DOI:10.13718/j.cnki.xsxb.2023.03.003

基于国密算法的电网 AMI 数据安全防护技术①

欧家祥，　胡厚鹏，　何沛林，　宋强，　董天强

贵州电网有限责任公司，贵阳 550002

摘要：随着电力系统智能化的快速发展，大量智能终端采集设备接入电力系统. 为了有效提升电网高级量测体系(advanced metering infrastructure，AMI)中设备的安全防护能力，以电力系统费控二次系统为例，提出一种适用于电网 AMI 环境下的数据安全防护技术，通过引入数字证书实现电网数据传输过程中的双向身份认证. 考虑电网 AMI 环境，在采集终端计算能力不足的前提下攫取数据的主要信息，得到基于改进 SM2 的密钥交换协议，并对其进行了具体的安全性能分析、开销分析和效率测试. 结果表明，该技术具有较强的安全性和稳定性，在满足电网 AMI 数据传输安全的基础上，能够有效降低通信信息交换的开销耗损，并能同时满足多个终端的通信需求，有助于提升电网 AMI 的数据传输安全水平.

关　键　词：高级量测体系(AMI)；国密算法；费控二次系统；电力系统；智能终端；数据安全

中图分类号:TN915.853　　**文献标志码**:A　　**文章编号**:1000－5471(2023)03－0017－08

Data Security Protection Technology for Grid AMI Based on National Secret Algorithm

OU Jiaxiang，　HU Houpeng，
HE Peilin，　SONG Qiang，　DONG Tianqiang

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

Abstract：With the rapid development of power system intelligence，a large number of intelligent terminal collection devices are connected to the power system. In order to effectively improve the security protection capability of devices in grid AMI，this paper took the secondary system of power system fee control as an example，proposed a data security protection technology applicable to the grid AMI environment，realized two-way identity authentication in the process of grid data transmission by introducing digital certificates，seized the main information of data under the premise of the insufficient computing power of collection terminals in the grid AMI environment，and obtained a key exchange protocol based on the improved SM2 key exchange protocol was analyzed and tested for specific security performance，overhead analysis and efficiency. The results showed that the technology had strong security and stability，can effectively reduce the overhead consumption of communication information exchange on the basis of satisfying the data transmission security of grid AMI，and can meet the communication needs of multiple terminals simultaneous-

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：欧家祥，高级工程师，主要从事电力系统及其自动化、物联网技术研究.

ly, which helped to improve the data transmission security level of grid AMI.

Key words: advanced metering infrastructure(AMI); national secret algorithm; fee control secondary system; power system; intelligent terminal; data security

高级量测体系(advanced metering infrastructure, AMI)是当前我国能源互联网快速发展背景下建设现代化智能电网的重要参与成分,其本质是对电力用户信息进行测量、分析和处理的高级网络系统[1-2]. 供电企业通过在电力系统中构建AMI从而实现电力市场的多方智能交互,这是实现能源合理配置的必要基础. 在智能电网中存在大量的智能终端采集设备,AMI中的数据传输主要产生在不同终端和服务器之间. 一旦传输数据的安全性受到威胁,很有可能给电网造成难以估量的重大损失. 为了保证AMI在数据传输过程中的安全性,有必要针对敏感数据进行安全防护.

国内外学者针对AMI的安全防护开展了大量研究. 文献[3]着重研究了AMI的数据风险,基于家庭内网网关实现签名后再利用楼宇网关恢复信息,经过完整性校验与聚合以后实现安全管控;文献[4]研究了基于同态加密算法的数据聚合方法,通过多重编码完成数据加密;文献[5]考虑到智能电表的资源有限性,基于白名单提出了一种云安全防护方法;文献[6]提出了基于Paillier加密的同态加密以及替代复合加密工作的安全数据聚合方法.

