doi :10.3969/j.issn.1671-1122.2021.09.002

电力物联网安全通信协议研究

吴克河，程瑞，郑碧煌，崔文超
（华北电力大学控制与计算机工程学院，北京 102206）

摘　要：为了全面提高电力物联网安全综合防御能力，解决目前电力物联网终端安全防护及终端认证机制的缺失和不足、电力物联网中海量终端安全接入的问题，文章提出一种基于标识密码公钥体制的安全通信协议。该协议以设备指纹和 SM9 算法为基础，使用终端唯一识别标记代替传统的数字证书完成终端身份认证，并将其应用到电力物联网终端的数据加密传输中，最后对该协议进行安全性分析，并与传统电力通信接入网的安全接入协议进行对比。结果表明，文章所提协议能有效防范各类网络攻击，节省计算和网络资源，有效解决海量电力物联网终端的安全接入问题。

关键词：电力物联网；SM9；身份认证；安全接入；密钥协商

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2021）09-0008-08

中文引用格式：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.

英文引用格式：WU Kehe, CHENG Rui, ZHENG Bihuang, et al. Research on Security Communication Protocol of Power Internet of Things[J]. Netinfo Seurity, 2021, 21(9): 8-15.

Research on Security Communication Protocol of Power Internet of Things

WU Kehe, CHENG Rui, ZHENG Bihuang, CUI Wenchao
（*School of Control and Computer Engineering*, *North China Electric Power University*, *Beijing*,102206,*China* ）

Abstract: In order to comprehensively improve the security comprehensive defense capability of power Internet of Things (IoT) and solve the lack of security protection, terminal authentication mechanism of power IoT terminal, this paper proposed a secure communication protocol based on IBC (Identity-based Cryptography) system based on the fingerprint and SM9 algorithm, the terminal identity authentication was completed by using the terminal unique identification mark instead of the traditional digital certificate. It was applied to the data encryption transmission of the power IoT terminal. Finally, the security analysis of the protocol was carried out, and the comparison was made with the traditional power communication access protocol. The results show that the protocol can effectively prevent various network attacks, save computing and network resources, and effectively solve

收稿日期：2021-05-25
基金项目：国家重点研发计划 [2020YFB0905900]
作者简介：吴克河（1962—），男，江苏，教授，博士，主要研究方向为电力信息安全；程瑞（1989—），男，安徽，博士研究生，主要研究方向为网络信息安全；郑碧煌（1995—），女，福建，硕士研究生，主要研究方向为网络信息安全；崔文超（1986—）男，河南，讲师，博士，主要研究方向为软件智能化和网络信息安全。
通信作者：程瑞 chengrui@ncepu.edu.cn

the security access problems of mass power IoT terminals.

Key words: power Internet of Things; SM9; identity authentication; secure access; key agreement

0 引言

电力物联网和能源互联网是密不可分的，电力物联网的网络和信息安全直接涉及能源互联网的生产运行安全，是电网公司网络与信息安全需要考虑的一个重要内容[1]。截至2018年底，国网共接入各类终端5.4亿台（套）[2-4]，已基本实现对电网运行控制信息、用户用电计量信息的全面采集。面对海量异构、多级级联的物联终端设备，如何保证其能安全稳定地接入到电网公司安全防护体系具有重要的研究意义[5-8]。电力物联终端主要包括输变电、配电网、客户侧和供应链等领域终端。文献[9,10]研究了电力物联网的特征以及各个层次面临的安全威胁和攻击模式，并提出了相应的安全防护措施，提出了构建电力物联网安全防护架构。文献[11]针对电网电压监测装置提出了一套标准的信息安全接入规范。文献[12]在文献[11]的基础上提出了一种改进的安全通信协议，通过添加时间戳和数字签名的方式增强了网络通信的安全性。文献[13]基于SM2算法提出一个采用组件技术构建安全加密通道的方案并应用于电力二次系统安全防护。文献[14]针对电力终端接入电力企业内网的安全性问题，提出了一种改进的基于SM2密钥协商体系，确保了通信终端的抗抵赖性。文献[15]提出了一种智能电网终端的安全认证方法。该方法将智能电网终端认证系统结构分层，提高了系统部署的简便性和可扩展性，实现了灵活的通信机制和系统间的交互机制和终端验证的完整。文献[16]综合考虑终端设备的物理层、网络层和协议层异常特征，建立终端设备的画像，刻画终端设备的网络访问状态，结合特定攻击场景，可准确确定仿冒、恶意终端设备，实现异构全业务泛在电力物联网终端安全监控目标。目前电力物联网的安全接入体系仍采用传统的电力通信网安全接入体系中的数字证书方式进行身份识别，但随着电力物联网的推进，大量的电力物联终端接入智慧物联体系，现有的基于数字证书的认证方式计算成本较高，明显不适用于电力物联网。本文在保证通信安全的基础上，提出一种基于SM9算法的身份认证协议，并对提出的协议进行证明与比较，试验表明该方案能有效解决电力物联终端存在的接入问题。

