基于SM2的电力广域测量系统安全认证方案

吴宁[1]，蔡杰[1]，梁公豪[2]
（1.南瑞集团（国网电力科学研究院）有限公司，江苏 南京 211100；
2.南京邮电大学 计算机学院，江苏 南京 210023）

摘要：电力广域测量系统作为智能电网监测的重要部分，其安全至关重要。因此，为了保证电力广域测量系统中通信数据的完整性和机密性以及系统内部各个终端设备之间的通信安全，提出一种基于SM2算法的电力广域测量系统安全认证方案。该方案基于SM2算法以及数字证书技术实现相互认证，提高智能电网设备中PMU设备之间的数据通信安全性和可靠性。最后，通过安全分析和实验评估表明，该方案能够有效抵御中间人攻击、重放攻击、长时间窃听等多种攻击。

关键词：SM2（一种椭圆曲线公钥密码算法）；电力广域测量系统；同步相量测量单元；相互认证
中图分类号：TM73 **文献标识码**：A **DOI**：10.19457/j.1001-2095.dqcd24407

Security Authentication Scheme of Power Wide Area Measurement System Based on SM2

WU Ning[1]，CAI Jie[1]，LIANG Gonghao[2]
（1.*Nari Group Corporation / State Grid Electric Power Research Institute*，*Nanjing* 211100，*Jiangsu*，*China*；2.*School of Computer Science*，*Nanjing University of Posts and Telecommunications*，*Nanjing* 210023，*Jiangsu*，*China*）

Abstract: As an important part of smart grid monitoring system，the security of power wide area measurement system is very important. Therefore，in order to ensure the integrity and confidentiality of communication data in power wide area measurement system and the communication security between terminal devices in the system，a security authentication scheme of power wide area measurement system based on SM2 algorithm was proposed. Mutual authentication based on SM2 algorithm and digital certificate technology was realized by the scheme，which also improves the security and reliability of data communication between PMU devices in smart grid devices. Finally，the security analysis and experimental evaluation show that man in the middle attack，replay attack，long-time eavesdropping and other attacks can be resisted effectively by the scheme.

Key words: SM2（an elliptic curve public key cryptographic algorithm）；wide area measurement system（WAMS）；phasor measurement unit（PMU）；mutual authentication

随着电力系统规模的日益壮大，现代电力系统结构以及运行方式也日趋复杂，为保证电力系统的稳定运行，对电网可靠、动态、实时的监控具有十分重要的意义。传统的监控和数据采集系统（supervisory control and data acquisition，SCADA）已经不能满足稳定监控的要求，基于同步相量测量单元（phasor measurement unit，PMU）[1]的广域测量系统（wide area measurement system，WAMS）成为了电网稳定监控的有效技术手段。如图1所示，WAMS由PMU装置、全球定位系统（global positioning system，GPS）、高速通信网络设备、子站、主站分析系统等部分组成。然而，随着WAMS中连接的设备种类越来越多，各个设备之间的通信也越来越复杂。因此，WAMS中发生的安全与隐私问题也越来越多。

WAMS中保存着大量电网的实时状态信息，并且存在着大量诸如PMU这类的终端设备，因此WAMS中的通信安全十分重要。在通信过程中首先需要保证的就是身份的安全，因此需要一种安全可靠的身份认证方法。

目前，大多数通用的认证算法中都是采用RSA（Ron Rivest，Adi Shamir，Leonard Adleman三

作者简介：吴宁（1983—），男，硕士，高级工程师，Email：17341821@qq.com
通讯作者：蔡杰（1983—），男，本科，高级工程师，Email：caijie@sgepri.sgcc.com.cn

