# 产品特征

**CPU**

- ✓ 高性能 32 位 ARM 内核
- ✓ 三级流水线
- ✓ 小端模式
- ✓ 系统时钟可配置
  - 内部时钟：内部 OSC 时钟最高 30MHz
  - 外部时钟：接触界面时钟

**存储器**

- ➢ FLASH
  - ✓ 容量：256 KB
  - ✓ 页面大小：512 Byte
  - ✓ 擦写方式：页擦字节写
  - ✓ 擦写时间：擦时间可配，写 50μs
  - ✓ 比特逻辑值：擦除后为 1b，写 0b 后为 0b
  - ✓ 存储用途：数据及程序存储
- ➢ RAM
  - ✓ 容量：13 KB
    - 9 KB，CPU 数据区
    - 4 KB，加密协处理器数据区，CPU 可访问
- ➢ OTP
  - ✓ 一次编程存储器，存储产品唯一序列号，用户只读

**算法及外设**

- ➢ 对称算法
  - ✓ DES/TDES 算法引擎
  - ✓ SM1
  - ✓ SSF33
  - ✓ SMS4
- ➢ 非对称算法
  - ✓ RSA（CCP）
  - ✓ ECC（CCP）
  - ✓ SM2（CCP）
- ➢ 摘要算法
  - ✓ SHA1（CCP）
  - ✓ SM3 （CCP）
- ➢ 外设
  - ✓ CRC 引擎：16-bit CRC-CCITT
  - ✓ TRNG：随机数发生器
  - ✓ 加密协处理器 CCP
  - ✓ DMA：数据拷贝和数据比较
  - ✓ 3 个通用定时器/计数器，1 个 ETU 定时器

**对外接口**

# THK88-27

# USB KEY 芯片

**256 KB FLASH**

**13 KB RAM**

**Beta**

- USB 接口
  - ✓ USB device 控制器，支持 USB 全速
  - ✓ 满足 USB IF Full Speed Low Speed Electrical and Interoperability Compliance Test Procedure 要求的电气兼容性
- ISO/IEC 7816 从接口
  - ✓ 支持 T=0/T=1 协议
  - ✓ 支持 11 种波特率：F/D = 11H，12H，13H，18H，91H，92H，93H，94H，95H，96H，97H
  - ✓ 硬件自动发送 3BH
  - ✓ 支持 DMA
  - ✓ 专用 ETU Timer 用于发 60H
- ISO/IEC 7816 主接口
  - ✓ 支持 T=0/T=1 协议
  - ✓ 支持 10 种波特率：F/D = 11H，12H，13H，18H，91H，92H，93H，94H，95H，96H
  - ✓ 支持 DMA
  - ✓ 支持 3 路从接口
- SUART 接口
  - ✓ 硬件 SUART 控制器
  - ✓ 符合标准的异步串行通讯协议
  - ✓ 支持 DMA
  - ✓ 支持常用波特率：9600， 19200，38400，57600 等
- SPI 主/从接口
  - ✓ 支持 SPI/SDI/SQI 模式通信
  - ✓ 支持 DMA
  - ✓ 主接口通信速率可设
- I2C 主接口
  - ✓ 主接口通信速率可设
- PWM 接口
  - ✓ 支持任意方波输出
  - ✓ 支持 USBPHY/IO 捕获功能
- 键盘
  - ✓ 硬件实现键盘扫描，最大兼容 5*5 阵列键盘
- GPIO：
  - ✓ 27 个 I/O 端口
  - ✓ GPIO 可产生中断，可唤醒芯片

**安全性**

- 环境监测电路
  - ✓ 高/低电压检测
  - ✓ 高/低频率检测（针对 7816 时钟及晶体时钟）
  - ✓ 温度检测
  - ✓ 电源毛刺检测
  - ✓ 光检测
  - ✓ 过流保护
  - ✓ 主动屏蔽层