1 相关研究

1.1 PKI 和 IBC 技术

身份认证是密码学理论中的重要研究内容，在传统安全解决方案中，用户的身份认证常采用用户名密码认证或采用PKI/CA技术实现。该方式难以实现对海量用户的支持，同时难以在一些低端的智能设备里面实现，所以很难在物联网安全中得到广泛应用。PKI/CA系统中需要为每个设备、智能终端都颁发数字证书，且在使用过程中需要交换双方的证书，因此，在物联网这种用户数巨大、点对点交互频繁而随机的使用场景下，维护管理大量证书、进行在线交换，整体建设和维护成本非常之高，难以普及。

标识密码系统与传统公钥密码一样，每个用户有一对相关联的公钥和私钥。标识密码系统中，将用户的身份标识，如姓名、IP地址、电子邮箱地址、手机号码等作为公钥，通过数学方式生成与之对应的用户私钥。用户标识是该用户的公钥，不需要额外生成和存储，只需通过某种方式公开发布，私钥则由用户秘密保存。正因为标识密码技术轻管理、易加密等特性，广泛应用于物联网等应用场景[11]。

相比于PKI体系，IBC体系无需数字证书和CA中心，部署方便，适用于海量终端的安全系统，无需PKI中证书验证等计算过程，具备较低的计算代价，适用于计算能力受限的电力终端。

1.2 SM9 算法

我国政府非常重视标识密码算法的发展和应用，

努力从国家标准层面对其进行支持。从2006年开始，国家密码管理局就组织了相关领域的专家开展中国标识密码算法标准规范的制定工作，并于2008年颁发了商密算法型号SM9。2014年进行并完成对标准算法的完善和修改，算法于2016年3月由国家密码管理局正式对外公布，标准号为GM/T 0044-2016。

SM9算法同其他标识密码算法一样，安全性基于椭圆曲线双线性映射的性质，当椭圆曲线离散对数问题和扩域离散对数问题的求解难度相当时，可用椭圆曲线对构造出安全性和实现效率兼顾的基于标识的密码算法。基于SM9的标识密码是一种基于身份的公钥体制，通信双方能够根据彼此身份标识计算出对方的公钥，因而降低了密钥交换和密钥管理的复杂程度。因此，采用基于标识的密码体制的安全防护方法，既能满足电力物联网通信的认证安全需求，也降低了证书管理复杂度，减轻了网络通信带宽负担，适用于海量终端接入的电力物联网体系。在基于SM9标识密码实现的数据加解密算法中，用户的公钥来自身份信息，私钥由KGC生成。只要获得用户A的身份信息，用户B就可以得到用户A的公钥，从而加密一条消息，使之以密文的形式在网络上安全传输给A，A从SM9密钥中心处得到自己的私钥后，即可解密该消息，过程如图1所示。

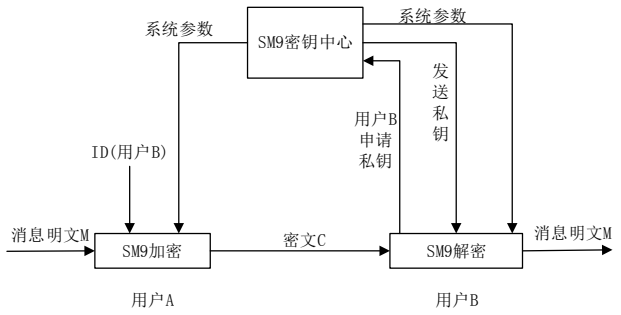

图 1 SM9 加解密示意图

基于SM9标识密码的数字签名是基于标识密码学实现的数字签名。在传统的基于证书的密码体制下，A若想验证B的数字签名，必须首先获得B的证书，通过证书中已有的签名来验证B的身份并通过B的公钥验证签名的有效性。而在基于SM9标识密码算法中，A可以通过直接获取B的身份信息ID来验证B的签名，过程如图2所示。

