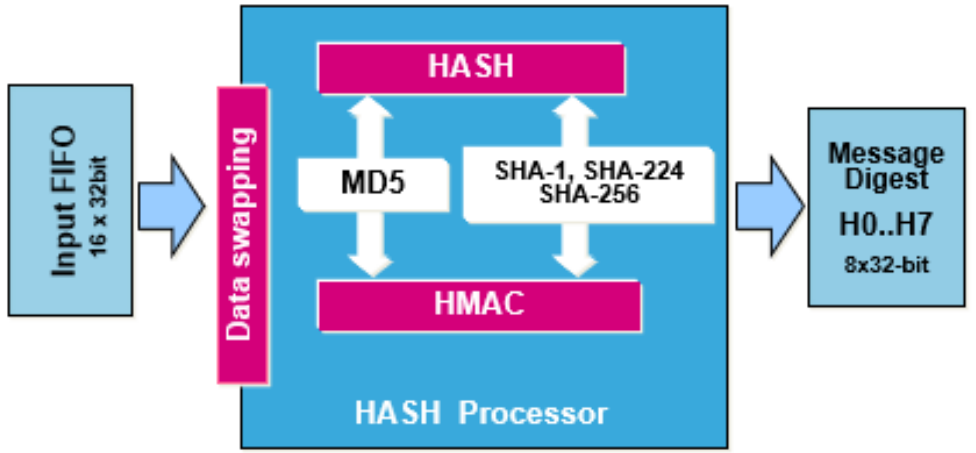
- **支持DMA加载输入和读取输出，8字深度FIFO**
- 该模块经过NIST FIPS认证
- **集成**该对称加解密硬件加速模块的STM32**系列有**

- STM32F215-217
- STM32F415-417-437-439-479
- STM32F750-756-777-779
- STM32H750-753-755-757

life.augmented

STM32的哈希模块 Hash

- 支持的哈希算法有
  - SHA-1， SHA-224， SHA-256
    - 消息摘要160位、224位、256位，可配置
    - 符合FIPS PUB 180-4标准
  - MD5
    - 消息摘要160位
    - 符合IETF RFC 1321标准
- 支持HMAC消息认证
  - 符合IETF RFC 2104 和 FIPS PUB 198-1标准
- 集成该哈希硬件加速模块的STM32系列

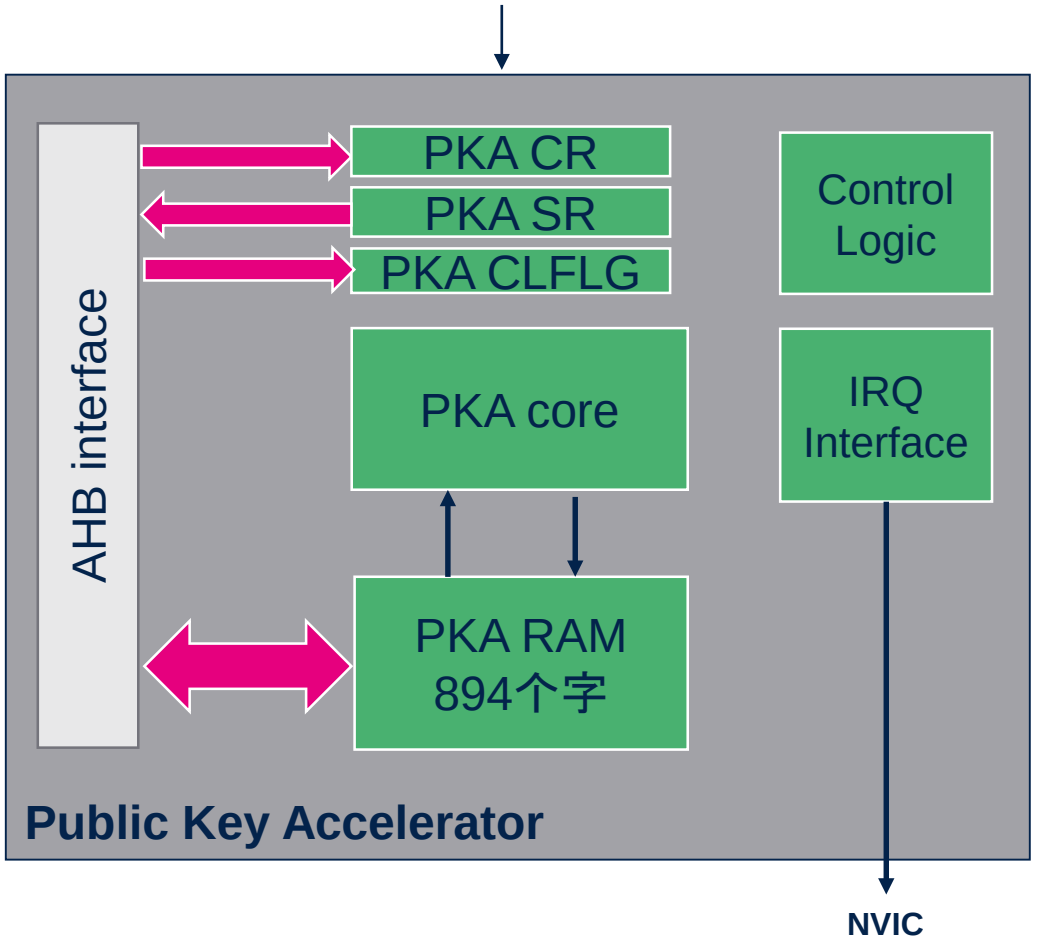


- STM32F214-217
- STM32F415-417-437-439-479
- STM32L4A6-4S5-4S7-4S9
- STM32F750-756-777-778-779
- STM32H750-753-755-757

life.augmented

STM32的非对称加解密加速器 PKA

- 支持的密钥长度
  - RSA – 3136位
  - ECC – 640位
- PKA可以对以下功能加速
  - RSA加密、解密
  - DSA和ECDSA签名和验签
  - DH和ECDH密钥交换
- 集成PKA加速器的STM32有
  - STM32WB、STM32L5



