Journal of Electric Power Science and Technology

Volume 35 | Issue 3 Article 23

9-14-2020

# Cyber security protection and hardware acceleration of distribution automation system based on autonomous security chip

Weidong NI
*Foshan Power Supply Company,Guangdong Power Grid Co , Ltd , Foshan 52800, China*

Lihui WU
*Foshan Power Supply Company,Guangdong Power Grid Co , Ltd , Foshan 52800, China*

Junfeng WANG
*Foshan Power Supply Company,Guangdong Power Grid Co , Ltd , Foshan 52800, China*



Recommended Citation
NI, Weidong; WU, Lihui; and WANG, Junfeng (2020) "Cyber security protection and hardware acceleration of distribution automation system based on autonomous security chip," *Journal of Electric Power Science and Technology*: Vol. 35: Iss. 3, Article 23.
DOI: 10.19781/j.issn.16739140.2020.03.023
Available at: https://jepst.researchcommons.org/journal/vol35/iss3/23

# 基于自主安全芯片的配网自动化系统网络安全防护及硬件加速

倪伟东，武利会，王俊丰

（广东电网有限公司佛山供电公司，广东 佛山 528000）

**摘　要**：针对配网自动化系统点多面广、分布广泛等特点，设计基于“网络层＋应用层”的双重防护方案，提出一种基于SM2、SM3、SM4国密算法与消息认证码组合的一次口令认证协议，实现配电主站与配电终端间双向身份鉴别及业务数据加密，确保通讯数据的完整性和机密性，解决配网自动化系统网络安全防护问题，一旦应用多核异构自主安全芯片进行硬件加速，将提高加密算法的运行速度和效率。

**关　键　词**：配网自动化；加密算法；双向身份鉴别；安全芯片；硬件加速

DOI：10.19781/j.issn.1673-9140.2020.03.023　**中图分类号**：TM764　**文章编号**：1673-9140(2020)03-0166-07

## Cyber security protection and hardware acceleration of distribution automation system based on autonomous security chip

NI Weidong, WU Lihui, WANG Junfeng

(Foshan Power Supply Company, Guangdong Power Grid Co., Ltd., Foshan 52800, China)

**Abstract**: According to the characteristics of distribution automation system, such as wide range of points and wide distribution, a dual protection scheme based on "network layer + application layer" is designed. A password authentication protocol based on the combination of SM2, SM3, SM4 national secret algorithm and message authentication code (MAC) one-time password authentication is proposed to realize two-way authentication and encryption of service data between distribution master station and distribution terminal. Therefore, this protocol ensures the integrity and confidentiality of communication data, solves the problem of network security protection of distribution automation system. Once the multi-core heterogeneous independent security chip is applied for hardware acceleration, the speed and efficiency of encryption algorithm will be improved.

**Key words**: Distribution network automation; encryption algorithm; bidirectional identity authentication; security chip; hardware acceleration

随着计算机、通信等信息技术的不断发展，电网安全面临的外部环境越来越恶劣，针对电网关键信息基础设施的攻击屡见不鲜，安全形势日趋严峻[1-2]。近年来，网络攻击手段更是层出不穷。2017

**收稿日期**：2019-05-05；**修回日期**：2019-10-09

**基金项目**：广东电网有限责任公司科技项目(GDKJXM20185496)

**通信作者**：王俊丰(1979-)，男，硕士，高级工程师，主要从事配电网管理研究；E-mail：528500_w@163.com

年全球爆发大规模"WannaCry"蠕虫勒索病毒感染软件事件，该软件攻击了 100 多个国家及地区近万台电脑，损失巨大。2019 年 3 月 7 日晚，委内瑞拉电力系统受到美国网络攻击，造成全国范围的大规模停电，在遭受严重损失的同时，也充分暴露出委内瑞拉的关键信息基础设施安全防护投入的不足。

