Journal of Electric Power Science and Technology

Volume 37 | Issue 4 Article 21

9-23-2022

Security authentication scheme for power terminals based on the SM9 threshold signature

Yuan La
China Southern Power Grid Co.,Ltd., Guangzhou 510530 ,China

Jiguang Zhao
China Southern Power Grid Digital Grid Research Institute Co., Ltd.,Guangzhou 510633 ,China

Wei Zhang
China Southern Power Grid Digital Grid Research Institute Co., Ltd.,Guangzhou 510633 ,China

Recommended Citation

La, Yuan; Zhao, Jiguang; and Zhang, Wei (2022) "Security authentication scheme for power terminals based on the SM9 threshold signature," *Journal of Electric Power Science and Technology*: Vol. 37: Iss. 4, Article 21.
DOI: 10.19781/j.issn.1673-9140.2022.04.021
Available at: https://jepst.researchcommons.org/journal/vol37/iss4/21

基于 SM9 门限签名的电力终端安全认证方案

喇 元[1],赵继光[2],张 伟[2]

(1. 中国南方电网有限责任公司,广东 广州 510623;2. 南方电网数字电网研究院有限公司,广东 广州 510633)

摘 要:考虑智能电网场景下海量电力终端的安全认证需求,针对密钥在电力终端安全便捷的存储、使用问题,提出基于 SM9 门限签名的电力终端安全认证方案。首先,将无证书标识密码技术应用于电力终端,以解决原有的 PKI 防护体系中证书管理复杂等缺陷;其次,结合门限密码学的思想,对标准的 SM9 数字签名算法进行改进,将 SM9 私钥进行分割、存储,并在电力终端使用私钥签名过程中,采用电力终端与服务端交互计算后合成签名的方法,再以此方法为基础构建电力终端的安全认证方案;最后,经详细理论推导和分析证明方案的正确性和安全性,并通过实验算例验证方案的有效性。

关 键 词:智能电网;电力终端;SM9 算法;门限签名;安全认证

DOI:10.19781/j.issn.1673-9140.2022.04.021 **中图分类号**:TM76 **文章编号**:1673-9140(2022)04-0183-06

Security authentication scheme for power terminals based on the SM9 threshold signature

LA Yuan[1], ZHAO Jiguang[2], ZHANG Wei[2]

(1. China Southern Power Grid Co., Ltd., Guangzhou 510530, China; 2. China Southern Power Grid Digital Grid Research Institute Co., Ltd., Guangzhou 510633, China)

Abstract: Considering the security authentication requirements due to the massive power terminals in the smart grid scenario, the problem of safe and convenient storage and use of keys in power terminals is studied, and a power terminal security authentication scheme is proposed based on SM9 threshold signature. First of all, the certificateless identity-based cryptographic technology is applied to the power terminal and it can solve the defect that certificate management in the original PKI protection system is relatively complex. Then, the threshold cryptography is introduced to improve the standard SM9 digital signature algorithm. The SM9 private key is split and then stored separately. When using the private key signature, a synthesizing signature is generated via an interactive calculation between the power terminal and the server. Based on this algorithm, a power terminal security authentication scheme is proposed. Finally, an example is analyzed to verify the correctness and security of the scheme.

Key words: smart grid; power terminal; SM9 algorithm; threshold signature; security authentication

智能电网是新一代电网的智能化,通过先进的传感、信息通信和自动控制技术,实现“发—输—变—配—用”以及信息、通信、跨环节电力系统的高度自动化、互动化和信息化[1-2]。随着智能电网建设

收稿日期:2020-02-25;**修回日期**:2020-06-08

基金项目:国家重点研发计划(2018YFB0904905);中国南方电网有限责任公司科技项目(ZBKJXM20180347)

通信作者:喇 元(1980-),男,硕士,高级工程师,主要从事电力信息化、信息安全等方面的研究;E-mail:spring_bold_168@163.com

的逐步推进,出现了海量电力终端设备[3],其数量庞大、种类繁多、分布广泛、通信手段多种多样,这些特点给智能电网信息安全防护带来了新的挑战,如何鉴别海量终端泛在接入和广泛互联过程中的身份,建立安全稳定的电力终端与服务端、电力终端与电力终端之间的交互认证和信任机制成为亟待解决的问题[4]。

