

智能世界 安全互联

上海爱信诺航芯电子科技有限公司

Shanghai Aisinochip Electronics Technology Co.,Ltd.

上海爱信诺航芯电子科技有限公司

地址：上海市闵行区合川路2570号科技绿洲三期二号楼702

电话：021-61259080

网址：www.aisinochip.com

公司微信账号



## 公司概况

上海爱信诺航芯电子科技有限公司成立于2008年1月，是行业领先的集成电路设计高新企业，主要从事安全和MCU芯片的研制，以服务社会、推动自主密码应用为己任，实现信息化系统的自主可控，量产的多规格系列化芯片在车联网、人工智能、物联网、工业控制、视频监控、智能识别、金融支付、电子政务等领域得到广泛应用。公司股东中有国家大基金、航天信息、小米长江产业基金等知名机构。

公司坚持自主研发，取得了一系列具有自主知识产权的成果和产品，在核心架构、算法实现和系统集成等方面拥有多项核心技术专利，并通过了高密二级、EAL4+、EAL5+、AEC-Q100等认证，并获得了中国芯最佳市场表现产品和中国芯最具投资价值企业等一系列荣誉。

## 荣誉资质

- 国家密码科技进步奖
- 上海市科技进步奖
- 国家高新技术企业
- 国家集成电路设计企业
- 国家软件企业
- 上海市科技小巨人企业
- 上海市专精特新企业
- 上海产学研合作优秀项目一等奖
- 上海市高新技术成果转化百佳
- 中国芯最佳市场表现产品奖
- 国家商用密码产品生产定点单位
- 国家商用密码产品销售定点单位
- 上海市专利工作试点企业
- 中国芯最具投资价值企业