电力系统具有通信数据量大、通信实时性要求高等特点，通信数据中包含电站所有关键信息，主站和配电终端之间数据交互的安全性非常重要。近年来，广大学者对电力二次系统安全防护领域做了大量研究[3-5]。针对海洋观测通信组网系统，文献[6]提出一种基于 AES、RSA 和 MAC 的一次性双向口令认证协议，利用 Hash 函数和 MAC 完成双向认证过程，虽然 AES 对称加密算法能够在一定程度上解决 RSA 非对称加密算法运行速度较慢的问题[7]，但在一次性双向口令认证协议中 RSA 算法还是存在消耗硬件资源较多的问题[8]。

随着计算机技术和密码技术的快速发展，传统基于 RSA 算法的密码体系不再能满足当前和未来网络安全要求。2011 年 7 月 1 日起，中国国家密码管理局明文规定今后使用公钥密码的信息系统需采用基于 SM2 算法的密码体系，SM2 算法除了比 RSA 算法有更高的安全性外，还具有不存在国外可利用后门的优点[9]。但相对于 RSA，SM2 算法的时间复杂度要高得多，这也是限制 SM2 算法在加密领域应用的一个主要原因。文献[10]分析了电网信息安全平台应用 SM2 算法存在的问题，提出了一个采用组件技术构建自行研制的安全加密通道的方案，使得安全平台能支持实现 SM2 算法；文献[11]针对现有的安全体系公钥算法大多采用 RSA 算法的问题，应用国产商用密码 SM2 密码体系，提出通信报文的安全传输问题的解决方案；文献[12]提出在电力二次保护设备嵌入式系统中运用 SM2 数字签名算法的方案，将国产安全加密算法体制应用于电力二次系统安全防护体系中，但并未考虑 SM2 算法时间复杂度高的问题；文献[13]提出在配电终端前增加加密模块装置，应用 SM2 加密算法来实现终端设备的安全防护改造，但增加加密模块提高了方案的成本，也提升了方案的不稳定性。

结合以上文献，该文研究基于自主安全芯片的配网自动化系统网络安全防护及硬件加速，提出一种基于 SM2、SM3、SM4 国密算法与消息认证码(message authentication code，MAC)组合的一次口令认证协议，来实现配电主站与配电终端之间的双向身份认证及交互数据的加密。针对各类非法攻击特点，对该文方案进行安全性分析，对比 AES 算法和 RSA 组合算法分析该文方案组合算法的优势。以硬件方式加密认证芯片，实现配网终端数据的加密认证，提高终端的防护水平，应用多核异构芯片架构进行硬件加速，提高混合加密算法的运行速度和效率。

## 1　配网自动化安全防护方案

### 1.1　配网自动化系统结构

配网自动化系统采用三层结构模型：感知层、网络层、应用层。如图 1 所示，配网自动化系统主站作为应用层，由生产控制大区和管理信息大区组成；网络层主要包括有线光纤网络、无线公网、无线专网 3 种类型；感知层中，前置机位于应用层的边界，用于接收配电终端采集的二遥数据和下发遥控指令等。

网络层通道的多样性，同时也给配网自动化系统带来多方面的安全结构型漏洞与威胁：系统交互数据易被窃听、系统交互报文易被篡改、配电主站和终端易被欺骗等。

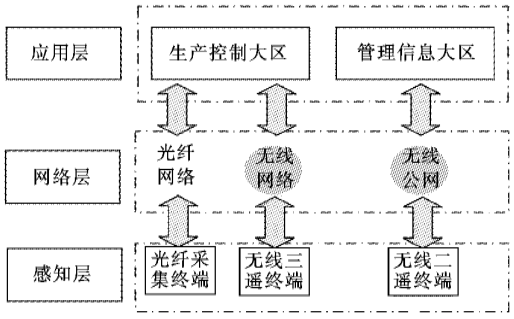


**图 1**　配网自动化系统三层架构

**Figure 1**　The diagram of three-layer distribution automation system

### 1.2　安全防护目标

配网自动化系统的快速发展，不可避免地会带来网络威胁多样化、点多面广等安全问题。配网自动化系统网络安全防护的目标是抵制恶意代码、黑客等各种形式对配电自动化系统发起的网络攻击和