为了解决电力终端的安全认证问题,各种密码算法和密码模块被应用到电力终端中。文献[5]提出了电力终端采用国产 SM2 密码体系的 SD 卡安全接入方案;文献[6]设计了一种配电终端设备安全加密模块,以此来实现对主站和终端的身份鉴别;文献[7]提出了利用椭圆曲线密码算法(elliptic curves cryptography,ECC)产生动态密钥来保证电力终端与电力专网之间信息的传输。但以上文献均需要电力终端集成密码芯片(密码硬件模块),且均基于 PKI 体系实现。文献[8]描述了电力终端安全芯片存在的不足,指出需通过软硬件结合方式构建轻量级的验签体系,实现电力终端分布式授权和高速安全接入认证。

为此,本文提出基于 SM9 门限签名的电力终端安全认证方案。基于 IBC 的标识密码体系(SM9 算法)不需要证书,终端的标识即为公钥,更适用于海量电力终端的认证,SM9 门限签名方案采用分割存储和使用私钥的方法,不依赖电力终端设备中安全芯片的支持,可以密码软件模块的形式应用于电力终端。

1 电力终端安全分析

1.1 电力终端信息安全现状

目前,中国电网接入的终端设备超过 5 亿只,规划到 2030 年,接入电网系统的各类保护、采集、控制终端设备数量将达到 20 亿台,届时整个电网将是接入终端设备最大的物联网生态圈。与此同时,电力终端的信息安全问题也越发突出,电力终端作为电力系统信息的采集者、被访问者和传输者,如何鉴别电力终端的身份、保证数据传输过程中的机密性和完整性等安全防护问题急需解决[9-10]。

现有的电力系统中多采用以 PKI 体系为主体的电力终端安全防护方案[11]。随着物联网和 5G 技术的发展和万物互联时代的来临,现有的 PKI 体系在面对智能电网海量终端接入的需求上面临着新的挑战,一方面,PKI 体系证书管理复杂,证书查找、更新、撤销等操作占用了较大的存储开销和计算量,且 PKI 体系的安全性高度依赖于证书服务机构(certificate authority,CA),存在着虚假证书、单点故障等问题。智能电网环境下电力各种终端设备种类繁多,且其数量持续增长,如果使用 PKI 体系保障其信息安全性,则对于数字证书的生成和管理成本以及在数字证书应用中的通信和计算成本将是巨大的。

1.2 IBC 技术的应用

1984 年 Shamir 开创性的提出了基于标识的公钥密码体系(identity based cryptography,IBC)的概念。在 IBC 体系中,用户的私钥由密钥生成中心(key generation center,KGC)根据主密钥和用户标识计算得出,用户的公钥由用户的标识确定。

基于标识的 IBC 密码体系可有效地解决 PKI 体系中数字证书管理的难题,它通过用户的身份标识用以生成用户的公私钥对,无需数字证书绑定。在 IBC 标识密码中,通信的双方能够根据彼此身份 ID 计算出对方的公钥,因而降低了密钥交换和密钥管理的复杂程度,利用 IBC 标识密码的数字签名和加密算法,可以方便地为智能电网电力终端提供身份认证、数据传输机密性等安全防护。

尽管 IBC 体系相对于 PKI 体系具有众多优势,但 IBC 密钥在电力终端安全便捷的存储和使用是 IBC 体系安全运行的关键,现有的安全方式多采用把密钥存储在电力终端安全芯片中,或把密钥以软件的形式存储在电力终端的内存中。智能电网环境下由于电力终端的类型广泛且接口不一,众多的电力终端没有预留安全芯片的接口,而把密钥直接存储在电力终端内存中的方式被攻击者破解的几率很大,安全风险较高。如何在电力终端中安全便捷的存储和使用 IBC 密钥成为本方案要解决的问题。

