重庆理工大学学报 自然科学
Journal of Chongqing University of Technology(Natural Science)

应用国密芯片的物联网安全节点设计

石少青, 崔 超, 肖 勇, 赵 云, 林伟斌

引用本文:
石少青, 崔 超, 肖 勇, 赵 云, 林伟斌. 应用国密芯片的物联网安全节点设计[J]. 重庆理工大学学报（自然科学）, 2022, 36(2): 162–170.

相似文章推荐（请使用火狐或IE浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

一种基于区块链的数据存储系统的设计

Design of a Data Storage System Based on Blockchain

重庆理工大学学报（自然科学）. 2019, 33(9): 190–195 https://doi.org/10.3969/j.issn.1674–8425(z).2019.09.027

基于公钥密码的通信网络安全加密系统设计

Design of Communication Network Security Encryption System Based on Public Key Cryptography

重庆理工大学学报（自然科学）. 2020, 34(10): 146–152 https://doi.org/10.3969/j.issn.1674–8425(z).2020.10.020

不定长量子密钥的彩色图像三重加密算法

Triple Encrypting Algorithm for Color Images Based on Indefinite Length Quantum Key

重庆理工大学学报（自然科学）. 2021, 35(11): 150–157 https://doi.org/10.3969/j.issn.1674–8425(z).2021.11.019

基于整数红–黑小波变换的图像加密算法

Algorithm of Image Encryption Based on Integer Red–Black Wavelet Transform

重庆理工大学学报（自然科学）. 2016, 30(12): 122–128 https://doi.org/10.3969/j.issn.1674–8425(z).2016.12.019

基于物联网的多传感器数据采集系统研究

Research of Multi–Sensor Data Acquisition Technology Based on Internet of Things

重庆理工大学学报（自然科学）. 2016, 30(10): 108–117 https://doi.org/10.3969/j.issn.1674–8425(z).2016.10.017

重庆理工大学学报(自然科学)
Journal of Chongqing University of Technology(Natural Science)
2022 年 第 36 卷 第 2 期
Vol. 36 No. 2 2022
doi: 10.3969/j. issn. 1674-8425(z). 2022. 02. 021

应用国密芯片的物联网安全节点设计

石少青,崔 超,肖 勇,赵 云,林伟斌

(南方电网科学研究院有限责任公司, 广州 510663)

摘 要:伴随物联网技术的快速发展,通讯数据安全问题的重要性日益突出,通讯数据安全直接影响个人隐私、人身安全乃至国家安全。针对物联网设备加密通讯和设备认证等应用场景,基于物理不可克隆函数的国密芯片,设计物联网安全节点,实现对物联网设备通讯数据的加密,防止相关数据被第三方窃取。物联网安全节点的测试与应用结果表明:所设计节点可稳定、高效地实现通讯数据加密,保障通讯数据在物联网设备中的安全传输。

关 键 词:信息安全;加密算法;数据加密

中图分类号:TN929.5 **文献标识码**:A **文章编号**:1674-8425(2022)02-0162-09

近年来,随着智能设备制造和电子通讯技术的快速发展,物联网通讯节点数量迅速增长,越来越多的数据通过通信系统进行传输。由于我国物联网设备节点基数相对更大,所以我国的物联网产业以后必将形成空前的市场份额并拥有强劲的发展潜力[1]。机遇往往伴随挑战,在拥有潜力的同时,黑客的攻击范围更广,业界所面临的安全挑战也更为严峻[2]。在过去几年中,各种黑客攻击层出不穷,攻击的目标涵盖了支付、基础设施、电子邮件、物联网等领域[3-4]。因此,如何保障通信系统的信息安全,是目前首要解决的问题。

由于我国的安全芯片产业起步较晚,安全芯片供应链长期以来被支持国际通用密码算法的国外安全芯片垄断。采用国外的密码技术或安全芯片,信息安全隐患巨大,一旦芯片被植入后门,后果不堪设想。十八大以来,党和国家高度重视信息安全产业的发展,安全芯片等相关信息安全产业已上升至国家战略高度[5]。虽然我国的自主国密芯片在功能和安全性上已经完全能够取代国外的安全芯片,但是受先入为主思想的影响,我国的自主国密芯片市场占有率并不高,仍有大量的设备在使用国外的安全芯片。只有加强对自主国密芯片的应用,通过自主可控的国产加密技术对数据进行保护,才能增加外部获取数据的难度,防止数据泄露,进而有效提升我国信息安全保障水平。

针对物联网设备的通讯数据安全问题,给出一种基于国密芯片的可应用于物联网设备的安全节点解决方案。该节点采用基于国密商用安全芯片为核心开发设计,能有效保证数据安全。一方面,本节点支持身份认证、信息加解密等功能,能够满足物联网设备的数据安全需求,另一方面,本节点采用自主国密芯片,在一定程度上推动了我国国密芯片的应用。

收稿日期:2021-03-31
基金项目:南方电网公司重点科技项目(090000KK52190161)
作者简介:石少青,男,高级工程师,主要从事电网电能计量研究,E-mail:shisq@csg.cn;通讯作者 崔超,男,硕士,主要从事集成电路设计和密码学研究,E-mail:cuichao@csg.cn。

本文引用格式:石少青,崔超,肖勇,等. 应用国密芯片的物联网安全节点设计[J]. 重庆理工大学学报(自然科学),2022,36(2):162-170.