恶意破坏，保障系统安全稳定运行。

### 1.3 双重安全防护方案设计

采用基于数字证书认证技术及国产商用密码算法的加密技术对配网自动化系统通信网络进行安全防护，配电自动化系统整体安全防护方案如图 2 所示。

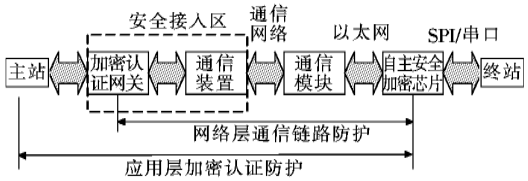


**图 2** 配网自动化系统安全防护方案

**Figure 2** Protection scheme of distribution automation system

在配网自动化系统中建立安全接入区，将安全接入区接入数据通信系统，实现对配电终端设备的数据过滤和安全接入控制；通过加密认证网关对感知层配电终端与应用层配电主站之间的通信数据进行签名，实现配电主站和配电终端设备之间的报文交互保护和双向身份鉴别；通过加密认证网关实现感知层终端的加密认证和访问控制，同时改造加密秘钥的更新机制和保存方式，保证通信数据的传输安全。

该文设计的‘网络层＋应用层’双重安全防护方案是通过在主站侧配置加密认证网关、终端侧配置加密芯片来共同实现的。在感知层配网终端中以硬件方式加密认证安全芯片，实现配网终端数据的加密认证，以软硬件协同设计方式实现所需的加解密算法。配电终端主控芯片将上行数据通过 SPI 或串口发送至安全芯片，安全芯片对上行数据签名并加密，并将签名加密后的数据通过网络口发送至主站，实现数据安全交互。

## 2 面向配网自动化系统的双向认证技术

### 2.1 应用层数据加密

通过应用层报文加解密实现主站终端双向加密认证，主站与终端数据交互流程如图 3 所示。数据交互流程：

第 1 步：主站向网关发起连接请求，请求与终端进行连接；

第 2 步：网关发起与终端之间的连接；

第 3 步：连接成功后，网关和终端之间建立安全通道；

第 4 步：网关将通道建立成功的结果返回给主站；

第 5 步：主站开始发起与终端的双向身份认证，采用基于 SM2、SM3、SM4 国密加密算法和 MAC 组合的一次口令认证协议进行双向身份认证；

第六步：认证成功，主站与终端之间开始进行业务交互。

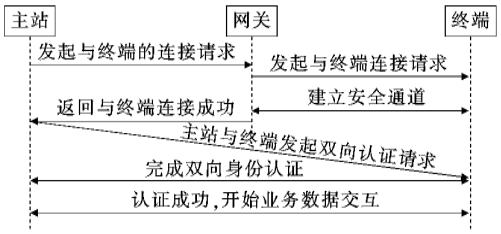


**图 3** 主站与终端数据交互流程

**Figure 3** Flow chart of data interaction between master station and terminal

### 2.2 基于 SM2、SM3、SM4 国密算法和 MAC 组合的双向认证技术

在终端和主站之间进行数据交互之前，需要进行双向身份认证。身份认证由主站发起，终端被动响应，一方对另一方认证失败，返回认证失败信息，不响应对方数据。首先需要通过注册阶段，具体请求和密钥产生过程如图 4 所示，流程中 $H(x)$ 表示 $x$ 的哈希值，$E(x)$ 表示用公钥(e,N)加密 $x$，$D(x)$ 表示用私钥(d,N)加密 $x$，$E_k(x)$ 表示用密钥 $E_k$ 加密 $x$。具体流程：

第 1 步：主站向配电终端发起连接请求；

第 2 步：配电终端通过 SM2 加密算法生成密钥对，包括公钥(e,N)和私钥(d,N)，发送公钥(e,N)至主站端；

第 3 步：主站采用国密 SM3 哈希算法计算主站 ID 口令信息的哈希值，即为 $H(PW_{MS})$，并使用公钥(e,N)加密哈希值 $H(PW_{MS})$，将 $E(H(PW_{MS}))$ 发送至主站端；