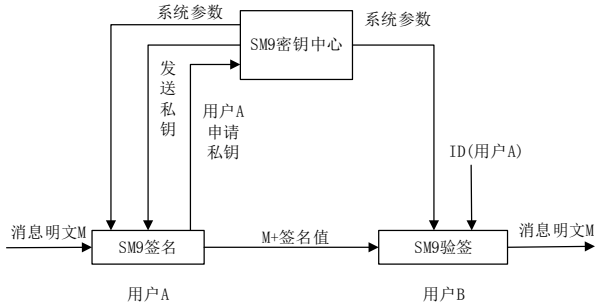

图 2 SM9 签名验签示意图

SM9标识密码算法以电力物联网终端层设备指纹等唯一标识作为公钥，无需数字证书，安全分发专属私钥。SM9标识密码算法与SM3摘要密码算法相结合，实现数据完整性验证与抗抵赖。认证过程无用户名密码传递，杜绝了弱口令、暴力破解、撞库攻击等安全问题，并且因为标识即公钥，无需证书交换认证过程，在安全的前提下，又兼顾了易用性。真正做到以密码技术为核心，从根本上解决物联网的安全问题。

2 基于 SM9 的安全通信协议

基于前文的背景知识，本文提出一种基于SM9算法的电力物联网的安全通信协议，使用SM9算法完成电力终端与物联接入网关之间的身份认证并协商出对称密钥，建立安全通信通道，从而保证数据传输的保密性、完整性以及终端身份的合法性。

2.1 基于 SM9 的加密与签名技术

SM9采用椭圆曲线对实现加解密和签名验签，椭圆曲线对具有双线性的性质，它在椭圆曲线的循环子群与扩域的乘法循环子群之间建立联系，构成了双线性DH、双线性逆DH、ζ-双线性逆DH和ζ-Gap-双线性DH逆等难题，从而保证了SM9算法的安全性和效率。SM9的加解密和签名验签的具体算法描述如下。

1）生成系统参数和主密钥

KGC选择随机数$k\in[1, N-1]$作为系统主私钥，并选取N阶循环子群G_1和G_2以及其生成元P_1、P_2，选择安

全哈希函数H_1, H_2:{0,1}*→Zq*计算出主公钥P_{pub}=k * P_2，KGC公开主公钥P_{pub}和{G_1，G_2，P_1，P_2，H_1，H_2}等参数并秘密保存主私钥k。

2）终端密钥生成

KGC选择并公开用一个字节表示的私钥生成函数识别符hid。为产生终端A的私钥d_A，KGC首先在有限域F_N上计算t_1=H_1(ID_A‖hid, N)+k,其中ID_A为终端A唯一标识，若t_1=0则按照步骤1）重新生成主私钥，否则计算t_2=k *t_1^{-1}，得到终端私钥d_A=[t_2]P_1。

