DOI:10.13718/j.cnki.xsxb.2023.03.002

计及多端互联通信的智能电网 AMI 新型密钥管理方案①

胡厚鹏, 肖艳红, 吴才远, 高正浩, 吴欣

贵州电网有限责任公司, 贵阳 550002

摘要: 针对智能电网高级量测体系(advanced metering infrastructure, AMI)中智能电表与配电自动化系统、分布式电源监控系统等通信过程中可能存在的信息安全问题, 提出了一种计及多端互联通信的智能电网 AMI 新型密钥管理方案. 首先基于电力系统 IEC 61850 标准建立了智能电表量测信息交互模型, 然后根据 AMI 在电力系统中的密钥实际管理需要, 提出了一种适用于 AMI 环境下的密钥管理架构, 并采用数据-密钥双向动态更新策略, 降低了网络密钥分发耗损与泄漏风险. 通过算法安全性和性能测试可知, 该新型密钥管理方法符合电力系统数据量测的安全需要, 能够有效保障智能电网 AMI 中多端互联通信过程中的信息安全.

关 键 词: 高级量测体系(AMI); 多端互联通信; 智能电网; IEC 61850 标准; 信息安全; 密钥管理

中图分类号:TN915.853 **文献标志码**:A **文章编号**:1000-5471(2023)03-0009-08

A New Key Management Scheme for AMI of Smart Grid with Multi-terminal Interconnection Communication

HU Houpeng, XIAO Yanhong,
WU Caiyuan, GAO Zhenghao, WU Xin

Guizhou Power Grid Co., Ltd., Guiyang 550002, China

Abstract: This paper proposed a new key management scheme for advanced metering infrastructure(AMI) of smart grid with multi-terminal interconnection communication to address the possible information security problems in the communication between smart meters and distribution automation systems and distributed power monitoring systems in smart grid AMI. Then, according to the actual key management needs of AMI in the power system, a key management architecture was proposed for AMI environment, and the data-key bi-directional dynamic update strategy was adopted to reduce the risk of network key distribution depletion and leakage. The algorithm security and performance tests showed that the new key management method proposed in this paper meet the security needs of data volume measurement in power system, can effectively guarantee information security in the process of multi-terminal interconnection communication in smart grid AMI.

Key words: advanced metering infrastructure (AMI); multi-terminal interconnection communication; smart grid; IEC 61850 standard; information security; key management

① 收稿日期: 2022-09-02
基金项目: 中国南方电网有限责任公司科技项目(066600KK52200003).
作者简介: 胡厚鹏, 工程师, 主要从事物联网应用技术研究.

在我国能源互联网迈入高速发展的时代背景下，实现电网用电信息和电力用户需求的精准互动响应，能够使用户的用电成本与供电企业的生产效益达到理想的平衡状态，这需要电网配备完整先进的高级量测体系(advanced metering infrastructure，AMI)以实现信息的及时互动. AMI主要涵盖用户的户内网络、用户终端智能电表、企业系统通信网络加上相应的电网量测数据管理系统，从而可以实现电力系统数据信息的准确、及时传递，对于电力系统的智能用电、电费调控、用户响应和“双碳”目标的完成具有重要的现实价值[1-2].

在AMI中，智能电表是用户与供电企业完成互动的关键节点，由于终端智能电表的通信交互对象包含用户的户内网络、电网量测数据管理系统的通信、配电自动化系统以及分布式电源监控系统，因此在AMI中整体呈现多端互联的状态，而由于智能电表的生产来源极为复杂，因此在通信标准不统一的情况下，其在AMI中与电力设备的兼容性和系统中的延展性存在一定的问题，这使得智能电表在多端互联状态下基于广域网(wide area network，WAN)完成与电网量测数据管理系统极有可能会面临严重的信息安全问题，而由于电网信息数据的特殊性，此类信息安全问题极有可能引发严重的停电事故，进而导致电网的经济利益受到严重损害[3-4].

