文章编号:1005-0523(2020)01-0106-07

一种基于SM2智能卡的微电网安全登录系统的设计

汤鹏志[1],张梦丽[1,2],丁仕晗[1],左黎明[1,2]

(华东交通大学 1.理学院;2.系统工程与密码学研究所,江西 南昌 330013)

摘要:为解决微电网系统中身份认证问题,设计了一种基于SM2智能卡的微电网安全登录系统。首先以SM2智能卡为核心,描述了用户身份认证过程;然后对其进行安全性分析,该方案具有防伪造、防篡改、防重放特性;最后在嵌入式开发平台上实现了该系统。实验结果表明,该系统具有一定稳定性和高效性,对微电网系统安全稳定运行具有一定意义。

关键词:微电网;身份认证;SM2签名算法;攻击

中图分类号:TP309.7 **文献标志码**:A

DOI:10.16749/j.cnki.jecjtu.2020.01.015

本世纪初,为解决分布式电源接入大电网成本高、控制困难等诸多问题,协调大电网与分布式电源间的矛盾,学者们提出了微电网的概念[1-2]。微电网将发电机、负荷、储能装置及控制装置等结合,对可再生能源和分布式发电技术的整合提供了灵活、高效的平台,对电力系统产生了重大意义[3-4]。随着计算机信息技术的发展,微电网也进入信息时代。微电网中发配电系统、能量管理系统、监视控制与数据采集系统等的应用使得微电网更加智能化、高效化[5-6]。但在开放式互联网下,智能微电网本身存在数据被篡改、非法用户入侵等诸多安全问题,严重影响了微电网的正常运行。其中系统登录窗口都是系统的首要入口,也是黑客攻击的主要目标,因此建立一个安全可靠的登录认证机制至关重要。早在1996年,Gritzalis等人[7]通过概率协议或零知识模型对传统的基于口令认证机制提出零知识概率组合协议,具有较高的安全性和适用性。近年来,人们从不同方面对身份认证技术展开了一系列研究。2017年,Hezil等人[8]基于两种生物特征模式的融合提出了使用人耳和掌纹进行身份识别认证,但是基于生物特征的身份认证技术应用代价较昂贵,且存在重放攻击。2018年,Wu等人[9]开发了一个基于击键动力学的安全系统,能够通过其独特的打字行为来验证甚至识别用户,但击键身份识别技术需要专门设计的击键装置和大量用户击键特征数据,具有一定局限性。2019年,Zawadzki等人[10]提出了一种基于经典共享秘密的量子身份认证的有趣协议,但其应用范围具有一定局限性。

为提高微电网系统安全性,设计了一种适用于微电网系统的基于SM2智能卡安全登录系统,以SM2智能卡为核心,配套读卡器和身份认证服务系统为辅,实现了用户登录时的身份认证过程,保证了微电网系统的稳定安全运行。

1 国密SM2数字签名算法[11-12]

1.1 系统参数组

1)系统参数。给定安全参数λ,选取q阶有限域F_q,椭圆曲线$E(F_q)$,$E(F_q)$的方程的两个元素a和$b(a,b\in F_q)$;$E(F_q)$上的无穷远点或零点O;$E(F_q)$上阶为n的基点$G=(x_G,y_G)(G!=O$且$x_G,y_G\in F_q)$。

2)用户密钥生成。用户A随机选取整数$d_A(1\leqslant d_A\leqslant n-1)$,并计算公钥$p_A=d_AG=(x_A,y_A)$。其中$d_A$作为用户私钥秘密保存,$p_A$作为用户公钥对外公开。

收稿日期:2019-05-22

基金项目:国家自然科学基金项目(11361024);江西省教育厅科技项目(GJJ170386);江西省研究生创新项目(YC2018-S250)

