RJGT102 V3.02 数据手册

武汉瑞纳捷电子技术有限公司

—Wuhan RunJet Electronic technology co. Ltd

特性

- 高性能防复制加密芯片
- 提供看门狗定时器和对外复位功能
- SHA-256 加密认证
- 提供用于写入用户自定义的 EEPROM 单元
- 遵循标准 I²C 总线协议
- 可锁定的 64 位用户 ID 号
- 2.97V～3.63V 的工作电压
- 可以对密钥和每个数据存储区单独加写保护
- 独立看门狗定时器，溢出周期用户可自定义
- POR（Power On Reset）上电复位延迟时间由厂家编程
- 支持低功耗模式

应用

- 汽车导航，车载 DVD，汽车定位，汽车监控，行车记录仪
- 手机，通信模块，路由器，对讲机
- 监控设备，IP Cmarera，NVR/DVR

订购信息

型号	功能	封装引脚
RJGT102WDP8	看门狗复位、加密保护	SOP-8L
RJGT102P8	加密保护	SOP-8L
RJGT102WDT6	看门狗复位、加密保护	SOT23-6L
RJGT102T6	加密保护	SOT23-6L

目录

1.简介

RJGT102 在单个芯片内集成了 176Byte 的 EEPROM，128Byte 寄存器页，8Byte 密钥，8Byte 的用户 ID/Serial Number，和 16Byte 的控制信息。RJGT102 是基于 SHA-256 的加密认证算法,同时提供可配置的看门狗定时器和对外复位功能，与 MCU 可通过 I²C 串行接口通信，芯片支持低功耗模式。

1.1 特性

1.1.1 安全性

— 高性能防复制保护集成电路

— SHA-256 加密算法认证

— 一次性可编程单元

1.1.2 存储器

— 提供用于写入用户自定义的 EEPROM 单元

1.1.3 外部设备特性

— 提供 I²C 外部总线接口，器件地址为 0x68。支持标准模式 100Kbit/s，快速模式 400Kbit/s 的数据传输

— 独立看门狗定时器，溢出周期用户可自定义

1.1.4 特殊功能

— 内置 POR 电路，可监控控制器及存储体的供电状态，对其进行复位

— 唯一对应的用户 ID

1.1.5 工作电压

— 提供单独的 3.3V 电源，内置 LDO 实现 3.3V 转 1.8V

— EEPROM 供电电压 1.8V

1.1.6 封装

— SOP-8L，SOT23-6L

1.2 RJGT102 架构图

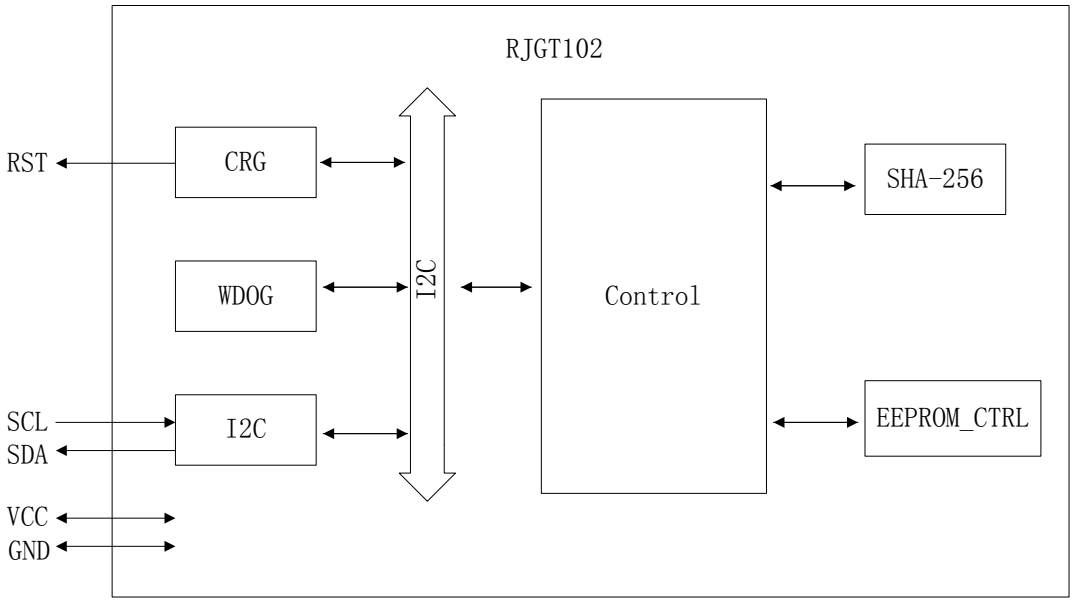


图 1-1 架构图

RJGT102 内部包括模拟模块（LDO,POR 和 OSC）,EEPROM 模块和数字逻辑模块等，控制引擎是其控制中心。RJGT102 芯片包含指令寄存器、源地址寄存器、目的地址寄存器等，该芯片根据指令寄存器的值进行译码，进行 SHA-256 运算和搬移等操作，完成认证加密工作。

1.3 引脚配置

1.3.1 SOP-8L 引脚配置

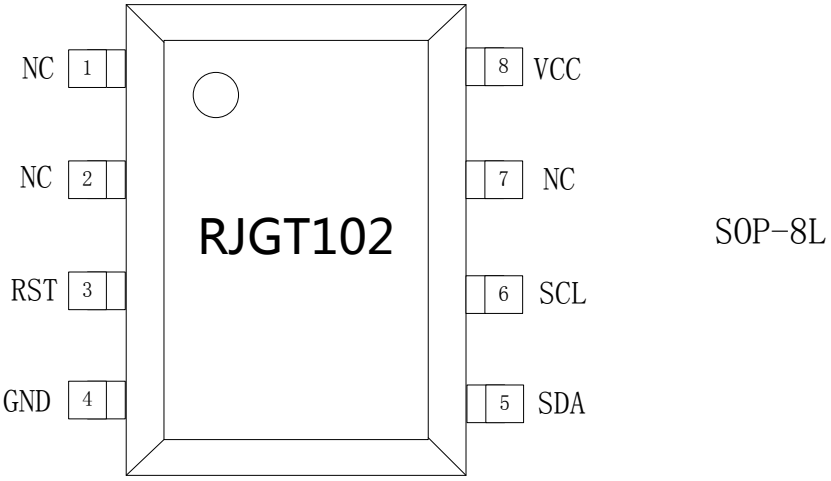


图 1-2 SOP-8L 引脚图

引脚	引脚名	描述	注释
1	NC		
2	NC		
3	RST	复位输出	可配
4	GND	接地	
5	SDA	I2C² C 串行数据，CMOS 输入，开路输出，双向 I/O 端口	
6	SCL	I2C² C 串行时钟输入端口	
7	NC		
8	VCC	数字电源电压	

表 1-1 SOP-8L 引脚说明

1.3.2 SOT23-6L 引脚配置

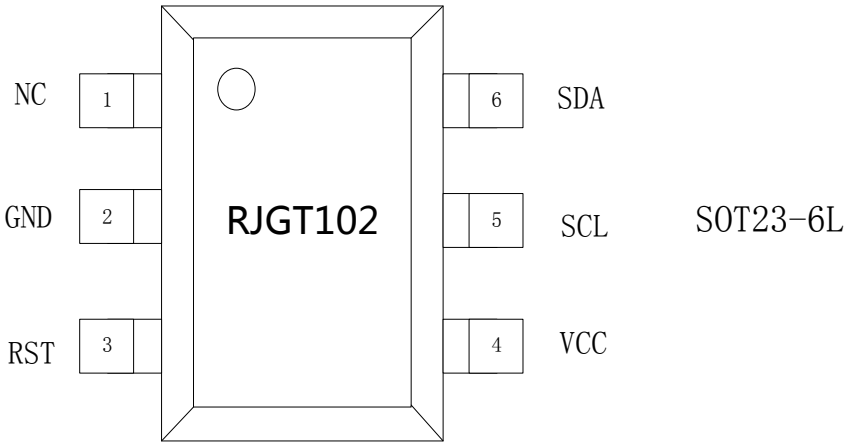


图 1-2 SOT23-6L 引脚图

引脚	引脚名	描述	注释
1	NC		
2	GND	接地	
3	RST	复位输出	可配
4	VCC	数字电源电压	
5	SCL	I2Cl² C 串行时钟输入端口	
6	SDA	I2Cl² C 串行数据，CMOS 输入，开路输出，双向 I/O 端口	