当前，我国法律法规对电网AMI通信过程中的信息安全防护提出了更高的要求. 由于电力系统AMI中包含有大量的通信终端，每个终端自身都设定有专用密钥，因此现有的电力系统AMI信息安全问题的核心在于确保密钥的安全性. 而目前国内外无论是学术界还是工业界对AMI的密钥管理方案的研究仍然处于探索阶段. 文献[5]针对AMI中的通信安全问题提出了一种综合保密及鉴权方法；文献[6]基于多种安全机制将经典的应用协议在AMI中进行应用，重点研究了AMI的加密及鉴权问题，但均未涉及密钥管理问题；文献[7]设计了一种基于公钥加密的安全算法，然而由于各个国家的智能电网建设情况不同，造成电网的AMI的形式也各不相同[8-9]，所以这一算法的应用具有显著的局限性；文献[10-11]重点研究了系统的密钥管理方案的架构设计；文献[12-14]针对电力系统中的数据采集与监视控制系统(supervisory control and data acquisition，SCADA)，即等通信网络，设计了相应的密钥管理方案，但是由于系统的结构以及具体应用目标存在差异，此类密钥管理方案难以适用于电网AMI中的密钥管理.

因此本研究将针对多端互联条件下电网AMI中的信息安全问题，设计基于IEC61850标准的量测信息交互模型，并针对性地设计相应的AMI密钥管理方案.

1 计及多端互联的电网AMI架构

1.1 电网AMI系统的基本结构

AMI是现代化智能电网的重要组成成分，可以鼓励用户积极参与电网的运营管理. AMI集成了多种先进技术以实现用户和供电企业的智能交互，前者能从AMI中收集到决策所必需的重要信息，后者则可根据AMI收集的信息数据优化系统运行并提升供电服务水平. AMI系统主要包括以下5个部分(图1).

1) 用户户内网络. 该网络可以为用户提供接入电网中智能电表等装置的智能接口，使得用户能够及时了解用电情况，并根据用户的用电习惯响应电价信号，同时还可限定供电企业的控制动作.

2) 智能电表. 智能电表可以被视为集成了多种功能的用户侧智能终端，其主要功能包含阶梯电价、双向计量和停复电预警等，并且可以实现对用电需求方的有效响应.

3) 通信体系. 供电企业、用户和可控的电力设备之间的交互信息通常通过WAN进行传递，因此通信标准应当具有开放性与双向性，同时应确保较高的安全性. 通信网络通常使用单个领域集中器采集计量数据并统一发送至AMI数控中心，而通信介质一般为光纤、铜线、互联网等. 在预测通信带宽需求的时候，必须对智能电网的发展趋势和潜在的供电服务加以考虑.

4) 电网量测数据管理系统. 电网量测数据管理系统是一种计量数据库，集成有多种数据分析工具，并且可以与其他多种电网应用系统完成信息共享和信息交互. 该系统的主要作用是确保AMI数据完整且准确.

5) 操作网关. 操作网关主要是实现不同结构网络之间的即时有效通信与协议的转换，主要基于智能电表或是PC端完成.

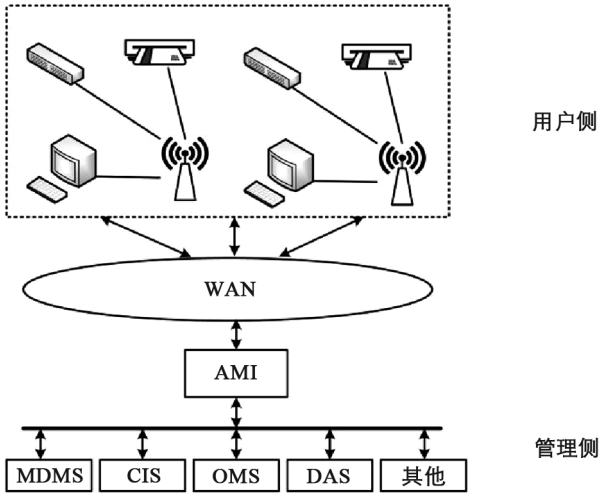

图 1　AMI 基本结构

1.2　电网 AMI 系统的通信环境

AMI 的信息种类包含量测数据、供电预警信息、需求侧响应项目的发布、准入及清退申请信息等. 按照信息交互两端的类型可以分为用电侧以智能电表为代表的上行信号和以高级管理应用为代表的下行信号. 两种信号的传递模型可划分为单播、多播和广播 3 种通信方式. 在实际应用中，这 3 种通信方式主要通过具有 IPSec 安全防护功能的终端公网安全通信模块进行，实现集中器、负控终端和配变终端安全传输服务，从而完整构成中心服务器—安全网关—无线通信机—无线网络—终端公网安全通信模块—终端的传输链，其主要应用场景见图 2.