作者简介:汤鹏志(1961—),男,教授,研究方向为信息安全。

1.2　SM2 签名生成算法

设待签名的消息为比特串 M,为了获取消息 M 的数字签名(h,S),作为签名用户 A 的具体签名生成操作如图 1 所示。

1.3　SM2 签名验证算法

为了检验收到的消息 M 及其数字签名(r,s),作为验证者的用户 B 具体验证签名操作如图 2 操作。

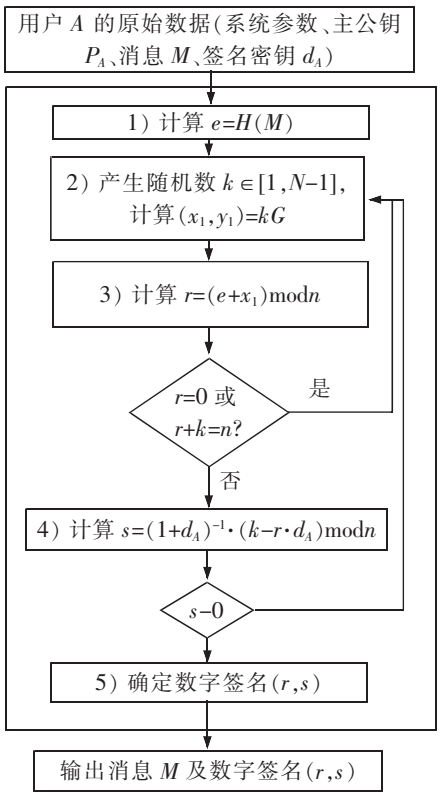

图 1　SM2 数字签名算法

Fig.1　The SM2 signature algorithm

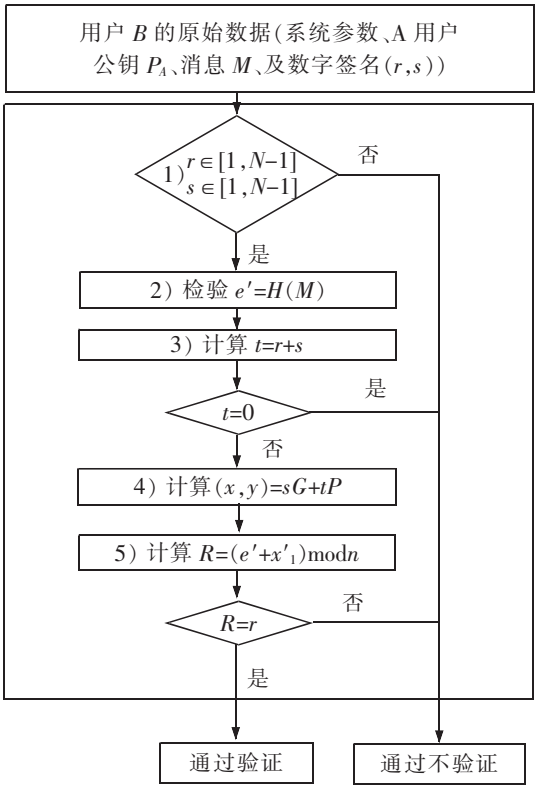

图 2　SM2 数字签名验证算法

Fig.2　The SM2 signature verification algorithm

2　系统整体架构设计

一种基于 SM2 智能卡安全登录系统,包括 SM2 智能卡、配套读卡器和身份认证服务系统三部分组成。其中 SM2 智能卡是拥有 SM2 签名功能的可进行读写的智能卡;配套读卡器为带有 NFC 功能或者蓝牙功能的移动端和蓝牙读卡器;身份认证服务系统由服务器端和数据库构成,如图 3 所示。