AisinoChip

2008

1月公司成立  
9月首款芯片量产

2009

国密产品  
生产定点单位

2011

首次通过EAL4+  
安全认证

2014

起草密码行  
业标准

2017

首款55nm芯片  
量产

2018

通过EAL5+安全认证

2020

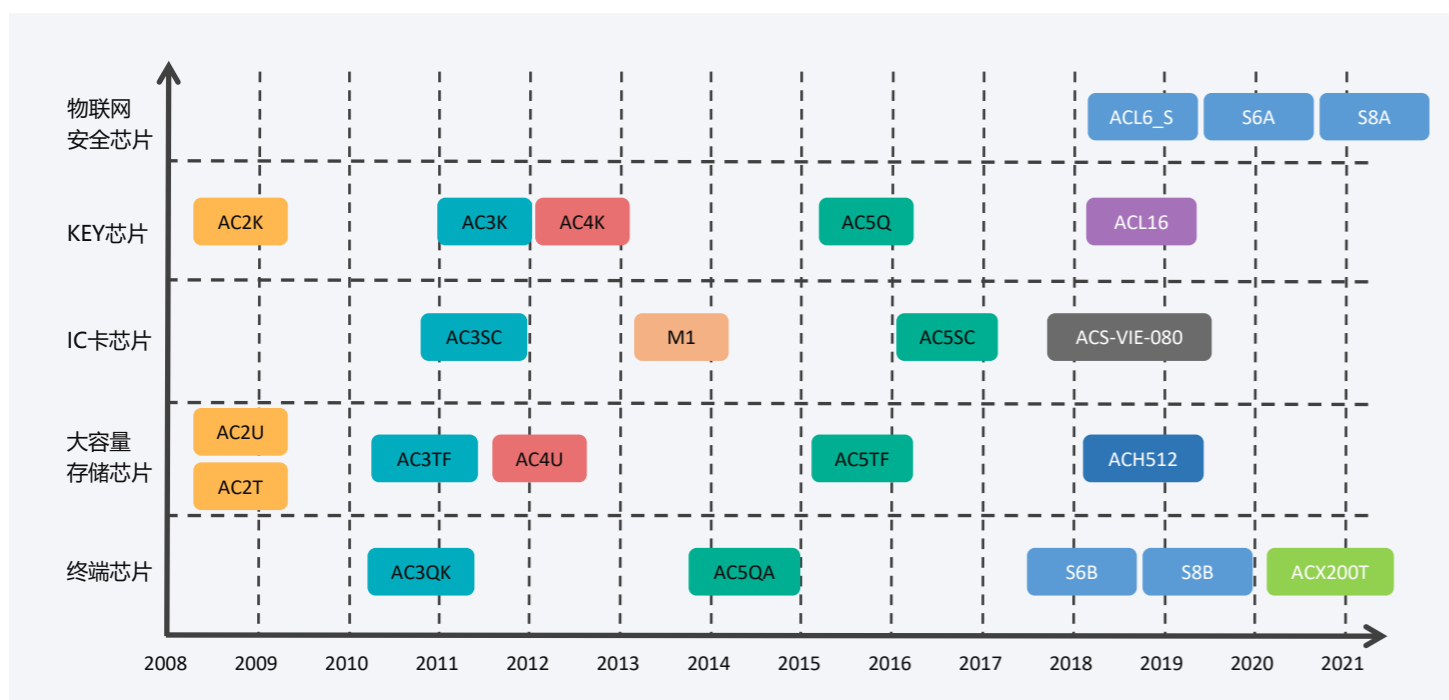
通过AEC-Q100  
车规认证

2021

获得小米长江产业  
基金投资

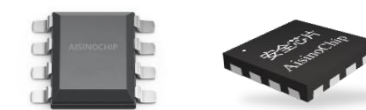
## 安全芯片产品线

上海航芯在芯片安全技术、处理器技术等领域坚持研发和创新，取得卓越成绩。十余年来，成功研发了多款安全芯片，丰富的产品线能够覆盖各行业不同需求应用。



## 安全芯片选型表

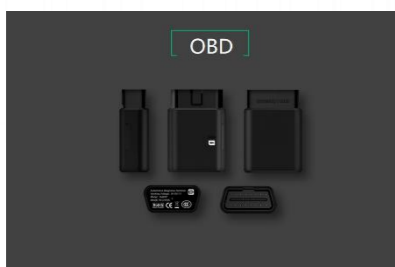
| 产品名称                   | 产品型号    | 主频MHz               | 工作电压       | 工作温度      | 芯片封装      | SRAM (KB) | eFlash (KB)   | 通信接口  | 安全算法   |
|------------------------|---------|---------------------|------------|-----------|-----------|-----------|---------------|---|--|
| ACL16_S                | SDQQN   | 48                  | 1.62-5.5V  | -40-125°C | QFN16     | 4         | 64            | UART、SPI、I2C、ISO7816、SWI                            | DES、3DES<br>ECC、AES<br>SHA1/256/384/512                        |
|                        | SCPQN   | 48                  | 1.62-5.5V  | -40-125°C | QFN16     | 8         | 128           |   |  |
|                        | SDQSN   | 48                  | 1.62-3.63V | -40-125°C | SOP8      | 4         | 64            |   |  |
|                        | SCPSN   | 48                  | 1.62-3.63V | -40-125°C | SOP8      | 8         | 128           |   |  |
| ACL16<br>AEC-Q100 认证   | QFN32A  | 48                  | 2.7-5.5V   | -40-85°C  | QFN32     | 16        | 256           | USB、UART、SPI、I2C、ISO7816                            | SM1/2/3/4、RSA<br>ECC、AES<br>DES、3DES<br>SHA1/256/384/512       |
|                        | QFN32B  | 48                  | 2.7-5.5V   | -40-85°C  | QFN32     | 16        | 320           |   |  |
|                        | QFN40A  | 48                  | 2.7-5.5V   | -40-85°C  | QFN40     | 16        | 256           | USB、UART、SPI、I2C、ISO7816、MIC                        |  |
|                        | QFN40B  | 48                  | 2.7-5.5V   | -40-85°C  | QFN40     | 16        | 320           |   |  |
| ACH512                 | QFN32   | 110                 | 1.68-5.5V  | -40-85°C  | QFN32     | 128       | 512           | UART、SPI、I2C  | SM1/2/3/4、SSF33<br>RSA、ECC、DES<br>3DES、AES<br>SHA1/256/384/512 |
|                        | QFN64   | 110                 | 1.68-5.5V  | -40-85°C  | QFN64     | 128       | 512           | USB、UART、SPI、I2C、ISO7816、MIM、eMMC/SD10<br>NandFlash |  |
|                        | LQFP100 | 110                 | 1.68-5.5V  | -40-85°C  | LQFP100   | 128       | 512           |   |  |
| ACS-VIE                | SC      | 30                  | 2.7-5.5V   | -40-85°C  | smartcard | 14        | EEPROM: 80 KB | ISO7816、14443                                       | SM1/2/3/4、SSF33<br>RSA、ECC、DES、3DES、AES<br>SHA1/256/384/512    |
| ACX200T<br>AEC-Q100 认证 |         | CPU: 100<br>算法: 300 | 2.7-5.5V   | -40-125°C | QFN48     | 64        | 512           | USB、UART、SPI、ISO7816                                | SM1/2/3/4、ECDSA<br>AES、SHA1、DES                                |
| ACX200A                |         | 算法: 300             | 2.7-5.5V   | -40-105°C | LQFP176   |           |               | SPI、XMI专用并口   | SM1/2/3/4、ECDSA<br>AES、DES、SHA1                                |



## 汽车电子

**ACL16**系列芯片通过国密二级认证、EAL5+安全认证，以及AEC-Q100车规认证，应用于ETC，T-BOX，OBD等汽车电子相关应用，为车联网安全保驾护航。

**ACX200T**面向5G车联网C-V2X应用的安全芯片，满足V2X场景下消息认证的专用安全芯片，采用公司自主的高速硬件加密引擎，支持国家标准SM2、SM3、SM4密码算法，同时支持国际ECDSA、AES、SHA-1密码算法。



### OBD

加密协处理器ACL16  
主频48MHz  
16KB SRAM, 320KB Flash



### ETC

ESAM模块, 主频48MHz,  
32KB EEPROM, 50万次擦写



### V2X

加密处理器ACX200T  
超高性能SM2、SM3、SM4密码  
算法



### T-BOX

加密协处理器ACL16  
主频48MHz  
16KB SRAM, 320KB Flash

## 指纹识别

**ACH512、ACM32FP4** 芯片采用高性能ARM内核，高主频、大容量存储，有出色的指纹算法处理能力。广泛应用于指纹模块、指纹挂锁、智能门锁、指纹U盘等领域。



### 指纹模组

- ACH512, 主频110MHz  
128KB SRAM, 512KB Flash
- ACM32FP4, 主频180MHz  
192KB SRAM, 512KB Flash



### 指纹挂锁

ACM32FP4, 主频180MHz  
192KB SRAM, 512KB Flash  
单芯片实现方案主控和算法处理



### 智能门锁

ACM32FP4  
单芯片门锁主控, 集成触控



### 指纹U盘

ACH512, 主频110MHz  
128KB SRAM, 512KB Flash  
单芯片实现指纹算法和U盘控制

## 网络安全认证

**ACL16**芯片有两种容量类型的片内eFlash (320KB和256KB), 两种类型容量的SRAM (16KB和32KB), 可应用于网络身份认证、电子政务、网银U盾、移动支付、金融支付终端、税务USBKey等。

**ACH512** 芯片是一款基于安全算法的高性能SOC芯片, 主要应用于eMMC/SD/Nandflash大容量存储设备、加密U盘、高速KEY等市场。

## 设备防伪

**ACL16、ACL16\_S**芯片是针对物联网认证、eSIM、防抄板和设备认证需求推出的高安全芯片。采用32位ARM Cortex-M0系列内核, 片内集成多种安全密码模块。



**网银U盾**  
ACL16, 主频48MHz  
16KB SRAM, 320KB Flash  
集成SM1/2/3/4国密算法



**支付终端**  
ACL16, 主频48MHz  
16KB SRAM, 320KB Flash  
集成SM1/2/3/4国密算法



**支付密码器**  
ACL16, 主频48MHz  
16KB SRAM, 320KB Flash  
国密二级认证



**医疗设备安全认证**  
ACL16, 主频48MHz  
16KB SRAM, 320KB Flash



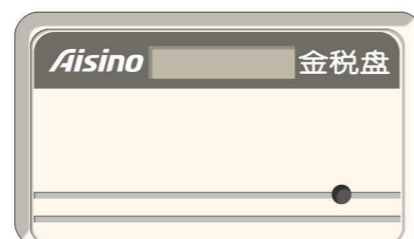
**打印耗材认证**  
ACL16, 主频48MHz  
16KB SRAM, 320KB Flash



