

基于国密算法的高安全RFID技术在电力设备管理中的应用

雷振江¹, 刘颖², 李良³, 夏雨², 王峥³, 孙向荣⁴, 丁岳³

(1. 国网辽宁省电力有限公司, 辽宁 沈阳 110000; 2. 国网辽宁省电力有限公司信息通信分公司, 辽宁 沈阳 110000; 3. 北京智芯微电子科技有限公司(国家电网公司重点实验室、电力芯片设计分析实验室), 北京 100192; 4. 江苏安智博电子科技有限公司, 江苏 常熟 215500)

摘要: 根据电力设备资产全生命管理的数据安全需求, 提出采用SM7算法对电力设备资产管理系统进行信息安全防护。国密SM7算法是国家密码管理局专门为RFID电子标签设计的商用密码对称算法, 密钥长度为128 bit, 安全性能优于其他RFID算法。RFID电子标签认证过程采用3次数据传输的鉴别方法, 即“双向认证”或“三重认证”流程, RFID电子标签的SM7算法模块支持加密和解密功能, 在认证过程中采用SM7算法来完成认证数据的加解密以实现电力系统与电力设备间的认证。采用国密SM7算法对电力设备资产信息进行安全防护, 电力系统与电力设备的电子标签先通过双向认证, 并以密文形式对电子标签的电力设备信息进行读取, 提高电力设备资产信息的安全性。

关键词: 无源无线; UHF RFID; 国密算法;

Application of high security RFID asset management system based on national secret algorithms in power system

LEI Zhenjiang¹, LIU Ying², LI Liang³, XIA Yu², WANG Zheng³, SUN Xiangrong⁴, DING Yue³

(1. State Grid Liaoning Electric Power Co., . Ltd., Shenyang 110000, China; 2. State Grid Liaoning Electric Power Co., . Ltd. Information and Communication Branch, Shenyang 110000, China; 3. State Grid Key Laboratory of Power Industrial Chip Design and Analysis Technology, Beijing Smart-Chip Microelectronics Technology Co., Ltd. Beijing 100192, China; 4. Jiansu Anzhibo Electronic Technolgy Co., Ltd., Changshu 215500, China)

Abstract: According the requirements of data security related to power equipment asset management, SM7 algorithm for data security protection for power equipment asset management system is adopted. SM7 is a commercial cryptography of symmetric algorithm, certified by State Cryptography Administration, particularly designed for RFID. The key length of SM7 is 128 bit, and its performance of security is superior to other RFID algorithm. The identification approach of the RFID certification process is three times data transition, namely “mutual certification” or “triple certification”. In addition, RFID SM7 algorithm module is functioned of encryption and decryption, in order to implement the certification between power system and power equipment, the encryption and decryption of data certification are completed by adopting SM7 algorithm. The data security protection of power equipment asset with SM7 algorithm, is mutual certified at the outset and reads the cryptography data on the power equipment, which would distinctly enhance the data security of power equipment asset.

Key words: passive wireless; UHF RFID; national secret algorithms

0 引言

电力物联网架构简单但组成复杂,包含多领域技术、融合多种应用,涵盖极其复杂的各类设备^[1-2]。因此,电力物联网不仅面临传统信息和网络模式的安全问题,还存在感知层中射频识别等带来的新的安全问题。

1) 感知设备终端攻击。感知设备、智能终端或设备由于功能简单、资源匮乏(即存储空间小、计算能力弱和电能使用受限)及数量巨大,常常部署在无人监控或环境恶劣的区域,容易被入侵者实施直接的物理攻击,进而实施物理破坏、克隆伪造、信息窃取、软件篡改及远端控制等攻击。

2) 本地无线通信攻击。近距离无线通信逐渐广泛应用,感知设备等通常通过无线方式进行信息采集。针对无线通信的开放性,入侵者通过伪造、窃听和重放等方式实现对无线网络的攻击,如非法介入、DoS攻击和篡改数据包等。

3) 指令控制攻击。入侵者伪造控制指令控制感知设备或智能终端,使得终端进行非正当操作从而实施攻击。由于感知设备和智能终端结构简单、成本低廉,并且资源和能力受限,通常很难判定控制指令或数据包是否伪造或已被恶意篡改,攻击者因此可以通过伪造指令、配置等信息进行攻击^[3-7]。