第 4 步：配电终端利用私钥(d,N)解密得到包含主站 ID 口令信息的哈希值 $H(PW_{MS})$，根据

$H(PW_{MS})$判断主站 ID 是否被重复记录，如果重复，则提示该 ID 已经被占用，并告知主站修改 ID 口令；如果不重复，则保存哈希值 $H(PW_{MS})$，并建立口令 ID 验证表，验证表包含主站的 ID 口令及其对应的哈希值；

第 5 步：终端返回注册成功。

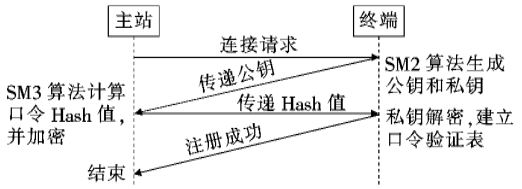


**图 4**　注册阶段流程

**Figure 4**　Flow chart of registration stage

注册成功后，主站和配电终端之间进行密钥协商和双向认证，如图 5 所示。完整流程：

第 1 步：主站端向配电终端发出验证请求，配电终端采用国密 SM4 算法产生密钥($E_k$)，同时产生一个随机数 $R_1$，并用公钥(e,N)加密密钥($E_k$)，最后发送加密密钥 $E(E_k)$和加密随机数 $E(R_1)$到配电终端；

第 2 步：配电终端使用终端私钥(d,N)进行解密，得到密钥($E_k$)和 $R_1$，并生成随机数 $R_2$，使用密钥($E_k$)加密 $R_1$ 和 $R_2$，发送密钥加密 $E(R_1)$和 $E(R_2)$到主站端；

第 3 步：主站端使用密钥($E_k$)解密得到 $R_2$，并验证 $R_1$ 是否一致。此时主站端调用密钥($E_k$)计算 Hash 值、$R_1$、$R_2$ 和主站 ID 口令 $ID_{MS}$ 的 MAC 值 $E_k(H(PW_{MS}),R_1,R_2,ID_{MS})$，并将主站 ID 口令与 MAC 值使用公钥(e,N)加密后，即将 $E(E_k(H(PW_{MS}),R_1,R_2,ID_{MS}))$发送到配电终端；

第 4 步：配电终端使用终端私钥(d,N)解密得到主站 ID 口令 $ID_{MS}$，根据 ID 查口令验证表得到 Hash 值 $H(PW_{MS})$，调用密钥($E_k$)计算 Hash 值、$R_1$、$R_2$ 和主站 ID 口令 MAC 值，并检验该值与主站端传过来的 MAC 值是否一致。如果一致，则配电终端认证主站成功，协议继续；若不一致，则验证失败，拒绝主站的认证请求；

第 5 步：配电终端调用密钥($E_k$)计算随机数 $R_1$、$R_2$ 和主站 ID 口令的 MAC 值，然后新的 MAC 值使用终端的私钥(d,N)进行加密后，即将 $D(E_k(H(PW_{MS}),R_1,R_2,ID_{MS})^*)$发送给主站端；

第 6 步：主站端使用公钥(e,N)解密得到新的 MAC 值，并调用密钥 $E_k$ 计算随机数 $R_1$、$R_2$ 和主站 ID 口令的 MAC 值 $E_k(H(PW_{MS}),R_1,R_2,ID_{MS})$，并检验 2 个值是否一致。如果一致，则主站端认证终端成功，协议完成；否则拒绝终端的认证请求。

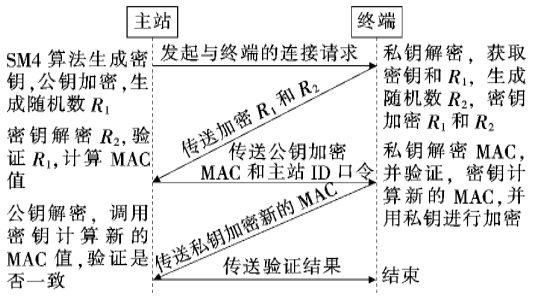


**图 5**　密钥协商和双向认证

**Figure 5**　Key agreement and bidirectional authentication

## 3　安全性分析

该文设计的组合加密算法能够防范重放攻击、数据泄密及伪造终端和主站身份等对配电主站系统的恶意攻击，其安全性分析如下。

### 3.1　重放攻击

由密钥协商和双向认证流程可知，每次计算和验证 MAC 时都引入了主站和配电终端选取的随机数 $R_1$ 和 $R_2$，即使传输数据被截取，在主站和终端选取的随机数不重复的情况下，计算的 MAC 值必不相同，故黑客截取数据进行重放攻击不可行。