Citation format:SHI Shaoqing, CUI Chao, XIAO Yong, et al. Design of security node of IOT base on national secret chip[J]. Journal of Chongqing University of Technology(Natural Science),2022,36(2):162-170.

1 安全节点电路设计

本节主要介绍安全节点的硬件电路设计,其中包括主控电路设计、电源电路设计、JTAG 电路设计和外围电路设计,最后通过 PCB 设计软件 Altium Designer 完成安全节点电路板设计。

1.1 主控电路设计

所设计安全节点的主控制器是国密芯片,所以关于主控电路的设计也是围绕国密芯片进行。所研制的国密芯片内部集成平头哥半导体研发的低功耗 32 位处理器 E802,该处理器支持 RISC-V 第三代指令系统架构的。芯片内部集成了国密加密算法 IP、物理不可克隆函数 IP 和主流通用接口。

由于所研制的国密芯片内部没有集成 flash 的硬件 IP,所以在搭建主控电路必须集成 flash 芯片才能保证国密芯片正常启动;选择 Atmel 公司生产的 SPI flash 芯片 AT25F512A 作为用户代码存储 flash。该芯片还提供了单独的写使能信号和写保护指令,进而实现对存储数据的保护。该芯片主要存储编译好的用户代码机器码,国密芯片启动后即通过 SPI 接口从 AT25F512A 芯片中获取用户代码,相关代码会被搬运存储在国密芯片内部集成的 SRAM 中按顺序执行。

1.2 电源电路设计

安全节点将采用集中供电端口,即电源统一由外部提供。通过前期对市面上主流的物联网设备进行调研发现,大部分物联网设备工作电压介乎 3.3 ~12 V。所研制国密芯片 IO 工作电压为 3.3 V、CPU 内核工作电压是 1.2 V,所以本安全节点的电源电路需将外部介乎 3.3 ~12 V 的电压转换成 3.3 V 和 1.2 V 的安全节点工作电压。目前主流的稳压电源转换解决方案主要包括线性稳压和开关稳压。线性稳压具有输出波纹小、响应速度较快和外围电路简单等优点,但是容易出现发热严重的现象。而开关稳压既可进行升压转换,也可以实现降压转换[6-7],且转换效率高,但缺点是噪声较大、成本较高。

本着实现低成本、减少硬件面积的原则,选择使用线性稳压的解决方案为安全节点提供工作电压。安全节点选择了亚德诺半导体公司生产的低压差线性稳压器件 ADP1711 和 ADP1712,通过这两款芯片稳定生成安全节点的工作电压。

1.3 JTAG 电路设计

所设计安全节点配备下载接口,方便其他开发人员利用安全节点进行产品研发。目前业界主流的裸机下载调试电路主要包括 JTAG 和 SWD,本文采用 14 端口的 JTAG 下载接口电路。在安全节点开发调试阶段,通过 JTAG 接口可以快速访问主控国密芯片的所有硬件寄存器,观察目前国密芯片的工作状态和运算数据,通过 JTAG 接口还可以访问 flash 芯片和外部串口等外设,可以有效提升开发人员的设备开发、功能仿真和联合调试效率。安全节点的仿真器使用的是平头哥半导体公司研发的 CKLink lite 下载器,该下载器可配置调试接口时钟频率从 10 kHz ~24 MHz,且该下载器同时支持 Windows 操作系统和 Linux 操作系统,极大方便了使用双系统进行开发的研发人员。安全节点通过 JTAG 接口与仿真器 CKLink 相连后即可实现在线仿真调试和程序烧写,CKLink lite 下载器及其接口原理图如图 1 所示。

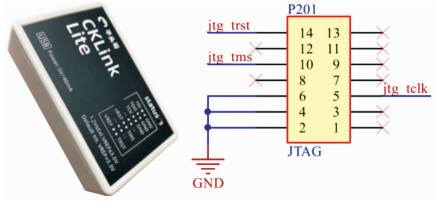

图 1 CKLink lite 下载器及其接口原理图

1.4 外围电路设计

安全节点在最小系统的基础上进行外围电路扩展,以提升安全节点的应用功能,本小节主要介绍 WiFi 模块接入、USB 转串口电路设计和传感器电路设计等外围电路的设计。

