ICP209安全芯片应用手册

1 ICP209安全芯片概述

ICP209芯片是具有高安全性的金融级加密芯片，基于 PKI 认证体系，通过 I2C 通信提供 API 实现高安全版权保护和配件认证。

ICP209标准方案提供安全认证和关键数据存储，用户 MCU 通过 I2C 通信调用ICP209 的 API，完成出厂初始化，安全认证，关键数据存储等功能。ICP209作为板级核心信任根对板级进行唯一性认证，关键数据和私钥数据存储在安全芯片中。

图 1-1 加密芯片原理示意图

2 版权保护方案介绍

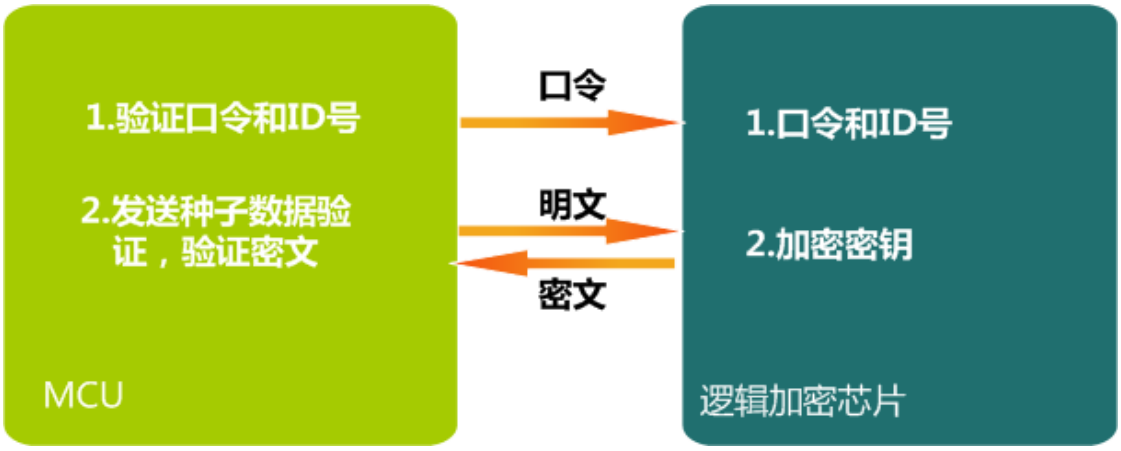
2.1 方案 1：逻辑加密芯片

芯片结构：EEPROM+逻辑电路

版权保护方案：口令认证，对称算法认证

优点：成本低，外围电路简单，开发简单

缺点：安全性低，易破解



2.2 方案 2：基于算法移植加密芯片

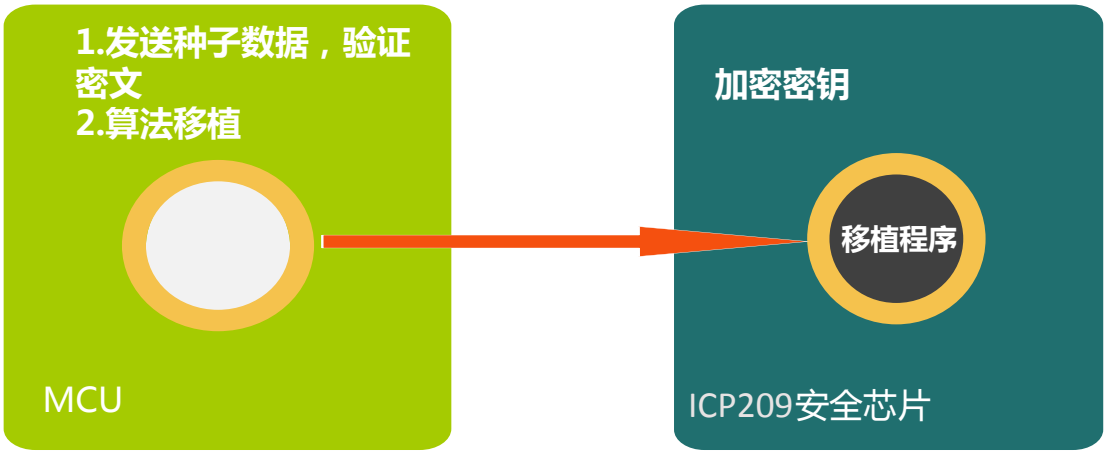
芯片结构：高安全性的金融级加密芯片

版权保护方案：

1. 主方案：算法移植，将 MCU 端部分程序移植到ICP209芯片中运行
2. 辅助方案：对称算法认证

优点：安全芯片运行部分 MCU 程序，MCU 无法绕过加密芯片独立运行。