表 1-2 SOT23-6L 引脚说明

2. EEPROM 和寄存器

EEPROM 空间共为 176Byte（1468Bit），空间按功能分为数据存储区、密钥存储区和控制存储区等。

2.1 数据存储区

数据存储区分为 4 个页（PAGE0～3），每页为 32 个字节大小。下表为数据存储区中每个寄存器的地址划分。

寄存器名称	寄存器描述	寄存器地址	位宽	寄存器类型
PAGE0	数据区 0	0x00～0x1F	8	RW
PAGE1	数据区 1	0x20～0x3F	8	RW
PAGE2	数据区 2	0x40～0x5F	8	RW
PAGE3	数据区 3	0x60～0x7F	8	RW

表 2-1 数据寄存器地址划分

注：对 Page0～3 的读写操作均需要先认证才能进行相应的读写（InitPage 命令不需要认证，但 InitPage 命令只能使用 1 次，使用一次后硬件自动禁掉 InitPage 命令）。

2.2 密钥存储区

密钥存储区寄存器分为 8 字节密钥、8 字节关键常数、8 字节用户 ID 或序列号，其地址的划分如下：

寄存器名称	寄存器描述	寄存器地址	位宽	寄存器类型
KEY	8Byte KEY+8Byte constans	0x80～0x8F	8	WO
UID_SN	64bit UID/Serial Number	0x90～0x97	8	RW
RESERVED	保留寄存器	0x98～0x9F	8	N/A

表 2-2 密钥区寄存器地址划分

注： 对 KEY 区域的操作只能通过 InitKey、GenKey 命令写入，不能读出。只能通过 InitUid 命令对 UID_SN 区域写，并通过 ReadMem 命令读，读 UID_SN 区域不需要身份认证。

2.3 控制存储区

控制存储区的大小为 16 字节，其包含的寄存器分为：看门狗、复位控制寄存器、保护控制寄存器等

寄存器名称	寄存器描述	寄存器地址	位宽	寄存器类型
WDOG_CNT	WDOG 喂狗间隔时间（4MHz 时钟）	0xA0～0xA2	8	RW
WDG_RST_CTRL	WDOG、RST 管脚控制信号	0xA3	8	RW
RST_CNT	RST 管脚输出有效复位信号脉冲宽度（4MHz 时钟）	0xA4～0xA6	8	RW
RESERVED	保留寄存器	0xA7	8	RW
PRT_PAGE0	保护寄存器：写入 0x5A 后，数据区 0 禁止写入	0xA8	8	RW
PRT_PAGE1	保护寄存器,写入 0x5A 后，数据区 1 禁止写入	0xA9	8	RW
PRT_PAGE2	保护寄存器：写入 0x5A 后，数据区 2 禁止写入	0xAA	8	RW
PRT_PAGE3	保护寄存器：写入 0x5A 后，数据区 3 禁止写入	0xAB	8	RW
PRT_KEY	保护寄存器:写入 0x5A 后，InitKey 命令被禁止	0xAC	8	RW
PRT_UID_SN	保护寄存器：写入 0x5A 后，UID/SN 区域禁止写入	0xAD	8	RW
PRT_CTRL	保护寄存器：写入 0x5A 后，0xA0~0xA6 区域禁止写入	0xAE	8	RW
DISABLE_INIT_PAGE	保护寄存器。写入 0x5A	0xAF	8	RW

	后，InitPage 命令被禁止			

表 2-3　控制存储区地址划分

注： 1.通过 WriteMem 和 ReadMem 命令对控制寄存器(0xA0～0xAF)操作，不需要进行身份认证。

2.保护寄存器一旦成功写入 0x5A 即永久生效，不能再次更改（类似于熔丝），即使芯片掉电也无法取消保护功能。向被保护的区域写数据，RJGT102 会终止命令，并返回异常状态（ES=0x11）。

2.4　其他寄存器定义

RJGT102 芯片除数据、密钥、控制等存储区外，还有其他许多的寄存器。RJGT102 芯片的芯片版本号为 GT102（0x71843032），下面简单介绍其他寄存器。

寄存器名称	寄存器描述	寄存器地址	位宽	寄存器类型
CMD	命令寄存器	0xB0	8	RW
Tar 注1	源地址寄存器	0xB1	8	RW
TAd	目的地址寄存器	0xB2	8	RW
ES 注1	状态寄存器	0xB3	8	RO
Sys_Ctrl	低功耗控制寄存器	0xB4	8	RW
RESERVED	保留寄存器	0xB5～0xB7	8	RW
VERSION0	芯片版本号	0xB8	8	RO
VERSION1	芯片版本号	0xB9	8	RO
VERSION2	芯片版本号	0xBA	8	RO
VERSION3	芯片版本号	0xBB	8	RO
RESERVED	保留寄存器	0xBC~0xBF	8	RW
BUFFER 注2	数据交换区	0xC0~0xFF	8	RW

表 2-4　其他寄存器地址划分

注：

1、源地址寄存器用来指定参与 MAC 计算的 PAGE 区，写入某个 PAGE 区的首地址（0x00/0x20/0x40/0x60）即可指定。

2、状态寄存器 ES 只有第 4 位和第 0 位有效，是一个只读寄存器，用于验证写入的完整性，00 表示

正在执行，01 表示正常执行完，11 表示异常执行完，10 表示非法状态。

3、从 RJGT102 读 PAGEn（n=0,1,2,3）、UID_SN（0x90～0x97）、控制寄存器（0xA0～0xAF）时，要通过数据交换区（0xC0 开始的地址）读取。向 RJGT102 更新 PAGEn 数据（InitPage 和 WritePage）、更新密钥（InitKey 和 GenKey）、下发主机认证随机数（AuthDev）等操作时，要预先将数据写入到数据交换区（0XC0 开始的地址），再执行相应的命令。当用 RJGT102 来认证主机时，要先将主机生成的 32 字节 MAC 存放到数据交换区后 32 字节（0xE0～0xFF）里，再执行认证命令。

3. I/O 端口

3.1 ESD 保护电路

RJGT102 的引脚都内置了 ESD 保护电路，如图 3-1 所示，对芯片起到了有效的保护作用。所有的引脚（包括电源和地引脚）都采用了正负脉冲、HBM 和 MM 两种测试模型进行测试，确保每个引脚的 ESD 性能符合标准要求。