将安信可科技所开发的 WiFi 模块 ATK-ESP8266 作为外接 WiFi 通信设备。该安全节点内置一款超低功耗的 32 位微控制器,主频可支持 80 MHz和 160 MHz,而工作模式支持 AP、STA 和 STA + AP。该安全节点整体面积较小,可以实现通过串口与外部控制设备通信,内置的 TCP/IP 协议栈,方便开发人员通过安信可科技提供的 SDK 进行二次开发使用,也可直接通过 AT 指令进行 WiFi 模块手动配置。该 WiFi 模块是目前物联网行业应用较为广泛的一款 WiFi 通信设备,所以本安全节点外围电路集成该 WiFi 模块,如图 2 所示

是 WiFi 模块及其接口原理图。

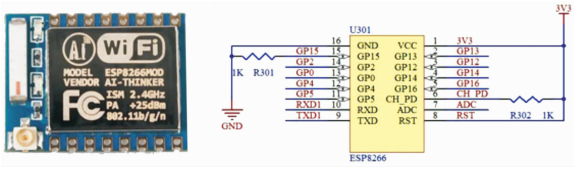

图 2 WiFi 模块及其接口原理图

目前还有很多物联网设备是需要进行串口通信的,所以本安全节点同样可以提供 USB 转串口的外围电路。本文设计一款 USB 转串口电路,方便安全节点与用户上位机进行数据交互,以快速实现用户指令。

本文的国密芯片包含 8 路 3.3 V 的 GPIO 端口,可以为开发人员提供更多的应用驱动解决方案。在安全节点的设计中,将提供 2 路单点按键和 2 路 LED,以方便开发人员增加应用场景的展示效果,还可以为开发人员设备调试提供更多手段。

1.5 安全节点硬件实现

通过前面具体电路的设计过程,针对安全节点的完整电路,通过 Altium Designer 完成安全节点 PCB 板的设计。由于需要结合物联网设备使用,所以电路设计面积必须尽可能小,类似目前物联网设备广泛使用的 WiFi 模块、蓝牙模块和 Zigbee 模块等通信模块,小巧、方便以适用于嵌入设计。

由于安全节点电路需要控制器件发热和整体面积,故选择通过手动布局完成电子器件布局。总结了以下电子器件手动布局经验法则:先大后小原则,对于尺寸较大的电子器件需要首先布局,尺寸较小的电子器件随后通过电路原理和工作模式进行合理布局[8];先难后易原则,首先要将必须联合工作的器件布局在一起,例如最小系统的控制器和时钟必须就近布局,那就需要布局初期定位;模块化原则,完成相同工作的电子器件尽量统一布局在相近的位置,组成类似外接模块的布局标准,这样能有效减少后期布线的难度。防干扰原则。大功率器件或者高频器件尽量减少靠近布局,否则可能会导致器件相互干扰或者 PCB 板某处发热严重的后果。

通过以上原则对安全节点进行器件布局,安全节点 PCB 板的元件布局情况如图 3 所示。

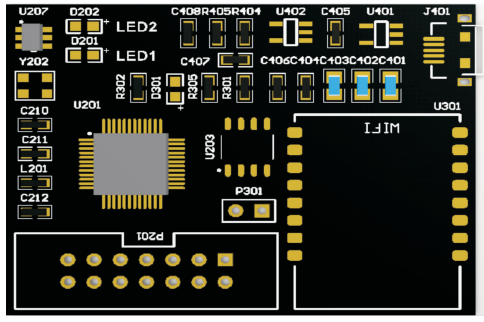

图 3 安全节点 PCB 板元件布局图

安全节点完成元器件布局后,就要对该 PCB 板进行布线操作。Altium Designer 在布线操作中提供了手动布线和自动布线 2 种工作模式。自动布线同样是适用于结构较为简单的电路设计,本文的安全节点电路设计较为复杂,故选择手动布线的方式完成安全节点的布线操作。手动布线遵循以下布线的经验法则[9]:优先原则,布线过程中按照电源线、信号线和地线的顺序进行布线,并且在合理范围内增加电源线和地线的宽度,以达到更好的电气性能;最短原则,在布线过程中应尽可能布最短路径,减小布线带来的阻抗,降低 PCB 板设计失败的可能;45°原则,拐角布线尽量采用 45°方式走线,尽可能避免 90°拐角,可以有效较少对信号完整性的干扰;规整原则,布线在尽可能靠拢走线,尽可能有序分布。