缺点：用户工作量增大，用户需要开发安全芯片程序，量产时需要搭建下载程序环境。



2.3 方案:3：基于 PKI 认证体系加密芯片

芯片结构：高安全性的金融级加密芯片

版权保护方案：

1. 基于 PKI 体系高安全认证，私钥保存在安全芯片中，硬件保护，无法读出，且每颗芯片密钥不同。
2. 关键数据加密存储和读取。

优点：安全性高，私钥保存在安全芯片中，硬件保护，无法读出，且每颗芯片密钥不同。安全芯片提供 API，无需用户开发安全芯片程序。

缺点：成本较逻辑加密芯片要高

3 产品特性

3.1 芯片

处理器	自行设计单周期 8051 核，主频 32MHz，支持睡眠模式
ROM	96KB
EEPROM	32KB
SRAM	8KB
接口	I2C/7816
封装	SOP8/DFN8/客户定制
国际算法	RSA/ECC/DES/3DES/SHA1/SHA256
国密算法	SM2/SM3/SM4/SSF33
安全资质	国密二级/国内 EAL4+

3.2 安全特征

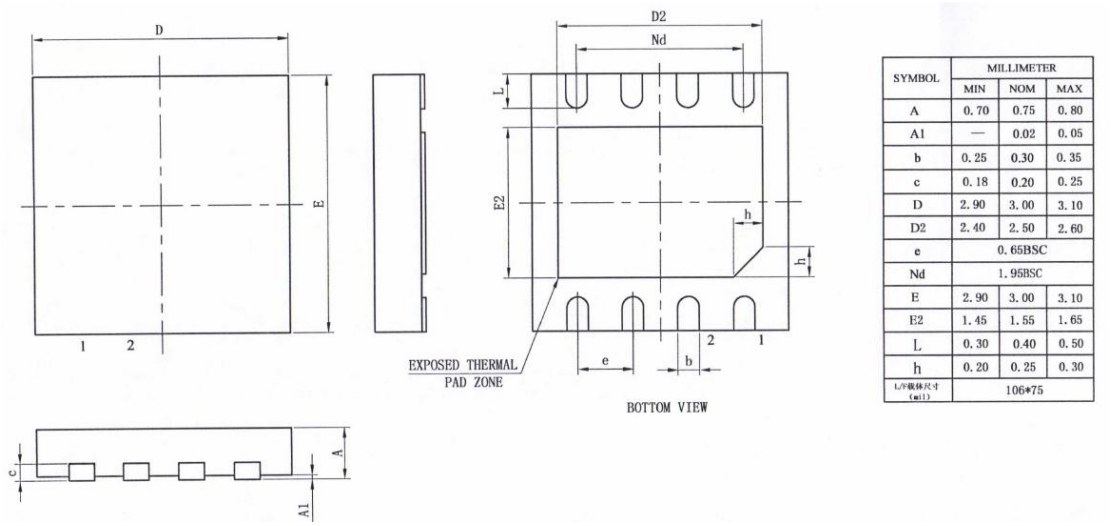
- 芯片全球唯一 SN 号
- 真随机发生器，通过国密安全检测。
- 支持对称和非对称算法体系
- 支持一卡一密
- 支持用户敏感数据加密读写
- 具有金属防护层和胶粘逻传感器层，探测到外部攻击后，内部数据不可逆自毁
- 总线和内存加密 ，时钟加扰