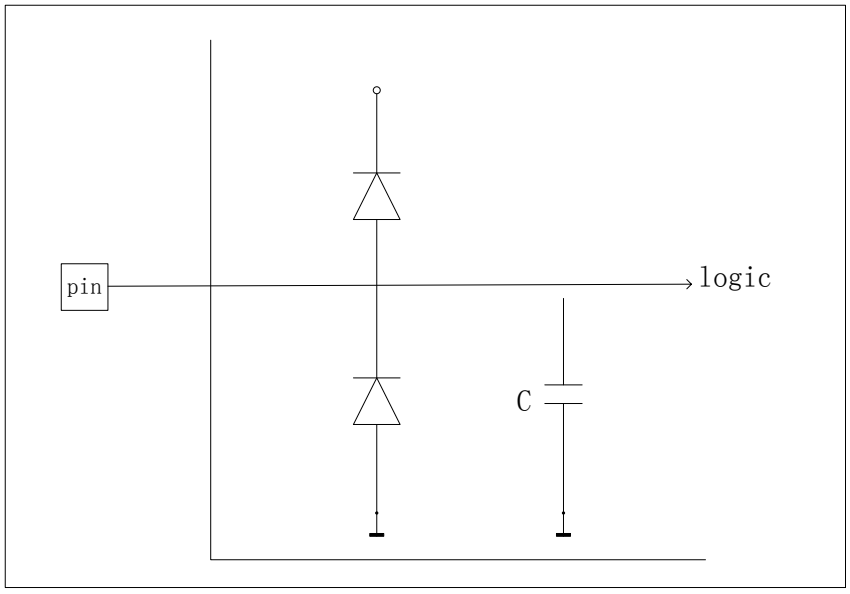


图 3-1　ESD 保护电路图

3.2 I/O 类型

3.2.1 时钟输入端口（SCL）

RJGT1102 芯片的 SCL 时钟输入单元是一个 CMOS 输入的缓存区。

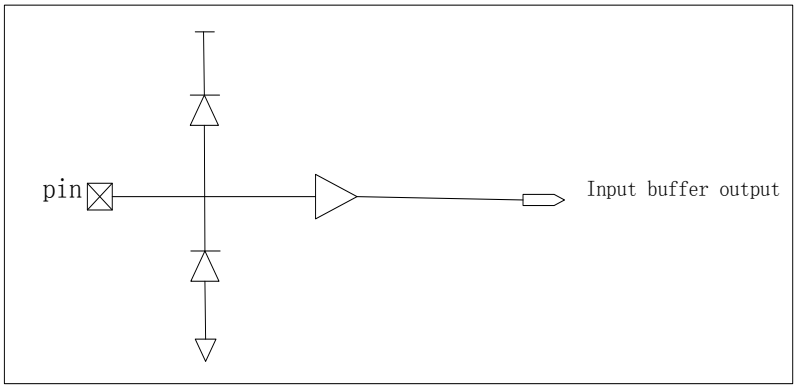


图 3-2 输入端口原理图

3.2.2 双向端口（SDA）

RJGT102 芯片的 SDA 数据单元是由 CMOS 输入和 N 沟道漏极开路输出（2mA）组成的双向缓存区。

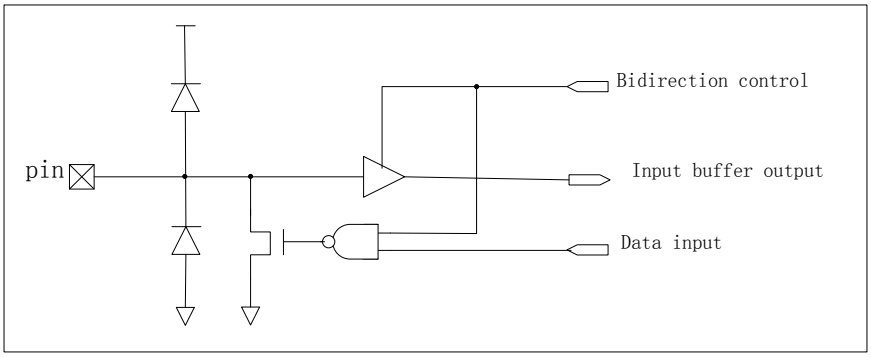


图 3-3 双向端口原理图

3.3 SDA 和 SCL I/O 级特性

快速模式下 I²C 总线器件的 I/O 级、I/O 电流、毛刺抑制、输出斜率控制和管脚电容的特性如下表：

参数	符号	标准模式		快速模式		单位
		最小值	最大值	最小值	最大值	
低电平输入电压： 固定的输入电平 V_{DD} 相关的输入电平	V_{IL}	-0.5 -0.5	1.5 0.3 V_{DD}	n/a -0.5	n/a 0.3 V_{DD}	V V
高电平输入电压 固定的输入电平 V_{DD} 相关的输入电平	V_{IH}	3.0 0.7 V_{DD}		n/a 0.7 V_{DD}	n/a	V V
Schmitt 触发器输入的迟滞： V_{DD} >2V V_{DD} <2V	V_{hys}	n/a n/a	n/a n/a	0.05 V_{DD} 0.1 V_{DD}		V V
有 3mA 下拉电流时的低电平输出电压 V_{DD} >2V V_{DD} <2V	V_{OL1} V_{OL2}	0 n/a	0.4 n/a	0 0	0.4 0.2 V_{DD}	V V
总线电容从 10pF 到 400pF 的 V_{IHmin} 到 V_{ILmax} 输出下降时间	t_{of}		250	20+0.1C_b	250	ns
输入滤波器必须抑制的毛刺脉宽	T_{SP}	n/a	n/a	0	50	ns
输入电压在 0.1 V_{DD}～0.9 V_{DDmax} 的各个管脚输入电流	I_i	-10	10	-10	10	uA
每个 I/O 管脚的电容	C_i		10		10	pF

表 3-1　IO 级特性

注：1、最大的 VIH= VDDma+0.5；

2、Cb=总线线路的电容，单位是 pF；

3、如果 VDD 被关断，快速模式器件的 I/O 管脚必须不能阻塞 SDA 和 SCL 线；

4、n/a=不可使用。

4. I²C 接口

I²C 接口通过 SDA 和 SCL 端口连接 RJGT102，SDA 是双向线路，SCL 是单向线路，为了提高驱动能力需要一个上拉电阻连接到 VDD。当总线空闲时，这两条线路都是高电平。SDA 线上的数据必须在时钟的高电平周期保持稳定，只有在时钟线 SCL 为低电平时才能改变 SDA 数据线状态。

4.1 I²C 总线总体特征

1、只要求两条总线：一条数据线（SDA），一条时钟线（SCL）；

2、连接到总线上的总线器件都有唯一器件地址；

3、它是一个真正的多主机总线，如果两个或更多的主机同时数据传输可以通过冲突检测和仲裁防止数据被破坏；

4、8 位数据传输速率可达 100Kbit/s，快速模式下可达 400Kbit/s；

5、连接到相同总线上的 IC 数量受总线上的最大电容 400pF 限制。

4.2 低功耗待机模式

系统提供低功耗待机模式：

1. 在 I²C 处于 IDLE 状态，并且加密引擎已经处理完后，系统进入低功耗待机状态；
2. 低功耗待机下的几种状态：
   i. *WDOG 使能：OSC 使能，关断除 WDOG、I²C 外模块的时钟；
   ii. *WDOG 关闭：OSC 不使能，关闭所有模块时钟；
3. 当 I²C 上有命令传输时，退出低功耗待机状态；
4. 低功耗状态在重新上电后就会自动退出。

RJGT102 进入低功耗模式的条件：SCL 和 SDA 信号处于高电平，I²C 总线被停止超过 2 秒。当 I²C 上有起始信号产生时，RJGT102 即可退出低功耗模式。

如果 SDA 线保持低电平超过 t_{WLO},设备将退出低功耗模式，并在延迟 t_{WHI}时间后，开始接受命令，在低功耗模式下，设备忽略任何 SCL 信号。

4.3 I² C 总线位传输

4.3.1 起始位与停止位

起始信号如图 4-1 所示。当时钟线 SCL 为高电平时，数据线 SDA 从高电平到低电平的变化将形成起始信号。

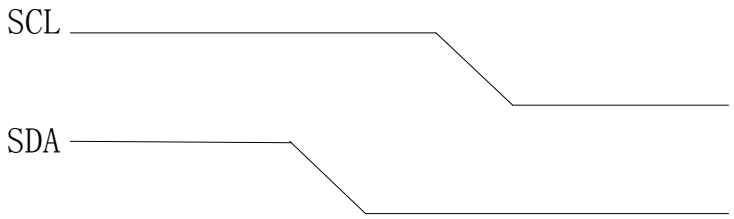


图 4-1 起始信号

终止信号如图 4-2 所示。当时钟线 SCL 为高电平时，数据线 SDA 从低电平到高电平的变化将形成终止信号。

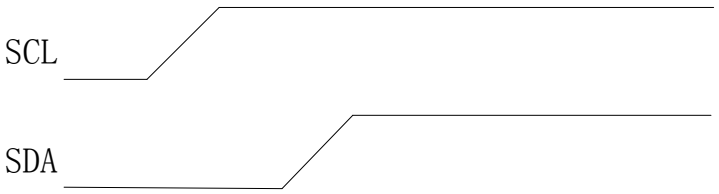


图 4-2 终止信号

4.3.2 数据有效性

在 I² C 总线启动后或应答信号后的第 1～8 个时钟脉冲对应于一个字节的 8 位数据传输。脉冲高电平期间，数据串行传输；低电平期间为数据准备，容许总线数据电平变换。如图 4-3 所示。

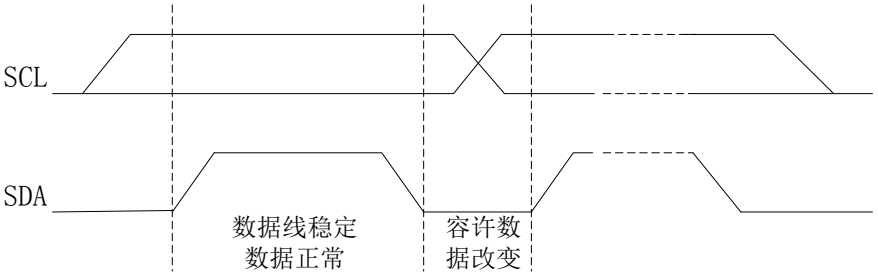


图 4-3 数据有效性

4.4 I² C 数据传输

4.4.1 I² C 字节格式

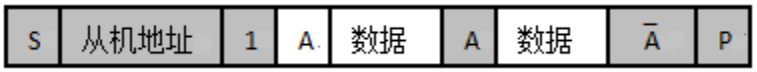
I²C 总线上传送的数据信号是广义的，既包括地址信号，又包括真正的数据信号。在起始信号后必须传送一个 7 位的从机地址(0x68)，第 8 位是数据的传送方向位(R/T)，用“0”表示主机发送数据（T），“1”表示主机接收数据（R)。每次数据传送总是由主机产生的终止信号结束。但是，若主机希望继续占用总线进行新的数据传送，则可以不产生终止信号，马上再次发出起始信号对另一从机进行寻址。在总线的一次数据传送过程中，可以有以下几种组合方式：