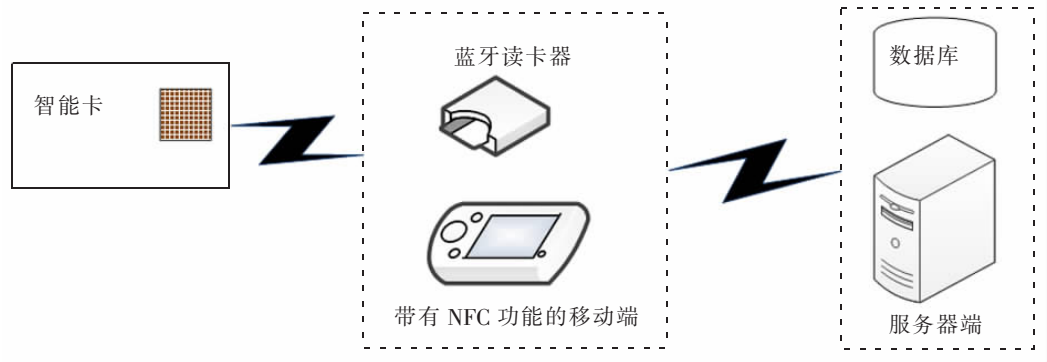

图 3　系统整体架构设计

Fig.3　System overall architecture design

身份认证服务系统主要包括服务器端和数据库。如图4所示,服务器端分为前端和后端。前端主要是用于界面展示,这里还用于展示根据随机数生成的二维码。后端主要由初始化模块、信息处理模块、身份认证模块和通信模块组成,其中初始化模块用于将智能卡的用户信息和公钥存入到数据库中,实现用户和智能卡的绑定;信息处理模块用于生成随机消息的二维码和解析收到的数据;身份认证模块主要用于对收到的SM2签名进行签名验证;通信模块用于服务器端和移动端的数据交互。数据库主要存放用户的关键信息,如用户名、用户公钥和智能卡ID。

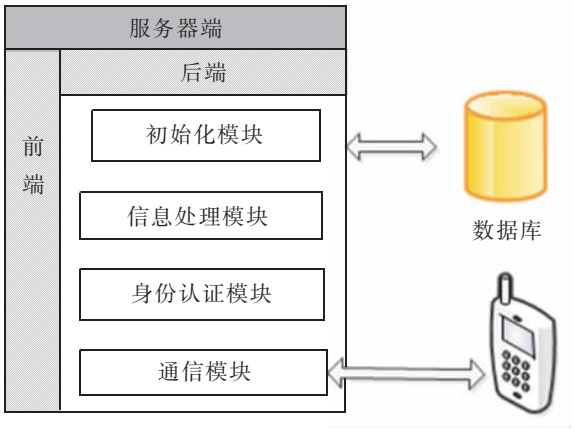

图4 身份认证服务系统
Fig.4 Identity authentication service system

3 登录认证流程

登录认证流程主要分为两个阶段,一个是用于绑定智能卡和用户的初始化阶段;另一个是用户登录系统时的身份认证阶段。

3.1 初始化阶段

在初始化阶段主要为每个用户绑定其所属的SM2智能卡,将SM2智能卡生成的相应用户公钥存到数据库中,实现一卡一用户绑定,主要步骤如图5所示。

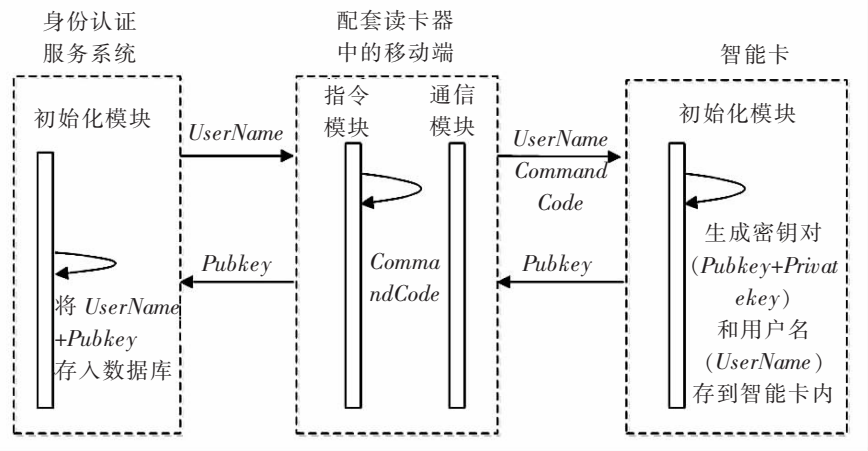

图5 初始化阶段
Fig.5 Initialization stage

步骤1:移动端通过其通信模块连接身份认证服务系统并获取用户名*UserName*,然后通过指令模块产生使智能卡生成密钥对和存用户名*UserName*的相关指令码*CommandCode*,通过移动端的通信模块将用户名*UserName*和指令*CommandCode*一同发给智能卡。

步骤2:智能卡收到的指令,初始化模块执行指令生成密钥对(公钥*Pubkey*和私钥*Privatekey*)并将用户名*UserName*存入智能卡中。

步骤3:移动端的指令模块产生读取智能卡公钥的指令,通过其通信模块操作智能卡获取智能卡的公钥*Pubkey*,然后将公钥*Pubkey*回发给身份认证服务系统。

步骤4:身份认证服务系统将收到的公钥*Pubkey*和用户名*UserName*一同存入到数据库中,存入成功后,则该用户的智能卡初始化完成,重复步骤1到步骤4直至所有的用户都被初始化或者所有的智能卡被