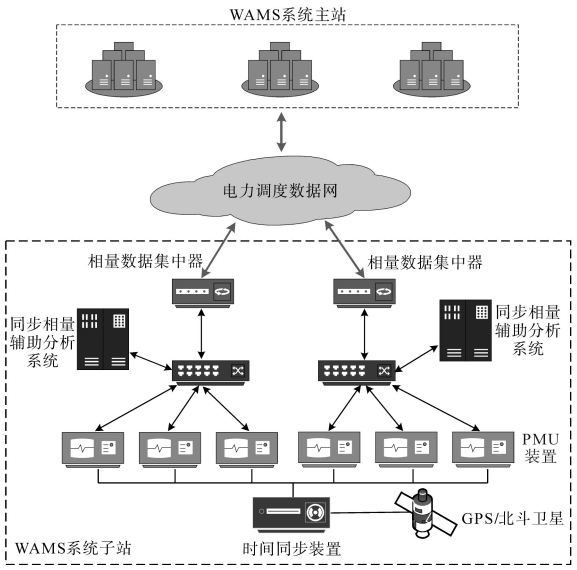

图1　WAMS结构图

Fig.1　WAMS structure diagram

人提出）算法来实现非对称加密和数字签名。然而，随着大整数分解技术的发展和完善，依赖于大整数因子分解困难性的RSA算法的安全性正遭到威胁。为了提升RSA算法的安全性，需要不断增加RSA算法的密钥长度。由于RSA算法的密钥长度提升与安全性提升之间是非线性的，因此这导致增加密钥长度之后加解密的速度大大降低，对硬件的计算要求也越来越高。同时，斯诺登事件爆发后，其泄露出的机密文档显示，RSA算法中可能存在美国国家安全局（national security agency，NSA）的预置后门，这对RSA算法的安全性产生巨大影响。因此，RSA算法变得不再适合WAMS这种存在大量硬件资源受限设备的系统中。

椭圆曲线密码学（elliptic curve cryptography，ECC）又称椭圆曲线加密算法，是一种基于椭圆曲线离散对数问题难解性的算法，它可以用更短的密钥提供比RSA算法更高等级的安全，即ECC算法具有很高的每比特安全强度，更适用于硬件资源有限的WAMS中。SM2（一种椭圆曲线公钥密码算法）算法是我国基于ECC椭圆曲线密码理论自主研发设计，并推荐使用256位曲线作为标准曲线。我国大力推动SM2国产密码算法替换目前所采用的RSA算法，一方面规避RSA算法存在的脆弱性和“预置后门”等安全风险，另一方面确保密码算法这一关键环节的自主可控，保障我国信息安全基础设施的安全可信。

在终端身份认证与安全通信方面，已经有许多学者展开研究。为了解决IEC 61850-90-5通信标准中密钥交换期间容易受到中间人攻击的缺陷，Farooq等人[2]提出一种基于证书的显式认证机制来缓解PMU通信网络中的中间人攻击。Varan等人[3]基于混沌加密算法设计了一种PMU设备双向安全通信方法。Hussain等人[4]提出一种基于密钥分配方案的安全机制，减轻了PMU受到的网络攻击。谢吉华等人[5]针对电力二次系统安全防护体系缺乏集中管理和审计，且现有的安全体系公钥算法均采用RSA算法的现状，提出了基于国产SM2密码体系的安全支撑平台的设计和实施方案。骆钊等人[6]利用缓存机制解决了传输层安全性协议（transport layer security，TLS）作为安全传输通道连接时间过长的问题，提出基于SM2密码体系的TLS协议在智能变电站远动通信中“长连接”与“短连接”相互配合的安全策略机制。Khan等人[7]设计了一个安全网关解决了电网中IEC 61850-90-5协议与IEEE C37.118.2协议之间的转换。贾冀芳等人[8]在OpenSSL基础上设计一种SM2与RSA自动切换的算法以满足在性能达标的前提下提高系统的安全性。Li等人[9]鉴于智能电网通信网络的安全需求和智能终端的固有特性，提出了一种新的身份验证方案，该方案使用最少的计算次数来解决网络攻击。吕良等人[10]基于数字签名和国密SM2算法提出了一种终端接入认证协商协议，保证了智能终端和企业内网数据中心的双向通信安全。Wu等人[11]根据SM2算法和密钥协商提供相互认证，提出了一种适用于智能电网的轻量级的安全认证和密钥协商方案。