2 相关知识

2.1 SM 系列国密算法

为了实现中国密码算法的自主可控,国家密码

管理局制定了一系列密码算法标准,包括 SM1、SM2、SM3、SM4、SM7 和 SM9 等。其中,SM1、SM4 和 SM7 算法为对称算法,且 SM1、SM7 算法不公开,使用该算法需要调用专有的密码芯片接口;SM3 为密码杂凑算法,主要用于数字签名和数据完整性保护等;SM2、SM9 为非对称算法;SM2 为椭圆曲线公钥密钥算法;SM9 是一种基于双线性对的标识密码算法。

国密 SM 系列算法在电力系统中得到了广泛的应用,基于 SM2/SM3/SM9 算法替换了国际 RSA/SHA1 算法,建立了电力系统密码应用防护体系和电力专用安全防护装置,实现电力设备的身份鉴别和数据完整性保护[12-14];对电力主站和终端之间、智能电表和计量模块等的业务数据采用 SM1/SM4 进行加解密操作,保证了业务数据的安全性。

2.2　SM9 数字签名算法

SM9 算法是中国采用的一种 IBC 标识密码标准,是中国自主设计、具有独特优势的安全高效密码算法,2018 年中国 SM9 算法正式成为 ISO/IEC 国际标准。SM9 算法的公开参数包括 $(cid, N, k, P_1, P_2, eid)$,其中,$cid$ 是曲线识别符,N 是循环群 G_1、G_2 和 G_T 的阶,k 是曲线 $E(F_q)$ 相对于 N 的嵌入次数,P_1、P_2 分别是 G_1、G_2 的生成元,eid 是双线性对 e 的识别符。

SM9 标准签名算法[15]包含密钥的产生、数字签名的生成和签名验证。

1)密钥产生。SM9 标识签名算法中用户的私钥由密钥生成中心 KGC 通过主私钥和用户的标识结合产生。KGC 产生随机数 $ks \in [1, N-1]$ 作为主私钥,计算 G_1 中的元素 $P_{pub\text{-}s} = [ks]P_2$ 作为签名主公钥,则主密钥对为 $(P_{pub\text{-}s}, ks)$,KGC 保存 ks,公开 $P_{pub\text{-}s}$。

用户 A 的标识为 ID_A,为产生用户 A 的签名私钥 d_A,首先,KGC 选择并公开用一个字节表示的私钥生成函数识别符 hid,并在有限域 F_N 上计算 $t_1 = H_1(ID_A \,||\, hid, N) + ks$,再计算 $t_2 = ks \cdot t_1^{-1}$;最后,计算 $d_A = [t_2]P_1$,即用户 A 的密钥对为 (ID_A, d_A)。

2)数字签名生成。设待签名消息为 M,作为签名者的用户 A 对其进行数字签名的过程:首先,计算群 G_T 中的元素 $g = e(P_1, P_{pub\text{-}s})$,并选取随机数 $r \in [1, N-1]$,计算群 G_T 中的元素 $w = g^r$;然后,计算整数 $h = H_2(M \,||\, w, N)$,再计算整数 $L = (r-h) \bmod N$;最后,计算群 G_T 中的元素 $s = [L]d_A$,得到消息 M 的签名为 (h, s)。

3)签名验证。作为验证者的用户 B 对收到的消息 M 和签名 (h, s) 验证,其签名验证过程:首先,检验 $h \in [1, N-1]$、$s \in G_1$ 是否成立,若成立则按顺序计算 $g = e(P_1, P_{pub\text{-}s})$、$t = g^h$、$h_1 = H_1(ID_A \,||\, hid, N)$;然后,按顺序计算 $P = [h_1]P_2 + P_{pub\text{-}s}$、$u = e(s, P)$、$w' = u \cdot t$;最后,计算 $h_2 = H_2(M \,||\, w', N)$,验证 $h_2 = h$ 是否成立,若成立则签名验证通过。

2.3　门限密码学

秘密共享是一种将秘密进行分割存储的密码技术,其主要思想是秘密持有者将秘密 S 分为 n 个子秘密并分发给持有者,其中,任意多于 t 个持有者可以恢复出秘密,t 个或少于 t 个持有者则不能得到原秘密的任何信息,此方案被称为(t, n)秘密分享方案。