**高速Key**  
ACH512, 主频110MHz  
128KB SRAM, 512KB Flash  
集成高速USB 2.0



**指纹Key**  
ACH512, 主频110MHz  
128KB SRAM, 512KB Flash  
单芯片实现指纹和Key功能



**金税盘**  
ACH512, 主频110MHz  
128KB SRAM, 512KB Flash  
集成高速USB 2.0

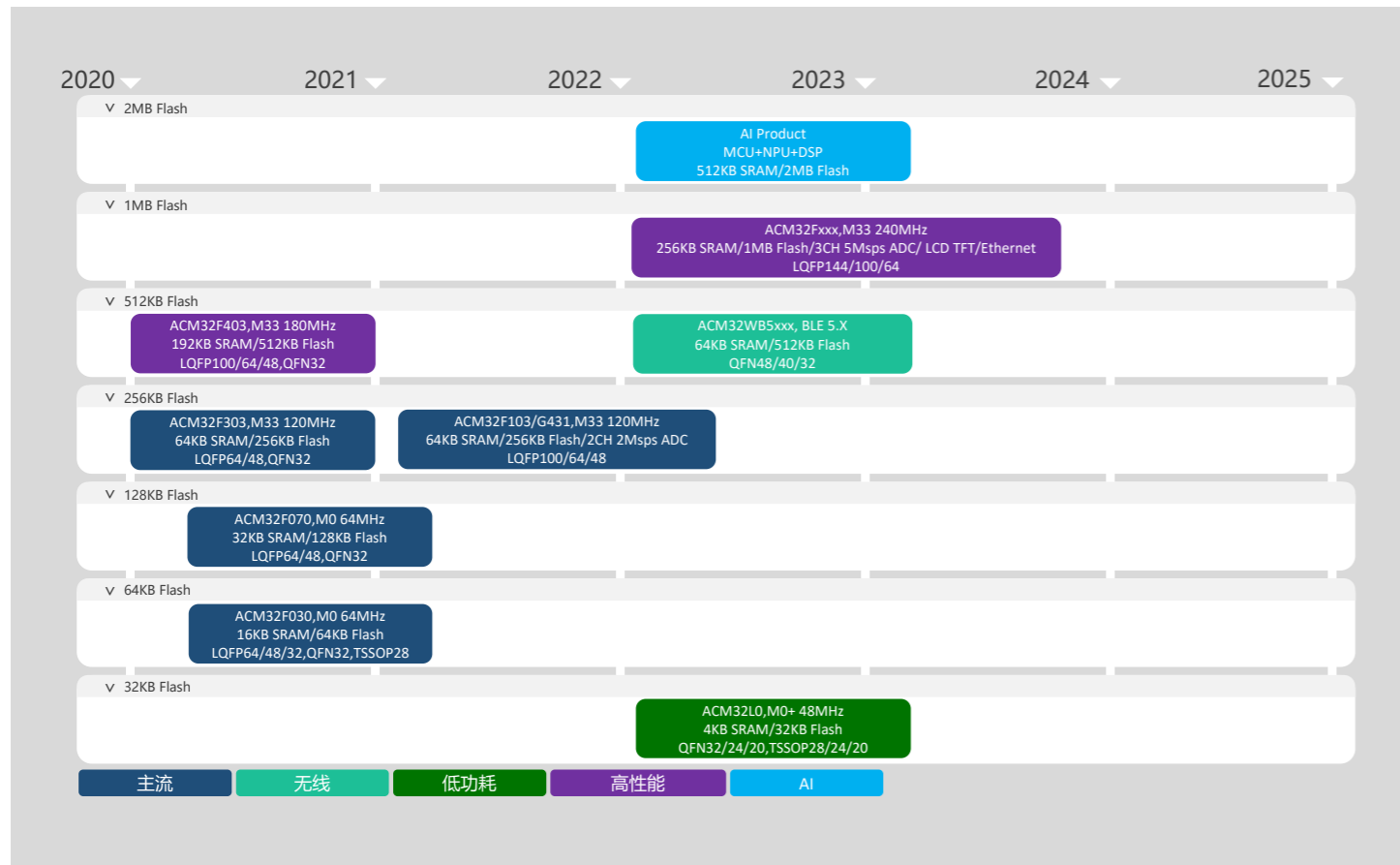


**嵌入式安全认证**  
ACL16\_S, 主频48MHz  
8KB SRAM, 128KB Flash



**配件认证**  
ACL16\_S, 主频48MHz  
8KB SRAM, 128KB Flash

## 芯片Roadmap (通用MCU、蓝牙芯片等)



## 专用芯片选型表

指纹门锁主控系列

| 产品型号           | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        |     | ADC 通道数 | DAC | USB FS | RTC | TouchKey 按键数量 | AES256/TRNG/CRC32 | Package |
|----------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|-----|---------|-----|--------|-----|---------------|-------------------|---------|
|                |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART | I2S |         |     |        |     |               |                   |         |
| ACM32FP001RBT7 | 1.7~3.6     | 64              | 32        | 128         | 7     | 56   | 3            | 2   | 2   | 1      | 19  |         |     |        | √   | 16            | √                 | QFN64   |
| ACM32FP401OKU6 | 1.7~3.6     | 180             | 192       | 2560        | 10    | 41   | 4            | 2   | 3   | 1      | 11  | 2       | 1   | √      |     |               | √                 | QFN48   |
| ACM32FP401REU7 | 1.7~3.6     | 180             | 192       | 512         | 10    | 57   | 4            | 2   | 4   | 1      | 16  | 2       | 1   | √      |     |               | √                 | QFN64   |
| ACM32FP401RKU6 | 1.7~3.6     | 180             | 192       | 2560        | 10    | 57   | 4            | 2   | 3   | 1      | 16  | 2       | 1   | √      |     |               | √                 | QFN64   |
| ACM32FP401TEU7 | 1.7~3.6     | 180             | 192       | 512         | 10    | 80   | 4            | 2   | 4   | 1      | 16  | 2       | 1   | √      |     |               | √                 | QFN88   |

指纹模组算法芯片

| 产品型号           | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        |     | ADC 通道数 | USB FS | AES256/TRNG/CRC32 | Package |
|----------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|-----|---------|--------|-------------------|---------|
|                |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART | I2S |         |        |                   |         |
| ACM32FP401KEU7 | 1.7~3.6     | 180             | 192       | 512         | 10    | 27   | 4            | 2   | 2   | 1      | 1   | 9       | 1      | √                 | QFN32   |
| ACM32FP400KKU6 | 1.7~3.6     | 180             | 192       | 2560        | 10    | 27   | 4            | 2   | 2   | 1      | 1   | 9       | 1      | √                 | QFN32   |

