文章编号:1674-2974(2022)04-0069-09 DOI:10.16339/j.cnki.hdxbzkb.2022269

面向变电站二次系统的安全加固终端设备实现

王晓明[1†],周柯[1],巫聪云[2]
(1. 广西电网有限责任公司 电力科学研究院,广西 南宁 530023;
2. 广西电网有限责任公司,广西 南宁 530023)

摘 要:随着信息化与工业化的高度融合,变电站二次系统智能化、自动化程度不断增强.人们在享受便利性的同时,也需直面网络带来的挑战与威胁.针对二次系统应用程序或工具在计算、传输过程中可能面临的机密性、完整性等安全威胁,基于USB接口的安全加固终端保护技术成为研究热点.传统的安全加固终端设备虽然生产方便,但其中的算法已经由厂商指定并下载到了相应的设备中.考虑到不同场景安全需求的差异较大,并且不同的用户存在多级的安全需求.通过Arduino IDE平台对AVR单片机进行编程,设计实现了一个通用算法的安全加固终端设备,不仅实现了身份认证、内容加密等功能,同时满足了用户自主选择的个性化需求,提升了整个二次系统的安全性和可控性.经测试,初步证明了该终端的可用性和健壮性.

关键词:电网系统;安全加固终端;单片机;变电站安全
中图分类号:TP309.1 **文献标志码**:A

Realization of Safety Reinforced Terminal Equipment for Secondary System of Substation

WANG Xiaoming[1†],ZHOU Ke[1],WU Congyun[2]
(1. Electric Power Research Institute of Guangxi Power Grid Co Ltd,Nanning 530023,China;
2. Guangxi Power Grid Co. ,Ltd,Nanning 530023,China)

Abstract: With the high integration of informatization and industrialization, the degree of intelligence and automation of the secondary system of substations has been continuously enhanced. While enjoying the convenience, we also need to face the challenges and threats brought by the Internet. In view of the confidentiality, integrity and other security threats that the secondary system applications or tools may face during the calculation and transmission process, the enhanced security terminal protection technology based on the USB interface has become a research hotspot. Although the traditional enhanced security terminal equipment is easy to produce, the algorithms in it have been specified by the manufacturer and downloaded to the corresponding equipment. Considering that the security requirements of different scenarios are quite different, and different users have multi-level security requirements, the AVR microcontroller is programmed through the Arduino IDE platform, and an enhanced security terminal equipment with general algorithms is designed and implemented, which not only realizes functions such as identity authentication and content encryption, but also meets the personalized needs of users′ independent choices and improves the security and controllability of the entire secondary system. After the test, the usability and robustness of the terminal are prelimi-

* **收稿日期**:2021-07-29
基金项目:南方电网科技项目(GXKJXM20200242)
作者简介:王晓明(1985—),男,山西平遥人,广西电网有限责任公司电力科学研究院高级工程师
† 通信联系人,E-mail:1063000160@qq.com

narily proved.

Key words: grid system; safety reinforcement terminal; microcontrollers; substation safety

实现电力系统能量流与通信系统信息流的高度融合,打造安全可靠、智能高效的电网系统是“工业4.0”时代的又一战略性规划.作为变电站信息的承载基础,二次系统本身包括多种功能应用.一方面,主站所下达的控制指令和参数设置指令都需要通过二次系统执行,但是控制指令在被窃取和篡改的情况下无法进行安全鉴别和数据完整性验证,主站在被劫持或人员误操作情况下对变电站进行的非法操作也无法辨识并隔离,存在引发电网安全事故的风险.另一方面,由于设备厂家往往采用个人携带的电脑、U盘和配置工具进行运维操作工作,存在现场二次系统配置维护终端不安全,设备升级软件版本和工程配置及备份不可控,管理配置正确性依赖于厂家等多种问题,给变电站二次系统的安全、可靠和稳定运行带来了很大的隐患.

为了增强终端设备的安全性能,国内外众多公司和学者针对加固技术进行了广泛的研究,设计并研发出以下三类主流的安全加固产品.加密狗是一种为软件开发商提供程序安全性扩展的外界保护硬件,其提供了对软件功能和数据的保护.但由于使用通用芯片,破解者可以通过分析探测芯片电路获取芯片里的程序内容,反编译获悉程序逻辑,从而克隆出一个完全相同的加密狗.动态口令作为一次一密技术(one time password)的代表,是一个用来生成动态口令的实体终端设备.由于加密结果随时间动态变化,通常仅为简单的数字组合,安全性受到一定限制.USB Key作为一类独立的安全加固终端,通过单片机或智能卡芯片内置了用于身份认证和数据加密的算法[1].但为了大规模生产需要,其中的算法已经由厂商指定并提前下载到了相应的设备中.如果开发者有特殊需求,只能自己向生产厂商定制,不仅制作周期长,成本也更大,必然耗费更多的人力物力资源.此外,由于二次系统不同场景的安全需求差异较大,致使不同的用户存在多级的安全需求,传统的安全加固设备虽然生产方便,但其功能局限性已经不足以满足用户.本文通过Arduino IDE平台对AVR单片机进行编程,设计实现了一个可自定义加密算法的安全加固终端设备,不仅实现了身份认证、内容加密等功能,同时满足了用户自主选择的个性化需求,提升了整个二次系统的安全性和可控性.