- 内嵌主动和被动防护层
- 芯片防篡改设计，序列号唯一
- 硬件错误检测
- 随机数发生器

3.3 应用领域

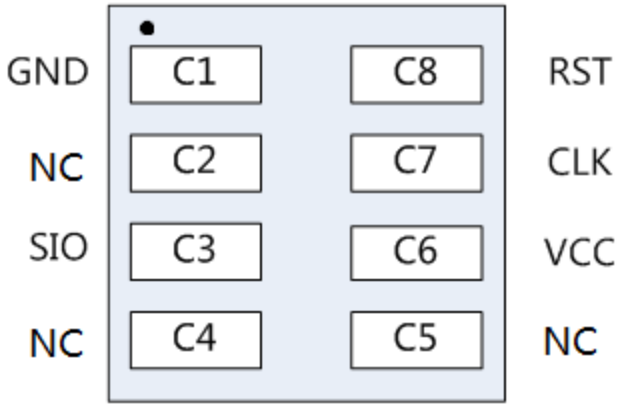
智能硬件，机顶盒、游戏机、墨盒、控制器、安防监控、汽车电子、平板电脑、路由器、DVR、 交换机、仪器仪表等各种电子产品终端。

4 外观尺寸和管脚定义



SYMBOL	MILLIMETER		
	MIN	NOM	MAX
A	0.70	0.75	0.80
A1	—	0.02	0.05
b	0.25	0.30	0.35
c	0.18	0.20	0.25
D	2.90	3.00	3.10
D2	2.40	2.50	2.60
e	0.65BSC		
Nd	1.95BSC		
E	2.90	3.00	3.10
E2	1.45	1.55	1.65
L	0.30	0.40	0.50
h	0.20	0.25	0.30
	106*75		

ICP209芯片 DFN8 封装尺寸图



- VCC-电源电压
- SIO- I²C 数据线
- CLK-I²C 时钟线
- RST-复位管脚
- NC-悬空

ICP209芯片 DFN8 封装管脚图

VCC 电压为 2.7V~5.5V

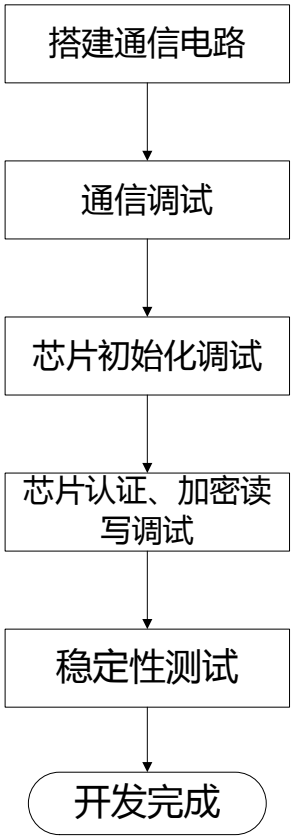
主机 MCU 与从机 ICP209 的通信符合标准 I²C 通信协议， MCU 的 I²C 管脚需要配置成上拉模式（如果没有上拉模式需要外部接上拉电阻，建议 4.7K）