现有AMI具有主站集中云化部署,终端智能化变为边缘计算节点的特点,为了满足当前电网计量业务安全防护的迫切需求,本研究针对电力系统中智能终端采集设备成分较多的费控二次系统,在深入研究现有费控二次系统安全防护体系的基础上,在AMI采集监测系统框架下提出一种改进SM2国密算法的密钥交换协议作为系统的边界防护手段,确保AMI数据传输的机密性与完整性.

1 电网AMI安全防护体系

1.1 费控二次系统架构

由于费控二次系统是电网AMI应用的典型场景,因此本研究主要针对费控二次系统展开讨论. 费控二次系统是指实现对电厂、变电站、公变、专变和低压用户等发电侧、供电侧、配电侧和售电侧电气数据采集、监测与分析功能的系统主站、通信通道和计量自动化终端[7-10].

图1是当前费控二次系统安全防护总体逻辑结构,给出了费控二次系统安全区域的划分、安全区域之间横向互联的逻辑结构、安全区纵向互联的逻辑结构以及网络安全防护设备的总体部署. 按照安全分区原则,费控二次系统各业务系统和功能模块分别置于不同的安全区:在生产控制大区,控制区的主要业务包括带控制的功能模块(如控制服务、负荷控制、低压集抄等模块);非控制区的主要业务包括计量自动化系统主站数据服务(存储计量自动化系统全量数据)和不带控制的功能模块(如厂站电能量计量、配变监测等模块). 在管理信息大区,生产管理区的主要业务包括全球广域网(world wide web, WEB)发布、镜像数据服务等功能模块.

1.2 AMI采集监测系统框架

为了实现AMI中智能终端身份防伪与数据防篡改的目的,在AMI的采集监测系统安全框架下进行密钥交换协议的设计.

采集监测类系统的安全框架主要是针对用电终端无线传输安全防护需求进行设计(图2),在设计过程中还需要同时考虑安全Ⅰ,Ⅱ,Ⅲ区中计量自动化系统所在的内部网络分区的安全防护需求以及各业务系统主机安全防护需求.

针对用电终端无线传输安全防护需求,在中心侧业务系统入口处部署安全通信网关,对接入业务系统的集中器等终端进行身份认证,并通过协议阻断、格式检查和协议分析等技术防止终端侧非法数据的跨网入侵. 此外,网关与接入终端之间通过密钥协商建立一条加密传输通道,对终端与业务系统之间的业务报文进行传输保护. 在集中器上安装安全通信模块,提供认证与加密服务,实现数据传输的机密性、完整性保护,防止攻击者从终端及终端回传数据的网络链路中侵入中心系统.