门限密码学是在秘密分享方案的基础上构建而来,是指采用秘密分享技术将标准的密码算法运算(数字签名或解密运算等)分布于一定数量的参与者集合中,只有有效的参与者子集进行联合,才能得到正确的数字签名或解密结果,而不合法的参与者子集则无法通过伪造参数得到正确的数字签名或解密结果。

3　电子终端安全认证方案

3.1　设计思路

本文利用门限密码学的思想,对标准的 SM9 算法进行改进,将 SM9 私钥分割成 2 份,一份存储在电力终端,一份存储在电力终端所在的服务端,设计适用于智能电网电力终端 SM9 算法的(2,2)门限签名方案。

电力终端安全认证的参与方包括电力终端、电力终端所在的服务端以及服务端密钥中心 KGC,基于 SM9 门限签名的电力终端安全认证设计思路如图 1 所示。

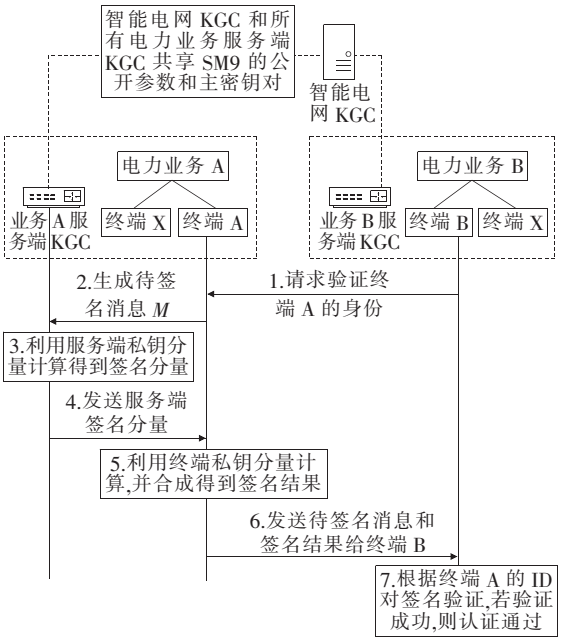

图 1 基于 SM9 门限签名的电力终端安全认证设计思路

Figure 1 Design of power terminal security authentication based on SM9 threshold signature

3.2 电力终端设备注册

电力终端 A 若要接入智能电网中的某业务,则需将该电力终端的 ID_A 等信息提交给该业务的服务端密钥中心 KGC。KGC 选择并公开用一个字节表示的私钥生成函数识别符 hid ,然后,KGC 在有限域 F_N 上计算 $t_1=H_1(ID_A||hid,N)+ks$ 、$t_2=ks\cdot t_1^{-1}$。KGC 系统生成随机数 a ,计算私钥分量 $d_t=[a]P_1$、$d_s=a^{-1}\cdot t_2 \bmod N$ 。KGC 将 d_t 发送给电力终端,电力终端存储 d_t 并作为电力终端私钥分量;KGC 将 d_s 发送给电力终端所在的服务端,服务端存储 d_s 并作为服务端私钥分量。

3.3 安全认证

假设智能电网下不同业务的电力终端 A、B 之间建立通信进行认证,电力终端 B 对 A 的认证过程如下。

1)电力终端 A 生成签名消息。电力终端 A 随机生成待签名消息 M。

2)电力终端 A 生成签名分量。电力终端 A 计算群 G_T 中的元素 $g=e(P_1,P_{pub})$,然后生成随机数 $r_1\in[1,N-1]$,计算 $w_1=g^{r_1}$,并将 w_1 发送给电力终端所在的服务端。

3)电力终端 A 所在的服务端生成签名分量。首先,服务端计算群 G_T 中的元素 $g=e(P_1,P_{pub})$;然后,生成随机数 $r_2,r_3\in[1,N-1]$,按顺序计算 $w_2=g^{r_2}$ 、$w_3=w_1^{r_3}$ 、$w'=w_2\cdot w_{22}$ 、$h'=H_2(M||w',N)$;最后,服务端利用持有的私钥分量 d_s 计算 $s_2=d_s\cdot r_3$ 、$s_{22}=d_s\cdot(r_2-h)$,并将 h' 、s_2 和 s_{22} 发送给电力终端 A。