本文针对智能电网中的广域测量系统的特点，提出了一种基于SM2的广域测量系统安全认证方案。基于广域测量系统中终端的硬件限制，提出的解决方案可以减少双方通信过程中复杂的计算时间。建立连接时，终端必须完成身份认证，同时在数据传输前获取会话密钥。本文的主要贡献包括：

1）该方案使用SM2国密算法替换了传统认证方案中的RSA算法，使得认证过程做到自主安全可控。

2）通信终端之间完成认证之后，通过密钥协商过程协商出通信密钥。该密钥使用对称加解密算法，可以是SM1或者RC4等对称加密算法。

3）通过安全性分析和实验结果分析，该方案可

以抵抗中间人攻击、重放攻击等常见的网络攻击。

1 测量系统认证方案

假设攻击者δ可以获得同步向量系统中任何终端的公钥，并且攻击者还拥有以下属性：

1）δ能够访问公共通信线路，因此δ可以随意增加、删除、修改、查询通信中的消息。

2）δ可能是系统中的不诚实用户并冒充中间人。

3）δ无法攻破可信第三方证书授权（certificate authority，CA）认证中心，即无法获取CA的私钥。

本文提出了一种基于SM2数字签名技术和公钥密码体制的广域测量系统认证方案。假设广域测量系统中的设备都从一个可信的第三方CA机构处获得签署的证书，并且设备内置CA机构的证书。在所提出的方案中，双方在完成相互身份认证之后，将在密钥协商期间生成之后通信期间使用的会话密钥。表1中是方案中使用的一些符号参数。

表1 符号参数描述

Tab.1 Description of symbol parameters

符号	描述
A，B	设备A与设备B
d_i	设备i的私钥
P_i	设备i的公钥
ID_i	设备i的身份标识
S_K	会话密钥
C_i	设备i的证书
r_i	设备i生成的随机数
SN	通信序列号
$E_{p_i}(m)$	使用设备i的公钥对原文m进行SM2公钥加密
$D_{d_i}(m)$	使用设备i的私钥对密文m进行SM2私钥解密
$S_{d_i}(m)$	使用设备i的私钥对消息m进行SM2签名
$V_{P_i}(sig,m)$	使用设备i的公钥，签名原文m对签名sig进行验证
$VCert(P_i,C_j)$	使用i的公钥验证j的证书
$H(m)$	对消息m进行SM3哈希计算

1.1 系统初始化

假设通信双方为A与B，A与B首先在本地生成256位的私钥d_A与d_B。私钥由随机数生成器生成，A和B向CA机构发送证书请求时连同加密过的私钥发送。CA解密后获取私钥并通过SM2公钥生成算法为通信方生成公钥，同时为其生成证书并用自己的私钥签名。证书中包括公钥P_A和P_B、身份标识ID_A和ID_B、版本号、序列号、证书签署机构标识、证书签署机构的签名、证书有效期等信息。之后，A与B将执行相互身份认证。系统初始化过程如图2所示。

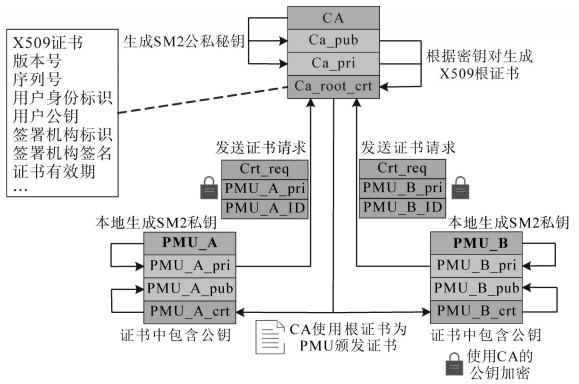

图2 系统初始化

Fig.2 System initialization

1.2 相互认证

步骤1：A生成随机数r_A和SN，计算$Request = SN \| r_A \| S_{d_A}(r_A) \| C_A \| H(SN \| r_A \| S_{d_A}(r_A) \| C_A)$，并将$Request$发送给B。

