DOI: 10.7667/PSPC170813

基于 SM2 的配电网 Modbus 报文安全性研究

邹晓峰[1]，肖远兴[2]

(1. 国网上海市电力公司电力科学研究院，上海 200437；2. 上海欣能信息科技发展有限公司，上海 200025)

摘要：配电网信息系统采用国产安全算法，能避免国外算法可能存在的后门陷阱。提出一种应用于配电网 Modbus 报文的国密 SM2 安全方法。研究配电网信息系统的特点，分析非对称加密算法的特点以及国密算法 SM2 在配电网 Modbus 报文的适用性。采用 SM2 进行配电网信息系统的密钥在线管理，进而重点研究采用国密 SM2 算法对配电网 Modbus 报文进行数字签名，保证配电网信息的真实性和不可抵赖性。搭建实验平台测试基于 SM2 的密钥管理和配电网 MODBUS 报文交换情况。测试结果表明基于 SM2 的配电网信息系统能同时满足安全性和实时性要求。

关键词：配电网；通信网络；密码技术；国密算法；非对称加密

Modbus telegram security of distribution network based on SM2

ZOU Xiaofeng[1], XIAO Yuanxing[2]

(1. State Grid Shanghai Electric Power Research Institute, Shanghai 200437, China;
2. Shanghai Shineenergy Information Technology Development Co., Ltd., Shanghai 200025, China)

Abstract: Distribution network information system uses domestic security algorithm, avoiding the possible back door trap that may exist in foreign algorithms. A national cryptographic algorithm SM2 for Modbus telegrams in distribution networks is proposed. The characteristics of distribution network information system are studied. The characteristics of the asymmetric encryption algorithm and the applicability of the national cryptographic algorithm SM2 in the distribution network Modbus are analyzed. On-line key management of distribution network information system based on SM2 is adopted. Digitally signing Modbus telegrams of distribution network based on SM2 to ensure the authenticity and non-repudiation of distribution network information are elaborated. The experimental platform to test the SM2-based key management and distribution network Modbus telegram exchange is set up. The test results show that the SM2-based distribution network information system can meet the security and real-time requirements at the same time.

This work is supported by Science and Technology Project of Shanghai Electric Power Company (No. 52094015001V).

Key words: distribution network; communication network; cryptographic technique; national cryptographic algorithm; asymmetric encryption algorithm

0 引言

现代社会信息技术的进步，使计算机通信网络成为电力系统自动化的主要技术支撑平台，智能电网对信息通信网络的依赖性也日益增强。安全、可靠的通信系统是智能配电网系统实现的关键环节[1-2]，配电网各类智能终端的通信安全功能，由原来的“最好有”逐步变成“必须有”[3-5]。非对称密钥算法由于报文的发送方和接收方采用不同的密钥，密钥易于管理，成为配电网通信主要的安全技术。

国际上经典的非对称密钥算法主要有 RSA、Elgamal、背包算法、Rabin、HD 和 ECC 等[5]，但这些算法的陷阱后门问题至今还存在争议，对于电力系统这种关系国计民生的信息安全领域，应用我国自行掌握的核心算法确保电力系统信息安全具有重要意义。

本文根据配电网自动化系统的通信形式，结合配电网报文的结构特点，采用我国自主研发的 SM2 非对称密码技术，研究适用于配电网报文的安全方法。

基金项目：上海电力公司科技项目资助(52094015001V)

1　配电网自动化系统

作为用电端和电力系统末端相邻的纽扣环节，配电网具有地理分布广泛、通信方式多样化和情况复杂等特点[6]。不同地区的配电网各类自动化终端通常就近放置在配电网一次系统，并经通信网络与本地区的其他配电网终端交互，或接入路由器后与配电网主站或其他地区的配电网终端交换信息，经典的配电网自动化系统如图 1 所示[7]。

