RJGT102WDT6-加密芯片

产品名称	RJGT102WDT6-加密芯片
公司名称	深圳市恩优科技有限公司
价格	.00/个
规格参数	品牌:瑞纳捷 型号:RJGT102WDT6 功能:加密芯片
公司地址	深圳市宝安区西乡街道富成路36号西万大厦501
联系电话	0755-23225045 18680343006

产品详情

RJGT102是武汉瑞纳捷电子技术有限公司推出的一款高安全性、低功耗、操作简便的加密芯片，它使用SHA-256加密算法进行报文摘要计算，内置4个32字节的Page区可以存储用户应用数据，唯一的8字节UID序列号用于区分不同应用功能，并且每片RJGT102芯片都有唯一的芯片id。该芯片适合应用于防抄板，防抄软件，管控工厂生产数量，防止方案外泄等场合。RJGT102有SOT23-6L和SOP-8L两种封装形式，如下图所示。

EEPROM包含176Byte的数据存储区。其中Page0、Page1、Page2和Page3各32Byte，用于存储用户数据；8Byte用于存储密钥Key；8Byte用于存储用户UID；16Byte用于存储芯片的控制信息，即用于保存芯片看门狗和POR电路的配置信息；剩下16Byte的保留数据区。

RJGT102芯片Page、InitKey和UID数据区都有自己独立的保护寄存器，通过向这些寄存器写入0x5A可以永久锁定这些寄存器，使其无法再被修改。所以当通过I2C接口向RJGT102中写入需要的数据后，如果希望其不再被修改，就可以通过配置这些保护寄存器来永久锁定写入芯片中的数据。

RJGT102内置看门狗WDOG和上电复位POR等安全保护电路。对于WDOG喂狗间隔可配置，复位有效电平极性可配置等特点。内置POR电路，当系统重新上电时，POR电路将复位系统，并初始化内部所有寄

存器；POR电路可保证芯片工作在一个正常的工作电压内，可有效保护芯片内控制器和存储体。

具备低功耗待机模式可有效减少不必要的系统功耗，在IC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。进入低功耗待机时有两种状态，一种是WDOG、OSC使能，关断除WDOG、IC外模块的时钟；另一种是WDOG关闭，OSC不使能，关闭所有模块时钟。当IC上有命令传输或者处于低功耗状态后重新上电时，RJGT102都会退出低功耗待机状态。

RJGT102芯片使用I2C接口通信，支持标准模式100Kbit/s和快速模式400Kbit/s的数据传输速率。只需要VCC、GND、SCL和SDA这4根线即可，SCL和SDA需要上拉电阻。RJGT102与MCU的连接电路如下图所示。

RJGT102包含指令寄存器、源地址寄存器、目的地址寄存器以及状态寄存器等。芯片根据这些指令寄存器的值进行译码、SHA-256运算和搬移等操作，从而完成加密认证过程。

RJGT102通过I2C接口操作寄存器：（1）指令寄存器REG_MCMD用来指定操作类型；（2）源地址寄存器REG_TAd用来指定参与MAC计算的Page区；（3）目的寄存器REG_TAd用来指定操作具体操作目的；（4）状态寄存器ES指示当前操作后的状态；（5）数据交换区Zone1(0xC0开始的32字节地址) 保存主机输入用于运算的数据；（6）数据交换区Zone2（0xE0开始的32字节地址）用于保存接收的MAC认证数据。

RJGT102是如何实现用户数据安全的呢？

RJGT102使用SHA-256算法对保存在芯片内的8字节的密钥Key、32字节的Page数据(任意一个Page区)、8字节的UID、8字节的关键常数(固化在芯片内部)以及外部获取的8字节随机数进行SHA-256计算，并输出32字节(256位)的报文摘要MAC，如下图所示。

基于SHA-256算法的特性，RJGT102就可以对运行在系统应用程序的启动过程中通过外部的秘钥进行产品合法性的认证和校验，来保证主设MCU内部固件应用的安全合法性(即未被篡改过)，从而保证产品设备运行的安全性。

RJGT102芯片保障用户产品运行安全的实现过程

首先，主机MCU会产生一个随机数，并将该随机数发送给RJGT102芯片；RJGT102接收到随机数后，利用事先保存在内部的数据以及该随机数进行SHA-256计算，得到对应的Hash值，记作MAC2，并将MAC2输出给主机；其次，主机MCU通过自身保存的相关数据(Usid、key和page等数据)和生成的随机数，计算对应的MAC1值；然后，主机将从RJGT102获取的MAC2值和自身计算的MAC1进行比较，如果两者相同则认为认证通过，两者不相等则认证失败，退出运行或自动复位。当认证通过后，主机就可以继续后续操作，并通过RJGT102芯片的认证读和认证写接口进行读取保存在RJGT102中的关键操作数据来完成后续关键操作。(注意，上面的操作都是通过I2C接口完成的，并且相应的数据已经通过RJGT102的相关指令烧录到安全芯片内部)，具体流程图如下所示。

RJGT102进行认证的常见方案有三种，分别是RJGT102认证主机、主机认证RJGT102、主机和RJGT102相互认证，上面例举的是其中的一种认证机制，其他的认证方案大体过程相同，只是操作细节有所不同。

RJGT102从两个层次上保证了设备运行的安全性：一种是通过认证校验固件本身的安全性，即通过RJGT102与主机直接的相互认证过程，保证了主机运行环境的安全性；另一种是通过认证保存在RJGT102中的关键数据的安全性，即保存在RJGT102中的重要数据只有是必须通过安全认证的合法用户才能读取和修改，这样就保证了设备重要数据操作的安全性。

RJGT102包含几个常用的操作命令，通过这些命令完成相应的认证操作。

操作命令

用途说明

用户UID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UID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。

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。