- 对抗 SPA/DPA 攻击
- 看门狗电路
- 数据双备份
- 内存加密存储
- 总线加密传输
- 随机时序，随机噪声

**工作参数**

| 符号 | 中文名称 | 条件 | 最小 | 典型 | 最大 | 单位 |
|---|---|---|---|---|---|---|
| TMEccp | 模幂运算耗时，使用 CCP 加密引擎 | 1024-bit,48MHz，带 CRT | | 50 | | ms |
| TKG | RSA 密钥生成时间 | | | 2.0 | | s |
| TSE | Sector 擦时间（注 1） | | 1 | | 4 | ms |
| TBP | Byte 写时间 | | 38 | 50 | 63 | μs |
| TDR | 数据保持时间 | | 10 | | | year |
| NSE | 页面擦写次数 | | 100 k | | | cycle |
| fEXT | 外部时钟频率 | | 1 | | 5 | MHz |
| fINT | CPU 及硬件模块时钟频率 | | 3.75 | | 30 | MHz |
| fCCP | CCP 协处理器时钟频率 | | 6 | | 48 | MHz |
| VCC | 电源电压 | | 2.7 | | 5.5 | V |
| IUSB | USB 工作电流 | | | 10 | 30 | mA |
| Isuspend | USB Suspend 状态电流 | | | 400 | 500 | μA |
| ICC7816 | 7816 模式工作电流 | VCC= 5.0V | | 10 | 30 | mA |
| | | VCC= 3.0V | | 10 | 30 | mA |
| ISB7816 | 7816 模式静态电流 | VCC= 5.0V | | 300 | 500 | μA |
| | | VCC= 3.0V | | 300 | 500 | μA |
| TAMB | 环境温度 | | -25 | | 85 | °C |

注 1：使用快擦方式

# 产品描述

THK88-27 是基于 ARM 内核的 32 位 USB KEY 控制器安全芯片。

芯片具有存储器保护单元（MPU），对存储器的访问权限进行保护；程序和数据共享 256KB FLASH 存储器。COS 开发者可灵活划分程序空间和数据空间大小及权限。

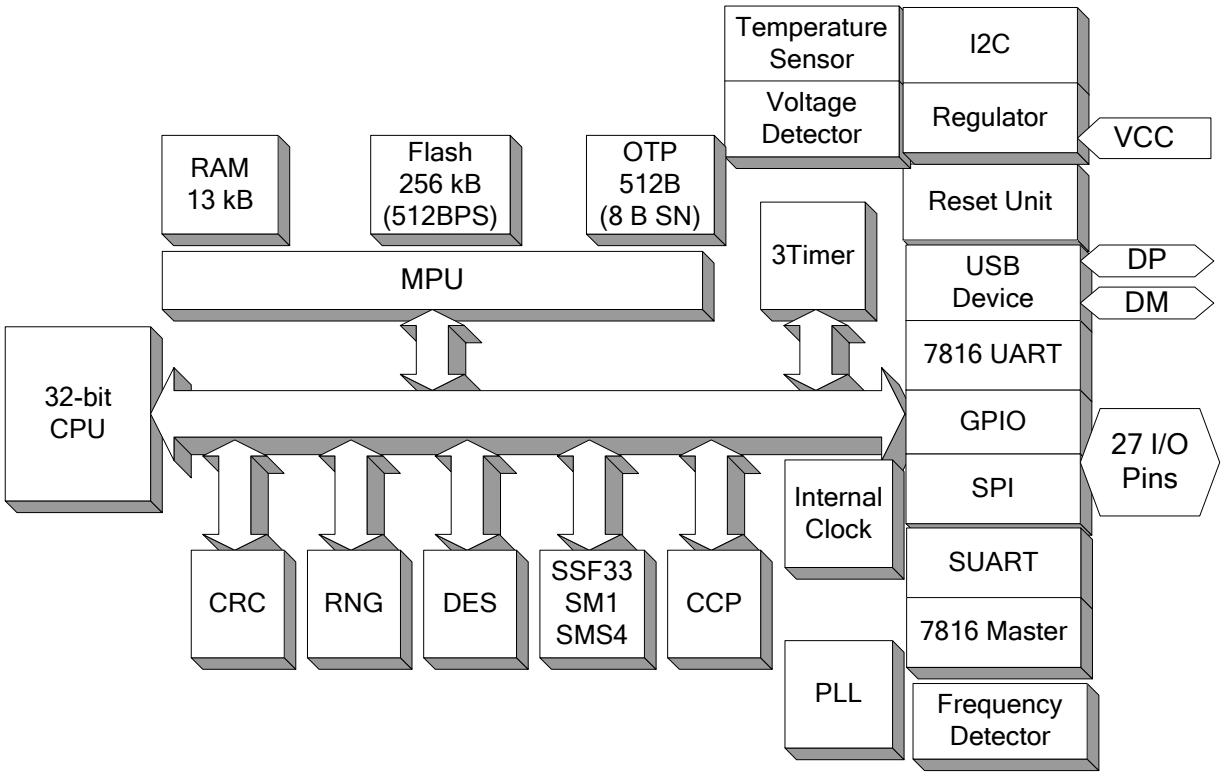
芯片内部硬件实现了国家商用密码产品所需的 SSF33、SM1 和 SMS4 算法专用加密模块、DES/3DES 加密模块。芯片提供 32 位硬件加密协处理器 CCP，可用于实现多种公钥算法及摘要算法如 RSA、ECC 或 SM2。芯片内嵌 32 位真随机数发生器 RNG，可满足 COS 开发者的密码学应用，可节约软件开销，提高软件实现效率。