步骤2：B接收到A发送过来的请求$Request$之后，首先从中获取$SN \| r_A \| S_{d_A}(r_A) \| C_A'$与$H(SN \| r_A \| S_{d_A}(r_A) \| C_A)'$，计算$H[SN \| r_A \| S_{d_A}(r_A) \| C_A']$，并判断$H[SN \| r_A \| S_{d_A}(r_A) \| C_A']$是否等于$H[SN \| r_A \| S_{d_A}(r_A) \| C_A]'$，如果不等于，则断开连接。其次从$Request$中获取$C_A$并使用本地$C_{CA}$中的$P_{CA}$验证$C_A$，即计算$VCert(p_{CA},C_A)$，如果结果为False，则断开连接。之后B从$C_A$中获取$P_A$，从$Request$中获取签名$S_{d_A}(r_A)$与$r_A$，如果$V_{P_A}[S_{d_A}(r_A),r_A]$验证结果为True，则成功认证A的身份，否则验证失败。

步骤3：B生成随机数r_B，计算$Reply = (SN + 1) \| r_B \| S_{d_B}(r_B) \| C_B \| H[(SN + 1) \| r_B \| S_{d_B}(r_B) \| C_B]$，并将$Reply$发送给A。

步骤4：A接收到B发送过来的$Reply$，首先从中获取$(SN+1) \| r_B \| S_{d_B}(r_B) \| C_B'$与$H[(SN+1) \| r_B \| S_{d_B}(r_B) \| C_B]'$，计算$H[(SN+1) \| r_B \| S_{d_B}(r_B) \| C_B']$，并判断$H[(SN+1) \| r_B \| S_{d_B}(r_B) \| C_B']$是否等于$H[(SN + 1) \| r_B \| S_{d_B}(r_B) \| C_B]'$，如果不等，则断开连接。其次从$Reply$中获取$C_B$并使用本地$C_{CA}$中的$P_{CA}$验证$C_B$，即计算$VCert(P_{CA},C_B)$，如果结果为False，则断开连接。之后A从$C_B$中获取$P_B$，从$Reply$中获取签名$S_{d_B}(r_B)$与$r_B$，如果$V_{P_B}[S_{d_B}(r_B),r_B]$验证结果为True，则成功认证B的身份并完成相互认证，否则验证失败。

通信双方A与B相互认证过程如图3所示。

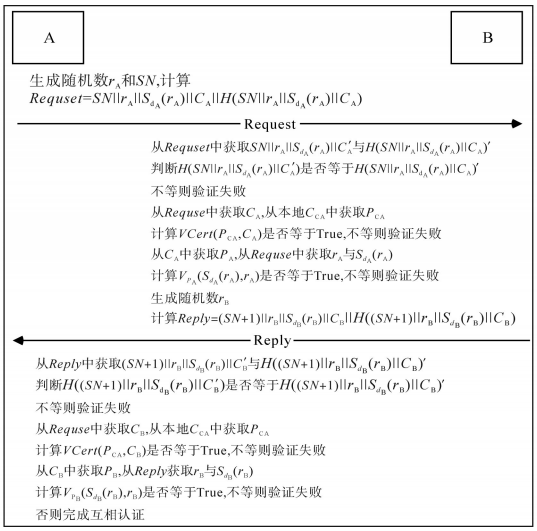

图3　相互认证图

Fig.3　Mutual authentication diagram

1.3　密钥协商

当A与B相互认证完成,开始通信密钥的协商。如图4所示,双方协商会话密钥的过程主要分为以下三个步骤:

步骤1:A生成随机数r_A和SN,将$Request=SN||E_{P_B}(r_A)$发送给B。

步骤2:B使用私钥d_B解密得到$r_A=D_{d_B}[E_{P_B}(r_A)]$,同时生成随机数$r_B$,计算$S_K=r_A\wedge r_B$,将$Reply=(SN+1)||E_{P_A}(r_B)||H(S_K)$发送给A。

步骤3:A使用私钥d_A解密得到$r_B=D_{d_A}[E_{P_A}(r_B)]$,同时计算$S'_K=r_A\wedge r_B$以及$H(S'_K)$。比较$H(S'_K)$与$H(S_K)$是否相同,如果相同,那么会话密钥就是$S_K$,否则协商失败。

A与B通过使用对方的公钥加密自己生成的随机数实现安全地交换密钥协商的信息,最终协商出的会话密钥将用于双方通信信息的对称加解密。双方间的通信基于TCP连接,双方每次连接都需要重新验证身份并协商会话密钥,因此每个会话密钥只能在一次连接中使用。当连接关闭时,会话密钥将不再使用。

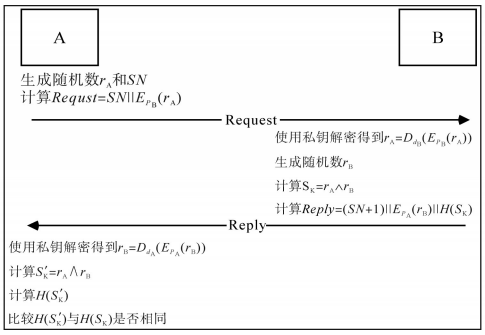

图4　密钥协商过程图

Fig.4　Key negotiation process

2　安全分析

2.1　中间人攻击

在提出的方案中,攻击者δ虽然可以获取通信的内容、系统中所有人的公钥和证书,但是由于δ无法获取通信双方的私钥以及CA的私钥,因此无法冒充中间人获取其中一方的认证。在双方通信时会将自己的证书和签名发送给对方,接收时使用本地内置的CA的公钥来验证证书并使用证书中的公钥来验证签名,双重验证保证消息发送者是合法的用户。因为δ没有CA的私钥,即使δ冒充中间人同时修改证书与签名也无法通过CA公钥验证证书这一步,所以无法发动有效的中间人攻击。

2.2　重放攻击

在方案中,通信发起者A在发送*Request*时会附带一个随机的序列号*SN*,并且接受者B回复时发送的*Reply*中会将*SN* + 1加入,当其中一方接收到另一方的消息时首先会检查并验证*SN*。

假设A发送了一个消息给B,消息中的序列号是*SN*,此时A会保存自己发送的上一个序列号的值*SN*。B回复A时发送的*Reply*中的序列号是*SN* + 1,A检查此序列号确实比保存的*SN*大1便会保存接收到的序列号*SN* + 1。此时攻击者δ发送多个重复的包含*SN* + 1的*Reply*,那么A检测到序列号和上一次接收并保存的一样则忽略这些消息。

2.3　长时间窃听

在方案中,由于双方通信是基于TCP连接的,因此每次双方重新连接都会认证并协商一个会话密钥,即会话密钥是不断改变的。所以攻击者δ想要长时间窃听加密的通信信息就需要不断破解会话密钥,这是十分困难的。

2.4　消息注入攻击

在方案中,通信双方完成密钥协商后会使用相同的密钥S_K来对称加解密通信的信息。由于会话密钥S_K只有通信双方知道,因此攻击者δ无法获取密钥S_K来加解密通信信息,所以攻击者δ无法在信息中注入违法内容。

2.5　模拟攻击

在方案中,用户B是通过验证A的证书和签名来认证A的。如果A能够通过双重验证便可以和B通信,否则便检测出模拟攻击。由于方案是假设可信第三方CA是安全的,攻击者δ无法获取CA的私钥以及通信双方的私钥,因此攻击者无