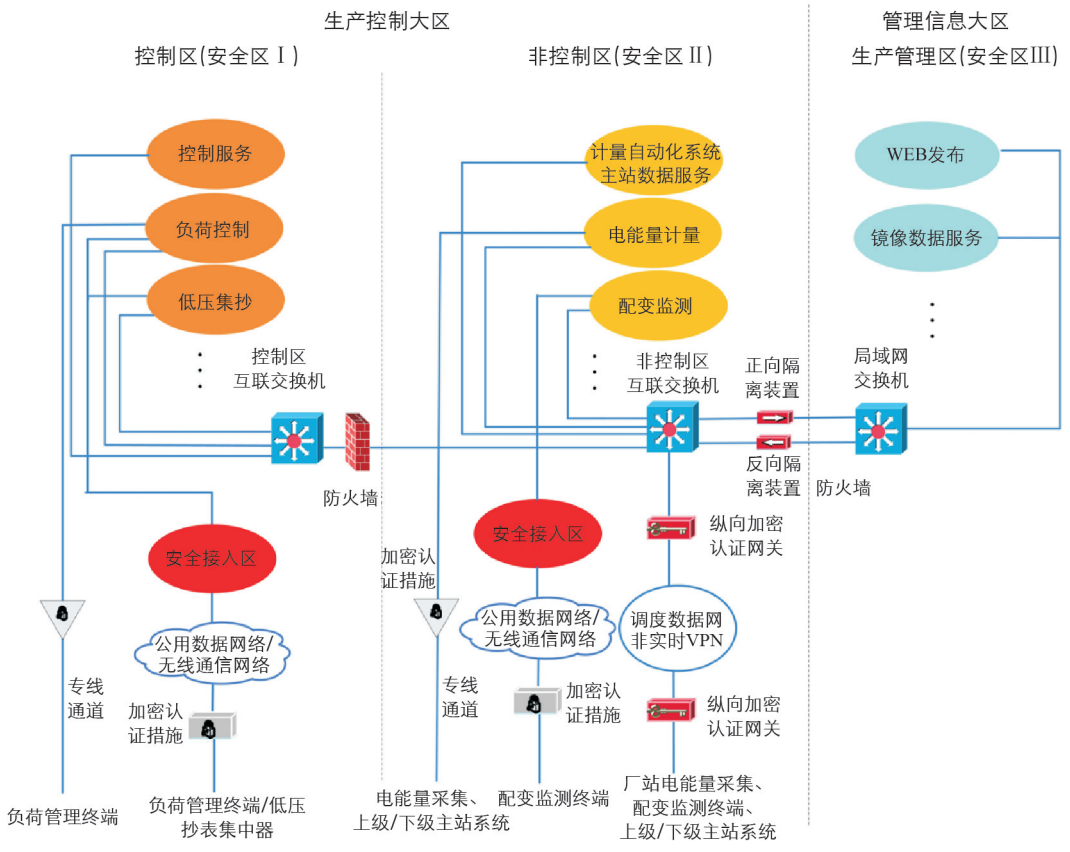

图 1　费控二次系统总体逻辑结构

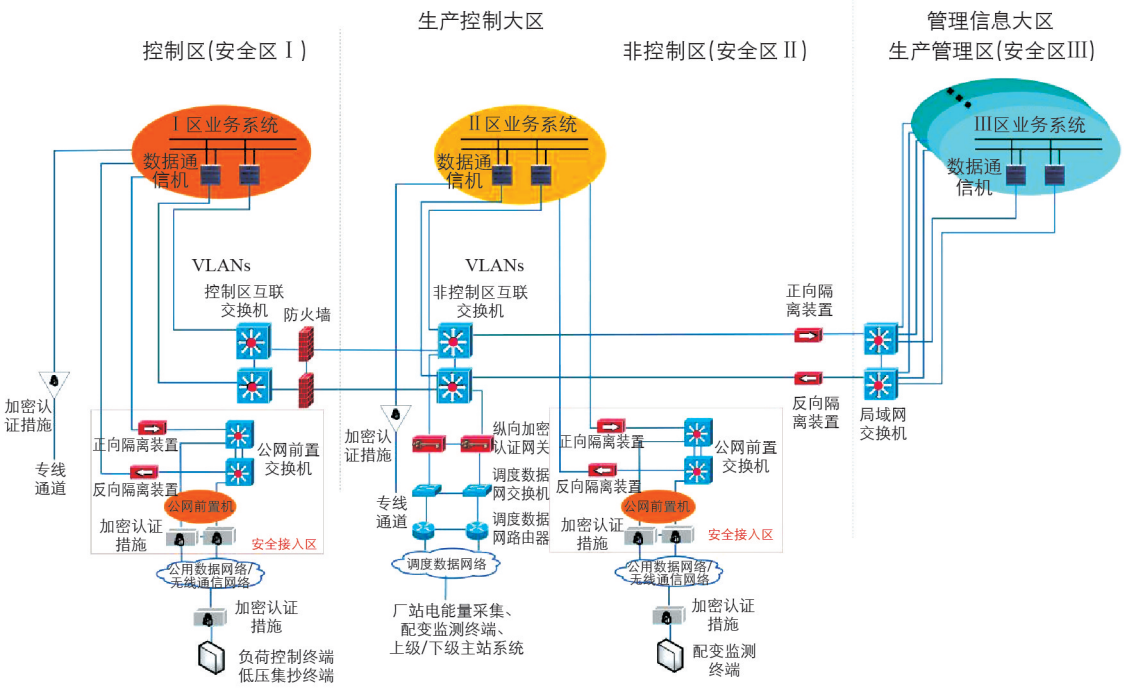

图 2　AMI 采集监测系统基本架构

2　改进 SM2 算法

2.1　SM2 算法基本流程

由于 SM2 算法具有运算维度小、加密效率高等优点，因此本研究选用 SM2 算法用于加密. SM2 算法

实质上是一种椭圆曲线迪菲－赫尔曼密钥交换(elliptic curve diffie-hellman key exchange，ECDH)算法，其所涉及的参数见表1[11-12].

表1 SM2算法参数

参数或函数	意义
e_n	n号用户的私钥
S_n	n号用户的公钥
T	EC基点
a_n	密钥交换过程中n号用户的临时随机数
b	余因子
c	$[(\log_2 n)/2]-1$
U_n	n号用户的可识别标识
$KDF()$	密钥派生函数
$Hash()$	密钥杂凑函数
K	生成的会话密钥
$E_A(B)$	利用B对信息A进行加密
$H(B)$	利用SM3对信息A进行散列
Se	会话可辨别标识

假设用户P和Q在进行密钥协商时取得的数据长度是klen比特，用户P表示的是会话发起方，同时用户Q表示的是会话响应方. 两者通过以下流程获取会话密钥.

用户P

P1：随机生成$a_P \in [1, n-1]$；

P2：计算EC点$R_P=[a_P]T=(x_1, y_1)$；

P3：将R_P传输给用户Q；

用户Q

Q1：随机生成$a_Q \in [1, n-1]$；

Q2：计算EC点$R_Q=[a_Q]T=(x_2, y_2)$；

Q3：从R_Q筛选出域元素x_2，并对$\overline{x_2}=2^c+x_2 \,\&\, (2^c-1)$进行计算；

Q4：计算$t_Q=(e_Q+\overline{x_2}\cdot a_Q)\bmod n$；

Q5：验证R_P是否为椭圆曲线方程上的一点，若不满足则协商失败；若满足，则从R_P中取出域元素x_1，并计算$\overline{x_1}=2^c+x_1 \,\&\, (2^c-1)$；

