DOI: 10.7667/PSPC170218

一种高效的配电网报文数字签名实现方法

肖小兵，徐长宝，林呈辉，王 宇，刘 斌

（贵州电网有限责任公司电力科学研究院，贵州 贵阳 550002）

摘要：智能配电网越来越多地依赖通信网络交互信息，而通信网络更加多样化和开放化，使得通信报文在网络传输中遭受篡改、窃取、伪造等恶意第三方攻击的可能性日益突出。在研究智能配电网报文安全目标的基础上，提出一种基于椭圆曲线的智能配电网通信报文认证方法。首先分析了数字签名的原理，接着研究基于数字签名的智能配电网报文安全的具体实现方法，并在当前智能配电网平台上进行报文安全测试实验。测试结果证明，基于椭圆曲线算法的报文认证方法安全性较好，同时还能满足智能配电网的实时性要求。

关键词：智能配电网；通信安全；网络报文；数字签名；椭圆曲线

An efficient implementation method for distribution network packet based on digital signature

XIAO Xiaobing, XU Changbao, LIN Chenghui, WANG Yu, LIU Bin

(Electric Power Research Institute of Guizhou Power Grid Co., Ltd., Guiyang 550002, China)

Abstract: The smart distribution grid exchanges information relying on communications network increasingly, and the communication network becomes more diverse and open, which makes the communication packet vulnerable to be attacked by malicious third party such as information falsifying, forging, stealing. On the basis of researching packet security objectives of smart distribution network, this paper presents a packet authentication algorithm based on elliptic curve for smart distribution network communication. First the principle of digital signatures is discussed. Then the specific implementation of smart distribution network packet security based on digital signatures is introduced, and the packet security test is carried on the current intelligent distribution network platform. The experiment results show this packet authentication algorithm based on elliptic curve has better security and also can meet the real-time requirements of smart distribution network communication.

Key words: smart distribution network; communication security; network packet; digital signatures; elliptic curve

0 引言

智能配电网作为智能电网建设的关键环节，需要通过通信网络实现配电网信息的双向流动。智能配电网的主站和分散分布于配电网内的各类测量设备，依靠通信网络，实现信息的高效交互。智能配电网主站作为信息汇集中心，通过通信网络与各类保护控制设备通信以获得实时测量信息，实现对系统状态的监测。而各类保护控制设备也借助通信网络，接收控制主站的命令实现各类遥控操作，及时切除故障以保障系统安全[1]。

通信网络在智能配电网中起着越来越重要的作用，而且随着智能配电网向着纵深发展，通信网络将会得到更大规模的应用，但所面临的安全风险也将更加突出，通信网络存在的安全隐患和威胁对配电网运行的不良影响引起了业界的关注。电力通信网络一旦受到第三方恶意攻击，比如在通信网络系统中篡改报文或注入伪造的报文，则将可能造成断路器等开关的误动或者拒动，或导致配电网主站接收来自于各个测量装置的紊乱数据等恶劣情况，这将严重威胁电力系统的安全稳定运行，甚至引发灾难性事故。

不同于输电网通常采用专门的电力通信网络进行报文传送，配电网物理分布更加广阔，通常需要借助公网等通信网络，同时配电网存在着信息“最后一公里”等复杂化情况，配电网通信方式多样化，遭受外界恶意入侵的可能性很大，因此面临着更大的信息安全风险。

基金项目：国家科技支撑计划(2013BAA02B02)

1　安全性分析

电力信息安全已成为智能配电网建设的重要内容和先决条件。除了经典的加密算法以保证报文信息的保密性以外，对于智能配电网来说，电力信息安全性还包括了信息完整性、有效性以及不可抵赖性等重要特性[2]。

完整性：指智能配电网的报文信息能准确地由发送方传送到接收方，报文信息在传输过程中报文保持原始信息的一致性，没有因通信网络的噪声干扰而产生误码或是第三方恶意篡改报文内容而导致接收方所收到的报文与发送方所发出的报文不完全一致。