通过以上布线规则完成 PCB 板布线,安全节点最终完成布线后的 layout 结果如图 4 所示。

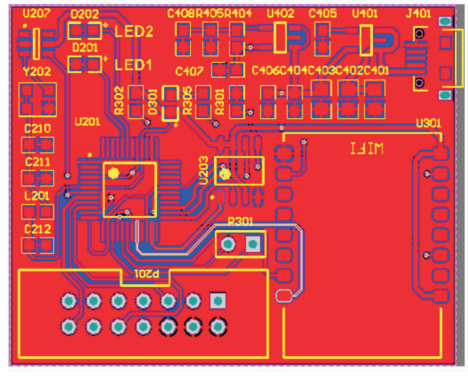

图 4 安全节点 layout 图

2 安全节点软件设计

安全节点的软件设计通过调用 SM2/SM3/SM4 国密算法模块实现,SM4 的作用是对需要加密的信

息进行加密/解密;而 SM2 则是实现公钥加密/私钥解密,SM3 作为密码杂凑函数供 SM2 调用。

发送方先用对称密钥对需要发送的信息进行 SM4 加密生产密文,然后用接收方的公钥对 SM4 的对称密钥进行加密并连同密文一起发送给接收方;接收方用私钥进行 SM2 解密得到 SM4 对称密钥,并利用对称密钥对密文解密得到明文。

2.1 SM4 加密函数

SM4 模块的工作主要分为 3 个部分:加解密数据分组、轮密钥生成以及加解密运算。其中数据分组即将输入数据统一分成 128 位的数据,方便后面进行数据加解密。轮密钥生成操作主要是对输入密钥进行逻辑运算,进而生成对应的轮密钥存储于内部的寄存器[10]。加解密操作则主要是对输入数据完成相应的逻辑处理,进而得到加解密输出数据。

用户输入明文或密文数据 N,此时 SM4 函数首先需要对数据 N 进行分解成 128 bits 一组的 $N1,N2,N3,\cdots,Ni$。随后将分别将每一组加载至数据通过输入数据寄存器中进行加解密操作。对应函数库函数为 SM4_Group_Divide(uint32 *key, uint32 *in,uint32 *out,uint32 mode),函数中最重要的部分是确定数据的组数,首先判断组数是否为整数。若组数不为整数则表明最后一组数据位宽不足,此时通过补零补齐。

在国密芯片的 SM4 模块中,通过软件实现工作模式控制、输入数据分组和模块工作状态读取,硬件则完成轮密钥生成和加解密逻辑运算。SM4 模块的核心算法模块并不是直接挂载在 AHB 总线,所以每次核心算法运算后,软件都要对状态寄存器进行读操作以确定模块工作状态。加密操作由于轮密钥由低到高的顺序进行使用,所以在进行轮密钥生成操作后,软件即可向输入数据寄存器输入加密数据。解密操作时则需要不断的对状态寄存器进行读操作,通过判断核心算法模块的轮密钥生成完毕后,再向输入数据寄存器输入解密数据。

输出数据寄存器将用于保存模块运算后的数据,输出数据寄存器数据要在 top_data_complete 信号上升沿到来之后进行更新。由于模块输出数据是 128 bits,而本文所采用都是 32 位寄存器,所以需要 4 个寄存器来保存输出数据。输出数据寄存器的数据保存周期是在前一次运算完成至下一次数据的输入,在这期间输出数据寄存器均有效可读的。

可配置的寄存器包含控制寄存器和输入数据寄存器,其中控制寄存器的 ENABLE 位是软件复位信号,软件正常工作时该复位信号需要保持低电平。输入数据寄存器数据更新时,控制寄存器的 UPDATE 位必须置高,通过控制寄存器的 MODULE 位可以确定输入寄存器的输入类型,其中包括加密数据、解密数据或是密钥数据。

2.2 SM3 杂凑函数

SM3 杂凑函数[11-12]包含 1 个头文件和 8 个源文件,分别执行输入数据、消息填充、数据分组、更新数据和输出数据等杂凑过程,表 1 所示为 SM3 的输入输出数据。

表 1 SM3 的输入输出

端口方向	变量	数据类型	含义
输入	Message	字节串	用户消息
输出	Hash Value	字节串	生成杂凑值

SM3 杂凑函数的软件流程如图 5 所示。

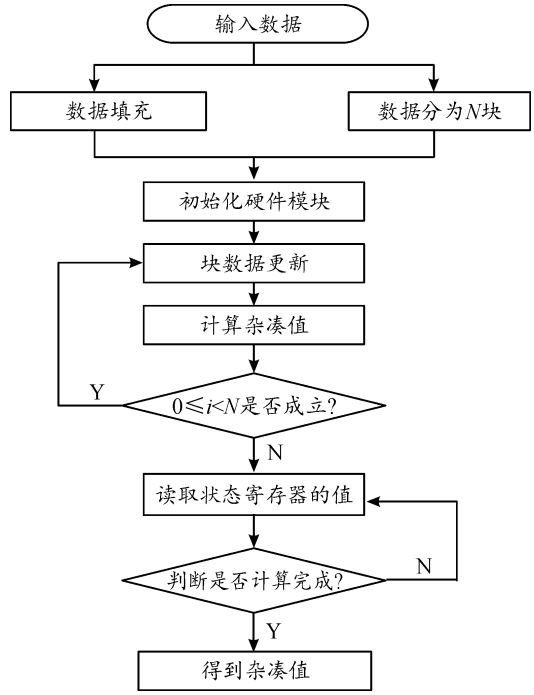

图 5 SM3 杂凑函数软件流程框图

SM3 杂凑函数的软件执行具体步骤如下:

1）输入数据

对应函数库函数为:Input_Message(in,len);

该函数读取用户输入长度为 len 的数据 in 进行数据拼接,如果用户需要对数据进行单独杂凑值运算可以通过 fscanf 直接读入数据。

2）数据填充

SM3 函数通过对低于 264 位的输入数据进行直接运算,在此假设数据 M 的数据位宽为有限位宽 N。函数首先将数据按照 512 位进行分块,最后不足 512 位的块也记录为一个数据块。

随后通过在输入数据的最后一位进行数据补 1 操作,即可实现在数据最后一个字节添加 0x80 后再增补 k 个 0,完成数据填充操作,最后完成模块的块数据更新。

3）硬件驱动

SM3 杂凑函数需要对底层硬件进行操作,所以通过定义相关结构体,以方便软件对相关寄存器的读写操作。

在 SM3 杂凑实际使用过程中,首先需要设置结构体的指针,使其可以指向 SM3 硬件模块的基地址,同时根据控制寄存器相关控制位的定义进行模块复位和初始化。随后通过输入数据寄存器开始写入用户数据,随后将控制寄存器模块工作使能控制位置高,SM3 模块开始进行逻辑运算[13]。软件通过对状态寄存器进行读操作,进而判断 SM3 模块的逻辑运算是否完成,若运算结束则通过输出数据寄存器将运算结果输出,该结果即为用户所需的杂凑值。

2.3 SM2 函数

SM2 函数需要对输入数据进行 2 次预处理,然后生成加解密密钥对数据[14],最后完成签名验签操作。

SM2 函数对输入数据的第一次预处理是通过签名方的用户标识和公钥进行拼接和杂凑运算,最后获取杂凑结果 $Z1$,同时杂凑值 $Z1$ 将会用于第二次数据预处理。如表 2 所示为到二次数据预处理的输入输出端口。

表 2 预处理 1 的输入输出

端口方向	变量	数据类型	含义
输入	*ID*	字符串	用户 *ID*
输入	*Q*	字符串	用户公钥
输出	*Z*1	字符串	预处理 1 的输出

SM2 函数完成第一次数据预处理后即进行第二次数据预处理[15],本次数据预处理通过对 $Z1$ 值和待签名数据 M 进行数据拼接并通过杂凑运算得到摘要数据 H,杂凑值 H 则是作为签名验签的输入。如表 3 所示是第二次数据预处理的输入输出端口。