## 通用MCU选型表

ACM32F030系列, ARM 32bit Cortex-M0

| 产品型号          | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        | ADC 通道数 | CAN | RTC | 比较器 | 运放 | TouchKey 按键数量 | LCD            | AES256/TRNG/CRC32 | Package |
|---------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|---------|-----|-----|-----|----|---------------|----------------|-------------------|---------|
|               |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART |         |     |     |     |    |               |                |                   |         |
| ACM32F030E8P7 | 1.7~3.6     | 64              | 8         | 64          | 7     | 23   | 3            | 2   | 2   | 1      | 10      | 1   |     | 2   |    |               | √              | TSSOP28           |         |
| ACM32F030K8U7 | 1.7~3.6     | 64              | 8         | 64          | 7     | 26   | 3            | 2   | 2   | 1      | 10      | 1   |     | 2   | 1  |               | √              | QFN32             |         |
| ACM32F030K8T7 | 1.7~3.6     | 64              | 8         | 64          | 7     | 26   | 3            | 2   | 2   | 1      | 10      | 1   |     | 2   | 1  |               | √              | LQFP32            |         |
| ACM32F030C8T7 | 1.7~3.6     | 64              | 16        | 64          | 7     | 40   | 3            | 2   | 2   | 1      | 11      | 1   | √   | 2   | 3  | 12            | 4*24           | √                 | LQFP48  |
| ACM32F030R8T7 | 1.7~3.6     | 64              | 16        | 64          | 7     | 56   | 3            | 2   | 2   | 1      | 11      | 1   | √   | 2   | 3  | 16            | 4*40/6*38/8*36 | √                 | LQFP64  |

ACM32F070系列, ARM 32bit Cortex-M0

| 产品型号             | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        | ADC 通道数 | CAN | RTC | 比较器 | 运放 | TouchKey 按键数量 | LCD            | AES256/TRNG/CRC32 | Package               |
|------------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|---------|-----|-----|-----|----|---------------|----------------|-------------------|-----------------------|
|                  |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART |         |     |     |     |    |               |                |                   |                       |
| ACM32F070KBU7    | 1.7~3.6     | 64              | 32        | 128         | 7     | 26   | 3            | 2   | 2   | 1      | 10      | 1   |     | 2   | 1  |               | √              | QFN32             |                       |
| ACM32F070KB7     | 1.7~3.6     | 64              | 32        | 128         | 7     | 26   | 3            | 2   | 2   | 1      | 10      | 1   |     | 2   | 1  |               | √              | LQFP32            |                       |
| ACM32F070CB7     | 1.7~3.6     | 64              | 32        | 128         | 7     | 40   | 3            | 2   | 2   | 1      | 11      | 1   | √   | 2   | 3  | 12            | 4*24           | √                 | LQFP48                |
| ACM32F070RB7 (S) | 1.7~3.6     | 64              | 32        | 128         | 7     | 56   | 3            | 2   | 2   | 1      | 19      | 1   | √   | 2   | 3  | 16            | 4*40/6*38/8*36 | √                 | LQFP64 (10x10 or 7x7) |

ACM32F303系列, ARM 32bit Cortex-M33架构

| 产品型号          | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        |     | ADC 通道数 | DAC | CAN | USB FS | RTC | 比较器 | AES256/TRNG/CRC32 | Package |
|---------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|-----|---------|-----|-----|--------|-----|-----|-------------------|---------|
|               |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART | I2S |         |     |     |        |     |     |                   |         |
| ACM32F303KBU7 | 1.7~3.6     | 120             | 32        | 128         | 10    | 26   | 4            | 2   | 3   | 1      | 1   | 10      |     | 2   | 1      |     | 2   | √                 | QFN32   |
| ACM32F303CB7  | 1.7~3.6     | 120             | 32        | 128         | 10    | 38   | 4            | 2   | 3   | 1      | 1   | 10      | 2   | 2   | 1      | √   | 2   | √                 | LQFP48  |
| ACM32F303RBT7 | 1.7~3.6     | 120             | 32        | 128         | 10    | 52   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | √                 | LQFP64  |
| ACM32F303KCU7 | 1.7~3.6     | 120             | 64        | 256         | 10    | 26   | 4            | 2   | 3   | 1      | 1   | 10      |     | 2   | 1      |     | 2   | √                 | QFN32   |
| ACM32F303CCT7 | 1.7~3.6     | 120             | 64        | 256         | 10    | 38   | 4            | 2   | 3   | 1      | 1   | 10      | 2   | 2   | 1      | √   | 2   | √                 | LQFP48  |
| ACM32F303RCT7 | 1.7~3.6     | 120             | 64        | 256         | 10    | 52   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | √                 | LQFP64  |

ACM32F403系列, ARM 32bit Cortex-M33架构

| 产品型号              | Voltage (V) | Max Speed (MHz) | SRAM (KB) | eFlash (KB) | Timer | GPIO | Connectivity |     |     |        |     | ADC 通道数 | DAC | CAN | USB FS | RTC | 比较器 | 运放 | AES256/TRNG/CRC32 | Package               |
|-------------------|-------------|-----------------|-----------|-------------|-------|------|--------------|-----|-----|--------|-----|---------|-----|-----|--------|-----|-----|----|-------------------|-----------------------|
|                   |             |                 |           |             |       |      | UART         | I2C | SPI | LPUART | I2S |         |     |     |        |     |     |    |                   |                       |
| ACM32F403KCU7     | 1.7~3.6     | 180             | 96        | 256         | 10    | 26   | 4            | 2   | 3   | 1      | 1   | 10      |     | 2   | 1      |     | 2   | 3  | √                 | QFN32                 |
| ACM32F403CCT7     | 1.7~3.6     | 180             | 96        | 256         | 10    | 38   | 4            | 2   | 3   | 1      | 1   | 10      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP48                |
| ACM32F403RCT7     | 1.7~3.6     | 180             | 96        | 256         | 10    | 52   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP64                |
| ACM32F403VCT7     | 1.7~3.6     | 180             | 96        | 256         | 10    | 84   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP100               |
| ACM32F403KEU7     | 1.7~3.6     | 180             | 192       | 512         | 10    | 26   | 4            | 2   | 3   | 1      | 1   | 10      |     | 2   | 1      |     | 2   | 3  | √                 | QFN32                 |
| ACM32F403CET7     | 1.7~3.6     | 180             | 192       | 512         | 10    | 38   | 4            | 2   | 3   | 1      | 1   | 10      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP48                |
| ACM32F403RET7 (S) | 1.7~3.6     | 180             | 192       | 512         | 10    | 52   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP64 (10x10 or 7x7) |
| ACM32F403VET7     | 1.7~3.6     | 180             | 192       | 512         | 10    | 84   | 4            | 2   | 4   | 1      | 1   | 16      | 2   | 2   | 1      | √   | 2   | 3  | √                 | LQFP100               |

## 工业应用



### 工业缝纫机

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
支持CAN通信



### 工业机器人

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
三角函数硬件加速  
支持CAN通信  
支持-40~125°C工作温度



### 烟雾传感器

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
动态功耗<80uA@MHz  
睡眠功耗<1uA  
低功耗唤醒

## 健康医疗



### 额温枪

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
支持4\*40/6\*38/8\*36 LCD驱动  
集成运放



### 血氧仪

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
支持4\*40/6\*38/8\*36 LCD驱动  
集成运放