Q6：计算EC点$V=[h\cdot t_Q](S_P+[\overline{x_1}]R_P)=(x_1, y_r)$，若$V$为椭圆曲线上的无穷远点，则协商失败；

Q7：计算$K_Q=KDF(x_a \| y_V \| U_P \| U_Q, \text{klen})$；

Q8：将R_P的坐标(x_1, y_1)和R_Q的坐标(x_2, y_2)转换为比特串，并计算$S_Q=Hash(0\times 02 \| y_c \| Hash(x_V \| U_P \| U_Q \| x_1 \| y_1 \| x_2 \| y_2))$，此为可选项；

Q9：将R_Q和S_Q发送给用户P；

用户P

P4：从R_P中取出域元素x_1，并计算$\bar{x}_1=2^c+(x_1 \,\&\, (2^c-1))$；

P5：计算$t_P=(e_P+\overline{x_1}\cdot a_P)\bmod n$；

P6：验证R_Q为椭圆曲线方程上的一点，若不满足则协商失败；若满足，则从R_Q中取出域元素x_2，并计算$\overline{x_2}=2^c+(x_2 \,\&\, (2^c-1))$；

P7：计算EC点$U=[b\cdot t_P](S_Q+[\overline{x_2}]R_Q)=(x_U, y_U)$，若$U$表示的是EC上的无穷远点，则表示协商结果为失败；

P8：计算$K_P=KDF(x_\nu \| y_\nu \| U_P \| U_Q, \text{klen})$；

P9：将 R_P 的坐标（x_1，y_1）和 R_Q 的坐标（x_2，y_2）变换成为比特串，并计算 $S_1 = Hash(0 \times 02 \| y_u \| Hash(x_u \| U_P \| U_Q \| x_1 \| y_1 \| x_2 \| y_2))$，然后检验 $S_1 = S_3$ 是否存在，若为否，则示协商结果为失败；

P10：计算 $S_P = Hash(0 \times 03 \| y_U \| Hash(x_U \| U_P \| U_Q \| x_1 \| y_1 \| x_2 \| y_2))$，然后将 S_P 输送给用户 Q，此为可选项.