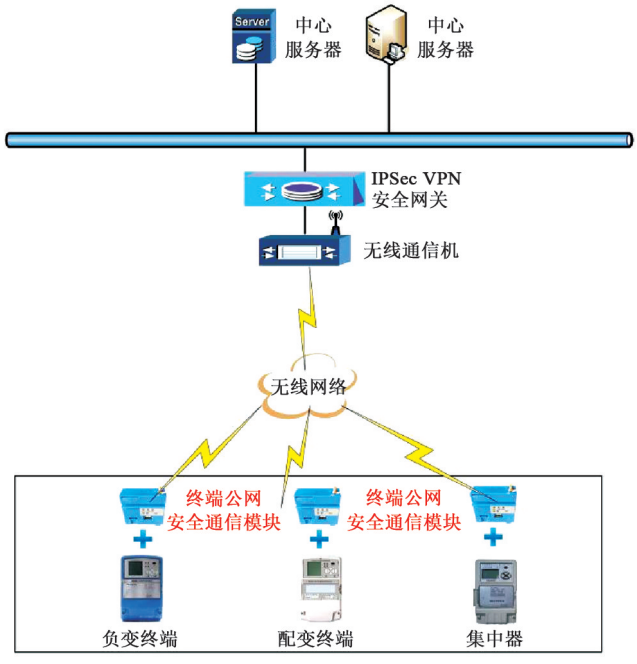

图 2　AMI 安全通信应用场景

1.3　电网 AMI 系统的安全防护体系总体部署方案

为了保障本研究提出的 AMI 密钥管理方案处于安全的通信环境下，因此将采用特定的安全防护体系作为方案的基础实施环境. 本研究的电网 AMI 安全防护体系从应用架构上可分为感知层、网络层、平台层和应用层. 通过这 4 个层面的建设，可让电力行业在任何时间、地点、人、物之间实现信息连接和交互，产生共享数据，从而为用户、电网、发电、供应商和政府社会服务，其总体的应用结构见图 3.

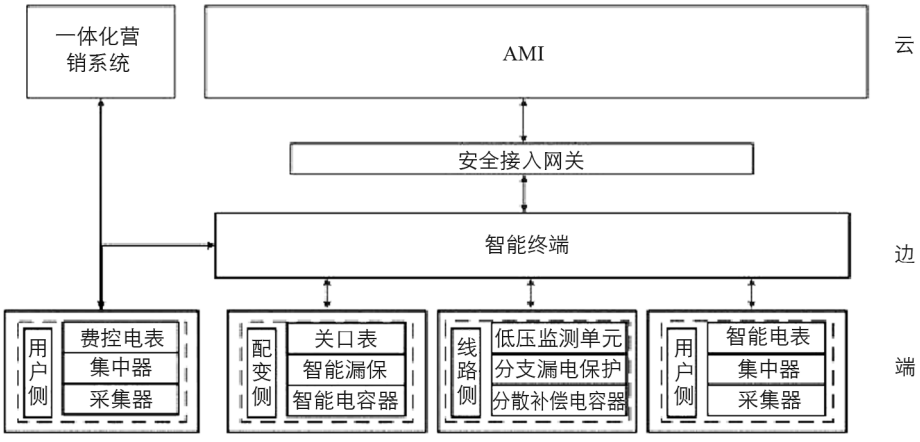

图3 电网AMI安全防护体系应用结构

2 智能电表量测信息交互模型

为了统一电网AMI的通信标准，考虑到IEC 61850是国际通用的电力标准，因此本研究遵照IEC 61850标准设计了智能电表量测信息交互模型，以抽象通信服务接口为核心给出了功能和实际应用技术分割的多种通信服务模型，如DATA和LN等，以及模型的实际响应流程. 此类通信模型的服务接口基本覆盖全部电网通信业务，具有极强的适应能力和延展性，使得IEC 61850能够快速、高效地完成电网通信模型的建立并具有高度的普适性和延展性. 抽象通信服务接口主要包括客户/服务器模型以及对等网络模型，前者主要用于调控和读取信息，后者主要提供周期采样量测值的呈递等服务. 智能电表各功能所涉及的通信模型见表1，智能电表量测信息交互模型见图4.