正常工作时复位管脚 RST 需要接高电平（低电平有效）。

5 基于 PKI 系统方案开发指南

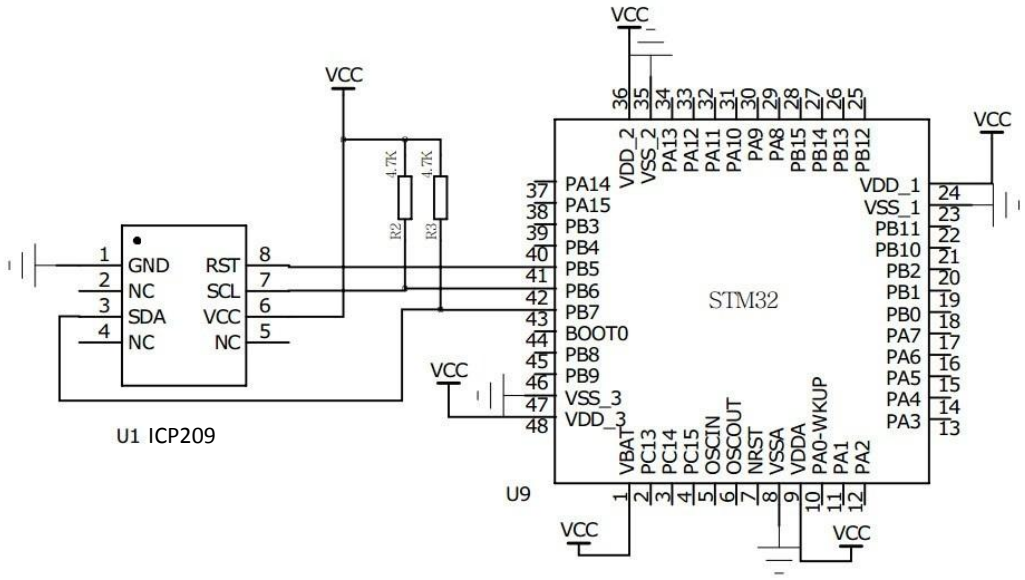
5.1 开发步骤

开发流程主要分为 6 个步骤，如下图所示



步骤 1：搭建通讯电路

ICP209采用标准 I²C 接口通讯，SIO、CLK 分别为数据、时钟线，RST 为低电平有效(正常工作需要接高电平)，典型电路图如下，



ICP209典型电路图

步骤 2：通讯调试

通讯时序与标准 I²C 一致。实现 MCU 与 ICP209之间的数据交互。

步骤 3：芯片初始化调试

在出厂前需要执行初始化，用于产生非对称认证、对称认证、读写加密用到的密钥，初始化指令包括：

1) 验证 PIN(必选)

ICP209内置 8 字节固定 PIN，完成出厂初始化必须验证 PIN 权限

2) 生成证书(非对称认证必选)

发送生成证书指令，ICP209产生认证公私钥对，并使用根私钥签发证书并保存（证书包含认证公钥），用于非对称算法认证

3) 设置对称认证密钥(对称认证必选)

设置对称认证密钥为对称算法认证供对称密钥

4) 设置读写密钥(加密读写必选)

设置读写密钥为读写数据提供加解密密钥

5) 配置读写空间(可选，不配置时，明文读写、密文读写空间各占 2K)

ICP209预留 4K 用户读写空间，通过配置读写空间指令，可以把 4K 空间配置成加密读写空间和明文读写空间两部分，配置读写空间指令带有 1 字节参数，代表加密读写空间的大小(单位：页，每页 128 字节)，比如：参数为 0x8，加密读写空间为 128*8=1K，明文读写空间为 4-1=3K。

6) 结束初始化(必选)

结束初始化流程

步骤 4：芯片认证、加密读写调试

1) 非对称算法认证：

MCU 读证书，取出证书中的认证公钥，并用根公钥验证公钥合法性。主机 MCU 对 ICP209安全芯片发起认证请求，ICP209通过认证私钥签名返回签名结果，MCU 通过认证公钥对应答结果验签。

2) 对称算法认证：

主机 MCU 对ICP209安全芯片发起认证请求，ICP209安全芯片通过预置对称密钥进行加密应答，MCU 通过对称密钥验证应答结果。

3) 关键数据读写功能：

使用 AES-CCM 算法对需要读写的数据进行加密保护，加密密钥使用初始化预置的读写密钥，ICP209提供了 4K 的用户空间用于存取用户关键数据。

4) 辅助算法接口：

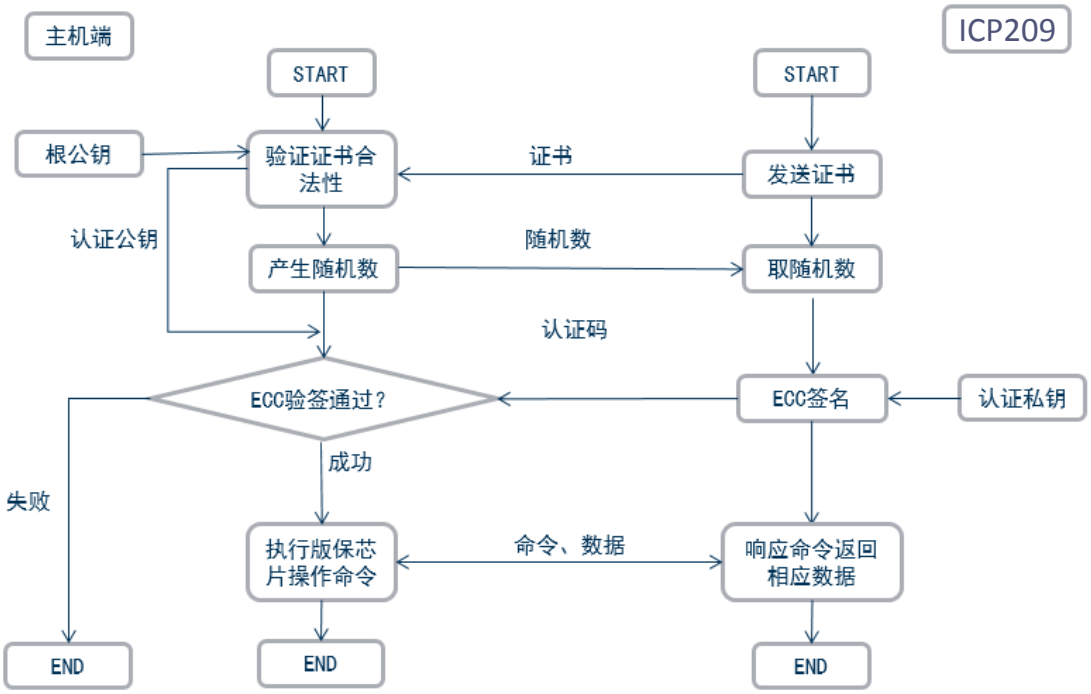
为方便用户获取曲线参数符合芯片要求的公私钥对，安全芯片提供产生公私钥对指令，用户可以选择通过该功能生产合法的根公私钥对供出厂初始化时使用。