3）数据加密算法

设需要发送的消息为M，加密步骤如下。

（1）计算对端公钥Q_B=[H_1(ID_B‖ hid, N)]P_1 + P_{pub}；

（2）产生随机数r∈[1,N-1]，计算第一部分密文C_1=[r]Q_B；

（3）计算g=e(P_{pub}, P_2)，得到w=g^r；

（4）计算K=KDF(C_1‖w‖ ID_B, $klen$)，若K不全为0，则K=K_1⊕K_2，可得到第二部分密文C_2=M⊕K_1；

（5）计算C_3=MAC(K_2, C_2)，输出密文C=C_1‖C_3‖C_2。

4）数据解密算法

设定收到的密文C=C_1‖C_3‖C_2，解密步骤如下。

（1）验证C_1∈G_1是否成立，若不成立则报错并退出；

（2）令w'=e(C_1, d_B)，计算出K'= KDF (C_1‖w'‖ ID_B, $klen$)，K'=K_1'⊕K_2'，若K'为全0，则报错并退出；

（3）计算M'=C_2⊕K_1'；

（4）计算u=MAC(K_2', C_2)，若u不等于C_3，则报错并退出；

（5）输出明文M'。

5）消息签名算法

设待签名的消息为M，签名步骤如下。

（1）计算群G_r中的元素g=e(P_1, P_{pub})；

（2）产生随机数r∈[1, N–1]，计算h=H_2(M‖g^r, N)；

（3）计算整数L=(r–h) mod N,若L=0则返回出错；

（4）计算群G_1中的元素S=[L]d_A；

（5）输出M的签名为(h, S)。

6）消息验签

对于M'及其数字签名(h', S')，验签步骤如下。

（1）验证h'∈[1, N–1]和S'∈G_1是否成立，若不成立，则验证不通过；

（2）计算g=e(P, P_{pub})，令t=$g^{h'}$、h_1=H_1(ID_A‖hid, N)、P=[h_1]P_2 + P_{pub}；

（3）计算群G_T中的元素u=e(S', P)，w'=u * t，h_2=H_2(M'‖w', N)；

（4）检验h_2=h'是否成立，若成立则验证通过；否则验证不通过。

按照上文中的密钥生成步骤，终端在上线前需完成密钥的发行，密钥由处在信息内网的SM9密钥中心（KGC）根据设备ID和特定算法产生并安全保存到终端安全芯片内部，且不可导出和复制。当电力物联网终端需要接入物联管理平台时，首先要与部署在安全区的接入网关进行通信并完成身份认证并协商出本次会话密钥，该密钥只能用于本次通信数据的加解密且可动态更换。如果在认证过程中出错，网关会关闭与终端的连接，记录失败原因并上传管理平台，避免恶意终端对电力信息内网造成危害。

当终端认证成功后，使用安全芯片对数据进行签名和基于SM1硬件加密算法的对称加密运算，并将密文发送到接入网关，网关验证签名后解密获得明文数据，进而转发给物联管理平台。当超时或解密出错时，关闭通信连接，并通知终端重新发起协商，原对称密钥作废。

安全通信协议包括密钥协商协议和数据加密协议，下面分别对其进行阐述。

2.2 密钥协商协议

终端与网关建立TCP连接之后，需要立即与远端进行会话密钥协商，只有协商好会话密钥之后，才能进行后续的数据加密通信，在密钥协商完成之前，不得进行任何其他数据信息（非密钥协商的数据信息）的发送，否则，TCP连接将被关闭。本文设计的密钥协商的过程如图3所示。

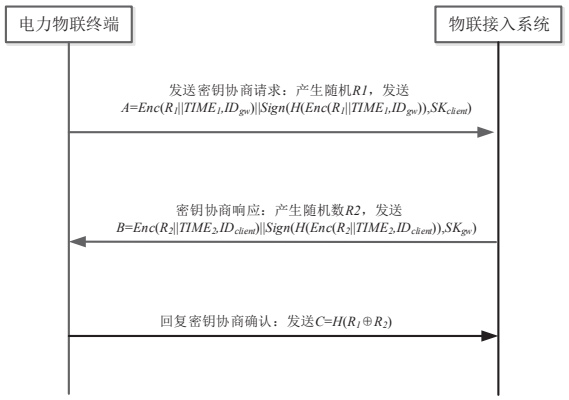

图 3 密钥协商交互

密钥协商分为协商请求、协商回复和协商确认，其中，终端发起协商请求，网关进行回应，最后由终端发送协商确认，具体步骤如下。

1）终端发送密钥协商请求。密钥协商请求报文格式如表1所示。利用芯片生成真随机数，该随机数作为会话密钥的一部分参与后面运算，并使用预置的网关ID对随机数和时间戳按照前面的加密步骤进行SM9非对称加密，得到密文$C_1=Enc(R_1\|TIME_1, ID_{gw})$。为了确保消息的不可抵赖性，需对原始报文进行签名处理，使用SM3算法对请求报文$REQ_1=(Type \| SubType \| Len \| Ver \| SN \| SIM \| ID_{client} \| C_1)$摘要运算得到$M_1=SM3(REQ_1)$，最后使用SM9私钥对$M_1$进行签名处理$S_1=Sign(M_1, SK_{client})$，将密文和签名值按照表1既定的报文格式发送到物联接入网关。

表 1 密钥协商请求报文格式

名称	说明
类型	密钥协商类型
子类型	密钥协商第一步
长度	数据总长度
版本号	版本号
SN	客户端随机分配的序列号
SIM 卡号	SIM 卡卡号
设备 ID	终端唯一 ID 号（芯片 ID）
$Enc(R_1\|\|TIME_1, ID_{gw})$	随机数和时间戳的密文
$Sign(Hash(REQ_1), SK_{client})$	本端私钥签名