表1 智能电表各功能所涉及的通信模型

功能名称	通信模型
数据采集与处理	“关联”“数据集”“缓存报告”“日志”“数据读取”“定量控制”
负荷控制	“关联”“控制”
需求侧项目交互	“关联”“文件传输”
故障记录和上传	“非缓存报告”“日志”
系统支持	“时间同步”“文件传输”“日志”

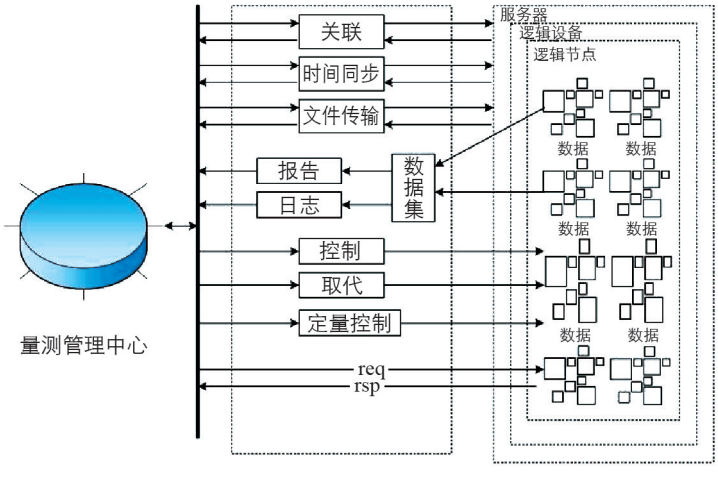

图4 智能电表量测信息交互模型

3　AMI 密钥管理方案

3.1　密钥框架

本研究设计的 AMI 密钥管理框架可以同时实现 3 种通信模式，其中所用的符号定义见表 2.

表 2　AMI 符号定义

符号	定义
N	上行信号数目
M	需求侧项目数目
U_i	AMI 中第 i 个用户，其中 U_0 表示的是下行信号，其余表示上行信号
K_i	AMI 中第 i 个用户的密钥
GK_i	第 i 个需求侧项目密钥
TK_i	会话的密钥
GTK_i	第 i 个需求侧项目组播通信的会话密钥
A_i	产生 TK_i 的附属值
GA_i	产生 GTK_i 的附属值
C_i	产生 A_i 的 AMI 中第 i 个用户响应的计数器
GC_i	产生 GA_i 的 AMI 中第 i 个用户响应的计数器
I	需要加密的信息
EI	完成加密的信息
E_i	AMI 中第 i 个用户前一天的用电数据
D_E	E_i 的收集日期
SS	发送端的信息签名
SR	接收端的信息签名
P_j	第 j 个需求侧项目
RQI_j	第 j 个需求侧项目的准入申请
RQO_j	第 j 个需求侧项目的退出申请
RPS	下行信号回复申请成功
RPF	下行信号回复申请失败
Kb	一个安全的 b bit 长密钥产生算法
Rb	一个安全的 b bit 长随机生成函数
$C_K(I)$	对称密钥加密算法
$EC_K(EI)$	对称密钥解密算法
$\oplus$	异或
$\parallel$	级联
$H(K)$	哈希函数
$F_K(A)$	基于密钥 K 的鉴权函数

本研究 AMI 的密钥管理框架见图 5，可定义 $AK=(U, K, R)$. 其中 U 表示的是含有全部上行信号的非空有限集，其计算公式为

$$U=\{U_1, U_2, \cdots, U_N\} \tag{1}$$

K 表示的是涵盖全部密钥的非空有限集，其计算公式为

$$K=\{K_0\}\cup\{K_1,K_2,\cdots,K_N\}\cup\{GK_1,GK_2,\cdots,GK_M\} \tag{2}$$

其中：$\{K_1,K_2,\cdots,K_N\}$ 表示的是用户密钥的集合，$\{GK_1,GK_2,\cdots,GK_M\}$ 表示的是组用户密钥的集合，$\{K_0\}$ 表示的是根密钥.