步骤 5：稳定性测试

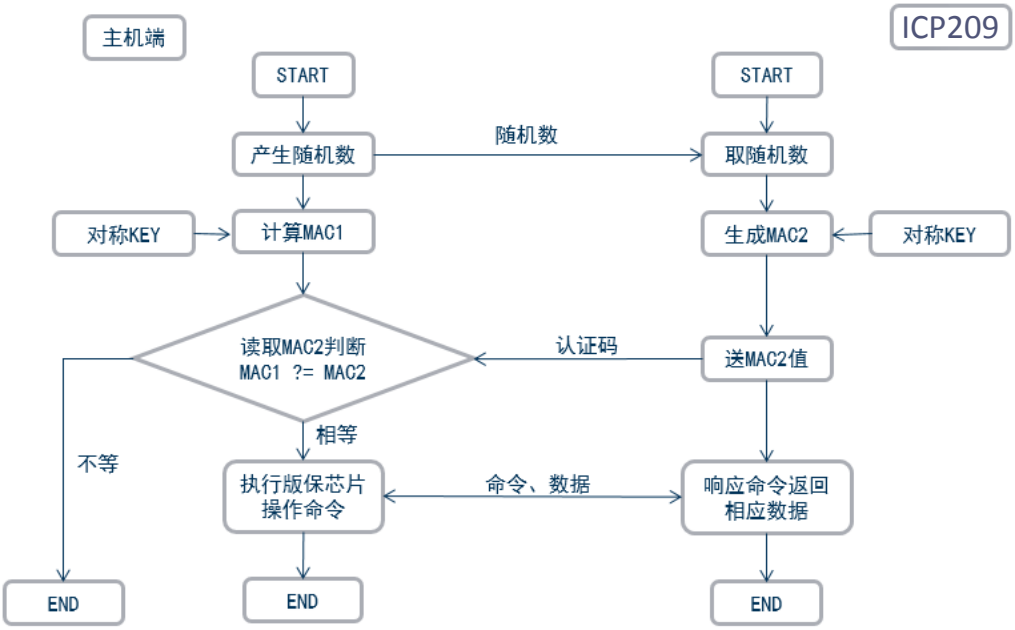
建议客户充分测试稳定性，并进行环境测试、老化测试后再进行批量生产。

5.2 方案流程

ICP209安全芯片基于 PKI 认证方案、对称认证方案流程图如下：



PKI 认证方案流程图



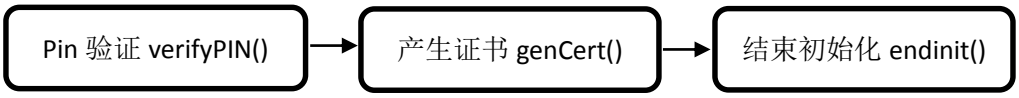
对称认证方案流程图

5.3 基于 PKI 体系方案例程

方案提供 MCU 例程，对ICP209的操作封装成底层 API，应用层直接调用 API 即可完成交互。以下四种功能相互独立，可以单独或者组合使用。

- **非对称算法认证：**

初始化芯片，每颗芯片只需初始化一次

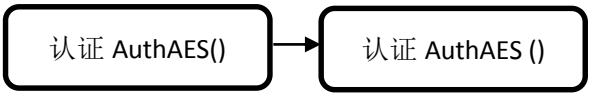


上电读证书，然后可以进行多次认证

- **对称算法认证：**

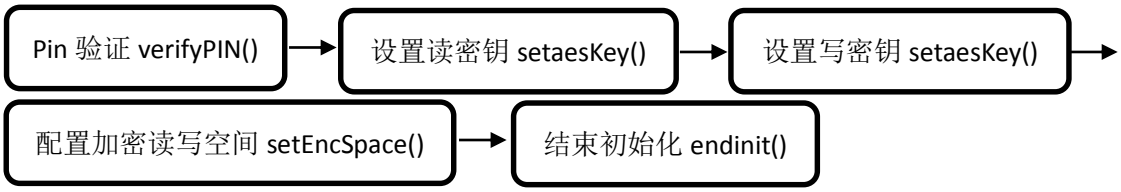
初始化芯片，每颗芯片只需初始化一次

上电后即可进行多次认证



- **加密读写数据**

初始化芯片，每颗芯片只需初始化一次



上电后即可进行多次加密读写

- **明文读写数据**

无需初始化，上电后即可进行多次明文读写

6 通信指令

6.1 通信格式

MCU 与ICP209的通信采用标准 I²C 通信协议，最高速率可以达到 150Kbps。通信过程中需要把指令打包成如下格式：

MCU→ICP209	1 字节指令长度	指令+参数	异或值
MCU←ICP209	1 字节指令长度	数据+状态字	异或值

交互过程采用一问一答形式，即：MCU 发送一条指令到ICP209，ICP209开始执行运算，此时如果 IIC 总线有数据，ICP209不会回应 ACK，当运算执行完成，MCU 开始读取运算

结果，此时 ICP209才会回应 ACK。

MCU 发送数据到 ICP209

起始信号->0x54->数据（LV）+XOR->结束信号

MCU 读取ICP209数据：

起始信号->0x55->数据（LV）+XOR ->结束信号