（1） 主机向从机发送数据，数据的传送方向在整个过程终不变：

注：有阴影部分表示数据由主机向从机传送，无阴影部分则表示数据由从机向主机传送。

A 表示应答，A 非表示非应答（高电平），S 表示起始信号，P 表示终止信号。

（2） 主机在第一个字节后，立即从从机读数据：



（3） 在传送过程中，当需要改变传送方向时，起始信号和从机地址都被重复产生一次，但两次读/写方向位正好反相。

4.4.2 应答

I²C 总线上的所有数据都是以 8 位字节传送的，发送器每发送一个字节，就在时钟脉冲 9 期间释放数据线，由接收器反馈一个应答信号。 应答信号为低电平时，规定为有效应答位（ACK 简称应答位），表示接收器已经成功地接收了该字节；应答信号为高电平时，规定为非应答位（NACK），一般表示接收器接收该字节没有成功。 对于反馈有效应答位 ACK 的要求是，接收器在第 9 个时钟脉冲之前的低电平期间将 SDA 线拉低，并且确保在该时钟的高电平期间为稳定的低电平。 如果接收器是主控器，则在它收到最后一个字节后，发送一个 NACK 信号，以通知被控发送器结束数据发送，并释放 SDA 线，以便主控接收器发送一个停止信号 P。

4.5 时钟的同步

在 I²C 总线上传送信息时的时钟同步信号是由挂接在 SCL 线上的所有器件的逻辑“与”完成的。SCL 线上由高电平到低电平的跳变将影响到这些器件，一旦某个器件的时钟信号下跳为低电平，将使 SCL 线一直保持低电平，使 SCL 线上的所有器件开始低电平期。此时，低电平周期短的器件的时钟由低至高的跳变并不能影响 SCL 线的状态，于是这些器件将进入高电平等待的状态。当所有器件的时钟信号都上跳为高电平时，低电平期结束，SCL 线被释放返回高电平，即所有的器件都同时开始它们的高电平期。其后，第一个结束高电平期的器件又将 SCL 线拉成低电平。这样就在 SCL 线上产生一个同步时钟。可见，时钟低电平时间由时钟低电平期最长的器件确定，而时钟高电平时间由时钟高电平期最短的器件确定。如图 4-4 所示。

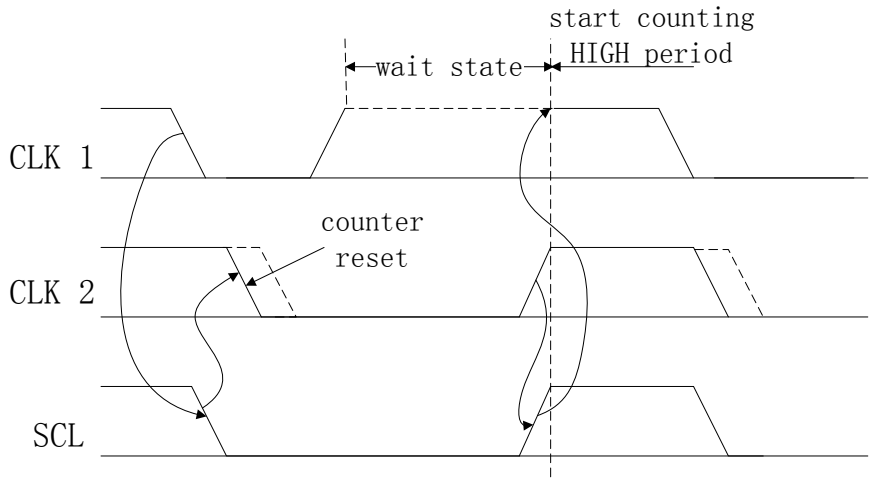


图 4-4 时钟的同步

4.6 I² C 总线寻址

4.6.1 7 位地址格式

数据的传输遵循图 4-5 所示的格式。在起始条件 S 后, 发送了一个从机地址 ，这个地址共有 7 位，对应 I² C 器件地址为 0x68，起始信号后的第一位是地址最高位（MSB）。紧接着的第 8 位是数据方向位 (R/W), 0 表示发送数据，写 1 表示读取数据 。读 数据传输一般 由主机产生的停止位 P 终止 但是 如果主机仍希望在总线上通讯 它可以产生重复起始条件 。

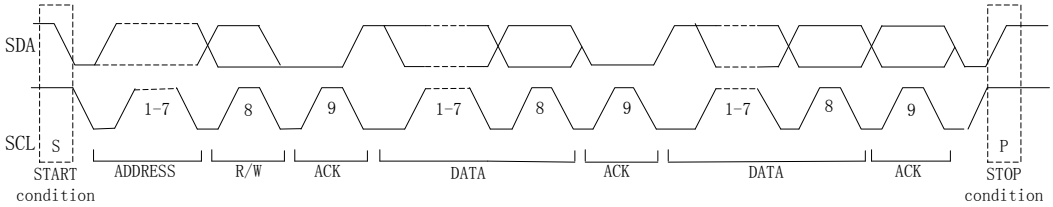


图 4-5 完整的数据传输

4.6.2 7 位地址寻址

I² C 总线有明确规定：采用 7bit 寻址字节（寻址字节是起始信号后的第一个字节）。

位：	7	6	5	4	3	2	1	0
	从机地址（0x68）							R/ $\overline{W}$

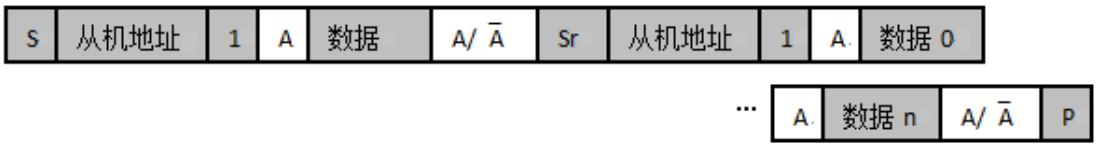
注：D7～D1 位组成从机的地址。D0 位是数据传送方向位，为“0”时表示主机向从机写数据，为“1”时表示主机由从机读数据。

主机发送地址时，总线上的每个从机都将这 7 位地址码和自己的地址比较，如果相同，则认为自己被主机寻址，根据 R/ $\overline{W}$ 位将自己确认为发送器或者接收器。从机的 7 位寻址位为固定位，只容许一个器件接入到总线系统中。

4.7 数据传输

写入：发送的第一个字节是从机地址和写标志位，第二字节是寄存器地址，接下来的是数据。

读出：发送的第一个字节是从机地址和写标志位，第二字节为要读的寄存器，第三字节是从机地址和读标志位，接下来的数据就是读出来的数据。



注：A 表示应答， A 非表示非应答（高电平），S 表示起始信号，P 表示终止信号。

4.8 I² C 总线特性

在规定的 SCL 时钟最小高电平和低电平周期决定了最大的位传输速率，标准模式器件是 100kbit/s 快速模式器件是 400kbit/s。标准模式和快速模式 I²C 总线器件必须能在它们最大的位速率下传输，或者是能在该速度下发送或接收。

I²C 总线 SDA 和 SCL 线路参数如表 4-1 所示

参数	符号	标准模式		快速模式		单位
		最小值	最大值	最小值	最大值	
SCL 时钟频率	f_{scl}	0	100	0	400	kHz
（重复）起始条件的保持时间。在这个周期后产生第一个时钟脉冲。	$t_{HD：STA}$	4.0		0.6		us
SCL 时钟的低电平周期	t_{LOW}	4.7		1.3		us
SCL 时钟的高电平周期	t_{HIGH}	4.0		0.6		us
重复起始条件的建立时间	$t_{SU：STA}$	4.7		0.6		us
数据保持时间	$t_{HD：DAT}$	0	3.5	0	0.9	us
数据建立时间	$t_{SU：DAT}$	250		100		ns
SDA 和 SCL 信号的上升时间	t_r		1000	$20+0.1C_b$	300	ns
SDA 和 SCL 信号的下降时间	t_f		300	$20+0.1C_b$	300	ns
停止条件的建立时间	$t_{SU：STO}$	4.0		0.6		us
停止和启动条件的总线空闲时间	t_{BUF}	4.7		1.3		us
每条总线线路的电容负载	C_b		400		400	pF
每个连接的器件低电平时的噪声容限（包括迟滞）	V_{nL}	$0.1V_{DD}$		$0.1V_{DD}$		V
每个连接的器件高电平时的噪声容限（包括迟滞）	V_{nH}	$0.2V_{DD}$		$0.2V_{DD}$		V