射频识别技术是物联网感知层的核心技术。RFID(Radio Frequency Identification, RFID),即射频识别,又称为电子标签。RFID技术是一种非接触式的自动识别技术,可通过一定频段的无线电信号识别特定目标并读写相关数据。电子标签主要用于将各类待标识物体建立唯一的身份标识。RFID作为通信和物联网领域的新兴技术,在电力系统的输变电设备管理、用电信息采集、电动汽车运营、电力用户用电服务以及电力设备资产管理等领域得以广泛应用。

1 RFID技术

基于RFID技术的电力资产管理系统组

成原理图如图1所示。其中包括了电子标签(Transponder)、阅读器(Reader)、客户机(Client)和服务器(Server)等。对整个超高频RFID系统而言,电子标签与阅读器通过RF电磁场进行数据交换,其数据链路包含了数据的调制/解调制、编码/解码、防碰撞算法以及相关的协议标准等。超高频RFID技术的基本原理就是将RFID电子标签安装在被识别的物体上,当RFID电子标签进入RFID系统的阅读范围时,利用空间电磁耦合对无源超高频RFID标签通电,并完成信息收发通信,实现标签和阅读器之间的非接触式信息通信。标签向阅读器天线发送携带信息,阅读器接收这些信息并进行解码,通过串口RS 232或RS 485,将阅读器采集到的数据实时送入客户机的终端处理系统,并通过网络传输给服务器,从而完成信息的全部采集与处理过程,达到自动识别被标识物体的目的。

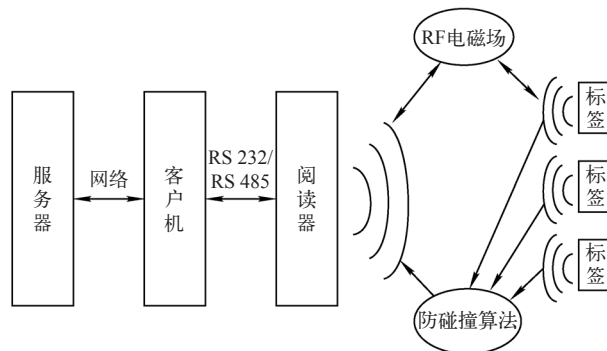


图1 RFID系统原理图

Fig. 1 Principle diagram of RFID system

2 双向身份认证技术

设备身份认证是保护系统安全的一个重要机制,鉴于本文中提供数据信息的RFID电子标签及传输数据的阅读器为对等的实体,RFID电子标签需要确保数据来源的可靠性,阅读器也需确保数据传向正确的对象。本文中的认证方式设计为双向认证,即RFID电子标签要验证阅读器的身份,阅读器也需验证RFID电子标签的身份。本文的双向身份认证由两次独立的单向身份认证构成。即A方先认证B方,然后B方再认证A方。

3 密码技术

密码技术是信息安全防护的重要手段之一，RFID系统采用密码算法对传输的数据进行加密。到目前为止，密码已经在诸多领域得到广泛使用。密码技术学科是结合电子通信、计算机科学和数学等多个学科于一身的交叉学科，它不仅具有确保信息机密性的信息加密功能，而且具有秘密分存、系统安全、身份验证和数字签名等功能。使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

国密算法SM1、SM2、SM3、SM4和SM7是国家密码局认可的加密算法，当芯片与外部进行数据交互时，为保证数据安全，通信过程中的数据都以密文形式传输。国密算法SM1、SM4是安全性较高的对称算法，对数据进行加密；国密算法SM2、SM3是非对称算法，用于数字签名；国密算法SM7为对称算法，对数据进行加密，多用在功耗要求比较高的设备。国密SM7算法适用于高安全RFID电力资产管理系统的信息安全防护。

4 基于国密算法的高安全RFID资产管理防护技术

以往的RFID电子标签和读写器不具备安全性，而带有国密SM7算法的RFID电子标签在和阅读器通信时，需要在双向认证成功后，才能进

行数据的传输，且传输时会对数据进行加密，形成密文传输。信息入侵者不能对RFID电子标签或RFID阅读器相关密文进行相关读写、创建、修改和删除等操作，从而保证数据的安全。

(1) RFID认证过程

带有国密SM7算法的RFID读写器在和RFID电子标签进行通信时首先要进行双向认证。认证时，RFID电子标签和读写器使用同样的国密算法SM7和相同的密钥，双方使用各自的随机数发生器，认证通过后无线基站才能访问RFID电子标签的安全数据区，双方通信的数据处于加密状态。大致流程如图2所示。