有效性：指智能配电网的报文信息能及时地由发送方传送到接收方，而且接收方能有效地识别发送方的真实身份。报文接收方在获得安全系统授权基础上，能正确识别报文发送方的真实身份，能实时、可靠地接收来于自己或授权的通信对象的报文，并有效地拒绝未经授权的通信对象的访问服务。

不可抵赖性：指智能配电网的报文发送方需对所发出的报文负责，含报文接收方在内的整个智能配电网信息安全系统能够有效证明该报文的发送方，发送方无法否认所发出的报文。由于类型众多的配电网智能电子设备分属于不同生产厂家和运营公司，报文的不可抵赖性的特点对于智能配电网区分信息来源和责任具有重要意义。

对于智能配电网信息安全来说，报文的完整性、有效性和不可抵赖性，其重要性不亚于报文信息的保密性[3]，能够保证报文信息完整、及时地送递到真实的智能配电网通信对象，并且能有效地证明智能配电网的报文的发送方身份，发送方无法否认自身所发出的报文。

当前学术界和工业界都已陆续开展智能配电网报文的完整性、有效性和不可抵赖性领域的研究，文献[4]研究在电力报文中通过哈希算法算出认证码，并将该认证码附随报文传送到接收方，以保证智能配电自动化中报文的真实性完整性；文献[5]提出一种多通道安全认证组播方法；文献[6]介绍了配电网终端对主站进行身份验证和对遥控命令进行完整性检查的过程，并基于 OpenSSL 开源加密库实现配电网终端遥控加密；文献[7]研究不同设备、不同协议间的数据转发机制，开发一种新型的数据通路复用装置并集成基于安全传输层协议的端到端加密功能。

上述的研究主要将密码技术直接应用到配电网的报文安全上，较少结合电力报文自身的特点进行算法安全性和实时性的综合平衡，部分文献只是介绍了构思和初步方案，还没深入到配电网安全报文的具体实现方法。

电力学术界逐步加强电力通信报文的安全性具体应用研究，尝试在保障电力报文传输安全性基础上，结合报文特点优化算法效率，文献[8]和文献[9]分别针对 IEC61850-9-2LE 和 GOOSE 两种实时报文进行了安全算法研究，取得了较好效果。但上述文献都是基于对称密钥进行配电网报文的完整性研究，基于对称密钥的安全方法存在着密钥难以高效管理等问题，尤其对于分散性较大但又有实时性要求的配电网系统来说，高效的对称密钥管理不易实现。

由于实际的智能配电网中，不容易建立一条独特的安全通信方式，用以保障智能配电网各个参与方进行对称密钥的安全交换[10]。因此，基于公钥的报文安全方法，由于报文发送方和接收方无需用到相同的密钥，是智能配电网报文安全交换的优选方法[11]。本文将研究基于公钥机制研究智能配电网报文的安全算法，采用基于数字签名的智能配电网报文安全方法，重点解决智能配电网信息的完整性、有效性以及不可抵赖性特性，并在当前智能配电网平台上进行性能实测，分析算法的安全性和实时性对智能配电网的适用性。

2　配电网数字签名认证方法

数字签名是指在网络通信系统中，通过对报文信息进行确认标识从而起到与手工签名一样的功能和效用，对报文进行数字签名的发送方需对所发出的报文承担对应的责任[12]。

相对于日常的签名方法存在可能模仿他人签名或是同个人不同时刻书写习惯导致字体差异等问题，数字签名具有更高的识别度和稳定的可信度。基于相同密钥的数字签名结果是完全一样的，在没有获得对应密钥的情况下，恶意第三方无法伪造正确的报文。

当前数字签名几乎都是基于公钥机制，报文发送方和接收方使用不同的密钥进行签名和验证，既降低了密钥泄露的风险，也因报文收、发双方使用不同的密钥而明确了报文的真实发送方，避免了双方互相推诿属于对方责任的问题。

由于加解密算法耗时较大，尤其基于公钥机制的加解密算法，算法耗时更加冗长；而且对于加解密算法而言，所需加密的信息越多，运算所需的耗时几乎成比例地增加。因此，为了减少数字签名耗时，当前经典的数字签名都采用了基于报文信息摘