注：1、Cb=一条总线线路的总电容，单位是 pF；

2、n/a=不可用；

I²C 总线时序定义如图 4-6 所示。$t_{HD;DAT}$

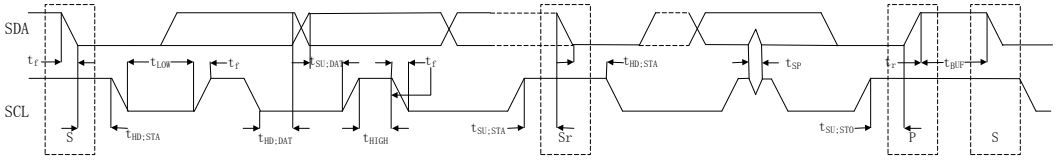


图 4-6 I²C 总线时序图

5. 初始化

RJGT102 内部包含一个 POR 电路，当系统电源打开时，POR 电路将复位系统，内部所有寄存器初始化。

5.1 初始化波形

RST 在 VCC 达到上电监控阀值电压 $V_{Threshold}$ 时进入高阻态，高阻态持续时间 t_1 为 19us。复位有效极性可配，缺省默认为低电平有效，复位时间 t_2 可配置，最高为 4s。如果 MCU 是低电平复位，则复位信号加下拉电阻，反之，则加上拉电阻。初始化波形如图 5-1 所示（默认低电平有效）。

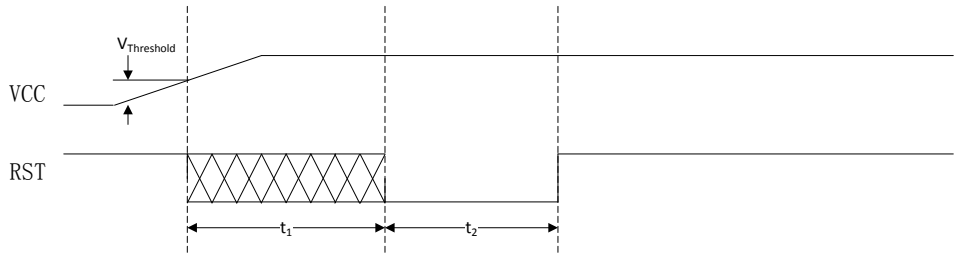


图 5-1 初始化波形

注：VCC : 3.3V 电源电压　RST:内部复位信号

6. UID 的使用

从生产管理和安全防伪的角度考虑，RJGT102芯片提供用户可编程的用户识别码(UID)，用来保证使用时每颗芯片的唯一性。使用者可根据自定义的编码规则（比如流水号），编制RJGT102芯片的UID号。在出厂前将保护寄存器PRT_UID_SN（0xAD）写0x5A即可锁定UID不被更改。

6.1 UID 使用特点

RJGT102内部存有64位的UID，，因此客户可以对自己生产的每一个产品，都设置唯一的识别号，从而对生产、测试、出库、返修等进行方便的管理。

1、64位UID寄存器地址为0x90～0x97；

2、保护寄存器PRT_UID_SN（0xAD）为非0x5A时，可以通过InitUid命令多次更改UID。

3、使用ReadMem命令（无需身份认证）可直接读出UID数据；

4、将保护寄存器PRT_UID_SN（0xAD）设置为0x5A，则UID数据被锁定无法更改(包括保护寄存器PRT_UID_SN本身)。

6.2 寄存器的具体使用

1、InitUsid命令用于初始化UID，具体操作步骤如下:

a) 清除命令寄存器，即通过I²C接口往命令寄存器（0xB0）写0x00；

b) 往Buffer（0xC0）依次写入8个byte的UID数据；

c) 填充命令寄存器（0xB0）为InitUsid命令（0xAA）；

d) 读状态寄存器（0xB3），判断是否为0x01(正常完成)，或者发生错误(0x11)。

2、读出UID：

a) 清除命令寄存器：通过I²C接口往命令寄存器（0xB0）写0x00；

b) 往目的地址寄存器（0xB2）填入UID起始地址（0x90）；

c) 填充命令寄存器（0xB0）为ReadMem命令（0x0F）；

d) 读状态寄存器（0xB3），判断是否为 0x01(正常完成)，或者发生错误(0x11)。

e) 若正常完成，则从Buffer（0xC0）地址依次读出8byte的UID数据。

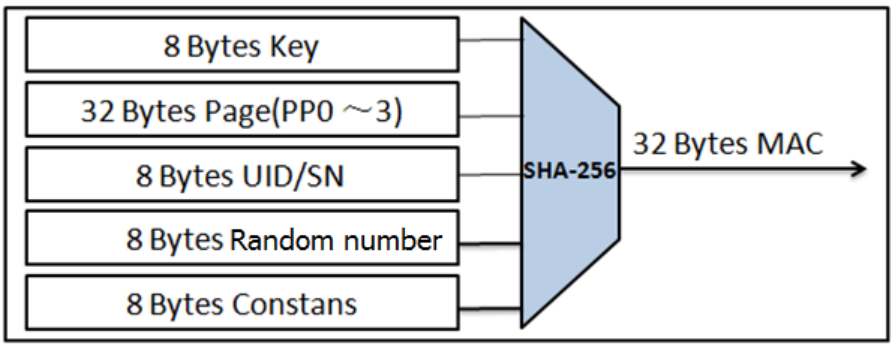
7. 加密认证

7.1 SHA-256 认证

安全哈希算法（Secure Hash Algorithm）主要适用于身份认证与数字签名,芯片内嵌SHA-256硬件电路，根据客户填写的密钥、随机数、UID等参数，SHA-256硬件电路会产生一个256位的消息摘要。当接收到消息的时候，这个消息摘要可以用来进行身份认证或者验证数据的完整性。由于SHA-256有如下特性：（1）不可以从消息摘要中复原信息；（2）两个不同的消息不会产生同样的消息摘要；（3）修改消息中的一个比特即会引起雪崩效应； 因此SHA-256电路能以很高的安全性提供身份认证功能。

7.2 SHA-256 输入与输出格式

SHA-256 加密模式输入包括 8 字节的密钥，32 字节的 PAGE 数据（任意一个 PAGE 区），8 字节的 UID，8 字节的随机数，8 字节的关键常数[注1]（芯片内部固化了）。输出 32 字节的报文摘要（MAC）。



注 1. 8 字节的关键常数为 0x80,0x00,0x00,0x00,0x00,0x00,0x01,0xb8

2. 随机数没有物理寄存器，主机下发的 8 字节随机数直接存放在数据交换区 0xC0 to 0xC7 中参与 MAC 计算。

8. 上电复位设计

8.1 WDOG 工作模式

1、 芯片支持 WDOG 规格可配（通过配置 EEPROM）；
2、 喂狗间隔时间可配（通过配置 EEPROM）；
3、 WDOG 产生的复位信号可以复位整个芯片；
4、 通过 I²C 接口的 STOP 信号产生喂狗信号 。

8.2 复位管脚输出

1、 复位有效电平极性可配；
2、 复位源头为 POR 和 WDOG。若需要 POR 输出，必须设置 RST 引脚使能；
3、 复位信号输出持续时间可配，一个复位周期，只有一个复位信号输出；
4、 配置信息存入 EEPROM 中，并有锁定功能。

8.3 功能描述

在由单片机构成的微型计算机系统中，由于单片机的工作常常会受到来自外界电磁场的干扰，造成程序跑飞而陷入死循环，程序的正常运行被打断，使单片机控制的系统无法继续工作，会造成整个系统陷入停滞状态，发生不可预料的后果。因此，需要看门狗复位电路来保证单片机运行状态稳定可靠， RJGT102 芯片集成了看门狗复位功能。

8.3.1 看门狗定时器

看门狗定时器电路喂狗通过 I²C 接口进行，MCU 在正常工作的时候，每隔一段时间将 SCL 或者 SDA 跳变即可完成喂狗，给 WDOG 清零。如果超过规定的时间不喂狗，WDOG 定时超过，会给出复位信号到 MCU，使 MCU 复位。

看门狗电路可监控 MCU 的工作状态。由计数比较模块、分频模块和复位计时模块组成。MCU 正常运行时，在计数值与预置值相等之前喂狗，则计数比较模块和分频模块都会被复位，不产生复位脉冲。看门狗电路可通过 I²C 总线访问。在看门狗启动之前，可以通过 I²C 总线将参数写入内部预置寄存器，启动看门狗后预置寄存器内容不可改变。