4)电力终端 A 合成门限签名结果。首先,电力终端 A 利用持有的私钥分量 d_t 计算 $s'=[r_1\cdot s_2+s_{22}]\cdot d_t$,然后,电力终端 A 得到消息 M 的签名 (h',s') 。

5)电力终端 B 对 A 认证。电力终端 A 将签名消息 M 和签名数据 (h',s') 发送给电力终端 B,电力终端 B 采用文 2.1 中的签名验证方法对 M 和 (h',s') 终端进行验证,若验证通过,则电力终端 B 对 A 的认证成功。

4 方案分析

4.1 正确性证明

电力终端门限签名方案的正确性证明过程如下:

1)由文 3.3 中 $w'=w_2\cdot w_{22}=g^{r_2}\cdot w_1^{r_3}=g^{r_2}\cdot(g^{r_1})^{r_3}=g^{r_1\cdot r_3+r_2}$,设 $r=r_1\cdot r_3+r_2$,则有 $w'=g^r$;w'值与文 2.2 标准签名中的 w 值一致;

2)由 $L=(r-h)\bmod N$、$d_t=[a]P_1$、$d_s=a^{-1}\cdot t_2 \bmod N$ 计算可得:$s'=[d_s\cdot L]\cdot d_t=[a\cdot a^{-1}\cdot t_2\cdot L]\cdot P_1=[t_2\cdot L]\cdot P_1=[L]\cdot d_A$,通过与文 2.2 中 SM9 标准签名比较,$s'$、$s$ 的计算结果一致。

4.2 安全性分析

本文利用门限密码算法的原理,把 SM9 算法的私钥 d 分割成私钥分量 d_t、d_s,d_t 存储在电力终端中,d_s 存储在电子终端服务端 KGC。由于攻击者获取服务端 KGC 的私钥分量 d_s 是困难的,即便攻击者获取了电力终端的私钥分量 d_t,也无法获得完整的私钥,从而保障了 SM9 算法私钥在电力终端安全便捷的存储,保障了电力终端使用 SM9 算法私钥签名过程中的安全性。

随机数的生成和使用对 SM9 的签名算法的安全性起着关键性的作用,本方案中电力终端和服务端分别产生随机数 r_1、r_2、r_3,其中,随机数 r_2、r_3 由服务端产生,有效防止了随机数攻击。

5　实验算例

在 Windows7 64 位操作系统的 keil、eclipse 开发平台下,选用一款支持嵌入式系统的电力终端,采用 c 和 java 语言对文中的认证方案进行验证。SM9 算法参数均使用 SM9 标识密码算法标准中推荐的值。

以某电力终端 A 为例,其 ID 的 16 进制为 0x456C6563 74726963 5F546572 6D696E61 6C5F416C 696365。电力终端 A 私钥 d 经门限分割成私钥分量 d_t、d_s,d_t 为 0x48629E98 90685A66 062684DB 46BEE3A9 F04E5502 C23F7AA9 6DC4C469 EBF5E533,0x5A35F8F6 11764616 C22985C6 95ACD52B 0C81C90B 4C37F2B7 FBDEC3F3 03297B6F;d_s 为 0x054B3C69 2C5891FB 42439397 E7422EAA 1766FE15 F2FF542B 08A4C153 D8D2B03F。

待签名消息 M 的值为 0x534D3920 54687265 73686F6C 6420416C 676F7269 74686D20 53636865 6D652066 6F722055 62697175 69746F75 7320506F 77657220 496F5420 5465726D 696E616C 20536563 75726974 79。

服务端生成的签名分量为 (h', s_2, s_{22}),其中,h' 为 0x9E3B983B 36AFE033 11110ED2 EC87E3D0 682122DC 066BE9E3 FFA6D1A7 398F6F27;s_2 为 0x01F4994C AF50EE8A 4DCAB590 F004A30F F7592F77 B52ABF85 BEC3636F 45B1C795 0C5EA673 A1B7048E C324A740 DBCE9B36 3B9FE73F 7C9C17DA C0883BAD C946E21F;s_{22} 为 0xFD49A73B EF4F2CA6 1F8244D4 EE824FAE 46412403 AC29FE11 0700B073 1EFD885E 8C9FF73F 242A8AEE DC6FDFDB 0556C44C 6A776ED1 B87F6001 95D1E15B CE50869E。