表 3 预处理 2 的输入输出

端口方向	变量	数据类型	含义
输入	*Z*1	字符串	预处理 1 输出值
输入	*M*	字符串	待签名消息
输出	*H*	字符串	摘要值

SM2 函数完成输入数据预处理后,随后即要进行密钥对生成操作,密钥对生成操作包括 32 字节的私钥生成操作以及其对应的公钥生成操作。

SM2 函数完成数据预处理和密钥对生成后即可进行签名验签[16-17]操作,如图 6 所示是签名验签的软件工作流程。

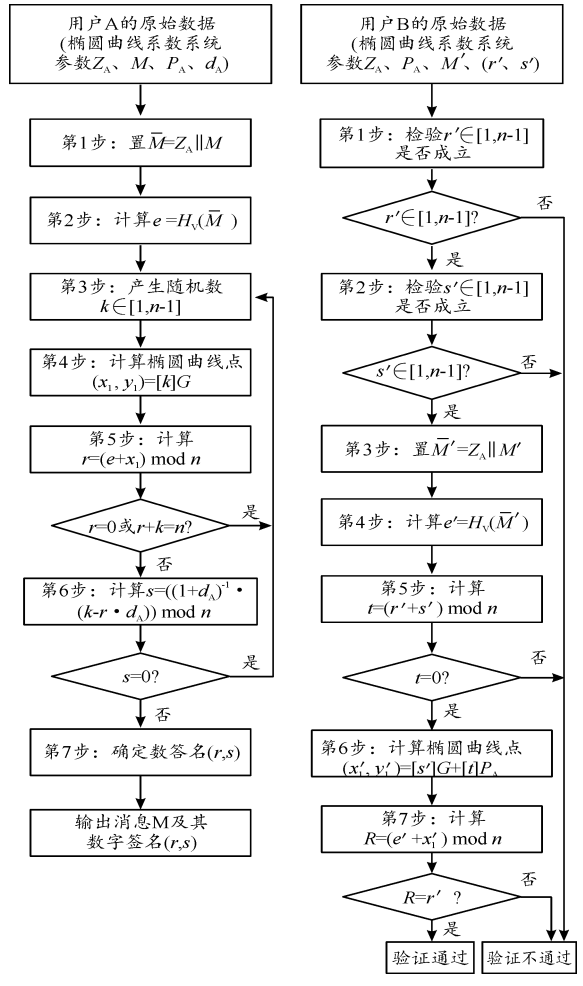

图 6 签名验签软件流程框图

SM2 函数在进行签名验签操作时,模运算均通过取模 N 进行计算,所有寄存器数据都保存在结构体指针 * initial 中,其中储存数据按照寄存器总线基地址依次进行偏移。在 SM2 模块工作前,软件需要配置控制寄存器相应控制位完成模块复位和初始化操作。通过输入数据寄存器[18]写入用户数据后,配置控制寄存器相应控制位选择工作模式和启动模块运算。软件通过读取状态寄存器的值判断 SM2 模块的运算情况,运算结束后需要配置控制寄存器相应控制位表明运算结束,随后通过输出数据寄存器输出运算结果。

2.4 抗侧信道攻击分析

侧信道攻击是指攻击者通过主通信信道以外的途径获取到的关于密码实现运行状态相关的信息,从而破解出密钥信息,典型的侧信息包括密码实现运行过程中的能量消耗、电磁辐射、运行时间等信息。没加入抗攻击设计的加密算法可以被攻击者轻易攻击而引起密钥泄露,因此需要加入抗攻击设计。

本设计需要保护的密钥包括 SM4 的对称密钥和 SM2 的私钥[19],采用的是抵抗简单功耗分析的方法。SM2 在用私钥进行点乘计算过程中,不同的私钥会进行不同次数的点加运算,因此可以根据计算的功耗曲线来判断出私钥,抵抗简单功耗分析的方法是通过平衡点加功耗使不同私钥执行的点加次数一致从而无法根据功耗曲线破解私钥。而 SM4 则是通过保证密钥扩展的功耗平衡而抵抗简单功耗分析。

3 安全节点功能测试

完成安全节点的设计后,通过文献[20]开发的身份认证及加密系统对安全节点进行功能测试,该系统是基于本课题的国密芯片开发的,可以快速完成安全节点的功能测试。

安全节点将作为测试的下位机,身份认证及加密系统是通过 Matlab 图形用户界面开发的上位机,上位机与下位机之间方通过 UART 进行数据通信。如图 7 和图 8 所示是身份认证及加密系统的发送方交互界面和接收方交互界面[21]。

图 7 身份认证及加密系统发送方交互界面

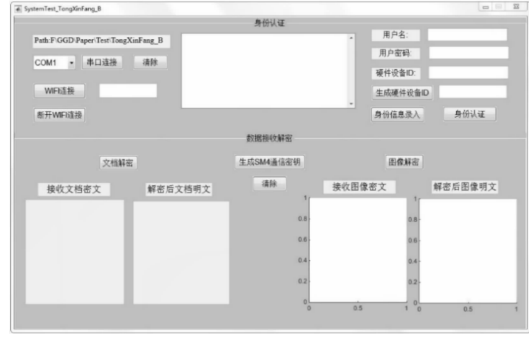

图 8 身份认证及加密系统接收方交互界面

3.1 WiFi 功能测试

安全节点通信方 A 在交互页面点击“创建 WiFi 热点”即可完成热点创建,创建 WiFi 热点结果如图 9 所示。

图 9 创建 WIFI 热点界面

安全节点通信方 B 在交互页面输入热点名称并点击“WiFi 连接”即可完成热点连接,连接 WiFi 热点结果如图 10 所示。

图 10 连接 WIFI 热点界面

通过 WiFi 功能测试结果表明安全节点的 WiFi 功能可以正常创建和连接,符合预期功能需求。

3.2 身份认证测试

安全节点[22]进行身份认证测试,需要生成硬件设备 ID,通过点击“生成硬件设备 ID”即可获取当前安全节点的唯一硬件 ID,同时该 ID 会直接显示在交互界面中。安全节点生成硬件设备 ID 结果如图 11 所示。

图 11 硬件设备 ID 生成结果

完成硬件设备 ID 生成操作后,即可录入用户信息。在身份认证及加密系统交互界面中输入用户名、用户密码和硬件设备 ID,随后点击“身份信息录入”按钮即可完成设备 A 的信息录入,同时设备 B 接收完成,如图 12 和图 13 所示。