8.3.2 复位输出

复位信号用于启动或者重新启动 MPU/MCU，令其进入或者返回到预知的循环程序并顺序执行。一旦 MPU/MCU 处于未知状态，比如程序“跑飞”或进入死循环，就需要将系统复位。

RJGT102 可以在上电的过程中产生复位信号，并阻止在上电时代码执行错误。在上电过程中，当 VCC 上升，RST 保持为复位状态，当 VCC 上升超过复位阀值，内部定时器将在 10ms 后产生一个复位信号。芯片管脚 RST 输出的复位时间可以配置，最高为 4s。一旦 VCC 达到 3.3V 时，RST 将为根据复位极性配置，处于无效状态。无论何时只要电源电压降低到复位门限 2.2V 以下（即电源跌落），RST 引脚就会输出复位信号。RST 管脚的驱动电流具体参数如表 8-1 所示。

RST 极性设置高电平有效				
符号	参数（V）	最小值（V）	典型值（V）	最大值（V）
$V_{RST-out}$(未触发输出)	VCC=0.4	0.1	0.28	0.38
	VCC=2.4	0.1	0.28	0.38
	VCC=3.0	0.1	0.28	0.38
$V_{RST-out}$(触发信号输出)	VCC=0.4	0.1	0.28	0.38
	VCC=2.4	2.28	2.35	2.4
	VCC=3.0	2.85	2.95	3.0
RST 极性设置低电平有效				
符号	参数（V）	最小值（V）	典型值（V）	最大值（V）
$V_{RST-out}$(未触发输出)	VCC=0.4	0.1	0.28	0.38
	VCC=2.4	2.25	2.35	2.4
	VCC=3.0	2.85	2.95	3.0
$V_{RST-out}$(触发信号输出)	VCC=0.4	0.1	0.25	0.38
	VCC=2.4	0.1	0.25	0.5
	VCC=3.0	0.1	0.25	0.5

8.3.3 寄存器描述

WDG__RST__CTR 为芯片看门狗复位控制寄存器，如表 8-2 所示。

Bit 位	寄存器名称	寄存器描述	寄存器类型
7:6	Reserved		RW
5	RstPolarity	RST 管脚极性控制信号： 0：低电平有效； 1：高电平有效	RW
4	RstEn	RST 管脚输出使能信号： 0: 使能 RST 管脚； 1: 禁止 RST 管脚	RW
2	RdBypass	PAGE0～3 数据读出模式： 0: 与 MAC 异或后送出； 1: 直接输出；	RW
1	Reserved		RW

0	WtdogEn	0：关闭看门狗； 1：开启看门狗；	RW

9. 操作命令

RJGT102 一共包括七个操作命令：

- 初始化用户 ID 命令（InitUsid），
- 初始化器件数据命令（InitPage），
- 初始化密钥命令（InitKey），
- 主机认证命令（AuthDev），
- 更新密钥命令（GenKey），
- 更新器件数据命令（WriteMem），
- 读取器件数据命令（ReadMem）。

9.1 初始化命令

初始化命令包括初始化用户 ID 命令，初始化器件数据命令，初始化密钥命令。通过主机输入用户 ID，密钥和 PAGE 区数据到设备，设备更新数据后会将状态返回主机，进行下一

命令。

9.2 主机认证命令

在工作模式，设备在接收到主机的随机数质询后会生成一个 MAC 值，并与主机计算生成的 MAC 值进行比较，比较匹配才通过认证，主机读取 ES 状态寄存器状态值，通过认证进行相应的读/写操作。寄存器 ES 是一个只读的传输状态寄存器，用于验证写入的完整性，00 表示正在执行，01 表示正常执行完，11 表示异常执行完。

在 SHA-256 加密模式下，主机必须通过源地址寄存器指定相应的 PAGE 区域，读取数据加密计算。

9.3 更新密钥命令

用户ID是一个由用户提供的识别码，用来协助应用软件识别RJGT102相关产品，以及快速找到可用的密钥，所以初始化用户ID后，可以将保护寄存器PRT_UID_SN（0xAD）写成0x5A来锁定UID不被更改。

更新密钥命令将密钥存储区中的密钥经过 SHA-256 加密得到的 MAC1，与主机 MAC2 比较后认证通过后，将 MAC1 的低 8 个字节作为新的密钥写入到密钥存储区。

9.4 读/写命令

在执行更新器件数据命令之前，主机必须通过目的地址寄存器指定要写入的区域，并在设备中加密计算 MAC 与主机 MAC 比较，才能够将数据写入到指定的寄存器区域。在指定目的地址寄存器和 SHA-256 模式下指定源地址寄存器时，设备会验证操作的合法性，并且判断访问区域是否被保护，如果不合法或者被保护，状态寄存器报错终止读/写命令。

读取器件数据命令无需判断访问区域是否被保护，并且密钥存储区无法读取。

10. 认证方案

10.1 认证方案流程

第一步，在产品生产时，通过预设密钥、UID、PAGE 区等关键参数来进行第三方授权，并能跟踪和确认其使用，防范非法使用程序代码。

第二步，在产品使用时，每次上电自检，系统先通过 RJGT102 执行认证过程，只有具备有效密钥的 RJGT102 才能成功地返回有效 MAC 值。如果检测到无效 MAC，处理器将结束操作，认证方案流程如图 10-1 所示。

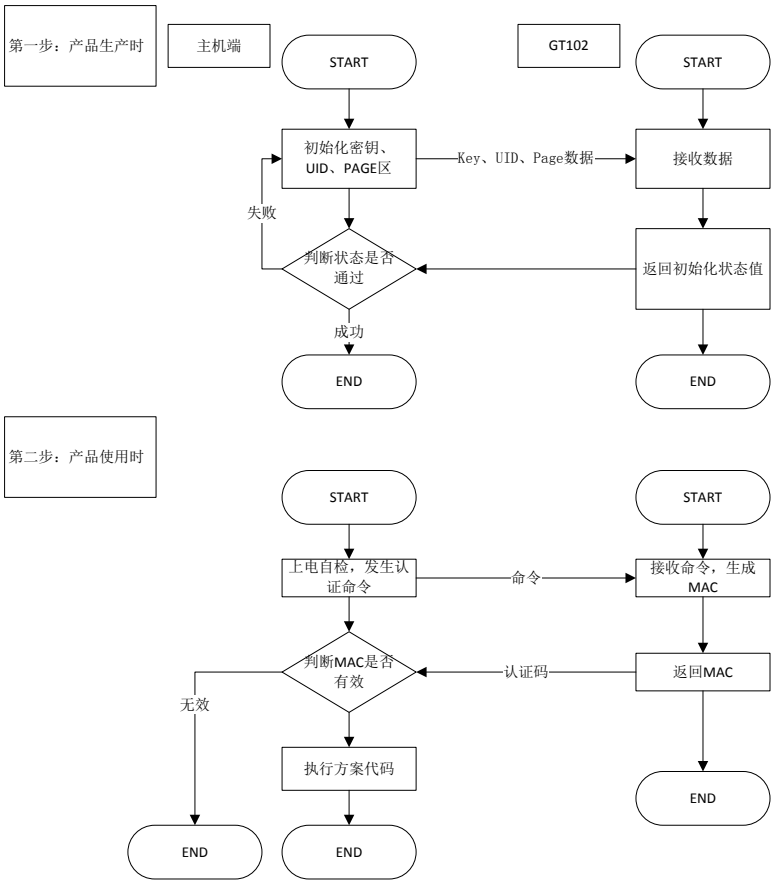


图 10-1 认证方案流程图

10.2 认证方案一

RJGT102 认证主机，认证通过后，主机确认 RJGT102 为有效的安全芯片，主机程序才能进行下一步操作。生产厂商可通过对 RJGT102 的管理和发放来保护产品的程序、硬件电路等，有效防止软件和硬件设计等知识产权被盗版。认证过程如图 10-2 所示。