1 背景及理论

1.1 变电站二次系统

目前,智能变电站系统普遍采用三层两网的物理架构,三层即站控层、间隔层、过程层,两网分别是站控层网络和间隔层网络.按照内部数据交互的过程,变电站二次系统的运维管理架构如图1所示.

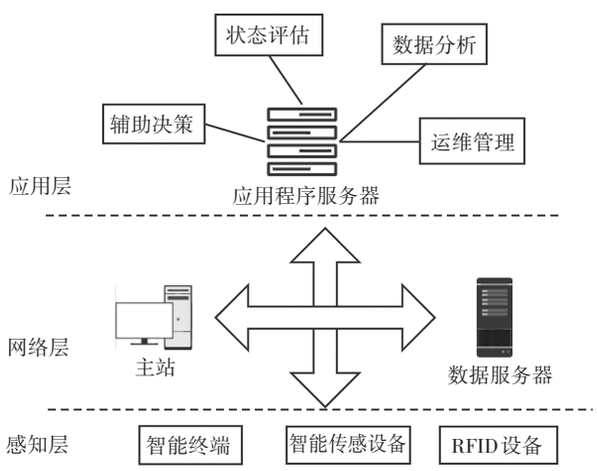


图1 变电站二次系统运维管理架构体系

Fig.1 The operation and maintenance management framework system of the secondary system of substation

其中,网络层作为终端中间层,负责接收智能感知层收集到的系统状态和信息,上送至应用层完成设备的在线监测和数据的统计分析等功能.作为数据的存储和中转中心,主站和数据服务器需要定期的运维管理和修护,并通过一定的安全技术降低信息泄露的风险.信息安全需要保障信息的机密性、完整性、可用性.对于把需要与外界进行交互的信息存放于内部的软件来说,如果将加密保护技术也包含在自身代码中,就很容易被调试、分析、反编译,最后被破解.因此,如何对二次系统进行安全加固,是整个电网系统稳定运行的重中之重.

1.2 Arduino

Arduino[2]主要是为AVR单片机设计的一个更加简单易操作、人性化的硬件开发平台. Arduino不同的型号采用了不同的单片机型号以及控制电路板,但通用了一个支持这些型号的专用编程开发软件. 由于Arduino对各种功能进行了再封装,以及给出了较多在各个方面的操作示例,开发者能更好地屏蔽底层的硬件开发细节,将更多的注意力转移到功能实现上来. 本实验使用的Arduino UNO型号本质上就是一块单片机控制板[3],且AVR单片机为控制核心.

1.3 IC和单片机

所谓IC即集成电路,是一种实现了某种电路功能(如计数器,加法器等)的微型电子器件. 借助于IC,电路板才能在毫米甚至微米级实现不同的功能. 单片机可以看作一台微型的计算机系统,与电脑PC机不同的是,其所有零件都在出厂之前被塑料壳封装在一个集成电路的内部.PC中的主要组件单片机内部都有,只是单片机的大多数部件集成在一起,共同构成一块IC芯片. 单片机作为嵌入式设备的典型代表之一,其使用领域十分广泛,在大多数物联网设备中都有单片机的身影. 市面上所称的"智能"电器,内部通常集成了单片机来进行电子器件的控制.

1.4 PIN码

所谓PIN码,一般是4位以上的便于记忆的"密码",但是它一般只包含纯数字,并且只与设置该PIN码的硬件关联,任何知道该PIN码的人都可以使用该设备. 对于有些设备而言,PIN码与账户密码功能相同,都可以访问该设备甚至进入该设备上已登录账户空间,但是PIN码一般不能替代账户密码修改账户信息[4].PIN码作为一种密码,保护的不是用户的使用权限,而是该用户所在设备的使用权限,而传统密码,一般是保护它所对应的特定用户数据的读写权限. 如果需要保护的设备都设置有相应的PIN码,那么知道PIN码就可以使用它所对应的固定设备,而只知道账户密码却不知道PIN码时,是无法使用设备的,也就无法访问账户数据. 如果不仅需要使用设备,也要对账户数据进行修改,则必须结合账户密码共同使用. 此时,PIN码和账户密码即实现了身份认证中的双因素认证.