### 3.2　数据泄露

在该文方案中，配网终端的口令验证表中仅包含主站 ID 口令对应的哈希值，并未储存密钥($E_k$)，故黑客即便通过未知数据泄漏渠道获得配网终端的口令验证表，在密钥保密的情况下，黑客也无法获得主站 ID 口令信息的 MAC 值。同时该密码体系使用国密 SM2 和 SM4 混合加密算法产生加密密钥，在主站和终端密钥协商过程中，加密数据每次只会被传送一次，即便部分加密数据被窃取，黑客也无法同时得到所有数据、随机数、密钥等，因此主站和终端之间数据交互的安全性能充分得到保证。

### 3.3　假冒终端

如果黑客想要假冒配电终端，需要得到密钥，并使用密钥计算随机数 $R_1$、$R_2$ 和主站 ID 口令的

MAC 值，但是主站和配电终端在密钥协商阶段各生成一次随机数，黑客也不可能同时获得密钥、公钥、私钥以及所有随机数，故黑客不可能通过假冒配电终端实现与主站之间的通信。

### 3.4 假冒主站

如果黑客想假冒主站，必须通过密钥计算随机数 $R_1$、$R_2$ 和 Hash 值、主站 ID 口令生成的 MAC 值来实现假冒，但全部计算数据被黑客窃取的可能性非常低，即使黑客能够窃取配电终端的口令验证表，并通过口令验证表获得主站 ID 对应的哈希值，在密钥和随机数均未知的情况下，也无法计算得到正确的 MAC 值。所以，黑客也不可能通过假冒主站实现与配电终端之间的通信。

## 4 自主安全芯片硬件加速

通过采用在终端装置中内嵌入自主安全芯片实现主站和配网终端之间的身份认证和数据加密，终端装置图和内嵌入自主安全芯片板件如图 6、7 所示。自主安全核基于支持国密标准算法的 IPSec 协议，由 MCU 与安全芯片(ESAM)组成，MCU 负责 IPSec 协议的处理及系统任务调度；ESAM 通过 SPI 接口与 MCU 连接，实现 SM2、SM3、SM4 国密算法、消息认证码 MAC 计算、证书解析等功能。

**图 6** 终端装置实物

**Figure 6** Physical illustration of terminal devices

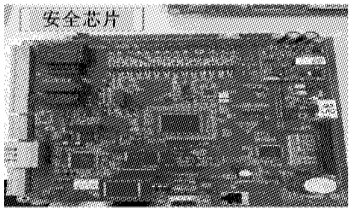


**图 7** 内嵌入自主安全芯片板件

**Figure 7** Illustration of embedded autonomous security chip board

### 4.1 系统设计

加密核通过 CPU 内部总线接口与应用核心相连，其硬件架构如图 8 所示，终端通过该安全核可实现功能：①调用安全芯片进行组合加密算法计算；②对 IPSec 安全芯片进行网络参数配置；③通过 IPSec 安全芯片进行网络数据转发处理等。