### 血压计

ACM32F070, 工作频率64MHz  
32KB SRAM, 128KB Flash  
支持4\*40/6\*38/8\*36 LCD驱动  
集成运放



### 激光测距仪

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
支持-40~125°C工作温度



### 智能电表

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash  
支持-40~125°C工作温度



### 智能安防

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash  
支持-40~125°C工作温度



### 按摩仪

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
支持多种PWM工作模式



### 筋膜枪

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
集成运放



### 体重秤

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
支持4\*40/6\*38/8\*36 LCD驱动  
集成运放

## 消费电子



### 智能门锁

ACM32F070, 工作频率64MHz  
32KB SRAM, 128KB Flash  
支持16个TouchKey



### 游戏外设

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash



### 智能穿戴

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
集成运放、比较器

## 电机驱动



### 电动工具

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash



### 空调机

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
集成运放、比较器  
工作温度-40~125°C



### 电动牙刷

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash



### 无线充电器

ACM32F030, 工作频率64MHz  
16KB SRAM, 64KB Flash  
集成运放



### 教育机器人

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash  
丰富外设接口  
支持-40~125°C工作温度



### 微型打印机

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash  
支持-40~125°C工作温度



### 无人机

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
三角函数硬件加速  
工作温度-40~125°C



### 手持云台

ACM32F403, 工作频率180MHz  
192KB SRAM, 512KB Flash  
工作温度-40~125°C



### 扫地机器人

ACM32F303, 工作频率120MHz  
64KB SRAM, 256KB Flash

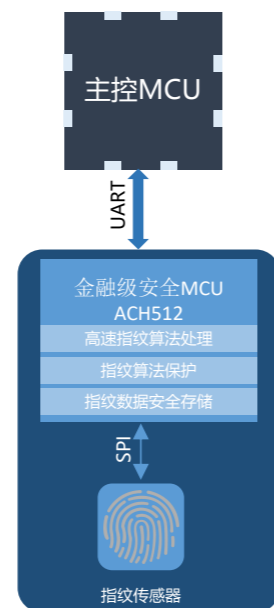
## 指纹模组方案

### 方案介绍

该指纹安全模块方案采用金融级安全芯片ACH512，保护指纹算法和指纹数据安全，可实现设备安全认证、数据传输加密，可实现高速度高分辨率指纹算法处理，接口简单，易于使用。

### 产品特点

- 金融级安全芯片ACH512
- 采用金融级安全芯片，抗各种物理攻击
- 支持全系列国密、国际算法 (DES/AES/RSA/ECC/SM1/SM2/SM3/SM4...)
- 通过国密、国测、银检中心等国家权威安全机构检测
- 密钥安全存储、防数据外泄
- 核心代码保护、防破解拷贝
- 固件更新认证和校验
- 高速指纹算法处理
- 支持88\*112、96\*96、160\*160、192\*192等分辨率



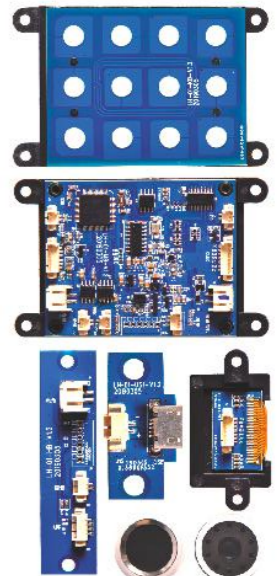
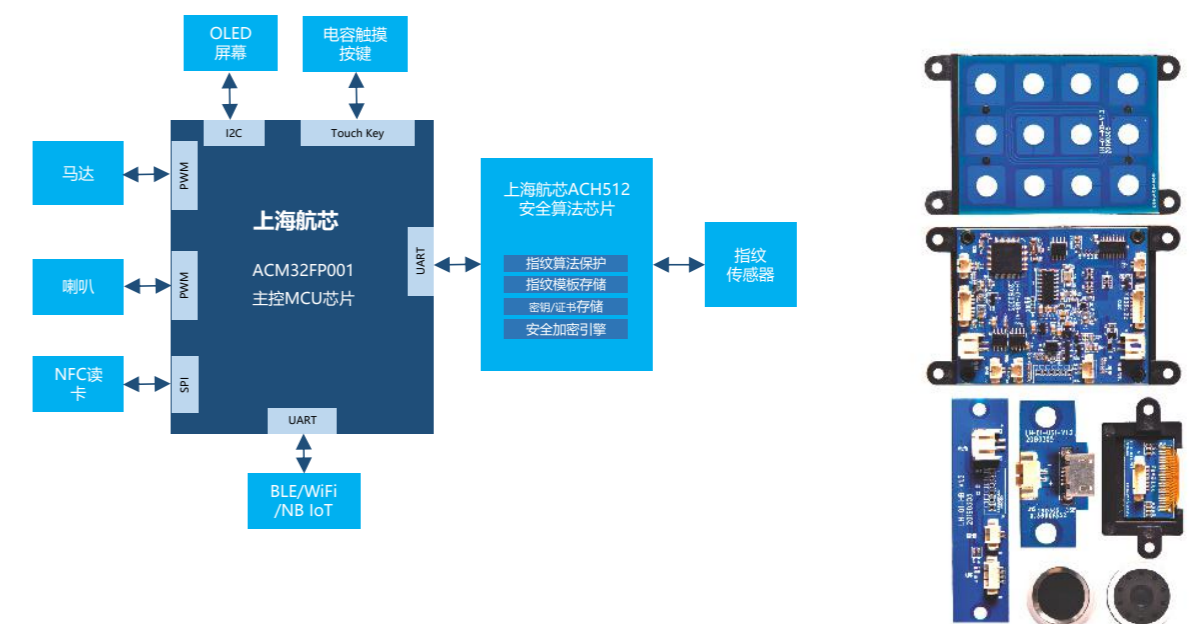
## 智能门锁方案

### 方案介绍

随着移动互联网技术、云技术、生物识别技术的开发与运用，智能门锁的技术水平已发生了巨大的改变，新一代智能锁在外观结构、开锁方式、管理模式等方面都有了革命性的发展，并成为智能家居中最重要和关键的部分。新型智能锁结合了生物识别、密码认证、机械钥匙、信息安全等技术，构建了一个多方位的安全体系，因此需要更高安全性的解决方案。

### 方案特点

- 主控采用集成TK的ACM32FP001芯片
- 指纹算法采用ACH512安全芯片，支持全系列国密、国际算法 (DES/AES/RSA/ECC/SM1/SM2/SM3/SM4...)
- 支持指纹、按键、钥匙、非接、蓝牙、APP远程等多种开锁方式
- 指纹、密码安全存储、敏感信息不外泄
- 云管端全链路安全加密传输
- 支持固件在线升级，升级包加密防篡改