1.5 网络安全基础

1.5.1 身份认证

身份认证主要用来确定认证者的物理真实身份同数据身份是否匹配[5]. 认证的方法分为以下三种:

1)根据你所知道的信息(what you know).

2)根据你所拥有的东西(what you have).

3)根据独一无二的身体(who you are).

物理身份和数据身份匹配的情况下,三种方法都是成立的,所以为了更高的安全性,从三种中选择其中两种来完成认证,即所谓的双因素认证[6].

1.5.2 加密算法

1)非对称加密.

公开密钥密码学(Public-key cryptography)又称非对称加密算法. 其非对称性主要体现在它需要公钥和私钥两种密钥,且二者不相同[7]. 如果其中一个密钥允许被公开,那么它可以叫作"公钥",另一个密钥则必须严格秘密保管,不能透露给其他人,称为"私钥". 具体地对一个明文进行加密时,若是使用公钥加密,则对方需要用与其配对的私钥才能解密,公钥自身不能解开[8];若是使用私钥进行加密,则对方只能用与其配对的公钥解密,私钥自身不能解开. 所以这种算法也叫作非对称加密算法. 按定义的话,公私钥匙是不能互相推导的. 但在实际实现过程中,保存私钥的文件中往往包含了一些关于公钥的信息,有的可能是直接包含了公钥,也有的可能是一些可以使私钥通过一定的方法得到公钥的信息. 常见的非对称加密算法有:国外著名的、使用最为广泛的RSA算法,椭圆曲线加密算法(简称ECC)以及国内的SM2算法[9].

2)对称加密.

对称密钥算法(Symmetric-key algorithm)也属于密码学中加密算法的一种. 之所以称为对称密钥,是因为加解密过程中使用的密钥相同,且由通讯双方共同享有,不允许泄露给他人. 实际上,多人通讯中为了通讯和管理密钥的方便,通常多个人之间只用单个密钥. 对称密钥的存在使得加密过程和解密过程非常相似,解密过程可以看作加密过程的逆运算. 常见的对称加密算法有国际上知名的DES、3DES(Triple-DES)、AES算法以及国密算法SM1、SM4等[9].

3)散列算法.

散列函数(Hash function)英文直译可以叫作哈希函数,由于其功能也可叫作摘要算法.它是一种从任何大小、任何类型数据(只要能表示成二进制串)中创建固定数据长度[10],用固定字符集表示的数字"指纹"的方法.散列函数可以把大量数据压缩成一个较短的固定字符串,也称为摘要,但它不能还原之前的数据.散列值的表示形式通常是阿拉伯数字和字母等可见字符组成的定长字符串.因为对输入数据的微小变化也会造成对应散列的剧烈变化,那么在散列碰撞概率微乎其微的情况下,散列函数是可以用来验证输入数据是否被篡改的,也就是可以用来保证信息的完整性.

2 安全加固终端设备的系统设计

2.1 总体设计框架

总的来说,本文所设计实现的是一个运行于AVR单片机上的、可自行配置算法的安全加固终端设备.这个系统主要通过单片机的串口与外界传输信息,在单片机内部实现身份认证和数据加密功能供处于外界的程序调用,并在功能的实现里加入多种可行算法.最后呈现的实物成果不仅需要实现USB Key等设备所能达到的基本功能,保证一定的安全性,同时也要保证外界程序的开发者可以根据自身需求选择调用需要的功能函数.这里的安全效果主要体现在:与算法相关的、需要被保护的、不希望被截获或窃听的核心信息(如密钥等)不会存在于调用方计算机内存里,也不会出现在通信信息交互的过程中.系统整体结构如图2所示,分为数据加密和身份认证两大部分.

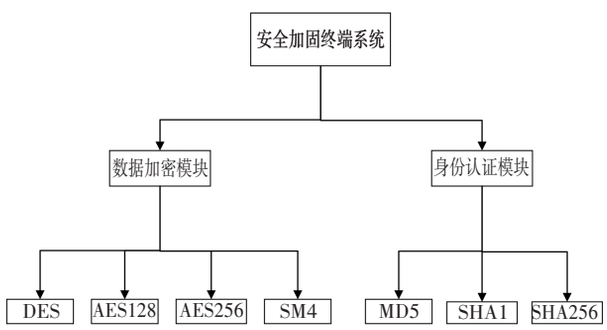


图2 安全加固终端系统架构图

Fig.2 System architecture of the enhanced security terminal

2.2 模块设计

本文主要设计实现了数据加密和身份认证两个功能.

2.2.1 数据加密

数据加密模块的信息交互实体主要涉及Demo调用程序和单片机.其中,调用程序传输指令和数据明文给单片机,单片机内部通过相关算法以及已经内置存储的密钥对明文进行加密然后发送回调用程序.整个过程中密钥不会在两者之间传递,这就保证了在没有密钥的情况下返回的密文是无法被轻易解开的,只能通过单片机的解密函数将密文再解密之后得到明文.详细的模块设计如图3所示.