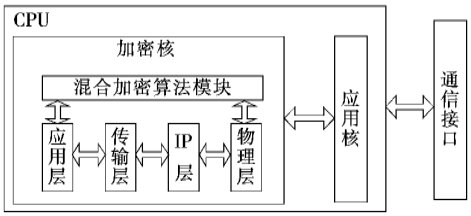


**图 8** 硬件架构

**Figure 8** Hardware architecture diagram

基于安全芯片的国密算法功能实现对嵌入式系统上可执行代码的完整性度量与验证，以及关键数据的加密保护。系统软件架构主要包括内核层、应用层、配置层几部分。内核层主要包括度量模块、管控模块和密码模块；应用层一方面负责与内核模块交互(如度量代理、事件通信等)，另一方面提供国密加密算法库和 MAC 计算算法；配置层给用户提供远程配置界面，包括日志管理、事件通知、系统配置等各个功能。软件架构如图 9 所示。其中，密码软件算法库为静态链接库，提供 SM2、SM3、SM4 等国密算法接口，如图 10 所示。SM2 公钥签名验签算法由密钥生成、数据签名、签名验证 3 个模块组成，签名验证模块验证签名，数据签名模块使用私钥对数据进行签名，密钥生成模块生成 SM2 公私钥对。SM3 哈希算法主要计算输入数据的哈希值。SM4 对称加密算法由加密模块、解密模块 2 个模块组成，加密模块实现对输入数据的加密，解密模块实现对输入数据的解密。

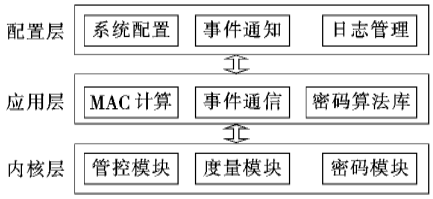


**图 9** 软件架构

**Figure 9** Software architecture diagram

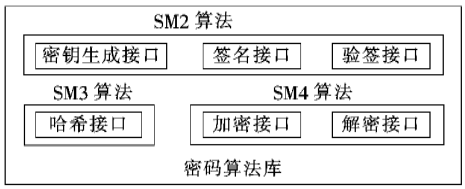


**图 10**　密码算法库

**Figure 10**　Cryptographic algorithm library

### 4.2　实验验证

将该文设计的混合国密算法与文献[7]采用的 RSA、MD5(信息摘要算法)、AES 与 MAC 组合加密算法进行比较，从对不同大小数据包加解密总的运行时间进行比较分析。安全芯片上应用设计的 hantan OS 全自主嵌入式操作系统，将混合国密算法和文献[7]已有混合加密算法应用于多核异构自主安全芯片上，主频设计为 100 MHz，对比在主频 100 MHz 单核 CPU 上应用混合国密算法运行数据，对比数据如表 1 所示。

**表 1**　混合加密算法总运行时间

**Table 1**　The total running time of hybrid encryption algorithms

| 结构 | 混合加密算法 | 运行时间/ms | | |
|---|---|---|---|---|
| | | 10 MB | 20 MB | 40 MB |
| 自主安全芯片 | 已有混合加密算法 | 262.4 | 432.4 | 765.6 |
| | 混合国密算法 | 236.3 | 372.1 | 656.2 |
| 单核 CPU | 混合国密算法 | 294.8 | 475.1 | 813.2 |

表 1 为已有混合加密算法和该文设计的混合国密算法对 10 MB、20 MB、40 MB 3 种大小数据包的加解密总运行时间，由表可以看出，2 种混合算法的加解密时间与数据包大小呈正相关；不管数据包有多大，SM2、SM3、SM4 和 MAC 组合的混合国密算法比文献[7]已有的混合加密算法在整个加解密过程中耗时更短，这说明该文设计的混合国密算法运行速度更快。对比国密算法在单核 CPU 和在多核自主安全芯片上加解密不同数据包总运行时间可以看出，多核异构的结构设计大大提升了算法的运行速度，速度提升约 25%。

基于国密混合算法和 RSA 、AES 混合加密算法在自主安全芯片和单核 CPU 上的实验验证表明：①使用 SM2 非对称国密算法对 SM4 对称国密算法产生的密钥进行加密，能够充分保证密钥的安全性，进而保障整体防护方案的安全性；②SM4 对称国密算法有极快的加解密速度，在该文设计的安全防护方案中，主体数据明文大部分采用的是 SM4 算法，SM2 算法仅被使用于对 SM4 算法生成的密钥这样数据量小的信息进行加解密，因此该文设计的国密混合算法加解密速度会更快；③多核异构的硬件设计能有效地提高算法的运行速度和效率。