2）网关处理请求并响应。网关收到终端数据后，首先根据报文类型判断消息合法性，若在协商阶段收到其他类型的数据则直接丢弃。对于正常的协商请求，网关使用私钥解密获得R_1与时间戳，判断时间是否新鲜，通过后则利用对应终端ID_{client}对签名数据进行验签处理；验签失败则上传日志并断开连接；验签成功后，网关保存终端的随机数R_1并生成随机数R_2，并使用对应终端的ID_{client}对R_2和时间戳进行加密得到密文$C_2=Enc(R_2\|TIME_2, ID_{client})$，网关发送的报文同样需要保证不可抵赖性，使用SM3算法对响应报文$REQ_2=(Type||SubType||Len||SN+1||C_2)$进行哈希运算得到$M_2$=SM3($REQ_2$)，对$M_2$签名得到签名值$S_2=Sign(M_2, SK_{gw})$，最后按照表2定义的报文格式将密文和签名值发给对应的终端同时合成会话密钥$DK=R_1\oplus R_2$。

表 2 密钥协商响应报文格式

名称	说明
类型	密钥协商类型
子类型	密钥协商第一步
长度	数据总长度
版本号	版本号
SN+1	序列号
$Enc(R_2\|\|TIME_2, ID_{client})$	对端 ID 加密随机数和时间戳
$Sign(\text{SM3}(REQ_2), SK_{gw})$	本端私钥签名

3）终端进行协商确认。终端收到合法协商确认包后，利用终端私钥解密获得网关随机数R_2和$TIME_2$，验证时间新鲜度，并对报文进行验签运算，验签成功后合成会话密钥$DK=R_1\oplus R_2$，最后对合成的DK值进行哈希处理得到M_3=SM3(DK)并发送网关。密钥确认报文格式如表3所示。

表 3 密钥协商确认报文格式

名称	说明
类型	密钥协商类型
子类型	密钥协商第一步
长度	数据总长度
版本号	版本号
SN+2	序列号
$TIME_3$	本地时间戳
SM3(R_1^R_2)	哈希值

4）网关协商确认。网关收到确认包后，首先进行新鲜度判断，并比较接收到的哈希值与自己计算的DK哈希值是否一致，此步骤是为了确保终端能收到正确的网关随机数，防止消息被篡改。若哈希值一致，表面双方各自拥有对端的正确随机数，协商成功后建立终端到物联管理平台的安全通信通道，否则网关上报

接入日志并关闭连接。

2.3 数据加密协议

采用基于商密算法的数据传输能有效保证数据的保密性和完整性。密文通信的格式如表4所示。

表 4 密文传输数据格式

名称	说明
类型	密文通信
子类型	无
长度	总长度
IV	随机 IV
TIME	当前时间戳
密文数据	加密报文
签名值	对报文进行哈希运算之后的签名值

当完成密钥协商的过程后，终端开始传输加密报文，物联接入网关收到报文后，首先使用密钥协商过程中生成的对称密钥DK和密文报文中的随机IV向量对密文数据进行SM1解密；解密完成后根据填充规则去掉解密后的数据里面的填充位，获得明文数据后，判断时间新鲜度，再进行数据验签；验签成功后，进行数据解密，随之将解密后的明文发送给物联管理平台。当物联接入网关收到物管平台返回的控制指令或报文响应时，首先需要将明文报文和当前时间填充成满足加密格式要求的报文并利用DK值和随机生成的IV向量对填充后的报文进行SM1加密，并利用自己的私钥进行签名操作，最后将加密报文和签名值发送给对应的终端。加密过程如图4所示。

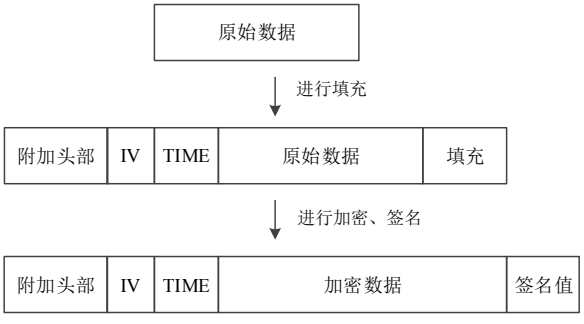

图 4 数据加密过程

3 协议安全性分析

1）重放攻击

在设计的通信协议中，通信双方会将自己的时间戳和签名值作为会话新鲜度标识发送给对端，对端收到报文后必须对新鲜度进行判断和验证，如新鲜度超时，便关闭本次会话，若达到重放阈值可直接阻断对端通信IP并上报物联平台；这对于重放攻击具有很好的抵抗性。