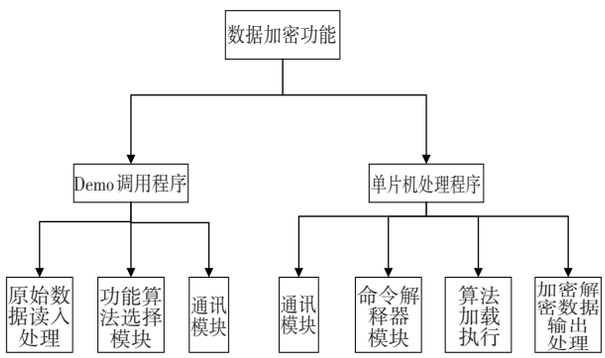


图3 数据加密模块图

Fig.3 Design of the data encryption module

其中,Demo调用程序主要通过通讯模块与单片机进行交互,使用者必须选择需要加密或者解密的数据以及算法之后,才能通过通讯模块将请求发送给单片机获得结果.单片机通过通讯模块接收到使用者的请求后,通过命令解释器模块获得用户需要加解密的内容以及要使用的算法,最后将结果通过通讯模块发送回调用者.

2.2.2 身份认证

身份认证功能的信息交互涉及Server端、Client端和单片机处理程序三方.Server端生成随机数发送给Client端,Client端再将随机数转发给单片机,单片机内部程序使用算法将随机数加密之后发回Client端,再由Client端发送给Server端,Server端使用相同算法验证随机数加密后结果是否相同,最后将验证信息发送回Client端完成身份验证.

此部分的模块设计如图4所示,首先是Client端通过登录模块发送登录请求给Server端,Server端通过通讯模块收到登录请求后通过随机数生成模块生成随机数,然后使用通讯模块将验证码发送给Client

端,Client 端再将收到的随机数发送给单片机,单片机通过通讯模块接收到随机数后,通过解释器模块解释后,使用指定的算法对随机数进行处理,并将处理后的结果发送回 Client 端,Client 端将该结果发送回 Server 端,Server 端也通过相同算法对随机数进行计算,其结果与收到的单片机处理结果进行比较,最后将验证信息发送回 Client 端的登录模块.

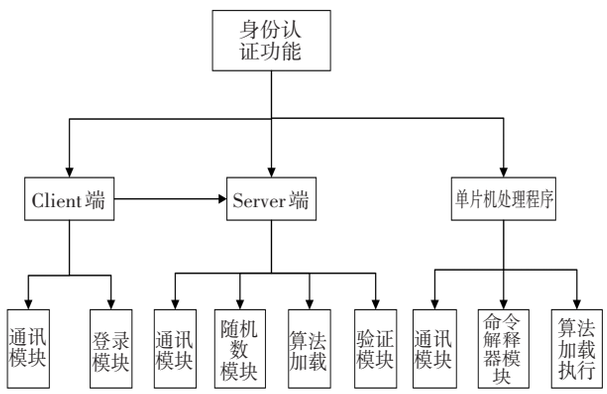


图 4　身份认证模块图

Fig.4　Design of the identity authentication module

2.3　程序流程

Demo 调用程序可以根据自身需要选择不同的语言开发,只要通过串口与单片机通讯即可.所以这里只展示了单片机内部程序实现的程序流程.

2.3.1　数据加密

图 5 是本系统数据加密功能的程序流程图.从上到下,先进行 PIN 码检测,PIN 码和存储在设备中的密钥(各个算法所需要的)组成了双因素认证.PIN 码验证通过后会等待用户继续输入指令,当接收到命令后,会对命令进行解释,其中包括了算法的选择,加密或者解密的选择[11-12].最后再选取相应的算法对已经传入进来的数据块进行加解密,然后把结果发送回调用者.

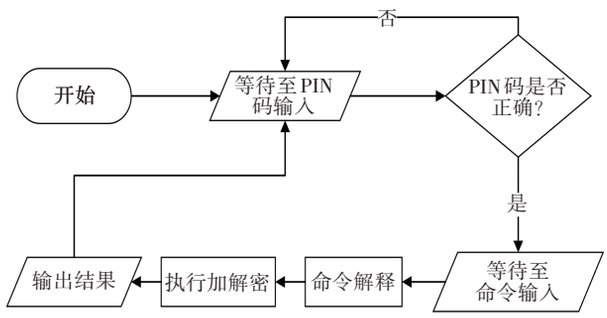


图 5　数据加密功能流程图

Fig.5　Process of the data encryption function

2.3.2　身份认证单片机部分的程序流程图

图 6 是本系统身份认证功能的程序流程图.从上到下,先进行 PIN 码检测,PIN 码和存储在单片机中的算法所使用的密钥组成了双因素认证.身份认证过程相对简单,只是对得到的随机数进行加密处理,这里可以使用 HMAC 系列摘要算法[13].通过将密钥和随机数混合后进行摘要,可以防止当随机数被截获、摘要算法被获悉时,攻击者轻易进行身份认证欺骗.使用随机数是为了防止重放攻击,使每次认证所需要的信息随着随机数改变而改变,截获的某一次的身份认证传输信息,在随机数改变后就无法生效.