初始化,即达到一用户一卡的目的,初始化工作完成。

3.2　身份认证阶段

身份认证阶段为系统核心阶段,主要为用户在登录系统时进行的身份认证过程,若身份认证成功,则可成功登录系统,反之,登录系统失败。具体步骤图 6 所示。

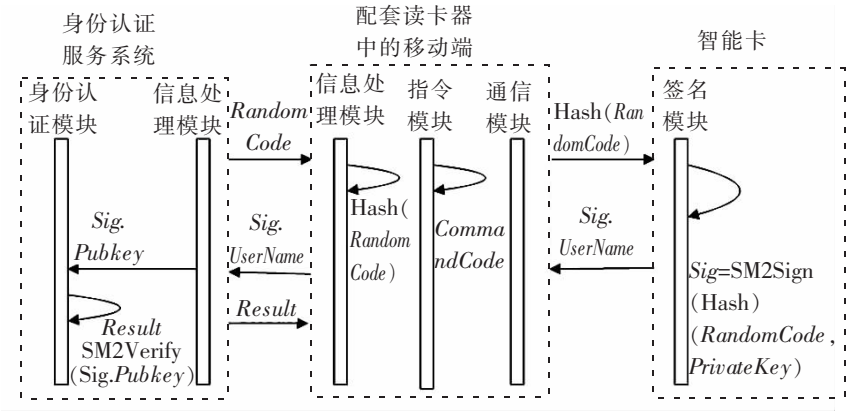

图 6　登录认证阶段

Fig.6　Login authentication stage

步骤 1:身份认证服务系统的信息处理模块定时生成带有随机码信息 *RandomCode* 的二维码。

步骤 2:移动端通过扫描二维码获取随机码信息,移动端的信息处理模块对获取的随机码进行哈希处理 Hash(*RandomCode*);同时指令模块产生操作智能卡进行 SM2 签名和读取智能卡内用户名的指令 *CommandCode*;最后通信模块连接智能卡传送哈希处理后的消息 Hash(*RandomCode*)和指令 *CommandCode* 发送到智能卡中。

步骤 3:智能卡执行指令,智能卡的签名模块对收到的消息 Hash(*RandomCode*)进行 SM2 签名算法:*Sig*=SM2Sign(Hash(*RandomCode*),*PrivateKey*);同时读取智能卡内的用户名 *UserName*,然后把签名结果 *Sig* 和用户名 *UserName* 返回给移动端。

步骤 4:移动端将接收的签名结果 *Sig* 和用户名 *UserName* 转发回身份认证服务系统。

步骤 5:身份认证服务系统根据收到的用户名 *UserName* 从数据库中检索出该用户对应的公钥 *Pubkey*,身份认证服务系统的身份认证模块用公钥 *Pubkey* 对收到的签名结果 *Sig* 进行如下 SM2 签名验证算法:*Result*=SM2Verify(*Sig, Pubkey*),若签名结果 *Result* 为 TRUE,则签名验证成功,即登录成功,进入系统主页;反之,则登录失败;同时将签名结果返回给移动端。

步骤 6:移动端将收到的签名验证结果显示到移动端屏幕上,用户可根据签名验证结果进行进一步操作,签名验证成功,则结束操作;签名验证失败,则可重复步骤 1 到步骤 5。

4　安全性分析

4.1　抗伪造攻击

SM2 数字签名算法已在随机预言机模型[13]下证明 SM2 数字签名方案可以有效抵抗存在性伪造攻击,并且在文献[14]证明 SM2 数字签名方案可抗密钥替换攻击,这里由于篇幅所限,不再详细进行证明,因此基于 SM2 智能卡的安全登录系统也具有抗伪造攻击。

4.2　抗重放攻击

在开放式互联网下,重放攻击是攻击者常用的攻击手段。攻击者通过拦截通信双方之前有效的通过签名验证的报文,然后将旧报文发送到认证服务系统,以破坏身份认证机制。重放攻击究其缘由是因为传送报文消息没有新鲜性,具有重复利用特性,本文提出的基于 SM2 智能卡的身份认证是对随机数进行签名,且每隔一分钟更新随机数,从而使得签名具有新鲜性,抵御重放攻击。