服务端将 (h', s_2, s_{22}) 的值发送给电力终端 A,A 的软件密码模块经计算合成后得到最终的签名结果 (h', s'),其中,s' 为 0x20619CEF 2611F592 77D54640 4AD49513 700ECE56 6513B1E6 79667577 5BA1CE4E 4E3D3855 5D1A18AB F229F28F F9784FBD 24DB768D 689A19FB A903E958 F8316B67。

电力终端 B 利用 A 的 ID 对电力终端 A 的待签名消息 M 和签名结果 (h', s') 进行验证,得到 h_2 为 0x9E3B983B 36AFE033 11110ED2 EC87E3D0 682122DC 066BE9E3 FFA6D1A7 398F6F27。通过比较,h_2 与 h' 一致,验证通过,即电力终端 B 对 A 的认证成功。基于 SM9 门限签名的电力终端认证算例验证过程如图 2 所示。

基于 SM9 门限签名的电力终端安全认证流程如下:
第 1 步　电力终端 A 注册。
A 的 ID 为 456C6563　74726963　5F546572　6D696E61　6C5F416C　696365
电力终端 A 私钥经门限分割成私钥分量 *d_t* 和 *d_s*
d_t 为 48629E98　90685A66　062684DB　46BEE3A9　F04E5502　C23F7AA9　6DC4C469　EBF5E533
5A35F8F6　11764616　C22985C6　95ACD52B　0C81C90B　4C36F2B7　FBDEC3F3　03297B6F
d_s 为 054B3C69　2C5891FB　42439397　E7422EAA　1766FE15　F2FF542B　08A4C153　D8D2B03F
第 2 步　电力终端 A 生成门限签名。
待签名消息 *M*:534D3920　54687265　73686F6C　6420416C　676F7269　74686D20　53636865　6D652066　6F722055
62697175　69746F75　7320506F　77657220　496F5420　5465726D　696E616C　20536563　75726974　79
服务端生成签名分量(h', s_2, s_{22}),其中
h'为 9E3B983B　36AFE033　11110ED2　EC87E3D0　682122DC　066BE9E3　FFA6D1A7　398F6F27
s_2为 01F4994C　AF50EE8A　4DCAB590　F004A30F　F7592F77　B52ABF85　BEC3636F　45B1C795
0C5EA673　A1B7048E　C324A740　DBCE9B36　3B9FE73F　7C9C17DA　C0883BAD　C946E21F
s_{22}为 FD49A73B　EF4F2CA6　1F8244D4　EE824FAE　46412403　AC29FE11　0700B073　1EFD885E
8C9FF73F　242A8AEE　DC6FDFDB　0556C44C　6A776ED1　B87F6001　95D1E15B　CE50869E
服务端将签名分量(h', s_2, s_{22})发送给电力终端 A,A 经门限合成得到签名结果(h', s'),其中,
s'为 20619CEF　2611F592　77D54640　4AD49513　700ECE56　6513B1E6　79667577　5BA1CE4E
4E3D3855　5D1A18AB　F229F28F　F9784FBD　24DB768D　689A19FB　A903E958　F8316B67
第 3 步　电力终端 B 对 A 的签名值进行验证。
电力终端 B 根据 A 的 ID 对签名消息 *M*、签名结果(h', s')进行验证,得到
h_2为 9E3B983B　36AFE033　11110ED2　EC87E3D0　682122DC　066BE9E3　FFA6D1A7　398F6F27
经过比较,h_2与 h'一致,电力终端 B 对 A 的认证通过!