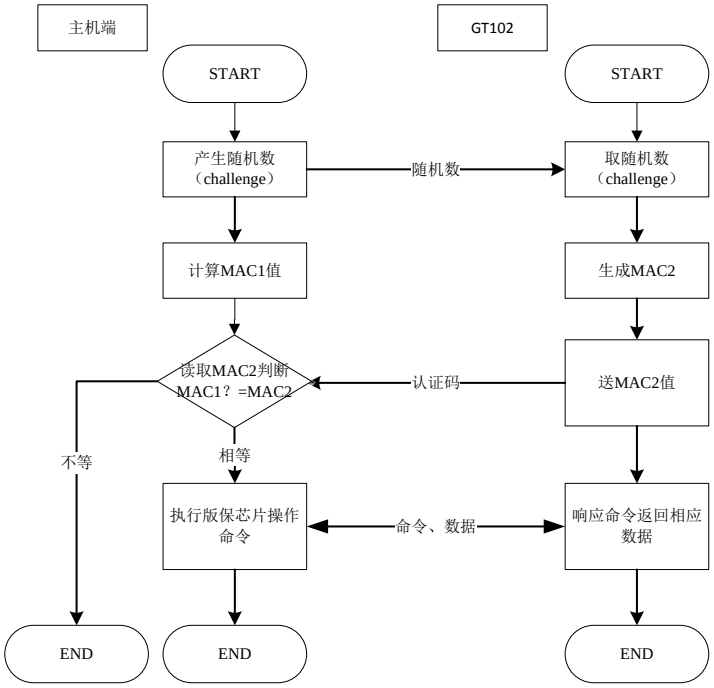


图 10-2 认证方案一

10.3 认证方案二

主机认证 RJGT102，认证通过后，RJGT102 确认主机是合法用户，可以对 RJGT102 芯片进行密钥升级，关键参数读取等操作。关键参数可以是密文形式存放，用来增强安全性。上述方案可以防止非法主机操作 RJGT102。认证过程如图 10-3 所示。

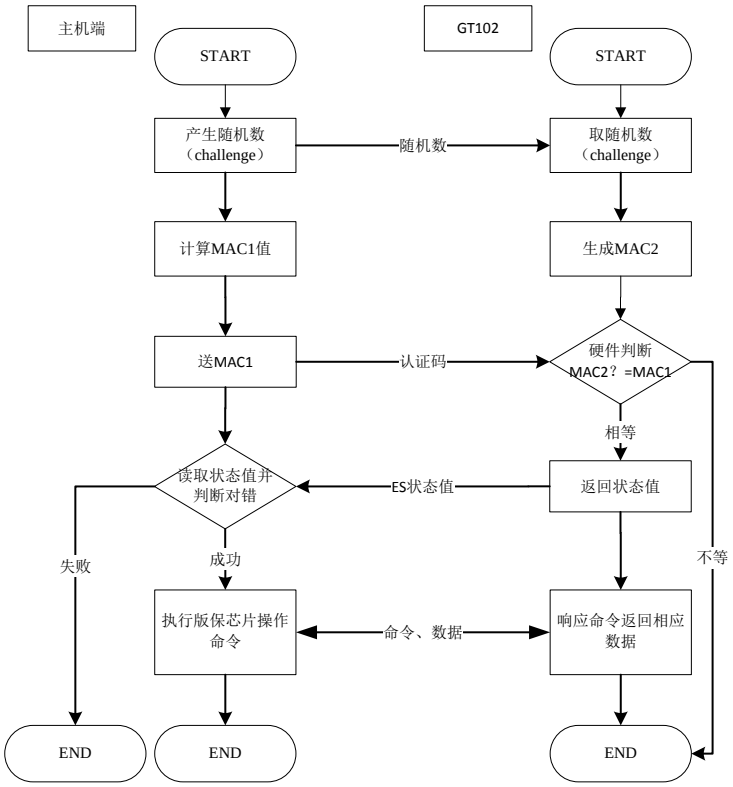


图 10-3 认证方案二

10.4 认证方案三

主机和 RJGT102 相互认证，认证通过后，主机可进入正常操作状态，同时可读取 RJGT102 中的关键参数，关键参数可以是密文形式存放，用来增强安全性。根据关键参数，主机可以选择条件执行部分子程序或完整程序。通过上述策略，主机系统可有选择的授权完整功能单元或者部分功能单元。认证过程如图 10-4 所示。

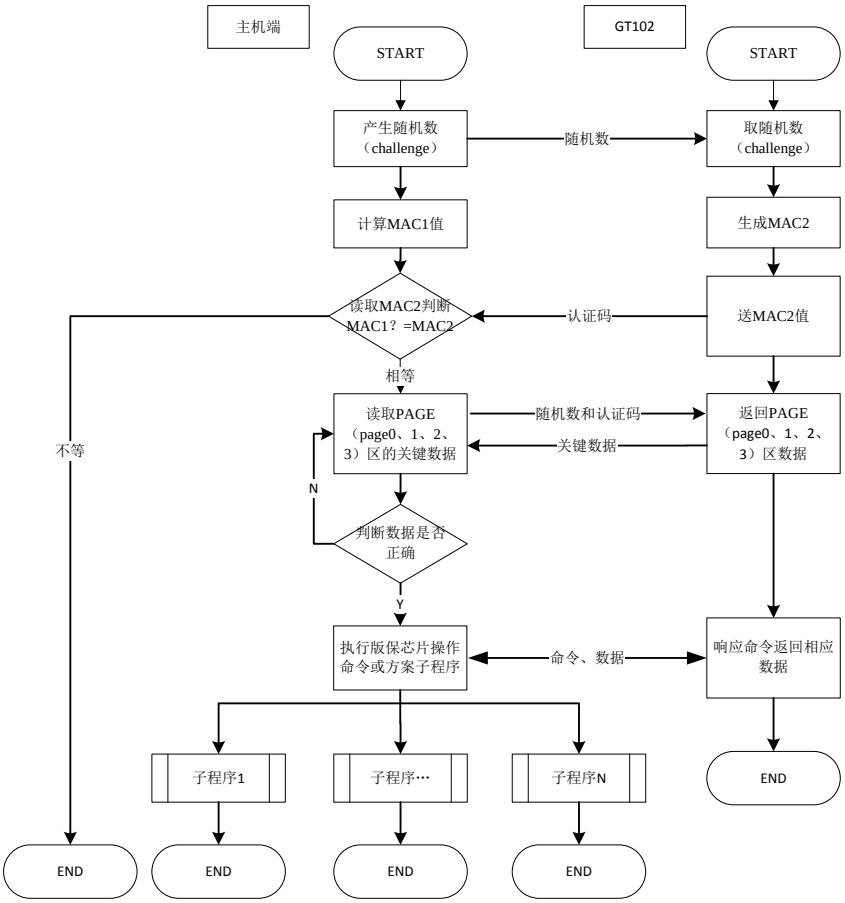

主机端
GT102
START
START
产生随机数（challenge）
随机数
取随机数（challenge）
计算MAC1值
生成MAC2
读取MAC2判断MAC1？=MAC2
认证码
送MAC2值
相等
不等
读取PAGE（page0、1、2、3）区的关键数据
随机数和认证码
关键数据
返回PAGE（page0、1、2、3）区数据
N
判断数据是否正确
Y
执行版保芯片操作命令或方案子程序
命令、数据
响应命令返回相应数据
子程序1
子程序…
子程序N
END
END
END
END
END

图 10-4 认证方案三

11. 电气特性

11.1 最大额定参数

最大参数如表 11-1 所示。

参数	最小值	最大值	单位
电压	3.0	3.6	V
存放温度	-35	120	℃
ESD	5500		V
V_{CC} 和 GND 的 DC 电流		0.7	mA

11.2 推荐工作条件

推荐工作参数如表 11-2 所示。

参数	最小值	最大值	单位
工作电压	3.0	3.6	V
工作温度	-40	85	℃

11.3 DC 特性

I/O 电压 3.3V 时 DC 参数如表 11-3 所示。

符号	参数	条件	最小值	最大值
V_{IL}	输入低电压	-	-	0.8V
V_{IH}	输入高电压	-	2.0V	-
I_I	输入电流	VCC = MIN VIN=GND or 3.6V	-	1uA
V_{OL}	输出低电压	IOL= 2mA	-	0.4V
V_{OH}	输出高电压	IOH= 2mA	2.4V	3.6V
I_{vcc}	VCC 电源电流	Active 8MHz, VCC = 3.3V	-	-
		Sleep mode	-	-

11.4 模拟 IP 参数

OSC(Ta = 25°C)参数如表 11-4 所示。

符号	参数	条件	最小值	典型值	最大值
f_{osc}	Switching Frequency		7.2MHz	8MHz	8.8MHz
$\triangle f_{osc}$	Frequency Variation	-40≤Ta≤80°C			±10 %
Dmax	Duty Cycle		48%	50%	52%