4.3 抗篡改攻击

在身份认证阶段,首先对身份信息进行哈希运算,然后利用SM2数字签名算法对传输的身份信息进行签名,若攻击者对当前通信的报文进行抗篡改攻击,将原报文信息(*UserName*,*Sig*)篡改为(*UserName*,*Cuangai_Sig*)并传送到身份认证服务系统进行签名验证,但是因为篡改后的签名*Cuangai_Sig*已不是对原有的*RandomCode*运行签名算法得到的真实签名,身份认证服务系统在验证签名SM2Verify(*Cuangai_Sig, Pubkey*)时就会验证失败,篡改攻击失败。

5 关键技术与实验仿真

在实验环境(电脑中央处理器:Intel i5-8500 U,内存:金士顿DDR4 16GB,操作系统:Windows7 64位操作系统)下,蓝牙读卡器为射频山东卡尔KT8003读卡器;移动端采用Android studio平台开发,并调用java版本的*BouncyCastle*库进行相关密码函数的调用;身份认证服务系统通过微软提供的Visual Studio 2012开发平台利用C#版本的*BouncyCastle*实现了登录认证过程,并模拟了通信双方传输数据的过程,关键实现代码如下。

5.1 身份认证服务系统生成二维码

身份认证服务系统首先生成随机数,然后根据随机数生成二维码,并每5 s更新下二维码,防止重放攻击,实现的关键代码如下。

```
var QRCodeInterval=setInterval(
 function(){
 //生成5位随机码
 str=toUtf8(RndNum(5));
 $().empty();
 $().qrcode({
        render:"table",
        width:200,
        height:200,
        text:str
 });
 }
,5000);
```

5.2 移动端通过蓝牙读卡器调用SM2智能卡进行签名

下面为在Android studio平台下读取SM2智能卡,调用SM2智能卡相关密码协处理器对扫到的二维码随机数*RandomCode*进行签名,并将签名结果*Sig*发送给身份认证服务系统的关键代码。

```
//使用蓝牙读卡器调用SM2智能卡进行签名
public boolean Bluetoothload(BluetoothReader mBluetoothReader,int slotNum, Resources res) throws Exception {
 //1.移动端成功通过蓝牙读卡器连接SM2智能卡
 boolean ret=false;
 ret=mBluetoothReader.cardPower(slotNum, CARD_POWERED);
 byte[] Sig;
 //2.从智能卡中读取出用户名
 byte[] UserName;
 UserName=Getcmd.getICCert2();
 //3.对扫描结果得到的随机数信息RandCde进行Hash
 byte[] hmsg=SM2Signer.HashM(QRCodeParam.RandomCode);
 //4.对Hash值进行SM2签名
```

```
Sig=Getcmd.cardSigh1(hmsg);
//5.将签名和用户名一起发送给身份认证服务系统
SendSig(Sig,Username);
}
```

5.3　身份认证服务系统验证签名

下面为运行在 Visual Studio 2012 开发平台的身份认证服务系统接收到签名 *Sig* 进行签名验证的关键代码,首先接收移动端传来的用户名和签名,然后根据用户名检索数据库,找到该用户所对应的公钥,然后用该用户公钥验证签名,最后将签名验证结果返回给移动端,如果验证成功,则该用户可以正常进入系统,反之,该用户被拒绝进入系统。

```
public override ArrayList SecurityLogin2(string RandomCode)
    {
        string msg =RandomCode;
        //1.接收移动端传来的用户名和签名
        string UserName = ctx.Request["UserName"];
        string Sig = ctx.Request["Sig"];
        //2.根据用户名检索数据库,找出该用户对应的公钥
        user u = IdalCommon.IuserEx.getUserByPubkey(UserName);
        if (u ! = null)//判断此卡是否有用户
        {
            string Pubkey = u.Pubkey;
            //3.验证签名信息,如果验证通过则返回当前用户对象的安全上下文信息
accctx = AccountsPrincipal.ValidateLoginBySignature(UserName,msg,Sig,Pubkey);
            if (accctx == null)//登录信息不对
            {
                msg ="签名验证失败:"+ UserName;
                Arraylists.Add(msg);
                Arraylists.Add(false);
            }
            else
            {
                msg ="签名验证成功! ";
                Arraylists.Add(msg);
                Arraylists.Add(true);
                Arraylists.Add(accctx);
            }
        }
        return Arraylists;//返回验证结果
    }
```