RFID电子标签和读写器认证流程分为如下步骤。

- 1) 阅读器发送获取安全参数的命令：Get_SecPara。
- 2) 标签发送安全参数，包括：安全模式、安全功能、密钥长度和密码算法等。
- 3) 阅读器用根密钥RK和TID生成鉴别密钥AK，根据安全参数中的安全功能，向电子标签发送请求鉴别命令：Req_SAuth。
- 4) 电子标签生成随机数 RN_t 发送给阅读器。
- 5) 阅读器生成随机数 RN_r 和会话密钥SK，使用AK加密 $RN_r||RN_t||SK$ 得到 $E_{AK}(RN_r||RN_t||SK)$ ，向标签发送双向鉴别命令。

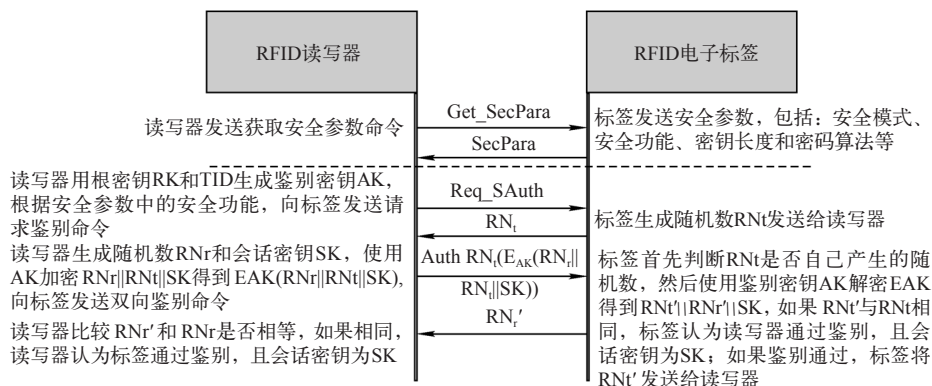


图2 基于国密SM7算法的RFID电子标签工作原理

Fig. 2 Working principle of RFID electronic label based on national secret SM7 algorithm

6) 标签首先判断 R_{Nt} 是否自己产生的随机数, 然后使用鉴别密钥 A_K 解密 $E_{AK}(R_{Nr}||R_{Nt}||SK)$ 得到 $R_{Nt}'||R_{Nr}'||SK$, 如果 R_{Nt}' 与 R_{Nt} 相同, 标签认为阅读器通过鉴别, 且会话密钥为 SK , 如果鉴别通过, 标签将 R_{Nr}' 发送给阅读器。

7) 阅读器比较 R_{Nr}' 和 R_{Nr} 是否相等, 如果相同, 阅读器认为标签通过鉴别, 且会话密钥为 SK 。

8) RFID标签在鉴别过程中出现任何错误, 标签不返回任何信息, 并回到仲裁状态, 等待下一轮选择和清点指令。鉴别过程为一条通信指令(分两次发送), 应根据鉴别流程一次完成。中间若被其他指令打断, 则认为鉴别失败。

认证过程中, SM7采用ECB模式实现加密和解密, 如图3所示。

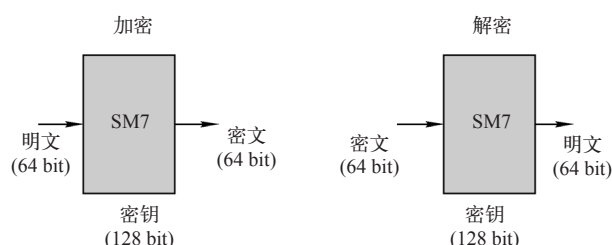


图3 RFID电子标签认证过程加解密原理

Fig. 3 The encryption and decryption principle of RFID electronic label authentication process