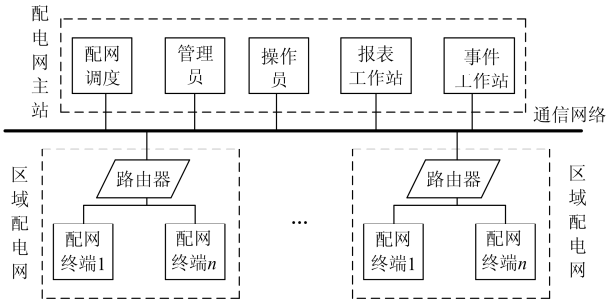


图 1 配电网自动化系统

Fig. 1 Automation system of distribution network

通信方式可能根据配电网具体情况，采用 GPRS/3G/4G 等无线方式或是光纤以太网、CAN 总线等有线形式，甚至采用有线和无线混合的灵活通信方式。无论采用何种远程通信方式，配电网自动化系统的通信报文内容都应该是没有遭受第三方篡改等恶意攻击的。基于现代密码技术的安全算法是保障报文真实有效的基本手段。

基于对称密钥机制的配电网信息加密方法，由于信息的发送端和接收端共用相同的密钥，存在身份认证困难、信息源难以确定和信息不具有不可否认性等问题；而非对称密钥算法不存在上述技术难题，随着配电网终端计算能力提高，并结合配电网报文结构进行安全算法优化，有望减少报文非对称加解密算法的耗时从而满足配电网信息系统的实时性要求[8]。

2　国密 SM2 算法

为了防止国际上经典的非对称加密算法存在后门等安全隐患，国家密码管理局于 2010 年提出了国家商用密码算法 SM2，并规定从 2011 年 7 月 1 日起，新研制的含有公钥密码算法的商用密码产品必须支持 SM2 算法，即国密 SM2 算法[9]。SM2 算法与 ECC 算法具有相同原理，但对 ECC 算法进行了优化，采取了更为安全的机制，同时 SM2 算法不像 ECC 算法那样对密钥长度和明文长度有严格要求，具有更优的灵活性、效率和安全性[10]。

SM2 标准包括总则、数字签名算法、密钥交换协议、公钥加密算法 4 个部分。总则规定了 SM2 算法的概要，数字签名算法、密钥交换协议以及公钥加密算法等 3 个部分分别详细介绍了 SM2 在各个领域的具体实现方法[11]。

对配电网报文采用数字签名方法，不仅可以保证配电网报文内容的完整性，防止报文信息遭受第三方恶意篡改，而且可以明确报文的来源，由于只有真实的报文发送方拥有私钥才能签发采用数字签名的报文，具有不可抵赖性[12]。

3　基于 SM2 的 Modbus 报文数字签名方法

配电网系统愈发依赖通信网络，以网络报文的形式来实现配电网的报文交换，逐步实现智能化功能。尽管 IEC61850 协议具有强大的功能，学术界已开始研究 IEC61850 协议在智能配电网中应用，但由于 IEC61850 协议是个庞大的电力自动化通信系统，实现较为复杂[13]。当前配电网系统实际应用中，还普遍采用 Modbus 通信协议。

Modbus 实现简单，通信协议效率高。Modbus 通信协议采用主从(Master-Slave)的通信模式；报文格式紧凑，而且具有良好的灵活性，可以根据具体应用场合的差异性，在报文格式上稍微调整。根据报文结构的差异性，Modbus 主要有 Modbus RTU 和 Modbus TCP 两种形式。

Modbus RTU 报文结构相对简单，如图 2 所示，Modbus RTU 报文结构由地址域(1 个字节)，功能码(1 个字节)，数据域(L+2 个字节，由具体应用场合需要决定其长度)和校验码(2 个字节)四部分组成。为了便于区分通信起止，采用不小于 3.5 个字节的空闲时间作为指令的起始和结束。

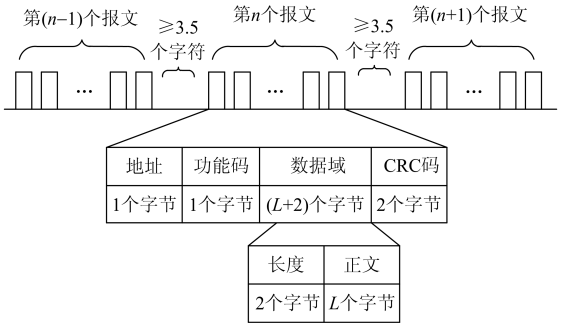


图 2 配电网 Modbus RTU 报文结构

Fig. 2 Modbus RTU packet structure of distribution network

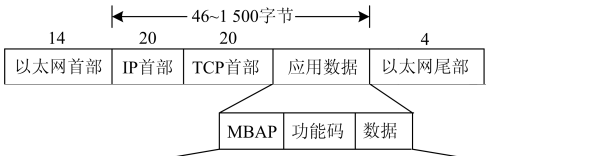
其中智能配电网 Modbus 报文的数据域表征配电网实质信息，是整个报文核心的主体内容。该数据域由数据长度(2 个字节，表征数据正文内容的长