注：当环型电压为 3.3V，CMOS 电压和 LVTTL 电压值相等。

POR 参数如表 11-5 所示。

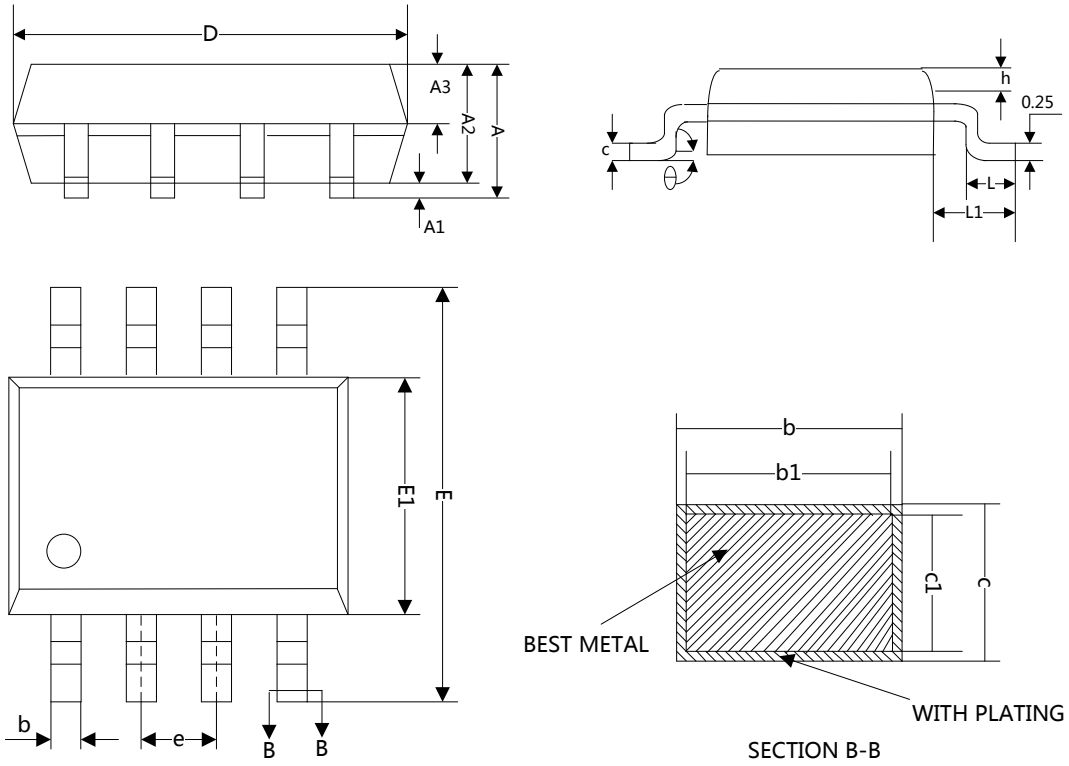
符号	最小值	典型值	最大值
V_t	1.88V	2.24V	2.67V
t_{delay}	5.4ms	10.2ms	20.5ms

Regulator (1.8V , VCC=3.3V, Ta=25°)参数如表 11-6 所示。

符号	参数	条件	最小值	典型值	最大值
V_{DD}	输出	No Load	1.81V	1.83V	1.85V
		0<Load<3mA	1.81V	1.83V	1.85V
I_{max}	输出电流最大值			10mA	

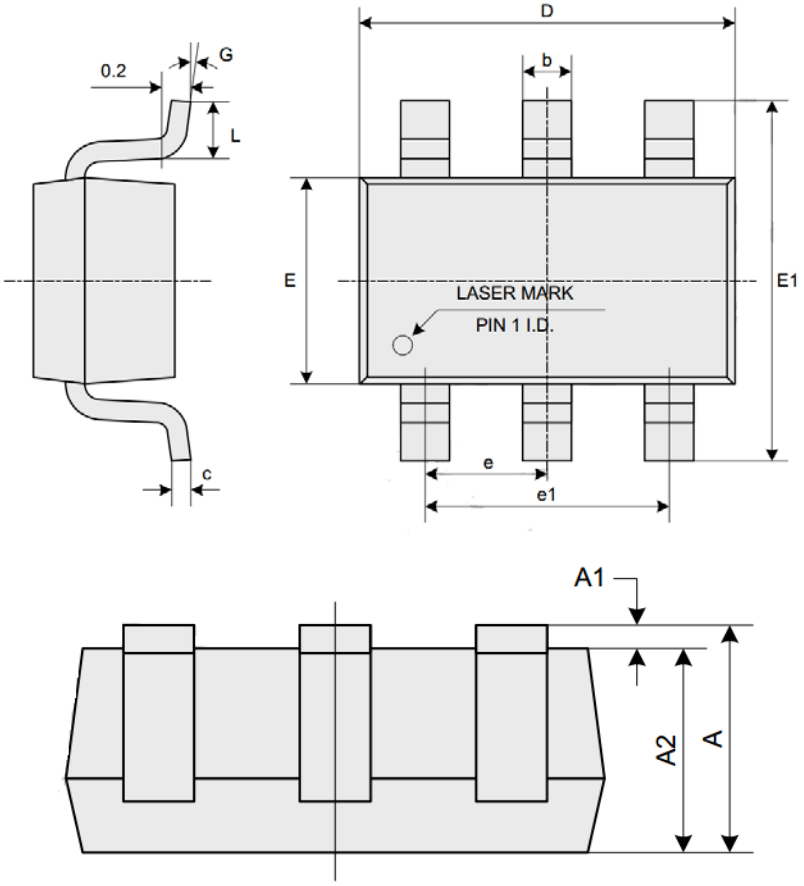
12. 封装尺寸

12.1 SOP-8L



符号	尺寸（mm）		
	MIN	**NOM**	**MAX**
A	-	-	1.75
A1	0.10	-	0.225
A2	1.30	1.40	1.50
A3	0.60	0.65	0.70
b	0.39	-	0.48
b1	0.38	0.41	0.43
c	0.21	-	0.26
c1	0.19	0.20	0.21
D	4.70	4.90	5.10
E	5.80	6.00	6.20
E1	3.70	3.90	4.10
e	1.27BSC		
h	0.25	-	0.50
L	0.50	-	0.80
L1	1.05BSC		
θ	0	-	8°
L/P 载体尺寸（mil）	80*80	90*90	95*130

12.2 SOT23-6L



符号	尺寸（mm）	
	MIN	MAX
A	1.050	1.250
A1	0.000	0.100
A2	1.050	1.150
B	0.300	0.500
C	0.100	0.200
D	2.820	3.020
E	1.500	1.700
E1	2.650	2.950
E	0.950（BSC）	
e1	1.800	2.000
L	0.300	0.600
G	0°	8°

武汉瑞纳捷电子技术有限公司

电话：027-59537580

Email：runjet@runjetic.com

地址：武汉市东湖高新区光谷大道61号光谷智慧园1501栋

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security ICs / Authentication ICs ***category:***

Click to view products by Runjet ***manufacturer:***

Other Similar products are found below :

A1007TL/TA4STZ DS2476Q+T DS28C36Q+T DS28C22Q+T DS2401-SL+T&R DS28E35P+ ATECC608B-RBHCZ-B DS28E18Q+T W74M12JWSSIQ ATECC508A-MAHAW-S SLB9660XT12FW440XUMA2 SLS32AIA020A4USON10XTMA2 SLB9645XT12FW13332XUMA1 DS2401T&R DS1990R-F5# DS2411P+T&R A1006TL/TA1NXZ ATAES132A-SHER-B ATSHA204A-RBHCZ-B ATECC608A-SSHDA-T A1006UK/TA1NXZ ATAES132A-MAHEQ-S ATECC608A-MAHCZ-S IPL-CHP ATAES132A-MAHER-S AT88SC118-SH-CN-T AT88SC118-SH-CM-T SE050A2HQ1/Z01SHZ SE050A1HQ1/Z01SGZ SE050B2HQ1/Z01SFZ ATECC608A-MAHCZ-T AT88SC118-SH-CM AT88SC118-SH-CN ATAES132A-MAHER-T ATAES132-SH-EQ ATAES132-SH-ER-T ATECC508A-MAHCZ-T ATAES132A-SHEQ-B ATAES132A-MAHER-T ATECC108A-SSHDA-B ATECC508A-SSHCZ-B ATECC508A-SSHDA-B DS2460S+ SLB9645TT12FW13333XUMA2 SLB9665TT20FW563XUMA3 SLB9670VQ20FW785XTMA1 SLM9670AQ20FW1311XTMA1 SLS32AIA010MLUSON10XTMA2 SLS32AIA010MKUSON10XTMA2 SLS32AIA010MHUSON10XTMA2