法通过相互认证环节。

3 实验与分析

实验使用官方推荐的素数域256位SM2椭圆曲线参数。实验使用的CPU为AMD Ryzen 7 5800H with Radeon Graphics,使用开发语言为Java(JDK14),使用密码库为bouncycastle。通过以上工具实现了SM2 X509 V3证书的签发,并模拟了第1节中提出的系统认证方案。当通信双方完成相互认证后,使用RC4对称加密来加密通信信息,RC4对称密钥长度设为256位。

3.1 系统初始化功能测试

当系统初始时本地没有证书,此时需要向CA机构申请证书。如图5中左半部分所示,初始时PMU终端从本地读取不到证书。当终端向CA机构提交证书申请请求时,会使用CA的公钥将本地256位私钥加密后发送给CA,CA会根据PMU的私钥生成公钥并为其生成X509证书。如图5右半部分所示,终端申请证书之后可以读取证书的基本内容。

图5 终端向CA申请证书前后图

Fig.5 Before and after terminal applies for certificate from CA

3.2 相互认证以及密钥协商功能测试

测试中使用两台相同配置的笔记本模拟两个PMU终端A与B之间的认证与密钥协商功能。当A与B都有合法证书时,如图6和图7所示。

图6 开始认证前图

Fig.6 Before starting certification

图7 认证成功之后图

Fig.7 After successful authentication

双方本地都存在SM2 X509 V3格式的证书,双方之一发起认证之后都能够协商出相同的RC4会话密钥并能够用于通信加解密。

3.3　抗攻击测试

3.3.1　重放攻击测试

当模仿攻击者多次发送相同的数据给PMU终端时,此时会通过检测数据中的序列号发现重放攻击。实验中模拟发送重复的数据给PMU终端,此时认证双方都会检查到序列号的异常,本方案可以抵抗重放攻击,抵抗攻击结果如图8所示。

3.3.2　中间人攻击测试

假设中间人无法获取合法的证书,但是可获取到PMU_B的合法证书。通过解析截获的认证数据,中间人使用自己的私钥生成签名然后附上PMU_B的合法证书以及Hash指纹后发送给PMU_A。这里使用PMU_B来模拟中间人,中间人将合法认证数据中签名替换成自己的签名,并生成Hash指纹。虽然中间人拥有合法PMU_B的证书并且使用SM2算法重新生成Hash指纹,能够通过Hash验证以及证书验证,但是由于没有PMU_B的私钥,因此无法通过签名验证。如图9所示,中间人最终因无法通过签名验证而无法完成身份认证,因此方案能够抵抗中间人攻击。