2）报文篡改

在通信的过程中，双方都会使用SM3算法对消息做摘要处理，并使用SM9对摘要做签名处理，若攻击者对报文进行修改，则对端在验证签名时会出错，从而可以防止非法数据进入内网，保证了数据的完整性和不可抵赖性。

3）中间人攻击

攻击者通过代理手段获取双方的通信数据，由于缺少通信双方使用的私钥和会话密钥，无法对通信数据进行解密处理，并且通信报文含有时间戳作为新鲜度，有效保证数据的保密性。

4）消息注入

本文提出的方案在身份认证和密钥协商完成后，在终端和物联平台之间建立了一条加密通道，会话密钥仅由已完成身份认证的用户知晓，攻击者无法获取共享会话密钥，无法进行数据解密并插入恶意信息，即使插入非法数据,对端无法通过验签或解密,该错误数据被丢弃。

5）完全正向保密

完全正向保密要求一个密钥只能访问由它所保护的数据，用来产生密钥的元素一次一换，不能再产生其他的密钥。一个密钥被破解，并不影响其他密钥的安全性。本文提出的通信协议具备此特性，根据双方的随机数可动态创建新密钥，由于双方都提供了一个在密钥协商时只有对方才知道的随机值，因此生成的每个新密钥都不同于先前创建的密钥。即使对方拦截了密钥，也不能长时间使用拦截密钥。另外，由于新密钥通过密钥协商产生，而不是从之前生成的密钥中获得的，因此敌手无法获得可用的会话密钥。

4 实验

本实验应用层的仿真在64位Centos下，采用C语言实现本文提出的安全通信协议并测试其安全性。另外使用安全网关和模拟终端服务器来测试并发终端的接入

处理时间。安全网关和模拟终端服务器运行在同等配置（Intel（R）Xeon CPU E3-1230 V3@3.40GHz）服务器上。图5为测试用的网络拓扑图。

图 5 测试拓扑图

实验在模拟终端服务器和接入网关上实现了认证和密钥协商过程。密钥协商请求核心代码如下。

```
//用网关ID加密随机数和时间戳
Create_Random (rand_c, 16 );
Get_CurrentTime (rand_c + 16 );
Sm9_Encrypt ( ID_GW, rand_c, 30, Buffer+41);
//拼包处理
Buffer[TYPE] = 0x01; Buffer[SUBTYPE] = 0x01;
*((u16 *)(Buffer + LENGTH)) = Change_Int(Length);
*((u16 *)(Buffer + VER)) = Change_Int(0x0100);
*((u16 *)(Buffer + SN_REQ)) = Change_Int(8000);
memcpy(Buffer + IDX_SIM_CARD_ID, SIM_ID, 16);
memcpy(Buffer + IDX_DEVICE_ID, CHIP_ID, 16);
TempBuffer = Buffer + Length–64;
//SM9签名运算
Sm3(Buffer, Length–64, TempBuffer);
Sm9_Sign(SK_CLIENT,TempBuffer, Buffer + 165);
```

网关收到密钥协商请求报文后采用SM9算法验证并发送密钥协商响应报文，密钥协商响应核心代码如下。

```
//使用私钥解密报文获取随机数和时间戳
Sm9_Decrypt (SK_GW, Buffer, rand_c);
//新鲜度比较
strcmp (rand_c+16,Get_CurrentTime (Time));
//使用公钥验签
Sm3(Buffer, Length–64, TempBuffer );
Sm9_Verify (ID_CLIENT, TempBuffer, Buffer+165 );
//用对应终端ID加密随机数和时间戳
Create_Random (rand_s, 16);
Get_CurrentTime (rand_s+16);
Sm9_Encrypt (ID_CLIENT, rand_s, 30, Buffer+8 );
//拼包处理
Buffer[TYPE] = 0x01; Buffer[SUBTYPE] = 0x02;
*((u16 *)( Buffer + LENGTH )) = Change_Int(Length );
*((u16 *)(Buffer + VER)) = Change_Int (0x0100 );
*((u16 *)(Buffer + SN_REQ)) = Change_Int(8001);
TempBuffer = Buffer + Length–64;
//SM9签名运算
Sm3(Buffer, Length–64, TempBuffer);
Sm9_Sign(SK_GW, TempBuffer, Buffer+133);
//合成会话密钥
DK=XOR(rand_c, rand_s, 16);
```