度，假定数据内容的长度为 L)和数据正文内容(数据正文内容的长度为 L 字节)组成。

Modbus RTU 采用两个字节长度的 CRC 码作为报文验证码，需要注意的是，该 CRC 验证码只能识别通信网络噪音引起的误码，但无法有效地抵抗第三方恶意篡改等网络攻击。

Modbus RTU 通常应用于 RS485 总线等速率较低的串行通信方式，所以报文结构尽可能精简，几乎没有数据冗余。同时 RS485 总线在工业现场中只适用于不超百米的短距离应用场合，遭受网络恶意攻击的风险相对较低；而采用国密 SM2 方法实现配电网 Modbus 报文的数字签名产生的报文摘要，长度将占据原报文较大比重，甚至长于源报文。因此，重点考虑 Modbus TCP 报文采用基于 SM2 的数字签名方法。

Modbus TCP 基于以太网 TCP/IP 通信方式，网络速度快，可以传送更多的配电网报文内容。Modbus TCP 作为 TCP/IP 一种具体应用方式，跟经典的 TCP/IP 协议族一样，是一组不同的协议组合在一起构成的四层协议系统，包括 14 个字节的以太网首部、20 个字节的 IP 首部和 20 个字节的 TCP 首部等经典的报文结构，如图 3 所示。



域	长度(B)	描述	客户端	服务器端
传输标志	2	标志某个Modbus询问/应答的传输	由客户端生成	应答时复制该值
协议标志	2	0=Modbus协议 1=UNI-TE协议	由客户端生成	应答时复制该值
长度	2	后续字节数计数	由客户端生成	应答时由服务器端重新生成
单元标志	1	定义连续于目的其他设备	由客户端生成	应答时复制该值

图 3 配电网 Modbus TCP 报文结构

Fig. 3 Modbus TCP packet structure of distribution network

除了经典 TCP/IP 所包含的上述报文结构，Modbus TCP 的关键数据主要体现在应用层。Modbus TCP 应用层部分的报文形式与 Modbus RTU 的报文结构类似，并根据 TCP 格式做了针对性的修改，Modbus TCP 协议前面添加 7 个字节长度 MBAP 报文头。

MBAP 报文头由 2 个字节的事务元标识符、2 个字节的协议标识符、2 个字节的数据帧长度和 1 个字节的单元标识符组成。事务元标识符用以识别该报文是请求报文还是响应报文；协议标识符用以判断协议类型，其中置于 0 为 Modbus 协议，置于 1 为 UNI-TE 协议；数据帧长度用以区分可变长度数据帧结束的数据帧长度；单元标识符用于标识从站地址。

Modbus TCP 与 Modbus RTU 不同的是，从站地址放在了 MBAP 帧头里，同时去掉 Modbus RTU 的从机地址。Modbus TCP 协议层的功能码、数据域两个报文域格式上虽然和 Modbus RTU 相同，但由于 Modbus TCP 基于高宽带的以太网，实际应用中可以传送更多字节的报文内容。

利用 Modbus TCP 一个报文就可以包含高达 1 500 字节的报文长度，完全可以消纳配电网报文数字签名产生的报文摘要。因此，采用国密 SM2 算法对配电网 Modbus TCP 数据域进行数字签名，以保证报文信息的安全性，数字签名的报文摘要增添在原报文的数据域后端部分，如图 3 所示，同时，根据数字签名的报文摘要长度，对应的修改 MBAP 报文头的数据帧长度。

4　基于 SM2 直接加密的配电网密钥交换

由于配电网地理分布广泛和电气设备类型多样化，智能电子设备能灵活接入配电网，可以减少设备的调试和运行成本[14]。智能电子设备具有即插即用功能的 SM2 安全模块能加强应用的方便性，首先体现在智能电子设备接入配电网信息系统中，智能电子设备与配电网主站信息系统的通信初始化过程，而其关键环节就是密钥的安全交换[15]。