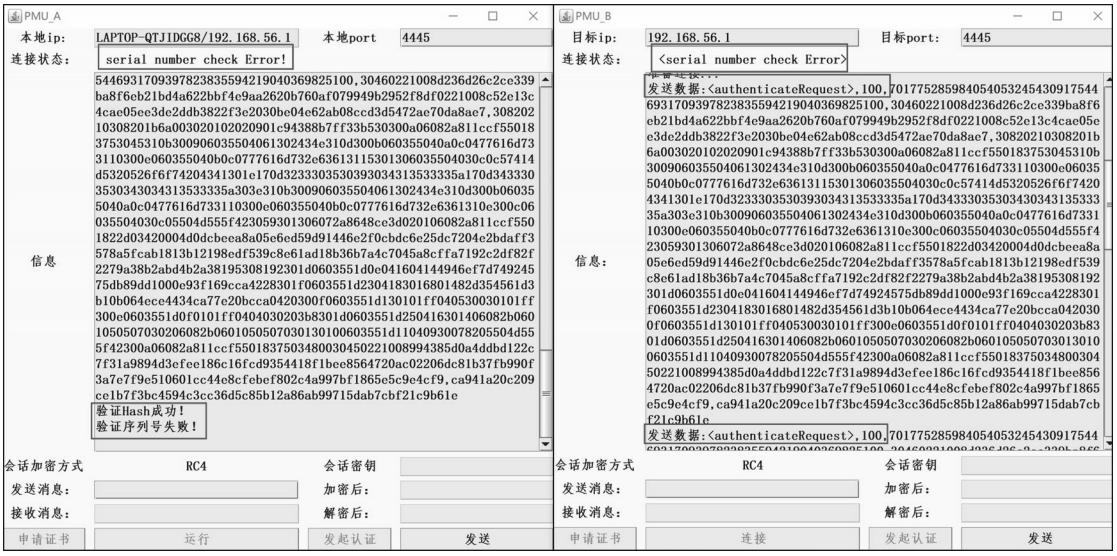

图8　抵抗攻击结果图

Fig.8　Resistance attack results

图9　中间人攻击认证结果图

Fig.9　Authentication results of man in the middle attack

4　结论

针对现有电网终端设备的认证通信安全问题,本文结合数字证书和SM2算法,设计了一种基于SM2的电力广域测量系统安全认证方案,并进行了安全分析。最后通过Java进行方案的仿真实验测试分析后,证明本文的方案在抵抗中间人攻击、重放攻击等攻击手段方面的优势。

参考文献

[1] 张闻勤，江千军，李武龙. 新能源电力系统振荡问题的广域协调控制方法[J]. 电气传动，2019，49(12)：71-76.
ZHANG Wenqin，JIANG Qianjun，LI Wulong. Wide-area coordinated control method for oscillations in renewable power systems[J]. Electric Drive，2019，49 (12)：71-76.

[2] FAROOQ S M，HUSSAIN S M S，KIRAN S，et al. Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5[J]. Electronics，2018，7(12)：1-13.

[3] VARAN M，AKGUL A，KURUGOLLU F，et al. A novel security methodology for smart grids：a case study of microcomputer-based encryption for pmu devices[J]. Complexity，2021(6)：1-15.

[4] HUSSAIN S M S，FAROOQ S M，USTUN T S. A security mechanism for IEEE C37. 118.2 PMU communication[J]. IEEE Transactions on Industrial Electronics，2021，69 (1)：1053-1061.

[5] 骆钊，谢吉华，顾伟，等. 基于SM2密码体系的电网信息安全支撑平台开发[J]. 电力系统自动化，2014，38(6)：68-74.
LUO Zhao，XIE Jihua，GU Wei，et al. SM2-cryptosystem based information security supporting platform in power grid[J]. Automation of Electric Power Systems，2014，38(6)：68-74.

[6] 骆钊，严童，谢吉华，等. SM2加密体系在智能变电站远动通信中的应用[J]. 电力系统自动化，2016，40(19)：127-133.
LUO Zhao，YAN Tong，XIE Jihua，et al. Application of SM2 encrypted system in telecontrol communication for smart substation[J]. Automation of Electric Power Systems，2016，40(19)：127-133.

[7] KHAN R，MCLAUGHLIN K，LAVERTY D，et al. Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid[J]. IEEE Access，2017，5：11626-11644.

[8] 贾冀芳，张立新，廖明耀. 基于OpenSSL的SM2与RSA自动切换算法的设计[J]. 计算机工程与应用，2018，54(3)：74-81.
JIA Jifang，ZHANG Lixin，LIAO Mingyao. Design of automatic switching algorithm between SM2 and RSA based on OpenSSL [J]. Computer Engineering and Applications，2018，54 (3)：74-81.

[9] LI W，LI R，WU K，et al. Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications[J]. IEEE Access，2018，6：71194-71207.

[10] 吕良，李瑞. 基于数字签名和SM2算法的终端接入认证协商协议[J]. 计算机与数字工程，2021，49(3)：530-535.
LÜ Liang，LI Rui. Terminal access authentication negotiation protocol based on digital signature and SM2 algorithm[J]. Computer & Digital Engineering，2021，49 (3)：530-535.

[11] WU K，CHENG R，CUI W，et al. A lightweight SM2-based security authentication scheme for smart grids[J]. Alexandria Engineering Journal，2021，60(1)：435-446.

收稿日期：2022-06-02
修改稿日期：2022-06-30