用户 Q

Q10：计算 $S_2 = Hash(0 \times 03 \| y_V \| Hash(x_V \| U_P \| U_Q \| x_1 \| y_1 \| x_2 \| y_2))$，然后检验 $S_2 = S_P$ 是否存在，若为否，则表示协商结果为失败，此非必选项.

此时用户双方在完成密钥协商后分别求解得到会话密钥，且 $K_P = K_Q$，其具体流程见图 3.

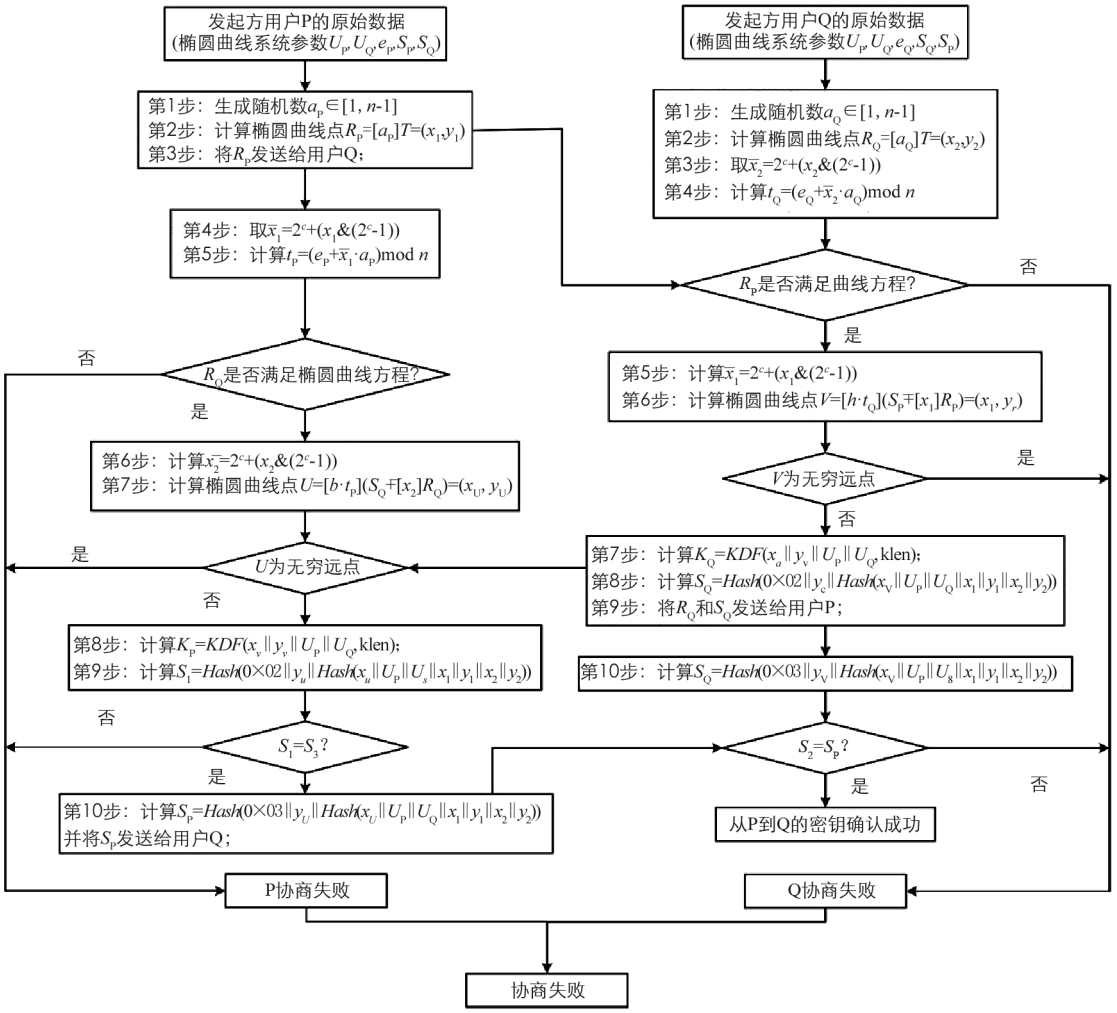

图 3　SM2 算法流程

2.2　算法改进

为了确保 AMI 数据传输过程中的安全性，本研究引入数字证书实现对传送报文的签名验证，确保连接的终端合规，最终通过密钥交换协议对证书进行检验. 其中会话发起方通过己方私钥对随机生成数完成 SM2 加密，同时利用 SM3 完成证书公钥的 Hash 运算并对结果采用 SM2 私钥签名，最后将签名和证书传送给可以完成身份认证的会话响应方，会话响应方验签成功后反馈回己方的数字证书，从而保证双向认证，确保安全[13-14]. 但是由于费控二次系统智能终端采集设备的运算性能不足，考虑到密钥交换过程中部分信息的传递即可实现整个过程而不需要花费大量的开销. 因此本研究针对费控二次系统对 SM2 按如下流程进行改进.

用户 P

P1：用户 P 产生随机数 a_P，会话可辨别标识 Se.

P2：用 Q 的公钥对 a_P 加密，并与 Se 和 ID_P 连接运行，得到 $P2=E_{F_P}(r_P)\|Se\|ID_P$；

P3：对连接结果进行 Hash 运算，得到 $P3=Hash(a_P\|Se\|ID_P)$；

P4：用 d_P 对 P3 签名，得到 $P4=E_{d_P}(Hash(a_P\|Se\|ID_P))$；