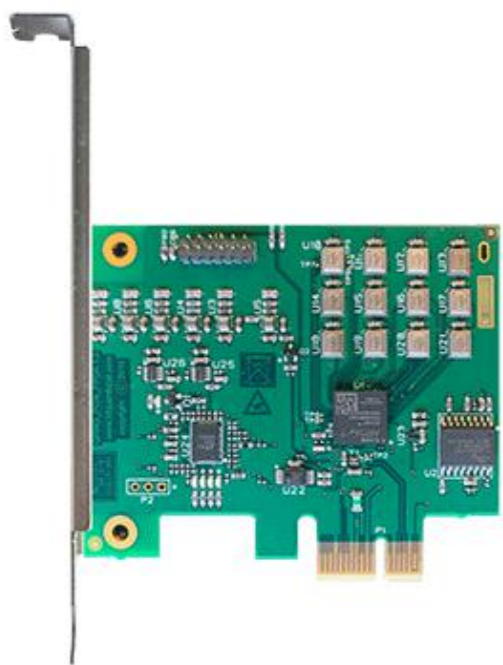
## 量子加密方案

### 方案介绍

量子随机数发生器是基于量子力学的概率性设计运行的，量子力学的概率性从根本上保证了随机序列的不可预测性，其随机性得到理论证明。

### 产品特点

上海航芯研发的量子随机数发生器具有高速、低功耗、稳定等特点，支持PCIE接口，最大输出速率达到200Mbps，随机数质量达到国密检测规范、NIST随机性检测标准等的要求，可以广泛应用于博彩、加密机、量子通信、信息安全等对随机数性要求较高的领域。



|      |               |
|------|---------------|
| 产品型号 | XXXX          |
| 生成速率 | 200Mbps       |
| 接口   | PCIE2.0       |
| 外观   | 板卡式           |
| 工作温度 | 0°C ~ 85°C    |
| 存储温度 | -40°C ~ 125°C |
| 功耗   | ≤1W           |
| 工作电压 | 5V            |

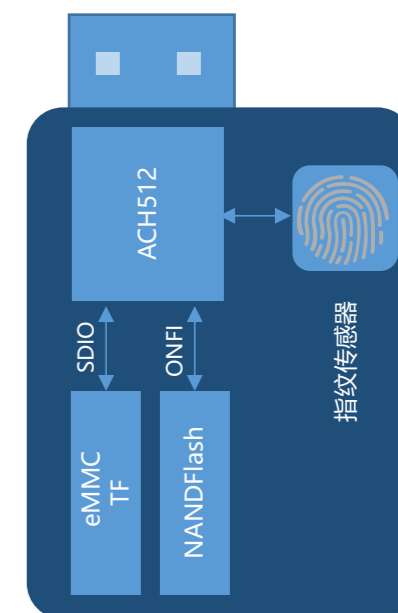
## 指纹加密U盘方案

### 方案介绍

本方案采用1颗芯片就可实现指纹算法处理、安全加密功能、nandflash访问，可有效保护指纹算法和指纹数据的安全，且开发简单，成本低。

### 产品特点

- 支持全系列国密、国际算法
- 高集成度、低成本
- 采用金融级安全芯片，抗各种物理攻击（DPA/SPA/电压/频率/温度等）
- 通过国密、国测、银检中心等权威安全机构检测
- 数据加密传输、设备防伪认证、密钥安全存储、防数据外泄



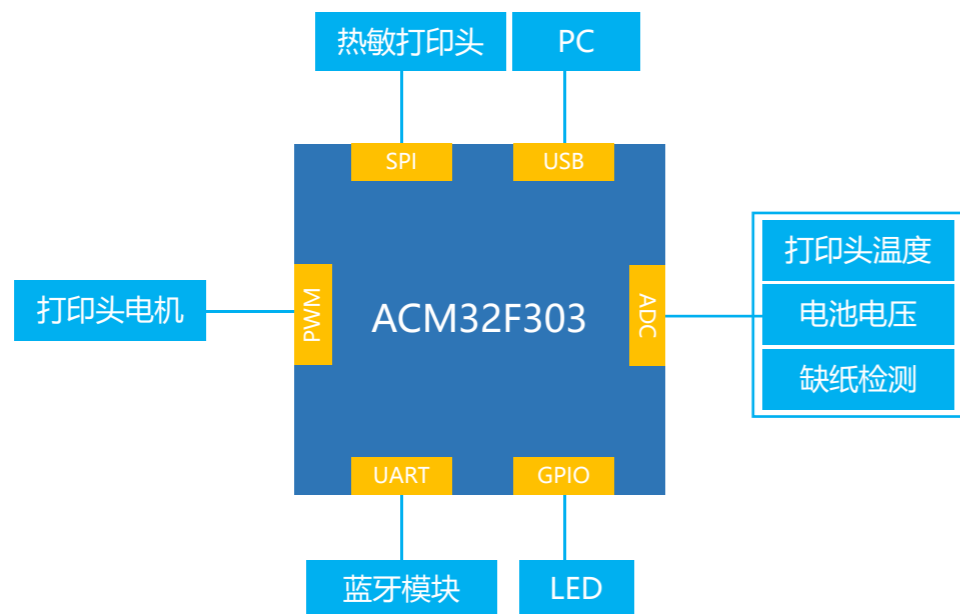
## 微型打印机方案

### 方案介绍

热敏打印机有选择地在热敏纸的确定位置上加热，由此就产生了相应的图形。加热是由与热敏材料相接触的打印头上的一个小电子加热器提供的。加热器排成方点或条的形式由打印机进行逻辑控制，当被驱动时，就在热敏纸上产生一个与加热元素相应的图形。控制加热元素的同一逻辑电路，同时也控制着进纸，因而能在整个标签或纸张上印出图形。热敏打印机有选择地在热敏纸的确定位置上加热，由此就产生了相应的图形。

### 产品特点

采用ACM32F303作为方案主控，ARM Cortex M33架构内核，工作频率120MHz，64KB SRAM，256KB Flash，内置USB 2.0接口，集成ADC、运放等。



## 配件安全认证

### 方案介绍

OWS 系列安全认证器是上海航芯基于单总线通讯自主开发的设备认证类的安全产品，单总线协议兼容1-Wire 协议。支持ECDSA、AES和SHA等硬件算法引擎、FIPS/NIST兼容真随机数发生器(TRNG)、2KB 安全EEPROM存储区、17位递减计数器和唯一的64位ROM识别码(ROM ID)。ECC公钥/私钥采用NIST定义的P-256曲线，提供ECDSA签名、验签等功能；AES 和SHA算法为数据强加密、双向质询-应答认证提供安全保障；唯一的ROMID可用作加密、认证运算的基本输入参数，也可作为应用中的电子序列号使用，在多器件的1-Wire网络中，ROM ID为节点地址。