研究智能配电网信息系统和智能电子设备采用 SM2 非对称加密算法进行的密钥交换，如图 4 所示，具体流程包括：

1) 智能电子设备接入智能配电网通信系统后，根据预先输入的智能配电网主站安全模块的通信地

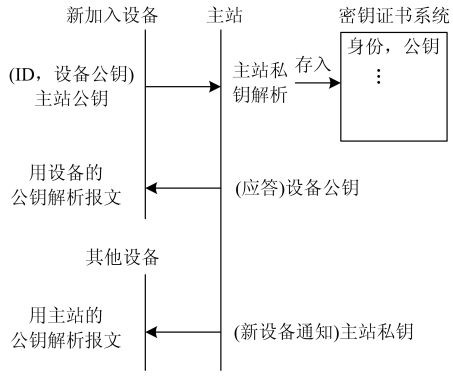


图 4 基于 SM2 配电网密钥交换

Fig. 4 Distribution network key exchange based on SM2

址和公钥，将自身的身份、公钥等信息，用主站的公钥加密后将上述信息通过通信网络发送到主站安全模块。

2) 主站安全模块接收到智能电子设备用主站安全模块公钥加密的报文后，用自身的私钥对该报文进行解密，并确认该信息的真实性。一旦判断该信息是可信的，则将新加入的智能电子设备身份和公钥信息加入到主站统一管理的密钥证书系统中。同时，主站安全模块将已确认该智能电子设备的答复信息发送到该智能电子设备。

3) 主站安全模块通过广播的方式，将新加入的智能电子设备通知当前智能配电网系统中运行的所有智能电子设备，并随时提供智能电子设备的公钥供有需要的智能电子设备查询。

4) 新加入的智能电子设备收到主站安全模块的认证信息后，向主站安全模块查询准备与之通信的智能电子设备的通信地址和公钥，并妥善保存。接收到特定智能电子设备的报文时，只需调用该智能电子设备的公钥对报文进行解密和认证。

在不影响当前智能配电网正常运行的前提下，通过上述初始化过程，新加入的智能电子设备以即插即用的方式自动地加入在线运行的智能配电网系统。

5 基于 SM2 数字签名的配电网报文认证

对配电网报文采用 SM2 数字签名方法，可以实现报文的完整性和不可抵赖性等安全目标。发送方实现签名功能，对待发送的报文信息通过哈希算法获得报文摘要，进而采用发送端的密钥对报文摘要进行数字签名，将签名结果增添到原报文，伴随原报文发送到接收端。接收方实现验证功能，对收到的报文通过哈希算法获得计算的报文摘要；同时用接收方的公钥对增添在原报文的签名结果进行解密，并与计算的报文摘要作比较，通过验证两个报文摘要是否一致判断报文的真实性[16]。

报文发送端和接收端的主要流程如图 5 所示。报文发送端 SM2 算法采用离散椭圆曲线的离散对数原理，对拟发送的配电网报文进行签名，主要包括 SM3 哈希运算和基于发送端私钥的 SM2 加密过程，主要步骤包括：