终端对密钥协商响应报文进行确认，最终发送密钥协商确认报文，确认报文的核心代码如下。

```
//使用私钥解密报文获取随机数和时间戳
Sm9_Decrypt(SK_CLIENT, Buffer, rand_s);
//新鲜度比较
strcmp(rand_s+16, Get_CurrentTime(Time));
//使用公钥验签
Sm3(Buffer, Length–64, TempBuffer);
Sm9_Verify(ID_GW, TempBuffer, Buffer + 133);
//获取会话密钥
DK=XOR(rand_c, rand_s, 16);
//拼包处理
Buffer[TYPE] = 0x01;Buffer[SUBTYPE] = 0x03;
*((u16 *)(Buffer + LENGTH)) = Change_Int(Length);
*((u16 *)(Buffer + VER)) = Change_Int(0x0100);
*((u16 *)(Buffer + SN_REQ)) = Change_Int(8002);
//杂凑运算
Sm3(Buffer, Length–32, TempBuffer);
memcpy(Buffer+Length–64, TempBuffer, 32);
```

为了对比海量终端接入的执行时间，在同样网络环境和主机配置的前提下，分别实现文献[11]和文献[12]的安全协议。图6显示了3种方案的执行时间对比。随着终端数目的增加，文献[11]方案和文献[12]方案的执行时间明显增加。

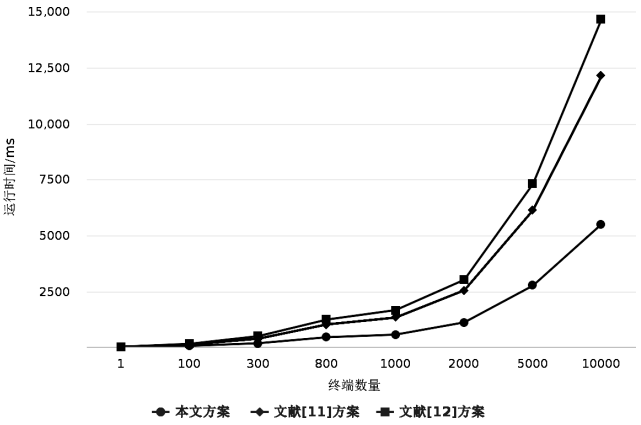

图 6 实验对比图

相比之下，本文方案在保证安全的基础上，一次完整的密钥协商只需约500字节的通信消耗，而其他

两种方案至少需要传输1500字节。本文方案占用更少的通信资源和计算资源，因此执行时间相对较低，效率更高，更适合海量终端的安全接入。

5 结束语

本文在研究标识密码公钥体制的基础上，结合SM9算法提出针对海量电力物联终端接入的安全通信协议，使用身份标识替代数字证书，能节省大量计算资源和通信资源，更适合资源受限的电力终端使用；同时通过在协议中添加时间戳和签名机制，提高了报文传输的安全性。最后对提出的协议进行安全性分析，表明可防范多种网络攻击，有效保证通信过程中的数据完整和终端可靠性。最后采用C语言进行实现并与其他几种通信协议进行对比，实验结果表明本文提出的方案在效率和性能上更具优势。

参考文献：

[1] State Grid Corporation of China. Ubiquitous Electricity Internet of Things White Paper 2019[EB/OL]. http://www.lianmenhu.com/blockchain-14145-1, 2019-10-16.

中国人民共和国国家电网有限公司 . 泛在电力物联网白皮书 2019[EB/OL]. http://www.lianmenhu.com/blockchain-14145-1，2019-10-16.

[2] ZHAO Mengmeng, TANG Pingzhou, SUN Kun. Development and Prospect of Ubiquitous Power Internet of Things[J]. Journal of North China Electric Power University, 2020, 47(5): 63-74.

赵萌萌，唐平舟，孙堃 . 泛在电力物联网发展与展望 [J]. 华北电力大学学报，2020，47（5）：63-74.

[3] LIU Lin, QI Bing, LI Shan. Demand and Development Trend of Power Communication Network for New Business of Power Internet of Things[J]. Power Grid Technology, 2020, 44(8): 3114-3128.