其中时钟线 SCL 在整个交互过程都由 MCU 控制。在 MCU 发送数据到ICP209的过程中，MCU 控制数据线 SDA 发送数据，ICP209回应 ACK；在 MCU 从ICP209读取数据时，第一个地址字节 0x55 由 MCU 发送，ICP209回应 ACK，剩余字节由ICP209控制数据线 SDA 发送，MCU 回应 ACK。

6.2 通信示例

以 MCU 从ICP209取 16 字节随机数为例，指令代码为 0x01，MCU 与ICP209完整的交互过程如下：

- MCU→ICP209：0x54 0x01 0x01 0x00

0x54 是ICP209的写地址，0x01 是指令的长度，0x01 是取随机数指令，0x00 是从指令长度（0x01）到指令结束（0x01）的异或值

- MCU←ICP209：0x55 0x011 0x11 0x22 0x33 0x44 0x55 0x66 0x77 0x88 0x99 0x00 0xAA 0xBB 0xCC 0xDD 0xEE 0xFF 0x90 0x81

0x55 是ICP209的读地址，0x11 是ICP209回复数据的长度，0x11~0x90 是ICP209回复的数据，其中 0x11~0xFF 是随机数，0x90 是状态字，代表执行成功，0x81 是从数据长度（0x11）到状态字（0x90）的异或值。

7 ICP209 安全芯片指令表

初始化指令

说明	指令	参数	返回	状态字
验证 PIN	0x27	8 字节 Pin	无	0x 90：成功 0x 6A：Pin 错误 0x 6D：指令不支持
生成不可导出认证密钥对和证书	0x 34	24 字节根私钥	无	0x 90：成功 0x 6A：失败 0x 6D：指令不支持
设置对称认证密钥	0x 42	16 字节密钥	无	0x 90：成功 0x 6D：指令不支持
设置读写密钥	0x 43	1 字节读写类型，	无	0x 90：成功

		0x0-写，0x1-读 16 字节密钥		0x 6D：指令不支持
配置密文读写空间	0x 47	1 字节密文读写空间(单位：页)	无	0x 90：成功 0x 6D：指令不支持
配置从机地址	0x48	1 字节地址，最低位为 0	无	0x 90：成功 0x 6D：指令不支持
熔断(熔断后不再支持初始化指令)	0x 90	无	无	0x 90：成功