要的数字签名方法。

基于报文信息摘要的数字签名方法，报文发送方对所发送的报文进行哈希运算，得到哈希值后对该值进行签名，并将该签名认证码与报文一起发送给报文接收方，接收方对该签名认证码进行验证，确认报文的真实性[13]。不同长度的智能配电网报文，采用哈希算法后得到的哈希值长度是固定的，也就是需要加解密的哈希值长度是固定的，而哈希算法耗时相对于公钥加解密算法耗时来说几乎可以忽略，因此，对于不同长度的智能配电网报文，采用对配电网报文哈希值进行数字签名的方法运算所需的耗时非常接近。

典型的数字签名流程如图 1 所示，智能电子设备需要发送报文时，作为发送方的智能电子设备首先用事先约好的哈希函数，对将要发送的智能配电网报文进行哈希运算得到哈希值，然后用自身保存的私钥对该哈希值进行加密，将密文形式的数字签名结果附带在报文后面，跟随报文一起发送给接收方。

作为接收方的智能电子设备收到报文后，首先用与发送方相同的哈希函数，对所接收的原始报文进行哈希运算得到哈希值，接着再用发送方的公钥对附加在报文后面的数字签名进行解密得到报文发送方的哈希值，进一步比较这两个哈希值是否一致，从而确定该报文是否来自于真实的发送方。

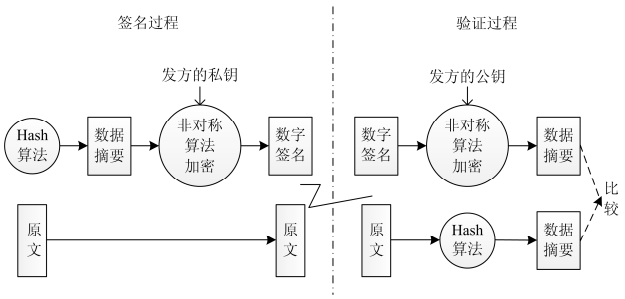

图 1 数字签名原理

Fig. 1 Principle of the digital signature

数字签名可确保消息的真实性和不可抵赖性，因为第三方在不得知发送方私钥情况下无法假冒发送方签名，只有真实地发送方签名才能通过接收方的验证。另一方面数字签名可确定消息的完整性。因为数字签名加密算法输入为待签名消息的哈希值，当消息受到篡改后哈希值也将发生变化，将无法通过最终的签名验证。

采用数字签名对配电网报文进行认证后，报文的接收方可以通过两个途径确定所接收报文的真实来源方。一方面，报文的网络地址表征了报文的来源，通过识别报文的物理地址和 IP 地址两种网络地址，可以直接判定报文来源，而且网络地址参与了哈希运算，是无法被篡改的，否则将导致哈希值有误；另一方面，配电网不同的智能电子设备通常拥有不同的公钥，对应的公钥存放在可靠的密钥管理中心，该公钥也表征了所对应的智能电子设备。

因此，基于数字签名的智能配电网报文，能同时满足配电网报文信息的完整性、有效性和不可抵赖性要求。而智能配电网信息涉及保护、测控等配电网生产区的重要内容，智能配电网报文的实时性要求很高，但基于公钥机制的加解密算法的应用难点之一就在于较大的算法耗时。因此，在保障智能配电网报文信息安全性基础上，选择高效的公钥加解密算法便成为了关键。

当前主流的公钥算法包括 RSA 算法和美国国家标准局提出的 DSA 算法等经典算法[14]，RSA 和 DSA 等公钥算法具有较好的安全性能，但运算速度较慢。跟经典的对称加解密算法相比，公钥加解密算法通常慢几个数量级，在实时性要求较高的智能配电网应用中有一定困难。

针对 RSA 和 DSA 等公钥算法耗时的问题，近年来提出了基于椭圆曲线密码 (Elliptic Curve Cryptography，ECC)的公钥加解密算法，ECC 算法只需用较短的密钥，便可以达到与 RSA、DSA 等经典公钥算法相同的安全程度，研究表明 160 bit 的椭圆密钥与 1024bit 的 RSA 密钥安全性相同[15]，ECC 算法具有运算效率高的优点。