1) 对报文进行 SM3 哈希算法获取报文信息摘要，进而用发送端的私钥对信息摘要进行 SM2 非对称加密。

2) 根据椭圆曲线上的基点，采用随机数发生器生成随机数 k。

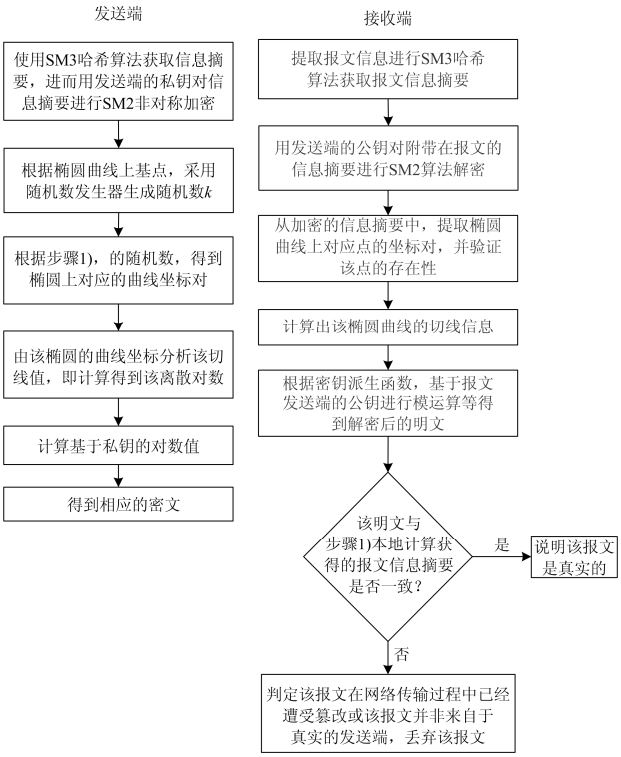


图 5 SM2 配电网报文数字签名方法

Fig. 5 SM2 digital signature method for distribution network

3) 根据步骤 1)的随机数，得到椭圆上对应的曲线坐标对。

4) 根据该椭圆的曲线坐标分析该切线值，即计算得到该离散对数。

5) 进一步计算基于私钥的对数值。

6) 得到相应的密文，作为配电网报文的信息摘要输出。

智能配电网接收端对所接收的报文进行验证，以判断是否来自于真实的发送端，涉及 SM3 哈希运算和基于发送端公钥的 SM2 解密过程，具体包括：

1) 提取报文信息进行 SM3 哈希算法获取报文信息摘要。

2) 用发送端的公钥对附带在报文的信息摘要进行 SM2 算法解密。

3) 从加密的信息摘要中，提取椭圆曲线上对应点的坐标对，并验证该点的存在性。

4) 计算出该椭圆曲线的切线信息。

5) 根据密钥派生函数，基于报文发送端的公钥进行模运算等得到解密后的明文。

6) 该明文作为报文接收端采用公钥解密所接收的配电网报文的信息摘要明文，与步骤 1)本地计算获得的报文信息摘要进行一致性比较。

7) 如果步骤 6)的比较结果相同，说明所接收的

报文是真实的；反之，则可判定该报文在网络传输过程中已经遭受篡改或该报文并非来自于真实的发送端，丢弃该报文。

6　实验测试

搭建基于以太网的配电网信息系统，5 台工控机通过以太网交换机接入到该总线系统中，如图 6 所示。5 台工控机采用性能完全一样的 PC 机，重要的参数包括：4 GB 内存，CPU 主频最高至 3.70 GHz 的 i3-6100 处理器；网口采用自适应的百兆以太网卡。

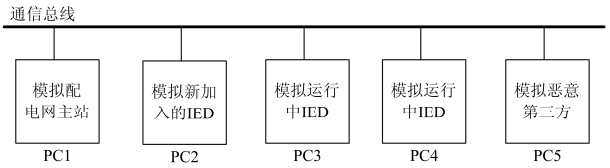


图 6 配电网测试平台

Fig. 6 Test platform of distribution network

其中 1 台工控机 PC1 模拟配电网主站，1 台工控机模拟新加入 PC2 的配电网智能电子设备，2 台工控机模拟 PC3、PC4 已经在线运行的配电网智能电子设备，1 台工控机 PC5 模拟试图进行网络攻击的恶意第三方。

6.1 SM2 加解密算法实验

首先随机生成一个长度为 32 字节 SM2 私钥。由 SM2 非对称加密算法原理可知，公钥是 SM2 曲线上的一个长度为 64 字节的曲线坐标点，由横坐标和纵坐标(x, y)两个分量来表示；在 X.509 证书中，SM2 公钥表示为 04 标记开始的 2 个 32 byte 的 BigInteger。

本文为了理解方便，采用坐标(x, y)方法来表示 SM2 公钥。随机生成的私钥以及对应的公钥后，输入配电网 Modbus TCP 报文应用层数据域作为采用 SM2 非对称加密的明文，产生对应的密文，如图 7 所示。