## 5　结语

通信技术和网络技术在配网系统中的广泛应用，使得配网自动化系统数据交互更加便利，但同时也使得自身安全问题变得更加复杂和紧迫。该文设计基于配网自动化系统“网络层＋应用层”的双重防护方案，提出一种基于 SM2、SM3、SM4 国密算法与 MAC 组合的一次口令双向认证协议，实现主站与配电终端间的双向身份认证及数据加密，保证配网系统数据交互的安全性，双向认证协议能够抵抗所有已知非法攻击，防止配网系统遭受恶意破坏陷入瘫痪。应用多核异构进行硬件加速，保证配网自动化系统安全防护方案高速稳定运行。

**参考文献：**

[1] 池喜洋，竺炜，刘长富，等. 含大型风电场的电网安全经济优化调度[J]. 电力科学与技术学报，2018，33(1)：125-131.
CHI Xiyang，ZHU Wei，LIU Changfu，et al. Security and economic optimization dispatch for power grid integrating large-scale wind farm[J]. Journal of Electric Power Science and Technology，2018，33(1)：125-131.

[2] 曾鸣，刘英新，赵静，等. “云大物移智”与泛在电力物联网融合的安全风险分析及安全架构体系设计[J]. 智慧电力，2019，47(8)：25-31.
ZENG Ming，LIU Yingxin，ZHAO Jing，et al. Security risk analysis and security architecture design of widespread power internet of things with the use of cloud computing big data internet of things mobile internet and smart city technology[J]. Smart Power，2019，47(8)：25-31.

[3] 邹春明，郑志千，刘智勇，等. 电力二次安全防护技术在工业控制系统中的应用[J]. 电 网 技 术，2013，37(11)：

3227-3232.

ZOU Chunming, ZHENG Zhiqian, LIU Zhiyong, et al. Application of cyber security in industrial control systems based on security protection technology for electrical secondary system[J]. Power System Technology, 2013, 37(11): 3227-3232.

[4] 王保义,杨丽.基于安全网关的电力二次系统安全防护[J].电力系统通信,2008,29(19):28-32.

WANG Baoyi, YANG Li. Security protection of power secondary system based on security gateway[J]. Telecommunications for Electric Power System, 2008, 29(19): 28-32.

[5] 秦超,张涛,林为民.基于数字证书认证的电力安全拨号认证系统[J].电力系统自动化,2009,33(19):52-55.

QIN Chao, ZHANG Tao, LIN Weiming. A digital certificate authentication-based electric power safe dialing authentication system[J]. Automation of Electric Power Systems, 2009, 33(19): 52-55.

[6] 徐天亮,王晨旭,王新胜.海洋观测通信组网安全及其硬件加速研究[J].海洋科学,2018,42(1):15-20.

XU Tianliang, WANG Chenxu, WANG Xinsheng, et al. Research on safety and hardware acceleration of ocean observing communication networks[J]. Marine Sciences. 2018, 42(1): 15-20.

[7] Liu Z, Huang X Y, Hu Z, et al. On emerging family of elliptic curves to secure intemet of things: ECC comes of age[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(3): 237-248.

[8] Liu Z, Groszschaedl J, Hu Z, et al. Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things[J]. IEEE Transactions on Computers, 2017, 66(5): 773-785.

[9] Bai L, Zhang Y, Yang G. SM2 cryptographic algorithm based on discrete logarithm problem and prospect[C]// 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)), Yichang, China: IEEE, 2012.

[10] 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.

[11] 骆钊,谢吉华,顾伟,等.SM2 加密体系在智能变电站站内通信中的应用[J].电力系统自动化,2015,39(13):116-123.

LUO Zhao, XIE Jihua, GU Wei, et al. Application of SM2 encrypted system in smart substation inner communication[J]. Automation of Electric Power Systems, 2015, 39(13): 116-123.

[12] 陈闻卿,朱岩.SM2 数字签名算法在电力分界开关控制器中的研究与应用[J].电力科学与技术学报,2015,30(3):121-125.

CHEN Wenqing, ZHU Yan. Research and application of SM2 digital signature algorithm in power line switch controller[J]. Journal of Electric Power Science and Technology, 2015, 30(3): 121-125.

[13] 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 Power Systems, 2016, 40(19): 134-138.