刘林，祁兵，李姗 . 面向电力物联网新业务的电力通信网需求及发展趋势 [J]. 电网技术，2020，44（8）：3114-3128.

[4] WANG Siqi. Research on Smart Grid Monitoring System Based on Internet of Things[J]. Chinese Journal of Power Sources, 2018, 42(1): 125-127.

王思齐 . 基于物联网的智能电网监控系统研究 [J]. 电源技术，2018，42（1）：125-127.

[5] CHEN Xin, JIANG Yizhe, WANG Xue, et al. Research on the Development of Energy Internet from the Internet Perspective[J]. China Power, 2018, 51(8): 43-48.

陈昕，姜怡喆，王雪，等 . 互联网视角下的能源互联网发展研究 [J]. 中国电力，2018，51（8）：43-48.

[6] ZHOU Feng, ZHOU Hui, DIAO Yinglong. Thoughts on the Development of Key Technologies for Intelligent Perception in Ubiquitous Electricity Internet of Things[J]. Chinese Journal Electrical Engineering, 2020, 40(1): 70-82.

周峰，周晖，刁赢龙 . 泛在电力物联网智能感知关键技术发展思路 [J]. 中国电机工程学报，2020，40（1）：70-82.

[7] SHEN Bo, CAI Zexiang, DAI Guanquan, et al. Communication Analysis of Intelligent Power Distribution Information Collection Service for Ubiquitous Power IoT[J]. Electric Power Construction, 2019, 40(9): 27-34.

沈博，蔡泽祥，戴观权，等 . 面向泛在电力物联网的智能配用电信息采集业务通信分析 [J]. 电力建设，2019，40（9）：27-34.

[8] YANG Ting, ZHAI Feng, ZHAO Yingjie, et al. Definition and Research Prospect of Ubiquitous Electricity Internet of Things[J]. Automation of Electric Power Systems, 2019, 43(13): 9-20.

杨挺，翟峰，赵英杰，等 . 泛在电力物联网释义与研究展望 [J]. 电力系统自动化，2019，43（13）：9-20.

[9] KIMANI K, ODUOL V, LANGAT K. Cyber Security Challenges for IoT-based Smart Grid Networks[J]. International Journal of Critical Infrastructure Protection, 2019, 25(6): 36-49.

[10] SHRESTHA M, JOHANSEN C, NOLL J, et al. A Methodology for Security Classification Applied to Smart Grid Infrastructures[J]. International Journal of Critical Infrastructure Protection, 2020, 28(3): 1-19.

[11] Q/GDW11118-2013 Specification for Information Security Access of Voltage Monitoringdevices Based on Wireless APN Virtual Private Network[S]. Beijing: China National Standard Press, 2014.

Q/GDW11118-2013 基于无线 APN 虚拟专网的电压监测装置信息安全接入规范 [S]. 北京：中国标准出版社，2014.

[12] LIN Nan, CHEN Zuosong, ZUO Liming, et al. Security Analysis and Improvement of Access Protocol of Power Grid Voltage Monitoring Device[J]. Computer Engineering and Design, 2019, 40(11): 3085-3089.

林楠，陈祚松，左黎明，等 . 电网电压监测装置接入协议安全分析与改进 [J]. 计算机工程与设计，2019，40（11）：3085-3089.

[13] LUO Zhao, XIE Jihua, GU Wei, et al. Development of Power Grid Information Security Support Platform Based on SM2 Cryptosystem[J]. Automation of Electric Power Systems, 2014, 38(6): 68-74.

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.

[14] LI Wei, LI Rui, WU Kehe, et al. Design and Implementation of an SM2-based Security Authentication Scheme with the Key Agreement for Smart Grid Communications[J]. IEEE Access, 2018, 6(10): 71194-71207.

[15] WANG Yufeng, WU Lie, YANG Yun. Security Authentication Method of Terminal Trusted Access in Smart Grid[J]. International Journal of Security and its Applications, 2015, 9(7): 337-346.

[16] LU Qiong, CUI Wenchao. Research on Security Monitoring and Analysis Technology of Ubiquitous Power Internet of Things Terminal Layer[J]. Information Technology, 2020, 44(2): 121-125.

卢琼，崔文超 . 泛在电力物联网终端层安全监测分析技术研究 [J]. 信息技术，2020，44（2）：121-125.