- 可靠反制措施，防御安全攻击
  - 防DPA/SPA攻击，防DFA错误注入攻击
  - 电压/温度/频率检测，主动监测芯片屏蔽，检测并反制侵入企图
  - 存储器保护功能，所有储存的数据采用加密保护，防止侦测
  - 国密二级资质认证、国内EAL5+资质认证
- 高效公钥安全认证方案，支持外设安全认证
  - FIPS 186兼容的ECDSA P-256签名，支持质询/应答安全认证
  - ECDSA公钥/私钥对由芯片内部生成和用户外部导入
  - TRNG符合FIPS140-2要求，CRC16多项式符合  $G(x) = x^{16} + x^{15} + x^2 + 1$  要求
- 附加特性便于集成到终端应用
  - 17位一次性可设置、非易失递减计数器
  - 2KB EEPROM，可用于存储用户数据、密钥、控制寄存器和证书
  - 唯一且不可更改的64位ROM识别码(ROM ID)
  - 单触点、1-Wire接口与主机通信，通讯速率为62.5kbps
  - 工作电压：1.62V-3.63V，工作温度：-40°C至+125°C
  - 6引脚DFN封装(2\*2\*0.55mm)



打印机配件



原装电池



防抄板



智能家居



游戏外设

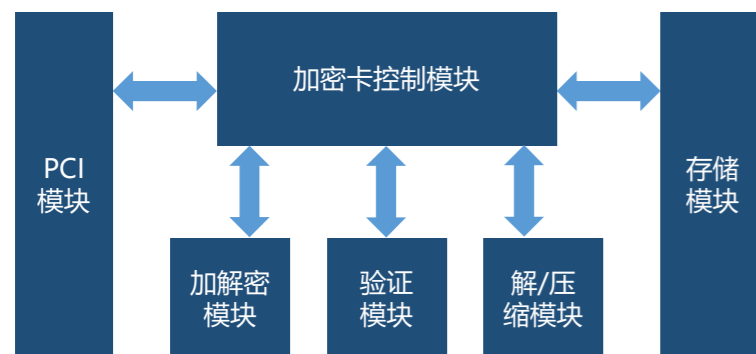


医疗设备

## 加密卡方案

PCI-E密码卡（标准半高密码卡、Mini PCI-E密码卡），符合PCI-E协议标准，符合国家密码管理局PCI密码卡相关技术规范并通过鉴定，可适用于基于PCI-E接口的信息安全应用，能够提供高速并发密码运算服务，满足应用系统对数字签名验签、数据加解密、数据完整性验证等需求，并能够提供完善的密钥管理机制。

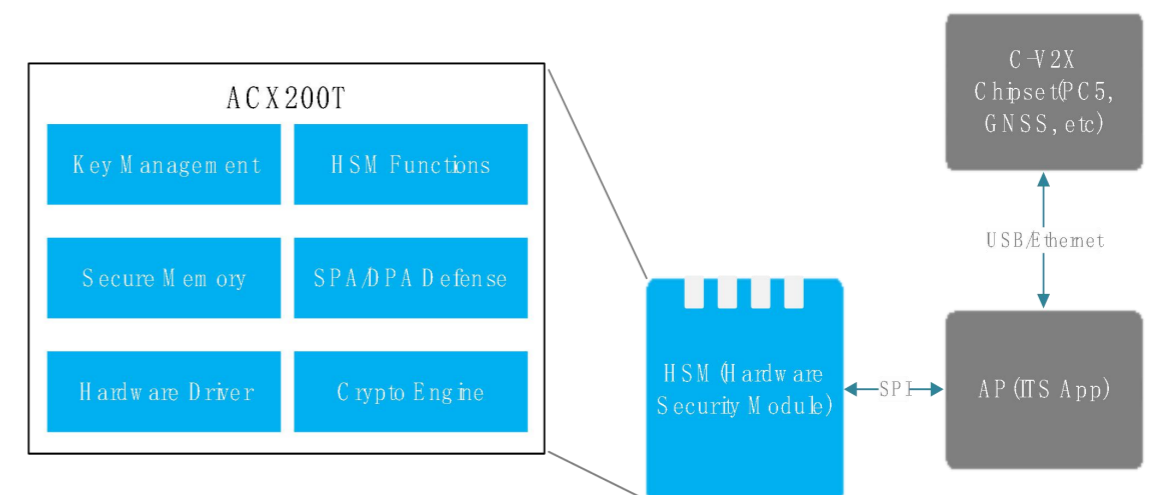
| 指标       | 操作   | 参数                       |
|----------|------|--------------------------|
| SM1      | 加解密  | 1Gbps                    |
| SM4      | 加解密  | 20Gbps                   |
| SM2      | 创建密钥 | 16000 次/秒                |
|          | 签名   | 16000 次/秒                |
|          | 验签   | 8000次/秒                  |
|          | 加密   | 8200次/秒                  |
| SM3      | 解密   | 16400次/秒                 |
|          |      | 4Gbps                    |
| 随机数生成    |      | 2Mbps                    |
| 随机源      |      | 双随机源                     |
| 对称密钥数目   |      | 1024个                    |
| SM2密钥数目  |      | 1024个                    |
| 文件系统     |      | 5M                       |
| AES      | 加解密  | 10Gbps                   |
| SHA-1    |      | 4Gbps                    |
| 物理接口     |      | PCI-E X8                 |
| 接口协议     |      | PCI-E V2.0/V3.0/V4.0向下兼容 |
| 支持操作系统   |      | 国产操作系统，如中标麒麟操作系统         |
| 并行处理     |      | 支持                       |
| 对称算法支持模式 |      | ECB/CBC/OFB              |
| 应用接口     |      | 支持                       |
| 内核接口     |      | 支持                       |



## V2X方案

ACX200T面向5G车联网C-V2X应用的安全芯片，满足V2X场景下消息认证的专用安全芯片，该款芯片采用公司自主的高速硬件加密引擎，支持国家标准SM1、SM2、SM3、SM4密码算法，同时支持国际ECDSA、AES、SHA-1密码算法。可实现网联汽车云端认证、安全数据通信、安全固件升级等需求，为车联网提供信息安全保障。

| 指标     | 操作  | 参数                                  |
|--------|-----|-------------------------------------|
| CPU核   |     | Cortex M3                           |
| SRAM   |     | 64KB                                |
| eFlash |     | 512KB                               |
| 工作电压   |     | 2.7V~5.5V                           |
| 工作温度   |     | -40°C~105°C                         |
| 接口     |     | USB2.0高速、2路SPI主从、2路UART、1路ISO7816主从 |
| 功耗     |     | 最大电流800mA                           |
| SM1    | 加解密 | 4Gbps                               |
| SM2    | 签名  | 12000 次/秒                           |
|        | 验签  | 6000次/秒                             |
| SM3    |     | 2.3Gbps                             |
| SM4    | 加解密 | 4.0Gbps                             |
| ECDSA  | 签名  | 10000 次/秒                           |
|        | 验签  | 5000次/秒                             |
| AES    | 加解密 | 3.8Gbps                             |
| SHA-1  |     | 1.8Gbps                             |