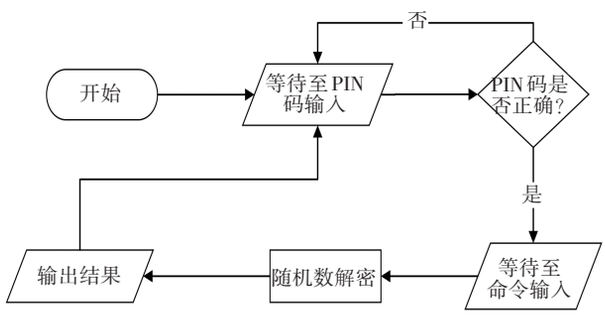


图 6　身份认证功能流程图

Fig.6　Process of the identity authentication function

3　安全加固终端设备的实现

3.1　通讯模块

Serial.print()函数为 Arduino 串口输出函数.由于单片机串口的 read 并不是阻塞的,所以需要循环判断 Serial.available()>0 来达到阻止程序前后运行的目的.又因为串口一位一位传输是需要时间的,所以需要有一个延迟来保证读取的时候所有字符都已经读入了缓冲区.

3.2　PIN 码校验模块

用户可在单片机代码中自定义全局变量 PIN 数值,然后通过 verifyPIN 函数逐个字符验证输入值 in 和全局变量 PIN 是否相等.

3.3　加解密模块

本系统共实现整合了 DES、AES128、AES256、SM4 四种加密算法.以 SM4 算法为例,给出实现过程:首先初始化 key 作为内置于单片机代码中密钥,input 是单片机得到的来自调用程序的输出,output 是单片机准备输出给外界的算法计算结果.设置好 key 和 input 后调用库函数 sm4_crypt_ecb 得到 SM4 结

果的输出 output,最后输出 output 即可.

3.4 摘要模块

本文包括 MD5 摘要、SHA1 摘要和 SHA256 摘要三大模块. 以 SHA256 摘要模块为例,首先设置电脑与 Arduino 进行串口通讯时的数据传输速率,进行 SHA256 对象初始化,然后把需要摘要的字符串传入 SHA256 对象进行哈希映射,最后用输出函数 print-Hash 输出结果.

4 系统测试

系统测试目的是验证整个设计总体所实现的功能是否满足需求,需要设计开发一系列 Demo 调用程序来调用单片机实现的功能. 这里的 Demo 程序模拟了正常程序对单片机的调用. Demo 调用程序使用的是 Python 语言开发. 在功能测试完毕的情况下,再对整个系统的性能如算法的执行时间进行一些测试. 最终完成的实物图如图 7 所示,目前已经使用 USB 接口与主机相连,为系统测试做好准备.

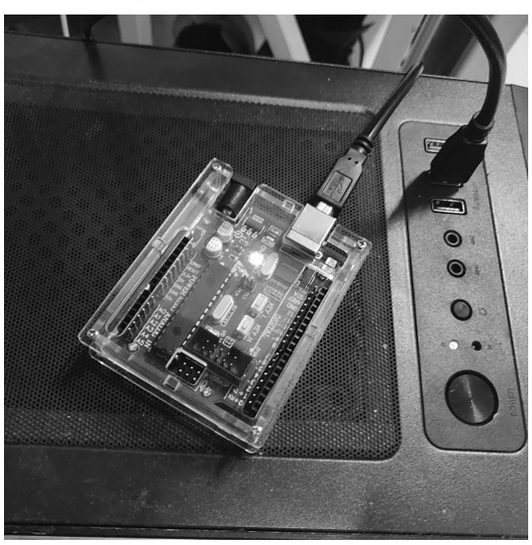


图 7 安全加固终端实物演示

Fig.7 Physical demonstration of the enhanced security terminal

4.1 数据加密模块集成测试

数据加密模块功能验证的方法是通过对同一字符串加密之后得到的密文再解密,判断结果是否能够得到原字符串,同时也可以与网络上在线加解密网站得到的结果进行比较. 原始用于测试的文本数据为 12345678abcdefghaaaaaaaahhhhhhhh,测试数据加密结果如图 8 所示.