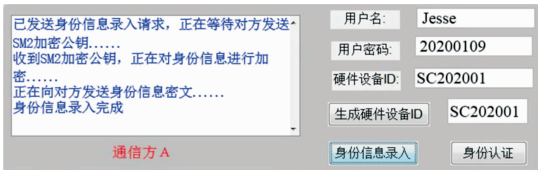

图 12 身份信息录入界面

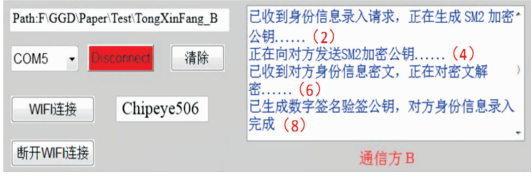

图 13 身份信息录入界面

安全节点设备完成信息录入后,再次进入即需要进行身份认证操作,对身份认证操作同步 4 种情况进行测试。

1)身份认证无误。通过交互界面输入正确的用户信息后点击“身份认证”按钮,即可通过身份认证。如图 14 所示是身份认证通过结果。

图 14 身份认证通过界面

2)用户名错误。当用户名输入错误进行身份认证时,交互界面会提示错误原因和告知认证不通过。如图 15 所示是身份认证用户名错误界面。

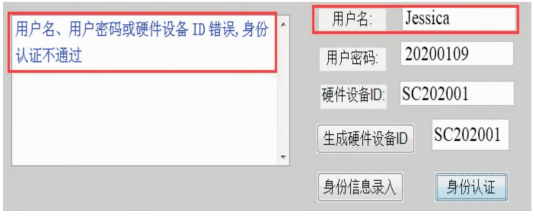

图 15 身份认证用户名错误界面

3)用户密码错误。当用户密码输入错误进行身份认证时,交互界面会提示错误原因及告知认证不通过。如图 16 所示是身份认证用户密码错误界面。

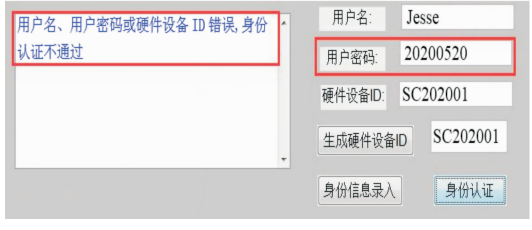

图 16 身份认证用户密码错误界面

4)硬件设备 ID 错误。当硬件设备 ID 输入错误进行身份认证时,交互界面会提示错误原因和告知认证不通过。如图 17 所示是身份认证硬件设备 ID 错误界面。

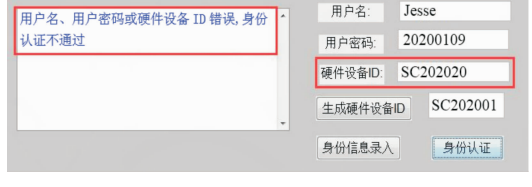

图 17 身份认证硬件设备 ID 错误界面

通过身份认证测试结果表明安全节点的身份认证功能正常使用。

3.3 文档加密测试

安全节点通信方 A 点击“打开文档”按钮即可在计算机本地选择需要加密的文本文件,文本数据会在“文档明文”显示窗口中进行显示。随后点击“文档加密”按钮,安全节点便会对文档明文数据进行加密操作,安全节点加密完成后密文将在

“文档密文”显示窗口中进行显示。最后点击“发送文档密文”按钮即可将密文数据发送至安全节点通信方 B。

安全节点通信方 B 完成密文接收后,密文数据将在“接收文档密文”显示窗口中进行显示。随后点击“文档解密”按钮即可对密文数据进行解密操作,安全节点解密完成后解密数据将在“解密后文档明文”显示窗口中进行显示,具体结果如图 18 所示,表明模块文本解密功能正常。

图 18 文本加密通信界面

3.4 图像加密测试

安全节点通信方 A 通过点击“打开图像”按钮即可在计算机本地选择需要加密的图像,同时图像内容将会在“图像明文”显示窗口中进行显示。随后点击“图像加密”按钮即可启动安全节点对图像数据进行加密操作,安全节点加密完成后密文将在“图像密文”显示窗口中进行显示。最后点击“发送图像密文”按钮即可把图像密文数据发送至安全节点通信方 B。

安全节点通信方 B 接收图像密文数据完成后,即可将图像密文在“接收图像密文”显示窗口中进行显示。随后点击“图像解密”按钮即可启动安全节点对图像密文进行解密,最后将解密后获得的图像在“解密后图像明文”显示窗口中进行显示。

如图 19 所示是安全节点图像加密通信结果,通过测试结果表明安全节点图像加解密功能正常。

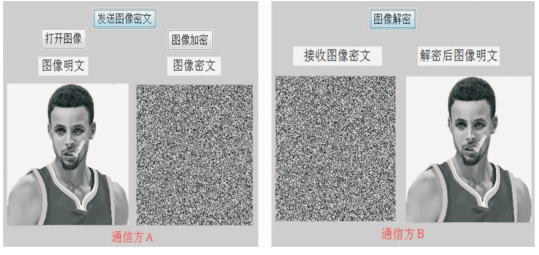

图 19 图像加密通信界面

4 结论

完成了以基于物理不可克隆函数的国密芯片为核心的面向物联网设备的安全节点的设计与实现。通过节点的调试结果表明该节点运行稳定,能够完成对通信双方进行身份认证,实现文档和图像的加密通信,达到预期研发目标。安全节点具有功耗低、加密性能强和运算速度快的优点,可以有效保障通讯数据在物联网设备信道间的安全传输,是当前物联网设备加密通讯的有效可行解决方案,针对物联网硬件安全性能提升有较大应用前景。

参考文献:

[1] 张盛仕. 基于国密算法加密技术的 SoC 设计与优化[D]. 广州:广东工业大学,2019.