(2) RFID电子标签信息加密

阅读器和RFID电子标签的双向鉴别通过后, RFID电子标签只响应盘点组命令和安全通信命令。安全通信协议流程如图4所示。

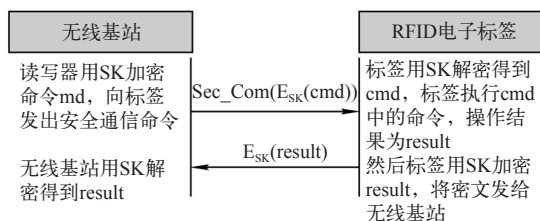


图4 安全通信协议

Fig. 4 Secure communication protocol

阅读器和RFID电子标签双向鉴别通过后, 安全通信流程如下。

1) 阅读器生成随机数 R_{Nr} , 用 SK 加密

cmd , 发送安全通信命令 $Sec_Com(ESK(cmd))$ 。

2) 标签用 SK 解密 $ESK(cmd)$ 得到 cmd , 标签执行 cmd 中的命令, 操作结果为 $result$; 然后标签用 SK 加密 $result$ 得到 $ESK(result)$ 发送给阅读器。

3) 阅读器用 SK 解密得到 $result$ 。

4) 阅读器和RFID电子标签的“鉴别”是双向认证的过程, 加密的主要原理是通过国密SM7算法对比读写器和RFID电子标签相互发送的指令及返回值, 即: 通过发送鉴别指令, 产生随机数; 然后, 将随机数与根密钥进行或运算, 传递给标签, 在标签一侧进行解密, 比对随机数是否一致, 来判定鉴别成功与否。

认证通过后, RFID电子标签处于安全状态, 电子标签的和阅读器之间的所有通信(包括读写命令参数及数据)采用流加密方式传输。加解密的初始密码采用认证流程第三部数据作为IV进行加解密后产生, 后续密钥采用SM7算法的OFB模式产生。

5 高安全RFID资产管理系统设计

RFID手持终端在和RFID电子标签进行通信时首先要进行双向认证。认证时, RFID电子标签和手持终端使用同样的国密算法SM7和相同的密钥(KEY), 双方利用各自的随机数发生器, 认证通过后无线基站才能访问RFID电子标签的安全数据区, 双方通信的数据处于加密状态^[8-9]。集成国密SM7算法RFID资产管理系统原理图如图5所示。

5.1 集成国密SM7算法的RFID电子标签设计

集成国密SM7算法的RFID电子标签系统可划分为6部分, 如图6所示。ANT(天线)是唯一的外部元件, 其余5部分在单芯片上集成, 包含PMU(Power Management Unit)、RF(Radio Frequency)、ANALOG和BASEBAND。各部分功能描述如下。

1) ANT: 接收和发射射频信号。

2) RF: ①将RF功率转换为DC功率;

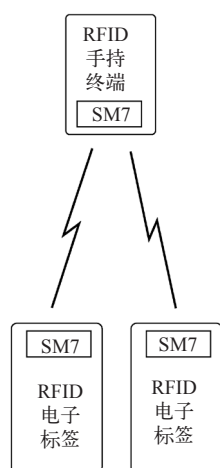


图5 集成国密SM7算法RFID资产管理系统原理图

Fig. 5 Principle diagram of RFID asset management system integrating national secret SM7 algorithm

②ASK解调并转换为数字电平；③改变天线端口阻抗。

3) PMU：对DC功率限流，稳压。

4) BASEBAND：①协议物理层；②协议MAC层；③非易失存储器。

5) ANALOG：为BASEBAND提供时钟、复位信号、随机数和标志位存储器。

6) SM7加密模块：实现SM7加密功能。

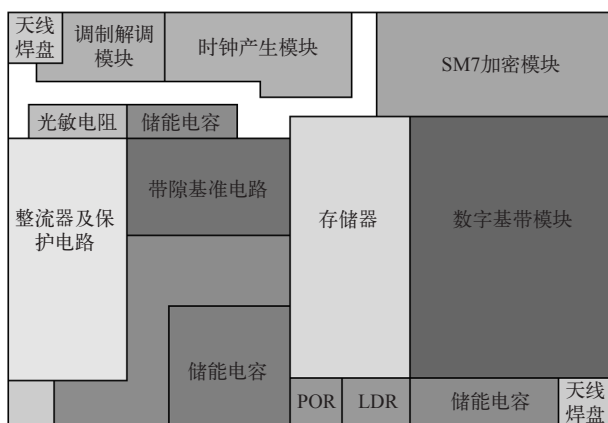


图6 集成国密算法的RFID标签系统架构详图

Fig. 6 Detailed architecture of RFID label system integrating national secret algorithm