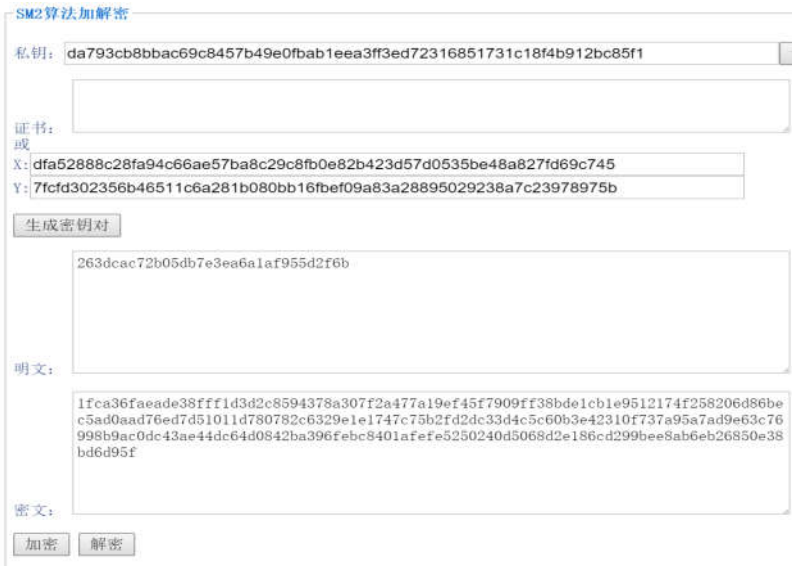


图 7 SM2 加解密实例

Fig. 7 Encryption and decryption example based on SM2

从实验结果首先可以直观看到，明文信息跟密文信息已完全不同，密文长度比明文长度要大很大。按国密 SM2 算法推荐的 256 位椭圆曲线，明文加密结果会比原长度会大 96 byte[17-18]。

具体分析密文的信息组成，根据国密 SM2 推荐的椭圆曲线公钥密码算法，首先产生随机数计算出椭圆曲线上的一个坐标点，该坐标点由 2 个 32 byte 的 BigInteger 大数，这是 SM2 加密结果的第 1 部分；第 2 部分则是真正的密文，是对明文的加密结果，长度和明文一样；第 3 部分是杂凑值，用来效验数据。

可以看出，SM2 加密算法比 ECC 等非对称加密算法具有更好的安全性，实现上也稍微复杂。当密钥和明文确定后，ECC 等非对称加密算法得到的密文是固定的。但 SM2 非对称加密算法比较特殊，如图 8 所示。

图 8 所示的明文和密钥与图 7 的一样，但所生成的密文完全不一样。这是因为 SM2 加密结果由 3 个部分组成，第 1 部分使用了随机数，因此即使同样的密钥和明文情况下，每次加密所得到的密文结果都可能不一样。

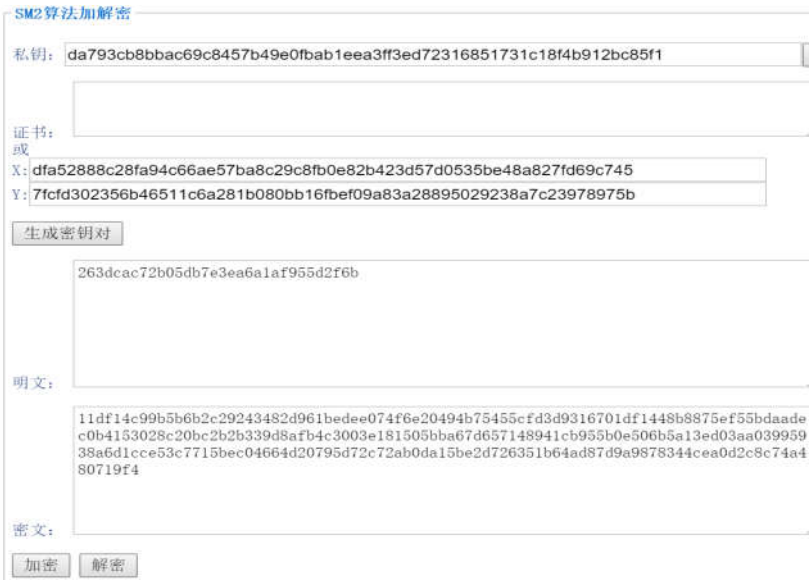


图 8 SM2 密文结果随机特性

Fig. 8 Randomness of SM2 ciphertext results

6.2 基于 SM2 密钥交换测试

密钥交换测试，主要实现配电网智能电子设备新接入配电网系统中，能在线实现密钥安全交换的功能。

首先分析安全性，模拟新加入智能电子设备的 PC2 首先组织好包含自身公钥和身份的报文信息，并用模拟配电网主站的 PC1 的公钥对该报文进行 SM2 算法加密后发送给 PC1，PC1 用私钥解析该报文。模拟恶意第三方的 PC5 虽然可以观察捕捉整个密钥交换的过程，但由于没有 PC1 和 PC2 的私钥，无法解析出所捕捉的密文对应的明文。