[2] 郝少华. 新一代智能变电站通信网络管理系统建模研究[D]. 北京:华北电力大学,2018.

[3] 燕科. 高速公路 ETC 系统国密算法迁移研究与验证[D]. 西安:长安大学,2016.

[4] PAAR C,PELZL J. 深入浅出密码学[M]. 马小婷,译. 北京:清华大学出版社,2012.

[5] 刘杰,龚维斌. 十八大以来我国公共安全体系建设的理念与实践创新[J]. 福建行政学院学报,2018(1):11-18.

[6] 王冬菊. 浅谈两种直流稳压电源[J]. 电子世界,2018(9):191-191.

[7] ZHAO Zhichao,LI Guohong. Switching power supply design suitable for motor control[C]//2017 29th Chinese Control And Decision Conference(CCDC). China:IEEE,2017:6064-6067.

[8] 王建农,王伟. Altium Designer 10 入门与 PCB 设计实例[M]. 北京:国防工业出版社,2013.

[9] 江敏. Altium Designer 在电子设计中的应用[J]. 无线互联科技,2018,15(15):62-63.

[10] 王德民,陈达. 基于 CUDA 的 SM4 加密算法高速实现[J]. 石家庄铁路职业技术学院学报,2017,16(1):59-63.

[11] 国家密码管理局. SM3 密码杂凑算法[S]. 北京:2010.

[12] 王卓. USB KEY 加密安全芯片的设计与实现[D]. 北京:中国科学院大学,2013.

[13] 王丽雪. 以自主国密芯片为核心的认证、加密系统的设计与实现[D]. 广州:广东工业大学,2019.

[14] 叶靖,胡瑜,李晓维. 非确定性仲裁型物理不可克隆函数设计[J]. 计算机辅助设计与图形学学报,2017,29

(1):166 - 171.
[15] 年旭升. 基于 UVM 的高性能总线架构的分析验证[D]. 西安:西安电子科技大学,2017.
[16] 徐崇耀. 基于国密算法和 PUF 技术的物联网安全芯片设计与实现[D]. 广州:广东工业大学,2018.
[17] 张玉清,周威,彭安妮. 物联网安全综述[J]. 计算机研究与发展,2017,54(10):2130 - 2143.
[18] 彭安妮,周威,贾岩,等. 物联网操作系统安全研究综述[J]. 通信学报,2018,39(3):22 - 34.
[19] 李岩,屈媛,陈仪香. 软硬件协同设计中的软硬件划分方法综述[J]. 单片机与嵌入式系统应用,2017,17(8):3 - 8.
[20] 杨润东,李子臣. 基于国密算法的新型电子邮件加密系统研究与实现[J]. 信息安全研究,2018,4(11):84 - 89.
[21] 郑欣. 基于国密算法的加解密和签名验签系统设计及其实现[D]. 广州:广东工业大学,2018.
[22] 钟丽,刘彦,余思洋,等. 嵌入式系统芯片中 SM2 算法软硬件协同设计与实现[J]. 计算机应用,2015,35(5):1412 - 1416.

Design of security node of IOT base on national secret chip

SHI Shaoqing, CUI Chao, XIAO Yong, ZHAO Yun, LIN Weibin

(China Southern Power Grid Research Institute Co., Ltd., Guangzhou 510663, China)

Abstract: With the rapid development of the number and performance of current Internet of Things devices, the trend of Internet of Everything has become more and more obvious. At the same time, the communication data security issues of IoT devices are facing increasingly severe challenges. The communication data security issues of these devices often involve personal privacy, personal safety and even national security. Against this background, this paper proposes secure node design based on the national secret chip, which can be widely used in scenarios such as encrypted communication and device authentication of IoT devices. This node uses the national secret chip design and development based on the national cryptographic algorithm and the physical unclonable function to realize the encryption of the communication data of the IoT device, prevents the relevant data from being stolen by the third party, and realizes the normal operation of the IoT device in a wide range of application scenarios. The test results and actual applications of this node show that the node can implement communication data encryption stably and efficiently, communication data can be safely transmitted in IoT devices.

Key words: information security; encryption algorithm; encryption

(责任编辑 王 欢)