R 表示的是 U 和 K 的映射关系的集合，可被定义为 $R_K\subset U\times K$，当存在关系 $(U,K)\subset R$ 时说明密钥 K 被用户 U 进行了储存. 此时可以定义该框架下的函数为

$$U_s(K)=\{U\mid(U,K)\in R\} \tag{3}$$

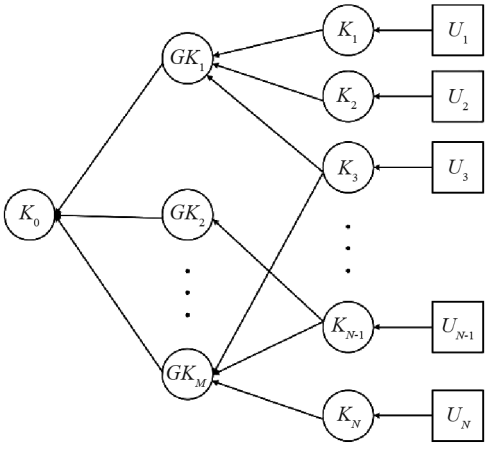

图 5 AMI 密钥管理框架

3.2 通信密钥管理方案及更新方法

可通过单播通信传递的信息包括计量数据、需求侧项目的准入及退出申请和远距离负荷控制，此类信息传递具有双向性，因此为了信息保密与完整，需要在新会话开展前更新. 其密钥管理方案流程为：

单播通信密钥管理方案流程

Step 1：发送端

$A_i=H(F_{K_i}(E_i\oplus D_E)\oplus C_i)$

$TK_i=H(K_i\oplus C_i)$

$EI=C_{TK_i}(I)$

$SS_i=F_{KTK_i}(EI)$

Step 2：信息传递

$U_0(U_i)\rightarrow U_i(U_0)$：$(EI||SS)$

Step 3：接收端

U_i(或 U_0)：$A_i=H(F_{K_i}(E\oplus DE)\oplus C_i)$

$TK_i=H(K_i\oplus C_i)$

$SS_i=F_{KTK_i}(EI)$

IF $SS=SR$

$I=EC_{TK_i}(EI)$

END IF

为了确保密钥的崭新程度，用户密钥必须定期保证更新，通过哈希函数更新可以防止网络分发开销和

密钥的独立，具体的更新策略见表 3.

表 3　单播通信密钥更新方法

参数	周期	方法
K_i	周期	$K'_i=H(K_i)$
C_i	单次会话前	$C'_i=C_i+1$
A_i	单次会话前	$A_i=H(F_{K_i}(E\oplus DE)\oplus C_i)$
TK_i	单次会话前	$TK_i=H(K_i\oplus C_i)$

可通过广播通信传递的信息包括需求侧项目发布和电价信息，其密钥管理流程与单播通信的一致，其密钥更新方法见表 4.

表 4　广播通信密钥更新方法

参数	周期	方法
K_0	周期	$K'_0=H(K_0)$
C_0	单次会话前	$C'_0=C_0+1$
A_0	单次会话前	$A_0=H(F_{K0}(E\oplus DE)\oplus C_0)$
TK_0	单次会话前	$TK_0=H(K_0\oplus C_0)$

可通过多播通信传递的信息主要包括电价信息和远程负荷控制信号，其密钥管理的基本流程与广播通信的类似，但是会存在用户加入或退出需求侧项目组，因此在更新方法上有所不同，其更新方法见表 5.

表 5　多播通信密钥更新方法

情况	参数	周期	方法
需求侧项目组员无变化	GK_j	周期	$GK'_j=H(K_j)$
	GC_j	单次会话前	$GC'_j=GC_j+1$
	GA_j	单次会话前	$GA_j=H(GC_j)$
	GTK_j	单次会话前	$GTK_j=H(TK_j\oplus GC_j)$
需求侧项目组员加入或退出	GK_j	周期	$GK'_j=Kb$
	GC_j	周期	$GC'_j=Rb$

4　方案性能分析

4.1　安全性分析

4.1.1　密钥的产生

方案中用户密钥以及组密钥的产生都是基于密钥生成器随机产生的，会话密钥的生成是基于前两种密钥加上附加值利用哈希函数产生. 因为用户密钥安全性较强，则基于哈希算法随机生成的附加值也具有高度随机性，使得会话密钥的安全性较高.

4.1.2　密钥崭新程度

本研究中密钥管理方法能够周期性自我更新，密钥更新的关键在于有无用户进出需求侧项目组，如有则需在期限内更新，从而有效应对攻击. 由于更新中采用了哈希算法，其差异在于会话密钥在更新中还引入了附加值，使得新密钥的独立性显著高于旧密钥.