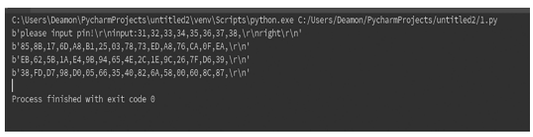


图 8 数据加密模块集成测试结果

Fig.8 Test results of the data encryption module

收到的字节数组具体为:

b′85,8B,17,6D,A8,B1,25,03,78,73,ED,A8,76,CA,0F,EA,\r\n′

b′EB,62,5B,1A,E4,9B,94,65,4E,2C,1E,9C,26,7F,D6,39,\r\n′

b′38,FD,D7,98,D0,05,66,35,40,82,6A,58,00,60,8C,87,\r\n′

第一部分是 PIN 的验证部分. 功能正常!

剩下的三部分分别是:

b′12345678abcdefgh′, b′aaaaaaaahhhhhhhh′, b′aaa\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00′三个字符串的加密结果.

与网站在线加密进行对比,见图 9,证明结果正确.

图 9 网站在线加密验证结果

Fig.9 Online encryption verification result

4.2 身份认证模块集成测试

Server 端服务程序结果如图 10 所示,成功接收到 Client 端的登录请求,并且接收到从客户端收到的来自单片机的随机数的哈希值. 最后经过运算发现服务端自己计算的 hash 函数值和传递过来的相等,最终给客户端发送登录成功字符串.

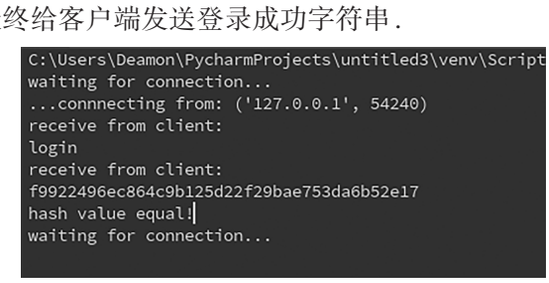


图 10 Server 端身份认证模块集成测试结果

Fig.10 Test results of the identity authentication module on the Server

图 11 所示为 Client 端运行结果,客户端收到来自服务端的验证码 1970,将其发送给单片机,经过单片机计算之后将结果发送回客户端,客户端收到了经过单片机哈希运算之后的散列值,然后将该散列值发送给服务端,服务端比较自己计算的散列值和收到的散列值是否相等,发现散列计算是相等的,最后客户端收到了服务端发送过来的 login success 字符串,证明身份认证通过.

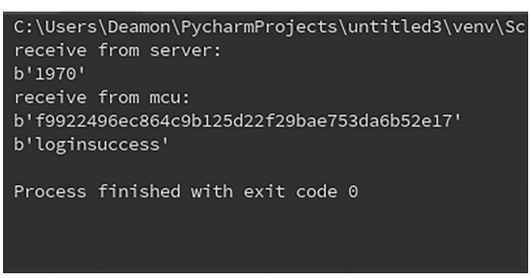


图 11　Client 端身份认证模块集成测试结果

Fig.11　Test results of the identity authentication module on the Client

4.3　算法性能测试

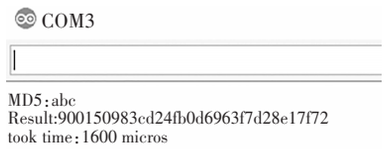
由于传统的安全加固终端中的算法已经由厂商指定并下载到了相应的设备中,无法单独测试单个功能的时间,因此我们只对本文所实现的加固终端算法进行测试统计.此外,与其他同功能设备相比,我们最大的优势在于整合多种该领域常用的算法,能够满足不同用户的安全需求,自身的对比分析更加全面有效,而且能为用户的个性化选择提供一定的参考标准.

4.3.1　摘要算法

如图 12 所示,单次 SHA256 耗时 32 116 μs,单次 SHA1 耗时 30 052 μs,MD5 的耗时只有 1 600 μs.可以发现 SHA1 和 SHA256 两者之间的耗时相差不明显,但是都明显比 MD5 长.也就是说,在对短字符串如“abc”摘要时,MD5 效率较高.

(a)SHA256 算法性能测试结果

(b)SHA1 算法性能测试结果



(c)MD5 算法性能测试结果

图 12　摘要算法性能测试结果

Fig.12　Performance test results of the digest algorithms

4.3.2　数据加密算法

对于同一数据,分别采用 DES、Triple DES、AES128、AES256、SM4 五种算法进行加解密实验,对于耗时进行统计分析,如表 1 所示.