## 安全监控方案

### 安全体系架构

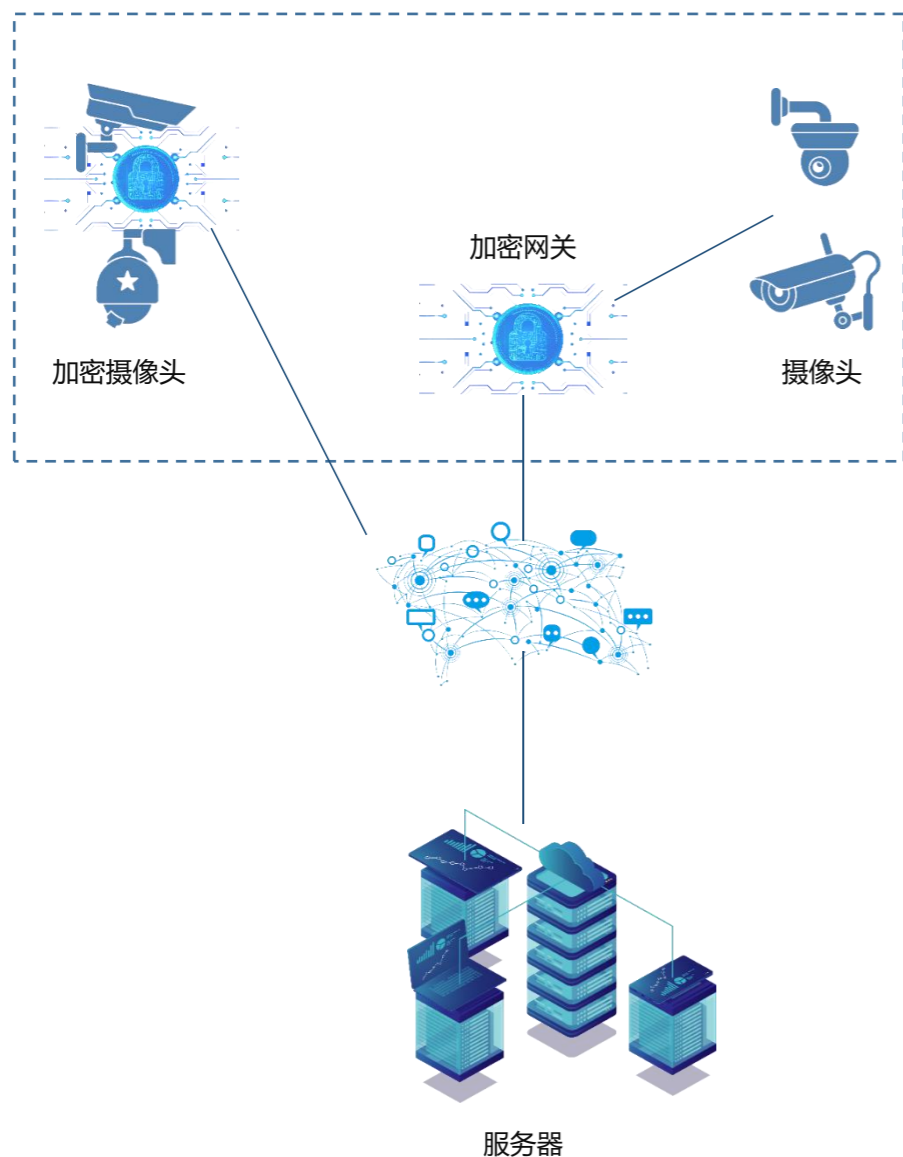
- 信源加密模式，解决数据采集、传输和存储的安全问题，防止信息泄露
- PKI体系身份认证机制，有效保证设备的安全接入，防止非法入侵和攻击
- 数据完整性校验机制，防止数据被非法篡改

### 相关标准

- GB 35114-2017 《公共安全视频监控联网信息安全技术要求》
- GBT-25724-2017, GBT-28181-2016

### 安全载体

- 加密模块
- USBKey
- 安全TF卡
- 视频编解码平台
- SVAC2.0
- H.264/H.265



## ESAM

航芯 OBE-SAM 产品是上海航芯自主开发的安全模块，主要应用于 ETC（不停车收费）系统，内嵌于车载设备 OBU 中。OBE-SAM安全模块中保存了车辆相关信息，收费站出入口信息，以及交易记录等等，模块采用安全芯片作为载体，密钥及敏感信息存放在安全芯片中，更加安全可靠。

航芯 ESAM 产品是上海航芯自主开发的安全模块，它是一个具有操作系统（COS）的安全存取单元，将其嵌入专用通用设备中，完成数据的加密解密、双向身份认证、访问权限控制、通信线路保护、临时密钥导出、数据文件存储等多种功能。可应用于水、电、气、暖 IC 表、汽车 T-BOX 通信、版权保护、工业控制等领域。

航芯 ACL16-SE 产品是上海航芯自主开发的安全模块，它是一个具有操作系统（COS）的安全存取单元，将其嵌入专用、通用设备中，完成数据的加密解密、双向身份认证、访问权限控制、通信线路保护、临时密钥导出、数据文件存储等多种功能。可应用于水、电、气、暖 IC 表、汽车 T-BOX 通信、版权保护、工业控制等领域。



|      | OBE-SAM                | ESAM                   | ACL16-SE                               |
|------|------------------------|------------------------|--|
| 接口   | ISO7816                | ISO7816、SPI            | ISO7816、SPI、UART                       |
| 存储容量 | 32KB, 50万次             | 10KB, 10万次             | 10KB, 10万次                             |
| 密码算法 | SM4                    | SM2、SM3、SM4            | RSA、DES、AES、SHA-1/-256、SM1、SM2、SM3、SM4 |
| 面向应用 | ETC专用                  | T-BOX、国VI、三表等通用领域      | 国VI、其它通用领域                             |
| 证书资质 | EAL4+、AEC-Q100<br>国密二级 | EAL4+、国密二级<br>AEC-Q100 | EAL5+<br>国密二级                          |
| 封装   | SOP8                   | SOP8                   | QFN32                                  |

荣誉资质