4.1.3　双向安全

更新过程中接收方会对数字签名开展认证，认证完成后进行解密，使得信息完整性得以保障，由于用户可以自由选择是否进出需求侧项目组，因此在此过程中必须保证双向安全. 故而在本研究中出现此类情况时，组密钥与附属信息将自动更新并再次分发给新组成员，以此保证双向安全.

4.2 分发开销计算

为了验证本研究提出的AMI密钥管理方案的优越性，进一步对方案的分发开销进行计算，其中单次更新的周期内的分发开销可以被定义为申请加入需求侧项目的用户数 N_1 与有用户加入或退出需求侧项目数 N_2 之和与单个含有密钥与有关数据的数据包的分发开销乘积. 分发开销计算结果见表6.

表6 分发开销结果

N_1	$N_2=5$	$N_2=10$	$N_2=15$
1k	2.345	2.496	2.525
2k	4.958	4.977	4.995
3k	7.454	7.458	7.466
5k	13.352	13.361	13.424
10k	25.682	25.702	25.713

由表6可以看出，分发开销不充分并不会对密钥的更新与AMI数据的传输产生较大影响，证明本研究提出的密钥管理方案能够有效避免分发耗损，降低了分发信息被截取的风险，有力保证了AMI通信的安全，证明本研究提出的AMI密钥管理方法具有较好的优越性.

5 结论

针对智能电网AMI通信过程中的信息安全问题，本研究提出一种计及多端互联通信的智能电网AMI新型密钥管理方案. 在电网AMI安全防护体系总体部署方案的基础上遵循IEC 61850标准建立了智能电表量测信息交互模型，设计了一种可允许单播、组播和广播3种通信方式并行的通信框架，降低了网络密钥分发耗损与泄漏风险. 通过性能分析可知，本研究提出的AMI密钥安全管理方案符合多端互联环境下电力系统AMI的安全需要，能够有力保障系统的信息安全.

参考文献：

[1] 肖勇，周密，钱斌，等. 微服务架构在网级电能量数据平台中的应用研究 [J]. 浙江工业大学学报，2021，49(3)：258-265.
[2] 王旭东，王高猛，林济铿，等. 基于AMI量测信息的低压配电网线路参数辨识方法 [J]. 中国电力，2019，52(5)：63-69.
[3] 王高猛，么莉，王文文. 基于AMI量测信息的变压器参数辨识方法 [J]. 电力系统及其自动化学报，2019，31(6)：38-42.
[4] 冯语晴，杨建华，黄磊，等. 配电网智能化评价指标体系研究 [J]. 电网与清洁能源，2017，33(3)：84-90.
[5] YAN Y，QIAN Y，SHARIF HAMID. A Secure and Reliable In-Network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid [C]. 2011 IEEE Wireless Communications and Networking Conference，IEEE Computer Society，2011：909-914.
[6] 罗鸿轩，金鑫，钱斌，等. 基于区块链的台区智能终端与智能电表安全防护方法 [J]. 南方电网技术，2021，15(4)：50-58.
[7] 佟为明，梁建权，李中伟，等. 基于数据可恢复的AMI无线传感器网络安全数据聚合技术 [J]. 电力自动化设备，2017，37(5)：211-216，223.
[8] 梁建权，金显吉，佟为明，等. 高级量测体系中无线传感器网络的密钥管理方案 [J]. 电力系统自动化，2016，40(19)：119-126.
[9] 李彬，温蜜，齐钰. 智能电网AMI系统中一种新型密钥管理方案 [J]. 计算机应用与软件，2016，33(1)：321-325.
[10] VAHE S，ROUWAIDA K，ALI C，et al. Identity Based Key Distribution Framework for Link Layer Security of AMI Networks [J]. IEEE Transactions on Smart Grid，2016，9(4)：3166-3179.
[11] GEORGE N，NITHIN S，KOTTAYIL S K. Hybrid Key Management Scheme for Secure AMI Communications [J]. Procedia Computer Science，2016，93：862-869.
[12] 郜克天，毛羽刚，荀鹏，等. OSGP轻量级密钥管理方案设计 [J]. 小型微型计算机系统，2015，36(10)：2340-2344.
[13] 路保辉，马永红. 智能电网AMI通信系统及其数据安全策略研究 [J]. 电网技术，2013，37(8)：2244-2249.
[14] 李国竞，段斌. 高级量测体系系统中收益保护分析与安全策略 [J]. 华东电力，2011，39(5)：707-710.

责任编辑 潘春燕