表 1　加解密耗时统计表

Tab.1　Time-consuming for different algorithms to encrypt and decrypt

算法名称	加解密耗时/μs
DES	35 748
Triple DES	107 240
AES128	69 680
AES256	69 680
SM4	70 580

总的来说,三重 DES 的耗时最长,单次 DES 的耗时正好是 AES 和 SM4 的一半左右.将单次 DES 与 SM4 算法进行比对,常规的 DES 加密算法是 64 位[14],而 SM4 算法作为一个分组算法,数据分组长度为 128 比特,密钥长度也为 128 比特,因此单次 DES 耗时比 SM4 算法耗时降低一半是合理的.对于 AES 算法,作为一种对称密钥算法[15],可以使用 128、192 或 256 位密钥,并且用 128 位数据块分组对数据进行加密和解密.在本文进行的实验中,AES128 和 AES256 的加密与解密耗时是一样的,可能是由于待加密数据的长度是相同的,使得 AES128 和 AES256 有类似的加密处理过程,AES256 没有进行额外的 4 轮 round key 生成以及对应的 SPN 操作.

如图 13 所示,对单次 DES 算法和三重 DES 算法进行进一步对比分析,发现加密一次 DES 算法耗时 17 872 μs,三重 DES 耗时 53 620 μs,有很明显的三倍关系.此外,我们重复进行 10 次实验,对两种算法的平均耗时进行统计,发现仍然满足三倍时间比例,如图 14 所示.

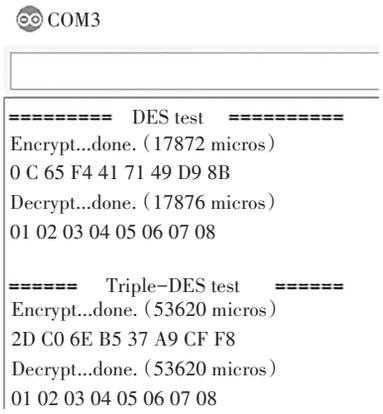


图 13 单次DES与三重DES性能对比

Fig.13 Performance comparison between single DES and Triple DES

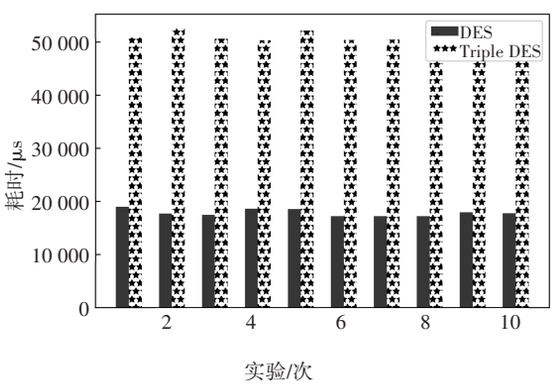


图 14 DES算法与三重DES算法平均耗时统计

Fig.14 DES and Triple DES algorithm average time consumption statistics

在图15中,通过将输入数据更改为16字节进行实验,我们发现SM4、AES256、AES128以及DES对于16字节的明文输入各个算法耗时是差不多的.而Triple DES仍满足三倍耗时的特点.

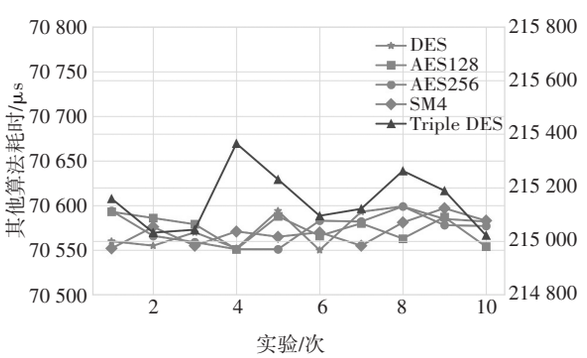


图 15 输入16字节数据的算法耗时统计

Fig.15 Algorithm time-consuming statistics for 16-byte data input

5 结 论

随着变电站建设的不断扩张,智能终端设备、应用程序和工具大量投入变电站现场应用.然而,这些装置的本体安全可信技术仍然受限,在使用过程中很可能被监听甚至篡改,为恶意的入侵提供了更多的可能[16].本文实现了一种基于USB接口的安全加固终端设备,避免了将安全技术封装在程序内部可能面临的反编译和被破解的风险,通过外接的方式保障二次系统主站及数据服务器在计算、传输过程中的机密性和完整性.此外,考虑到不同场景安全需求的差异较大,并且不同的用户存在多级的安全需求,改进了传统安全加固终端只能提前封装单个算法的固有缺点,将多种算法集成在一个单片机芯片上,不仅实现了身份认证、内容加密等功能,同时满足用户的个性化需求,能够根据实际应用场景自主选择内置算法,成本低、通用性好,对于二次系统应用功能级安全检测体系,实现AVC操作指令、智能告警等功能的安全加固具有一定的意义.

参考文献

[1] AN Y, ZHAO B, LI Y M. Research on software protection method based on USB Key [C]//19th IEEE International Symposium on Asynchronous Circuits and Systems. Wuhan, China, 2013: 210-213.