在安全性实验基础上进行耗时实测，首先统计单次的加解密算法的耗时，如表 1 所示，由于 PC1 和 PC2 采用相同性能的 PC 机，单次的加密和解密耗时几乎一样。

表 1 密钥交换耗时统计

Table 1 Time consuming for key exchange

类型	单次加密/ms	单次解密/ms	加解密总耗时/ms
PC1	0.427	0.701	1.559
PC2	0.427	0.702	1.130

进一步分析整个配电网密钥交换过程中，模拟主站的 PC1 和模拟新加入智能电子设备的 PC2 各自加解密的总耗时，PC1 耗时比 PC2 耗时稍大，这是因为模拟主站的 PC1 多了一个通知其他智能电子设备的加密报文。

6.3 基于 SM2 数字签名测试

分析模拟配电网主站的 PC1 与智能电子设备 PC3 的通信情况，为了防止模拟恶意第三方 PC5 的网络攻击，通信报文采用基于 SM2 的数字签名方法，以保证报文的完整性和不可抵赖性。

假设 PC3 发送用自身私钥签名的报文给 PC1，PC5 捕捉该报文并篡改报文信息后，发送篡改的报文给 PC1，PC1 通过 PC3 的公钥验证后发现签名摘要不一致，从而判断该报文完整性遭受破坏。

不可抵赖性方面，假设 PC1 利用 PC3 的公钥通过了报文的数字签名，则可判定该报文来自于 PC3，因为只有跟该公钥对应的私钥才能制造该报文，而该私钥只属于 PC3，PC3 无法否认可以通过自身公钥验证的报文来自于其他配电网智能电子设备。

测试基于 SM2 数字签名方法的耗时。选取长度为 100 字节、500 字节和 1 000 字节三种典型长度的 Modbus 报文，分别测试在签名端(即报文发送端)和验证端(即报文接收端)的耗时情况，如表 2 所示。

表 2 不同报文长度的数字签名耗时

Table 2 Time consuming for different length

长度	100 字节 /ms	500 字节/ms	1 000 字节/ms
签名端	0.431	0.451	0.475
验证端	0.707	0.725	0.749

从表 2 可见，相同长度的报文，签名端所用的耗时比验证端的耗时短，这是因为签名端采用的加密算法，比验证端采用的解密算法耗时短。

随着报文长度的增加，签名端和验证端的耗时都小幅度地增加，这是因为报文数字签名过程中，

签名端和验证端分别使用了一次 SM2 加密和解密，加解密耗时固定，但数字签名中用到了 SM3 算法，报文长度越长，SM3 的算法次数对应增加，因此，表 2 中的报文增长导致的耗时增加，主要由 SM3 哈希算法耗时组成。但耗时增加的幅度非常小，说明相对于 SM2 非对称加解密算法，SM3 哈希算法所需的耗时要短很多。

7　结语

国产安全算法能有效地避免国外算法可能存在的后门陷阱，在关系整个电力系统平稳运行的配电网信息系统中采用国密安全方法，可以抵御外界的恶意攻击。研究一种基于 SM2 非对称加密算法的配电网 Modbus 报文安全方法，采用 SM2 进行配电网信息系统的密钥在线管理和对配电网 Modbus 报文进行数字签名，保证配电网报文信息的真实性和不可抵赖性。

参考文献

[1] 陈晓杰, 徐丙垠, 陈羽, 等. 配电网分布式控制实时数据快速传输技术[J]. 电力系统保护与控制, 2016, 44(17): 151-158.
CHEN Xiaojie, XU Bingyin, CHEN Yu, et al. Real-time data fast transmission technology for distributed control of distribution network[J]. Power System Protection and Control, 2016, 44(17): 151-158.