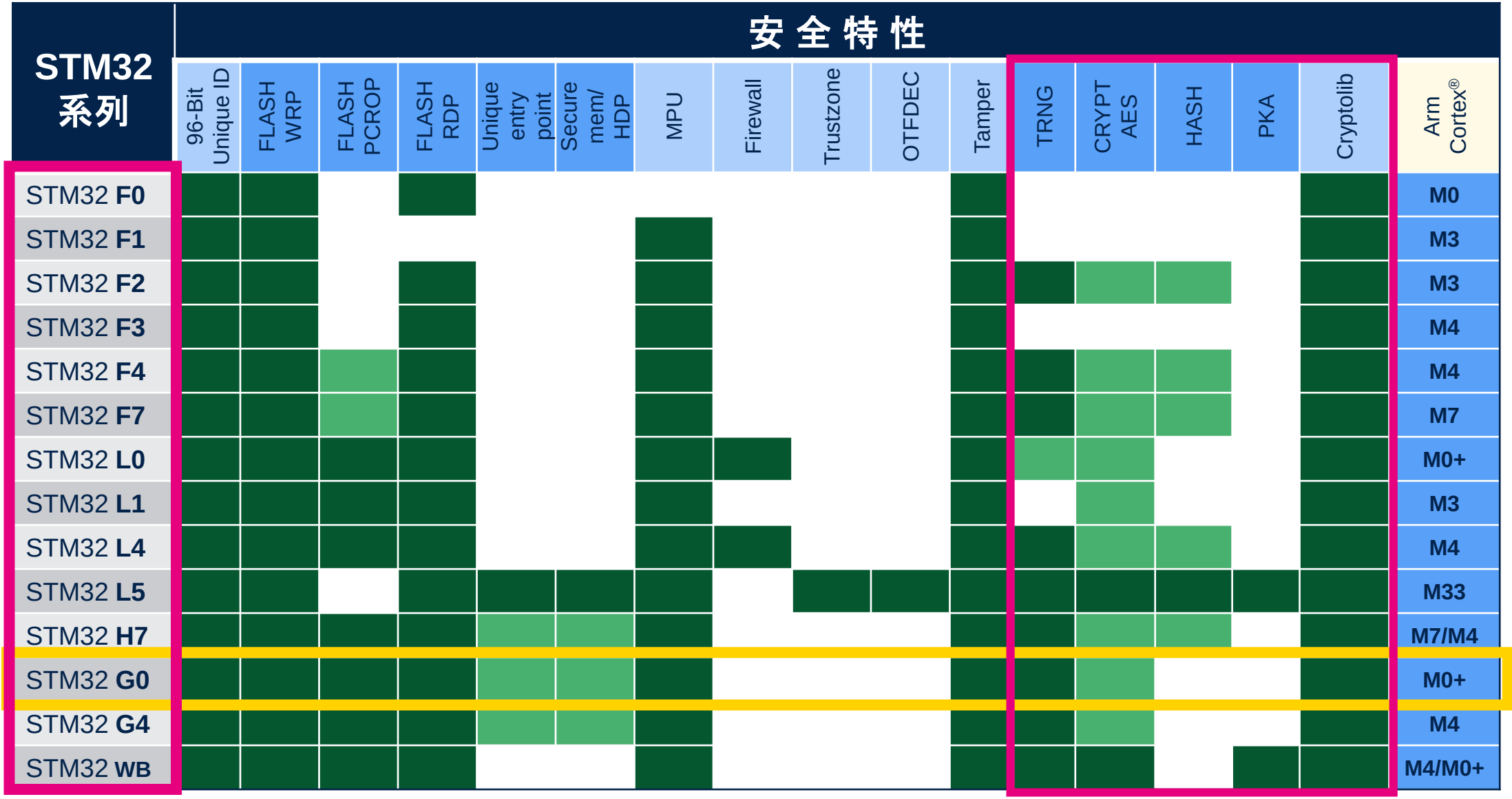
life.augmented

STM32加解密库 X-Cube-Crypto

- **支持所有主流加密、哈希、消息**认证和数字签名算法
  - **包含**软件实现，可运行在**STM32全系列芯片上**
  - ST发布库文件，用户调用**API使用**
    - **基于**Cortex-M0、M0+、M3、M4、M7
    - IAR、KEIL、RCC
    - **支持两种**优化模式：运行速度、存储消耗
  - **支持STM32上的RNG、AES和Crypto加速模**块
- 经过CAVP FIPS认证，无需再额外对算法
  - 认证，加速客户的安全认证过程

所有系列都有　　取决于产品型号

从产品系列来看 加解密模块



life.augmented

本期回顾

- **STM32加解密硬件模块**

  TRGN

  AES、Crypto

  Hash

  PKA

- **STM32加解密库**

  X-Cube-Cypto

  支持软硬件实现

谢　谢

life.augmented