P5：连接 $P2\|P4$，得到 $xP5=E_{p_g}(a_P)\|Se\|ID_P\|E_{d_P}(H(r_P\|Se\|ID_P))$；

P6：将 $P5$ 发送到用户 Q；

用户 Q

Q1：得到 P 的报文，验签得到信息 a_P，Se，ID_P；

Q2：用户 Q 生成随机数 a_Q，并计算 U_P，U_Q；

Q3：生成会话密钥 K，S_Q，S_2；

Q4：用 P 的公钥对 a_Q 加密，并连接 Se，ID_Q 和 S_Q，得到 $Q4=E_{p_P}(r_Q)\|Se\|ID_Q\|S_Q$；

Q5：对连接结果进行 Hash 运算，得到 $Q5=Hash(a_Q\|Se\|ID_Q\|S_Q)$；

Q6：用 e_Q 对 Q 签名，得到 $Q6=E_{d_8}(Hash(a_Q\|Se\|ID_Q\|S_Q))$；

Q7：连接 $xQ4\|Q6$，得到 $Q7=E_{P_\lambda}(a_Q)\|Se\|ID_Q\|S_Q\|E_{a_Q}(Hash(a_Q\|Se\|ID_Q\|S_H))$；

Q8：将 $Q7$ 发送到用户 P；

用户 P

P7：得到 Q 发送的报文，验签得到信息：r_Q，ID_Q，S_Q；

P8：计算 U_P，U_Q，并生成会话密钥 K，S_1；

P10：比较 S_1 和 S_Q；

P11：生成 S_P 并发送给用户 Q.

用户双方通过身份认证和密钥协商实现通信互联后，AMI 数据开始传输，若由于数据不合规而未能完成以上步骤将会获取错误验证码，智能终端采集设备将重新开始以上流程直到完成验证，因此通信安全得以确保.

3 方法性能分析

3.1 安全性分析

为了从机理上证明本研究提出的方法在安全防护方面的可行性，考虑到适应当前的主流攻击方式，本研究将从双向身份认证[15]、重播攻击[16]、中介攻击[17]、信息注入攻击[18]和长期窃听[19]等 5 个角度分析方法的安全性.