[2] 王良. 智能配电网自动化应用实践的几点探讨[J]. 电力系统保护与控制, 2016, 44(20): 12-16.
WANG Liang. Discussion on application practice of distribution automation[J]. Power System Protection and Control, 2016, 44(20): 12-16.

[3] 国家电网调〔2011〕168 号. 关于加强配电网自动化系统安全防护工作的通知[S]. 北京: 国家电网公司, 2011.

[4] 中国南方电网. 中国南方电网电力监控系统安全防护技术规范: Q/CSG1204009[S]. 广州: 中国南方电网有限责任公司, 2015.

[5] 国家电力监管委员会令. 电力二次系统安全防护规定[S]. 2004.

[6] 冯欣桦, 黎洪光, 郑欣, 等. 计及不确定性的配电网合环点安全性与经济性评估[J]. 电力系统保护与控制, 2015, 43(10): 30-37.
FENG Xinhua, LI Hongguang, ZHENG Xin, et al. Security and economy evaluation of closed loop point of distribution network considering uncertainty[J]. Power System Protection and Control, 2015, 43(10): 30-37.

[7] ZHANG Baohui, HAO Zhiguo, BO Zhiqian. New development in relay protection for smart grid[J]. Protection and Control of Modern Power Systems, 2016, 1(1): 121-127. DOI: 10.1186/s41601-016-0025-x.

[8] 郝海峰. 高可靠性遥测加密模块研究[D]. 西安: 西安电子科技大学, 2011.

[9] 张志华, 周捷, 丁可, 等. 非对称数字签名技术在配电自动化系统中的应用[J]. 电气自动化, 2012, 34(3): 39-41.
ZHANG Zhihua, ZHOU Jie, DING Ke, et al. The applications of asymmetric encryption of digital signature technology in distribution automation system[J]. Electrical Automation, 2012, 34(3): 39-41.

[10] 国家密码管理局. SM2 椭圆曲线公钥密码算法[S]. 2012.

[11] 国家密码管理局. SM3 密码杂凑算法[S]. 2012.

[12] 戚宇林, 刘文颖, 杨以涵, 等. 电力信息的网络化传输是电力系统安全的重要保证[J]. 电网技术, 2004, 28(9): 58-61.
QI Yulin, LIU Wenying, YANG Yihan, et al. Ensuring power security by networking transmission of electric power information[J]. Power System Technology, 2004, 28 (9): 58-61.

[13] 王智东. IEC61850报文安全性关键技术研究[D]. 广州: 华南理工大学, 2016.

[14] 沈郑毅, 刘天琪, 洪行旅, 等. 中心城市大型配电自动化设计方案与应用[J]. 电力系统自动化, 2012, 36(18): 49-53.
SHEN Zhengyi, LIU Tianqi, HONG Xinglü, et al. Design and application of center city distribution automation[J]. Automation of Electric Power Systems, 2012, 36(18): 49-53.

[15] 王智东, 王钢, 童晋方, 等. 智能变电站的密钥管理方法[J]. 电力系统自动化, 2016, 40(13): 121-127.
WANG Zhidong, WANG Gang, TONG Jinfang, et al. Key management method for intelligent substations[J]. Automation of Electric Power Systems, 2016, 40(13): 121-127.

[16] STALLINGS W. 密码编码学与网络安全原理与实践[M]. 北京: 电子工业出版社, 2015.

[17] 贺晓, 李俊, 陈洁羽, 等. 智能变电站配置文件管控系统建设方案研究[J]. 智慧电力, 2017, 45(8): 75-81.
HE Xiao, LI Jun, CHEN Jieyu, et al. Construction scheme study on configuration file management and control system in intelligent substation[J]. Smart Power, 2017, 45(8): 75-81.

[18] 邹磊, 薛明军, 姚亮, 等. 智能变电站采样异常处理方法的研究[J]. 陕西电力, 2017, 45(4): 39-43.
ZOU Lei, XUE Mingjun, YAO Liang, et al. Research and analysis on SV exception treatment method in smart substation[J]. Shaanxi Electric Power, 2017, 45(4): 39-43.

收稿日期：2017-05-31；　修回日期：2017-08-03

作者简介：

邹晓峰(1985—)，男，硕士，工程师，主要研究方向为电力系统控制保护技术；

肖远兴(1977—)，男，学士，工程师，主要研究方向为广域保护。

(编辑　张爱琴)