图 2　基于 SM9 门限签名的电力终端认证实验算例

Figure 2　Simulation of SM9 threshold signature verification for power terminals

6 结语

本文分析了智能电网环境下电力终端面临的信息安全问题，指出 IBC 标识密码体系比 PKI 体系更适用于智能电网场景下海量终端的安全认证。对于 SM9 算法私钥在电力终端安全便捷的存储和使用问题，本文结合门限密码学的思想提出了对 SM9 私钥进行分割，以此为基础构建了基于 SM9 门限签名的电力终端安全认证方案，方案不依赖于电力终端安全芯片的支持，可以密码软件模块的方式集成于电力终端中，解决了在安全便捷的前提下电力终端安全接入和终端的身份鉴别和认证问题。最后，通过论证和实验算例验证了方案的正确性和可行性。

参考文献：

[1] 冷喜武，陈国平，白静洁，等. 智能电网监控运行大数据分析系统总体设计[J]. 电力系统自动化，2018，42(12)：160-166.
LENG Xiwu，CHEN Guoping，BAI Jingjie，et al. General design of smart grid monitoring operation big data analysis system[J]. Automation of Electric Power Systems，2018，42 (12)：160-166.

[2] 王宏，闫园，文福拴，等. 国内外综合能源系统标准现状与展望[J]. 电力科学与技术学报，2019，34(3)：3-12.
WANG Hong，YAN Yuan，WEN Fushuan，et al. Standards associated with integrated energy systems：current situation and research prospects[J]. Journal of Electric Power Science and Technology，2019，34(3)：3-12.

[3] 苗新，卜广全，宋璇坤，等. 采用约束映射机制的 IPv4 电力终端接入 IPv6 网络的方法[J]. 电力系统自动化，2018，42(23)：168-173.
MIAO Xin，BU Guangquan，SONG Xuankun，et al. Access method of IPv4 electric power terminal to IPv6 network with constraint mapping mechanism[J]. Automation of Electric Power Systems，2018，42(23)：168-173.

[4] 赵兵，翟峰，李涛永，等. 适用于智能电表双向互动系统的安全通信协议[J]. 电力系统自动化，2016，40(17)：93-98.
ZHAO Bing，ZHAI Feng，LI Taoyong，et al. Secure communication protocol for smart meter bidirectional interaction system[J]. Automation of Electric Power Systems，2016，40 (17)：93-98.

[5] 王志贺，骆钊，谢吉华，等. 基于 SM2 密码体系的 SD 卡的电力移动终端安全接入方案[J]. 中国电力，2015，48(5)：75-80.
WANG Zhihe，LUO Zhao，XIE Jihua，et al. Secure access of electric power mobile terminal using SM2-crypto-system-based SD card[J]. Electric Power，2015，48(5)：75-80.

[6] 左高，方金国，向驰，等. 配电自动化终端设备中信息安全加密模块设计[J]. 电力系统自动化，2016，40(19)：134-138.
ZUO Gao，FANG Jinguo，XIANG Chi，et al. Design of information security encryption module for remote terminal units in distribution automation[J]. Automation of Electric PowerSystems，2016，40(19)：134-138.

[7] 杨传凯，菅永峰，任双赞，等. 基于改进认证协议的电力 LTE 专网安全接入技术[J]. 电测与仪表，2019，56(3)：91-96＋102.
YANG Chuankai，JIAN Yongfeng，REN Shuangzan，et al. Power LTE network security access technology based on improved authentication protocol[J]. Electric Measurement & Instrumentation，2019，56 (3)：91-96＋102.

[8] 张涛，赵东艳，薛峰，等. 电力系统智能终端信息安全防护技术研究框架[J]. 电力系统自动化，2019，43(19)：1-8＋67.
ZHANG Tao，ZHAO Dongyan，XUE Feng，et al. Research framework of cyber-security protection technologies for smart terminals in power systems[J]. Automation of Electric Power Systems，2019，43(19)：1-8＋67.

[9] 彭道刚，卫涛，姚峻，等. 能源互联网环境下分布式能源站的信息安全防护[J]. 中国电力，2019，52(10)：11-17＋25.
PENG Daogang，WEI Tao，YAO Jun，et al. Information security protection of distributed energy stations under the environment of energy internet[J]. Electric Power，2019，52 (10)：11-17＋25.

[10] 钟志琛，尚方，刘生. 新一代信息安全防护体系架构研究[J]. 中国电力，2016，49(S1)：16-20.
ZHONG Zhichen，SHANG Fang，LIU Sheng. Study on architecture of a new generation of intelligent trusted information security system[J]. Electric Power，2016，49 (S1)：16-20.

（下转第 226 页 Continued on page 226）