[2] 郎庆阳,吴明超,张楠,等. Arduino在压力监测项目开发中的应用研究[J]. 科技风,2019 (12):181.
LANG Q Y, WU M C, ZHANG N, *et al*. Application research of Arduino in the development of pressure monitoring project [J]. Technology Wind, 2019 (12):181. (In Chinese)

[3] 孙玲姣, 龙洋, 黄欣,等. 基于Arduino的电子技术实验教学改革探讨[J]. 电子世界, 2019 (3):34-35.
SUN L J, LONG Y, HUANG X, *et al*. Discussion on the reform of electronic technology experiment teaching based on Arduino [J]. Electronics World, 2019 (3):34-35. (In Chinese)

[4] 刘益和,沈昌祥. 一个信息安全函数及应用模型[J]. 计算机辅助设计与图形学学报,2005,17(12):2734-2738.
LIU Y H, SHEN C X. An Information security function and application model [J]. Journal of Computer-Aided Design & Computer Graphics, 2005, 17(12):2734-2738. (In Chinese)

[5] 杨京,周俊. 身份认证威胁与对抗措施分析[J]. 信息网络安全, 2010(11):83-84.
YANG J, ZHOU J. Analysis on the security threats of ID authentication and threat defense measure [J]. Netinfo Security, 2010

(11):83-84.(In Chinese)

[6] ZHAO D D, LUO W J. One-time password password authentication scheme based on the negative database[J].Engineering Applications of Artificial Intelligence: The International Journal of Intelligent Real-Time Automation, 2017, 62:396-404.

[7] 高明.浅谈对称加密算法与非对称加密算法的应用[J].电子世界,2015(15):59-60.
GAO M. Talking about the application of symmetric encryption algorithm and asymmetric encryption algorithm [J]. Electronics World,2015(15):59-60. (In Chinese)

[8] 蔡萌. 数据加密技术在计算机网络通信安全中的应用探析[J]. 通讯世界,2019,26(5):92-93.
CAI M. Analysis on the application of data encryption technology in computer network communication security [J]. Telecom World, 2019,26(5):92-93.(In Chinese)

[9] 吴志红,赵建宁,朱元,等. 国密算法和国际密码算法在车载单片机上应用的对比研究[J].信息网络安全,2019(8):68-75.
WU Z H,ZHAO J N,ZHU Y,*et al*. Comparative study on application of Chinese cryptographic algorithms and international cryptographic algorithms in vehicle microcotrollers[J]. Netinfo Security, 2019(8):68-75.(In Chinese)

[10] LIU J D,TIAN Y,WANG S H,*et al*. A fast new one-way cryptographic hash function[C]//2010 IEEE International Conference on Wireless Communications,Networking and Information Security. Beijing:IEEE,2010:302-306.

[11] 胡卫,吴邱涵,刘胜利,等.基于国密算法和区块链的移动端安全eID及认证协议设计[J].信息网络安全,2018(7):7-15.
HU W,WU Q H,LIU S L,*et al*. Design of secure eID and identity authentication agreement in mobile terminal based on Chinese cryptographic algorithm and blockchain[J]. Netinfo Security,2018(7):7-15.(In Chinese)

[12] 张平,陈长松,胡红钢. 基于分组密码的认证加密工作模式[J]. 信息网络安全,2014(11):8-17.
ZHANG P,CHEN C S,HU H G. Authenticated encryption modes based on block ciphers[J]. Netinfo Security,2014(11):8-17.(In Chinese)

[13] 李明,史国振,娄嘉鹏.基于密码服务平台的USB Key身份认证方案[J].计算机应用与软件,2018,35(9):288-291.
LI M, SHI G Z, LOU J P. USB Key identity authentication scheme based on encryption service platform[J]. Computer Applications and Software,2018,35(9):288-291.(In Chinese)

[14] 徐洪波,李颖华.DES加密算法在保护文件传输中数据安全的应用[J].信息网络安全,2009(6):24-26.
XU H B,LI Y H. The application of DES encryption algorithm to protect data security in the file transfer[J]. Netinfo Security,2009(6):24-26.(In Chinese)

[15] 张金辉,郭晓彪,符鑫.AES加密算法分析及其在信息安全中的应用[J].信息网络安全,2011(5):31-33.
ZHANG J H,GUO X B,FU X. AES encryption algorithm analysis and the application in information security[J]. Netinfo Security, 2011(5):31-33. (In Chinese)

[16] 崔光耀.打造国际市场安全中国造:解码飞天诚信国际化探索与实践[J].中国信息安全,2018(10):74-76.
CUI G Y. To build international market security made in China—decoding the international exploration and practice of flying integrity [J]. China Information Security,2018(10):74-76.(In Chinese)