5.2 手持设备设计

集成国密算法的手持设备主要是由两部分组成：一部分为工业平板电脑RAY907GB_ST；一部分为背板。两者通过串口相连，背板从工业

平板电脑取电。背板内部由四部分组成，分别为：天线、RFID读头、K60主控芯片和集成SM7算法的安全芯片。RFID标签通过RFID读头获取认证信息，通过安全芯片进行安全认证，RFID读头读取RFID标签加密数据，然后通过安全芯片进行解密^[10]。图7为手持设备原理图。

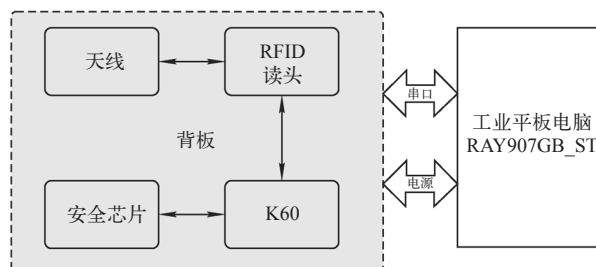


图7 手持设备原理图

Fig. 7 Handheld device schematic

5.3 高安全RFID资产管理系统实现

高安全RFID资产管理系统，RFID电子标签被预置密钥，手持终端内部集成安全芯片。安全芯片内部预置同一密钥，手持终端需要写RFID电子标签数据时，RFID电子标签与手持终端需要通过双向认证，如果认证不通过，则手持终端无法对RFID电子标签进行写操作。RFID标签在鉴别过程中出现任何错误，标签不返回任何信息，并回到仲裁状态，等待下一轮选择和清点指令。鉴别过程为一条通信指令（分两次发送），应根据鉴别流程一次完成。中间若被其他指令打断，则认为鉴别失败。

手持阅读器和RFID电子标签的双向鉴别通过后，RFID电子标签只响应盘点组命令和安全通信命令。

手持阅读器和RFID电子标签双向鉴别通过后，安全通信流程如下。

1) 手持阅读器生成随机数 R_{Nr} ，用SK加密cmd，发送安全通信命令 $Sec_Com(E_{SK}(cmd))$ 。

2) 标签用SK解密 $E_{SK}(cmd)$ 得到cmd，电子标签执行cmd中的命令，操作结果为result；然后标签用SK加密result得到 $E_{SK}(result)$ 发送给手持终端。

3) 手持阅读器用SK解密得到result。

手持阅读器和RFID电子标签的“鉴别”是双向认证的过程，加密的主要原理是通过国密SM7算法对比手持阅读器和RFID电子标签相互发送的指令及返回值，即：通过发送鉴别指令，产生随机数；然后，对随机数与根密钥进行或运算，传递给标签，在标签一侧进行解密，比对随机数是否一致，来判定鉴别成功与否。

认证通过后，电子标签的和手持阅读器之间的所有通信（包括命令、参数以及数据）采用流加密方式传输。加解密的初始密码使用认证流程第三部数据作为IV进行加解密后产生，后续密钥使用国密SM7算法的OFB模式产生。系统实物图如图8所示。



图8 集成SM7算法RFID资产管理系统

Fig. 8 Integrated SM7 algorithm RFID asset management system

6 结束语

引入基于国密算法的高安全RFID资产管理系统之后，资产信息安全性和可靠性得到提高，避免了通过篡改或伪造设备或终端，造成信息泄露事故^[11-15]。

本文以工程实践为主，结合国密SM7算法加密技术与电力设备管理制度相结合，确保电力设备资产信息安全性，后续工作中还需要继续完善理论，优化相关参数，以达到更好的应用效果。

参考文献

[1] 赵永柱，任晓龙，房涛．基于物联网RFID技术的电网资产精益化管理研究[J]．自动化与仪器仪表

表，2018(3)：7-9.

ZHAO Yongzhu, REN Xiaolong, FANG Tao. Research on lean management of power grid assets based on internet of things RFID technolog[J]. Automation and Instrumentation, 2018(3): 7-9.

[2] 吴飞，陈景晖，陈亚猛，等．基于RFID的电力资产管理的信息安全研究[J]．科技视界，2014(23)：298-300.

WU Fei, CHEN Jinghui, CHEN Yameng, et al. Research on information security of power asset management based on RFID[J]. Science and Technology Vision, 2014(23): 298-300.

[3] 张文丽，赵峰．RFID双向安全认证协议的设计及分析[J]．智能计算机与应用，2013，3(5)：91-93.