3.1.1 双向身份认证

在本研究的协议方案中，智能终端采集设备私钥通常由内部安全芯片所包含的随机发生器生成并存储，同时通过受信任的第三方 CA 基于公钥发出用户证书，故而终端需要合法才可以获得对应私钥. 会话发起方发送加密信息给会话响应方后，会话响应方通过检验获取的随机数与私钥求解得到的随机数的一致性来验证会话发起方的合法性；同理，会话发起方也可以借此检验会话响应方的合法性，从而实现双向身份认证.

3.1.2 重播攻击

重播攻击的定义是攻击方向目标主机传送目标曾获取过的数据包来冒充认证过的通信用户，从而破坏认证并完成数据截取. 而本研究的方案可以在双向认证过程中将过去的随机数和历史信息中的随机数进行对比，通过判断新鲜度检测出重播攻击并舍弃，从而有效克制重播攻击.

3.1.3 中介攻击

中介攻击主要是攻击方充当信息传输中介实现通信用户之间的通信过程，从而在此过程中实现对于数据信息的截取和篡改，影响正常的通信过程. 而在本研究的方法中，充当信息中介的攻击方在截取会话发

起方的认证信息后会因为没有获取到会话响应方的私钥而不能得到随机数以及序列号，从而无法冒充会话发起方窃取协商过程中的数据信息. 同理，充当信息传输中介的攻击方也不能冒充会话响应方向会话发起方传输信息.

3.1.4　信息注入攻击

当通信用户之间相互认证通过并完成密钥的协商以后，智能终端采集设备的计量信息将开始传送，而由于会话密钥仅由用户所拥有，因此攻击方不能对其截取和解密，从而防止非法信息注入通信数据.

3.1.5　长期窃听

由于本研究的方法在开展通信时需要完成用户双方的身份认证并在密钥协商后得到新的会话密钥，在此过程中随着新的通信通道不断生成，会话密钥也随之更新，攻击方不能快速得到新的会话密钥因此难以实现长期窃听.

3.2　开销分析

在传统的 SM2 中，通信用户在通信过程中需要交换 EC 点和 *Hash* 函数杂凑值，根据国家密码管理局规定，EC 点长度应为 64 bytes，而 *Hash* 函数杂凑值的长度应为 32 bytes，故而在通信过程中共计需要传输192 bytes的数据.

而本研究的方法中通信用户在通信过程中需要交换生成的随机数、会话可辨别标识以及身份认证标识. 前两者的长度均为 8 bytes，后者的长度为 16 bytes，因此基于本研究的方法实现密钥交换仅需 72 bytes，相比于传统方法减少 120 bytes，显著降低了开销损耗，确保了数据安全性.

3.3　效率测试

为了进一步验证方法的优越性，本研究测试了不同数量的智能终端设备开展通信传输时密钥交换的稳定性. 测试环境参数见表 2.

表 2　测试环境参数

环境	参数
CPU	Intel(R) Xeon CPU E5-2695 v3@2.30Ghz
开发语言	Linux C
内存	64 GB
硬盘容量	2 TB
操作系统	CentOS 6.0

本研究测试了费控二次系统智能终端采集设备数量 N 为 1，100，500，1 000 和 5 000 时密钥交换的执行时间，所得结果见图 4. 由图 4 可以看出，当智能终端采集设备数量增大时，总的执行时间也在稳步提升而执行进度未出现显著变化，这表明本研究提出的方法能够有效应对多终端接入 AMI 时发起的通信连接请求并稳定执行任务，具有较好的稳定性.