6　总结

本文设计了一种适用于微电网系统的基于 SM2 智能卡的安全登录系统以保证微电网系统高安全的身份认证。该系统由智能卡、配套读卡器和身份认证服务系统组成;并详细描述了用户身份认证过程;且该方案抗伪造攻击、抗篡改攻击和抗重放攻击;最后在嵌入式平台进行了实验模拟和仿真,通过长时间运行测试,证实了系统在高安全性的前提下也保证了高效性,对维持微电网系统的安全稳定运行具有一定意义。但是本文设计的基于 SM2 智能卡登录系统对 SM2 智能卡依赖性较强,若 SM2 智能卡丢失或被盗会对系统造

成一定危害,考虑到双因子甚至多因子身份认证[15-16]的特性,后续将研究“基于生物特征+密码学技术”的双因子身份认证。

参考文献:

[1] LASSETER B. Microgrids:distributed power generation[C]//Proceedings of the 2001 IEEE Power Engineering Society Winter Meeting. Columbus,OH,USA:IEEE,2001:146-149.

[2] LASSETER R H,PAIGI P. Microgrid:a conceptual solution[C]//Proceedings of the 2004 IEEE 35th Power Electronics Specialists Conference. Aachen,Germany,2004:4285-4291.

[3] 鲁宗相,王彩霞,闵勇,等. 微电网研究综述[J]. 电力系统自动化,2007,31(19):100-107.

[4] 盛鹃,孔力,齐智平,等. 新型电网-微电网(Microgrid)研究综述[J]. 继电器,2007,35(12):75-81.

[5] BIDRAM A,DAVOUDI A. Hierarchical structure of microgrids control system[J]. IEEE Transactions on Smart Grid,2012,3(4):1963-1976.

[6] LASSETER,R. H. Smart Distribution:Coupled Microgrids[J]. Proceedings of the IEEE,2011,99(6):1074-1082.

[7] GRITZALIS D,KATSIKAS S. Towards a formal system-to-system authentication protocol[J]. Computer Communications,1996,19(12):954-961.

[8] HEZIL N,BOUKROUCHE A. Multimodal biometric recognition using human ear and palmprint[J]. IET Biometrics,2017,6(5):351-359.

[9] WU C,WANG D,LIU R,et al. Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array[J]. Materials Today,2018,21(3):216-222.

[10] ZAWADZKI P. Quantum identity authentication without entanglement[J]. Quantum Information Processing,2019,18(1):7.

[11] 国家密码管理局. GB T32918-2016 SM2 椭圆曲线公钥密码算法[S]. 北京:中国标准出版社,2017.

[12] 汪朝晖,张振峰.SM2 椭圆曲线公钥密码算法综述[J]. 信息安全研究,2016,2(11):972-982.

[13] BELLARE M,ROGAWAY P. Random Oracles are Practical:A Paradigm for Designing Efficient Protocols[C]// /Proceedings of the 1st Acm Conference on Computer and Communications Security. ACM NewYork,US,1993:62-73.

[14] ZHANG Z,YANG K ,ZHANG J ,et al. Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks[C]// International Conference on Research in Security Standardisation. Berlin:Springer,2015:140-153.

[15] WANG D,LI W,WANG P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks[J]. IEEE Transactions on Industrial Informatics,2018,14(9):4081-4092.

[16] SUDHAKAR T,NATARAJAN V. A new three-factor authentication and key agreement protocol for multi-server environment[J]. Wireless Networks,2019(3):1-12.

A Microgrid Security Login System Based on Smart Card SM2

Tang Pengzhi[1],Zhang Mengli[1,2],Ding Shihan[1],Zuo Liming[1,2]

(1. School of Science,East China Jiaotong University,Nanchang 330013,China;
2. SEC Institute,East China Jiaotong University,Nanchang 330013,China)

Abstract: To solve the problem of identity authentication in microgrid system, a microgrid security login system based on SM2 smart card is designed. Firstly, with SM2 smart card as the core, the process of user identity authentication is described. Then the security of the scheme is analyzed. The scheme is characterized by anti-counterfeiting, anti-tampering and anti-replay. Finally, the system is implemented on the embedded development platform. The experimental results show that the system has a certain stability and efficiency, which has certain significance for the safe and stable operation of microgrid system.

Key words: microgrids;identity authentication;the SM2 signature algorithm;attack