ZHANG Wenli, ZHAO Feng. Design and analysis of RFID bidirectional security authentication protocol[J]. Intelligent Computer and Applications, 2013, 3(5): 91-93.

[4] 苏董杰．基于SM7国密算法非接触逻辑卡对Mifare 1门禁系统的升级方案[J]．中国集成电路，2012(3)：80-83.

SU Dongjie. An upgrading scheme of Mifare 1 access control system based on SM7 national secret arithmetic contactless logic card[J]. China Integrated Circuit, 2012(3): 80-83.

[5] 刘熙胖，梁松涛．智能终端安全体系研究与应用[J]．通讯世界，2015(18)：212.

LIU Xipang, LIANG Songtao. Research and application of intelligent terminal security system[J]. Telecom World, 2015(18): 212.

[6] 徐树民，刘建巍，田心，等．国产算法安全芯片与市场应用[J]．信息安全与通信保密，2012(2)：36-38.

XU Shumin, LIU Jianwei, TIAN Xin, et al. Domestic algorithmic security chip and its market applicatio[J]. Information Security and Communication Privacy, 2012(2): 36-38.

[7] 胡双喜，吕前进，梁友仁，等．基于国密算法的

- 智能终端语音加密系统设计[J]. 微型机与应用, 2017, 36(12): 1-3.
- HU Shuangxi, LV Qianjin, LIANG Youren, et al. Design of intelligent terminal speech encryption system based on national secret algorithm[J]. Microcomputer its Applications, 2017, 36(12): 1-3.
- [8] 梅欢. 基于国密算法的TF密码卡设计[J]. 中国科技信息, 2016(3): 57-58.
- MEI Huan. Design of TF password card based on national secret algorithm[J]. China Science and Technology Information, 2016(3): 57-58.
- [9] 卢兵岳, 慧清. 基于国密算法的LTE230系统终端安全的研究[J]. 供用电, 2018, 35(12): 14-20, 28.
- LU Bingyue, HUI Qing. Research on terminal security of LTE230 system based on state secret algorithm[J]. Distribution & Utilization, 2018, 35(12): 14-20, 28.
- [10] 杨勇, 黄金. 基于国密算法的超高频读写器设计[J]. 中国科技信息, 2016(23): 80-81.
- YANG Yong, HUANG Jin. Design of UHF reader and writer based on national secret algorithm[J]. China Science and Technology Information, 2016(23): 80-81.
- [11] 程晋格. 国密算法在数据存储及码流数据传输中的应用[J]. 中国集成电路, 2018(7): 15-18.
- CHENG Jingge. Application of state secret algorithms in data storage and code stream data transmission[J]. China Integrated Circuit, 2018(7): 15-18.
- [12] 刘迪, 牟鹏, 董爱强. 基于国密算法安全中间件的安全功能研究与设计[J]. 网络安全技术与应用, 2017(4): 74-78.
- LIU Di, MOU Peng, DONG Aiqiang. Research and design of security function of security middleware based on national secret algorithm[J]. Network Security Technology and Application, 2017(4): 74-78.
- [13] 高源, 安育欣, 张译. 基于RFID技术的电力物资仓储管理系统设计[J]. 自动化与仪器仪表, 2018(12): 83-86.
- GAO Yuan, AN Yuxin, ZHANG Yi. Design of power material warehousing management system based on RFID technolog[J]. Automation and Instrumentation, 2018(12): 83-86.
- [14] 乌兰格日勒, 张勇. 基于RFID的电力档案智能管控系统[J]. 福建电脑, 2018(12): 104-105, 124.
- Wulangerile, ZHANG Yong. Intelligent management and control system of electric power archives based on RFID[J]. Fujian Computer, 2018(12): 104-105, 124.
- [15] 云禄. RFID技术在电力企业固定资产管理中的应用及优势分析[J]. 现代国企研究, 2018(18): 39.
- YUN Lu. Application and advantage analysis of RFID technology in fixed assets management of electric power enterprises[J]. Modern SOE Research, 2018(18): 39.

作者简介



雷振江

雷振江(1972-), 硕士研究生, 高级工程师, 主要研究方向为信息技术研究与创新应用、信息化深化应用、科技创新与实践工作, 及其基于电网运行与发展的研究与实践。

刘颖(1975-), 高级工程师, 主要研究方向为信息技术、信息化建设和项目管理等。

(收稿日期: 2019-03-11) **EA**