应用指令

说明	指令	参数	返回	状态字
读取证书	0x 35	无	112 字节证书	0x 90：成功
非对称认证	0x 36	16 字节随机数	48 字节签名值	0x 90：成功 0x 6A：失败
对称认证	0x 37	16 字节随机数	16 字节密文	0x 90：成功 0x 6A：失败
加密写	0x 38	2 字节地址 1 字节明文长度 密文数据	无	0x 90：成功 0x 6A：失败
加密读	0x 39	2 字节地址 1 字节明文长度	密文数据	0x 90：成功 0x 6A：失败
明文写	0x 40	2 字节地址 1 字节明文长度 明文数据	无	0x 90：成功 0x 6A：失败
明文读	0x 41	2 字节地址 1 字节明文长度	明文数据	0x 90：成功 0x 6A：失败
生成可导出公私钥	0x 28	无	48 字节公钥 24 字节私钥	0x 90：成功 0x 6A：失败
取随机数	0x 01	无	16 字节随机数	0x 90：成功 0x 6A：失败
哈希算法	0x50	1 字节长度 算法输入数据	32 字节算法结果	0x 90：成功 0x 6A：失败

附录 ：

A. 工作环境

符号	描述	最小值	最大值	条件
To	工作温度（℃）	-25	85	
TS	存储温度（℃）	-40	125	
Vesd（HBM）	静电限值（kV）		±6	VCC、GND、CLK、RST、SIO、GPIO0
			±4	LA、LB
Vesd(CDM)	静电限值(V)		±500	所有管脚
Ilu	Latch-up 电流值（mA）		±200	Vin>VCC

B. 密钥说明

ICP209安全芯片有以下几种密钥：

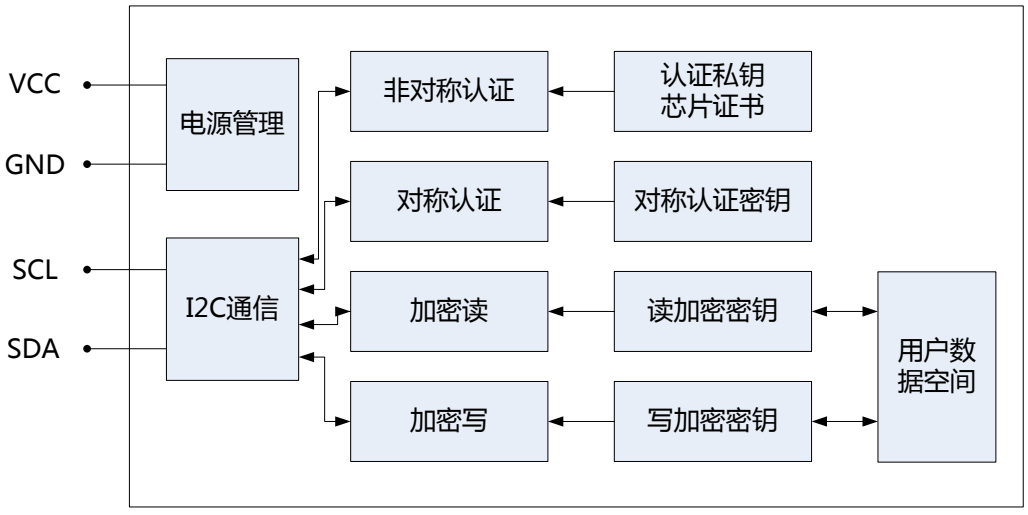
根公钥/根私钥：建议通过 0x28 指令生成(详见第 6 节指令表)，由用户保存根私钥，供出厂初始化时生成证书时使用，公私钥保存在 MCU 端，用于验证证书。

认证公钥/认证私钥：出厂初始化时调用指令 0x34 时由安全芯片生成，生成后认证私钥保存在安全芯片，无法读出。

对称认证密钥：由用户管理，MCU 端保存，出厂初始化时调用 0x42 指令初始化到安全芯片。

读/写加密密钥：由用户管理，MCU 端保存，出厂初始化时调用 0x43 指令初始化到安全芯片。

C. PKI 方案功能图



ICP209方案功能图