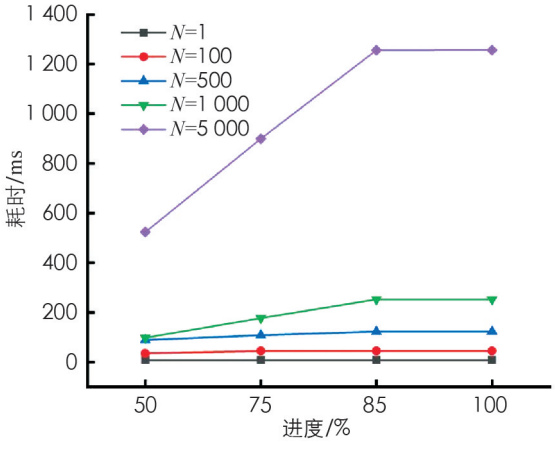

图 4　并发执行效率

4　结论

本研究针对电网二次费控系统，提出一种改进 SM2 国密算法的密钥交换协议，通过安全性分析、开销分析和效率测试对本研究提出方法进行验证，实验结果表明该方法在保障电网 AMI 数据安全方面具有较高的可行性. 能够确保 AMI 中终端用户

在通信过程中数据的机密性与安全性，有力保障了电网的信息通信安全，有助于我国能源互联网的建设.下一步将继续开展防护技术的优化，进一步提升防护效率和防护范围，以应对更多的新型安全攻击.

参考文献：

[1] 郑文迪，聂建雄，邵振国，等. 智能配电网状态估计研究现状和展望 [J]. 电力系统及其自动化学报，2021，33(4)：8-16.
[2] 肖勇，金鑫，王立博，等. 基于AMI的智慧用能多模汇聚网关装置研究 [J]. 计算机科学，2020，47(S1)：289-293.
[3] 刘小雪. 智能电网AMI网络安全机制研究 [D]. 长沙：国防科学技术大学，2014.
[4] 梁建权. 高级量测体系WSNs安全防御技术研究 [D]. 哈尔滨：哈尔滨工业大学，2016.
[5] GEORGE N，NITHIN S，KOTTAYIL S K. Hybrid Key Management Scheme for Secure AMI Communications [J]. Procedia Computer Science，2016，93(C)：862-869.
[6] MAHMOUD M E A，NICO S，KUMAR A P，et al. Privacy-Preserving Power Injection over a Hybrid AMI/LTE Smart Grid Network [J]. IEEE Internet of Things Journal，2016，4(4)：870-880.
[7] 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.
[8] 闫卫国，王高猛，林济铿，等. 基于AMI量测信息的低压配电网拓扑校验方法 [J]. 中国电力，2019，52(2)：125-133.
[9] 史玉良，张坤，荣以平，等. 智能电网系统中费控服务的优化调度研究 [J]. 计算机学报，2020，43(2)：272-285.
[10] 朱国富，张晓东，闫书芳，等. 基于电力用户用电信息采集系统的智能售用电管理系统的应用及技术 [J]. 电测与仪表，2015，52(S1)：13-16.
[11] 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.
[12] 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.
[13] 吴克河，程瑞，郑碧煌，等. 电力物联网安全通信协议研究 [J]. 信息网络安全，2021，21(9)：8-15.
[14] 王开轩，滕亚均，王琼霄，等. 隐式证书的国密算法应用研究 [J]. 信息网络安全，2021，21(5)：74-81.
[15] 李桐，周小明，任帅，等. 轻量化移动边缘计算双向认证协议 [J]. 信息网络安全，2021，21(11)：58-64.
[16] 曹守启，何鑫，刘婉荣. 一种改进的远程用户身份认证方案 [J]. 计算机工程与科学，2021，43(11)：1959-1965.
[17] 姚志强，竺智荣，叶帼华. 基于密钥协商的防范DHCP中间人攻击方案 [J]. 通信学报，2021，42(8)：103-110.
[18] 程希，曹晓梅. 基于信息携带的SQL注入攻击检测方法 [J]. 计算机科学，2021，48(7)：70-76.
[19] 黄开枝，万政，楼洋明，等. 基于极化码的无协商密钥物理层安全传输方案 [J]. 电子与信息学报，2020，42(12)：2946-2952.

责任编辑 潘春燕