芯片拥有丰富的对外接口，包括 USB Device 控制器，可支持 USB Full Speed 通信模式；3 组独立 7816 从接口及 1 组独立 7816 主接口，可实现 T=0 和 T=1 协议，支持多种通信速率；硬件 SPI 主/从模块、SUART 模块、I2C 模块、PWM、键盘扫描以及 27 个 GPIO 端口。

芯片不但有 MPU 进行保护，还提供了包括电压检测、频率检测、光、温度等机制，存储器冗余校验、加密存储机制；以对抗 SPA/DPA 攻击、物理攻击、剖片探测等。

THK88-27 是高性能、低功耗、具有丰富的内部协处理器和对外接口的安全芯片，可以作为智能密码钥匙 USB key、支付终端或者读卡器使用，用于国家商用密码专用算法应用、网络银行应用、家庭/个人支付、城市一卡通应用等对信息安全有较高要求的应用场合。

**产品架构图**




## 开发工具

- ✓ SCDS 系列硬件仿真器
- ✓ ULINK2 仿真器及目标板
- ✓ Demo 工程及 API（应用程序接口）示例代码
- ✓ 密码学算法库，包括 RSA、ECC、SM2、SM3、SHA1 等算法，开发者可直接调用
- ✓ 芯片的用户手册和应用笔记等
- ✓ DVG 及 VTP 软件工具，用于生成和下载 COS 脚本。

## 封装和管脚定义

封装：

| 封装形式 | 备注 | 应用领域 |
|---|---|---|
| Wafer | 8-inch | Any |
| COB | - | Any |
| SSOP28\QFN40\QFN48 | - | Any |

# 重要提示

本文档仅能以电子邮件加密附件形式提供有资质客户(个人或组织)，其官方电子邮件地址或企业名称已被水印于文档中权作签名之用。北京同方微电子有限公司保留对其他非法传播方式诉诸法律的权利。

北京同方微电子有限公司保留在无需声明前提下更新产品规格书及本文档的权利，客户可以通过联系本文档技术支持以获取产品规格书及文档的最新版本。由于本文档所描述之信息而引起的损失、损害及其他任何责任问题，北京同方微电子有限公司将不承担任何责任。

北京同方微电子有限公司建议将本文档所描述产品用于其设计的应用场景，在判断该产品是否适用之前，请仔细评估。对于特殊使用，包括但不限于航空、航天、军工、医疗以及生命维持系统，北京同方微电子有限公司无法保证适用性，不承担任何责任。

本文档不能作为知识产权(包括但不限于专利、商标、软件著作权)的授权依据。

# 联系我们

北京菱电创新科技有限公司
地　　址：北京市海淀区知春路132号805室
邮　　编：100086
电　　话：+86-10-82674978
传　　真：+86-10-62547616
电子邮件：kovintan@163.com