另外，智能配电网所采用的智能电子设备一般采用嵌入式系统构成。嵌入式设备的运算、存储和网络性能通常远逊色于服务器，而出于成本考虑，配电网的智能电子设备一般采用性能较低端的运算和存储芯片，不适合用于复杂的加解密算法。由于 ECC 公钥加解密算法具有运算效率高、存储空间占用小、带宽要求低等优点，ECC 公钥加解密算法更适合于智能配电网系统。

3 实现方法

智能配电网采用基于公钥机制的数字签名实现报文的安全性，与对称加解密算法相比，简化了密钥的分配方法，只需在现有的配电网系统中增加一个智能配电网密钥管理中心，如图 2 所示。密钥管理中心在确认配电网的各个智能电子设备的真实身份后，在该密钥管理中心登记智能电子设备的身份号和对应的公钥并妥善保存，防止公钥在没有管理中心存储过程中被恶意被篡改；同时密钥管理中心向各个智能电子设备开放，作为报文接收方的智能

电子设备在密钥管理中心可以查询到报文发送方的公钥[16]。

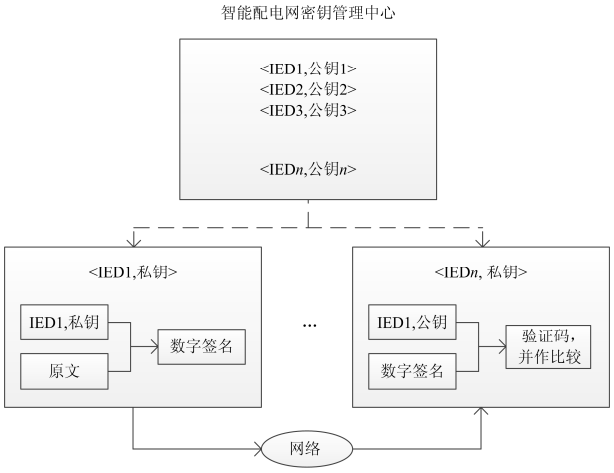

图 2 智能配电网密钥管理结构

Fig. 2 Key management structure for smart distribution network

各个智能电子设备除了在密钥管理中心存储公钥外，还需自身保存好与公钥对应的私钥，并确保私钥不对外泄露。否则一旦发生私钥外泄引起数字签名被伪造，各个厂家的智能电子设备将承担责任，因为只有其自身才拥有私钥。

密钥管理中心除了担当起密钥管理的主要功能外，还协调智能电子设备参与数字签名所需的具体函数和参数，包括具体的哈希算法类型(比如 MD5 或 SHA 系列等算法)和椭圆曲线数字签名算法的椭圆曲线参数。

各个智能电子设备协商好数字签名涉及的具体算法和参数后，作为发送方的智能电子设备，根据智能配电网信息交换范围需要，通过设置智能配电网报文统一格式中的接收地址，以单播或多播的方式，灵活地向一个或多个智能电子设备发送报文信息。

发送方首先组织好待发送的报文信息，并从组织好的报文中提取需要进行数字签名的内容，采用该密钥对该内容进行数字签名。而接收方则用发送方私钥对应的公钥，对报文数字签名进行解密并与发送方伴随报文传送过来的数字签名作比较，从而确定该报文是否来自于发送方的真实报文。

具体实现上，参与智能配电网通信的各方首先约定好所采用的哈希函数，并统一采用 ECC 算法对哈希值进行加解密运算，各个智能电子设备保存好自身私钥，并将对应的公钥放置于智能配电网密钥管理中心供其他智能电子设备查询。

1) 作为报文发送方的智能电子设备实现数字签名过程。发送方首先对组织好的智能配电网通信报文进行哈希运算，并提取自身的私钥对该哈希值进行 ECC 算法加密，将所得到以密文形式出现的数字签名附加在原始报文后面，并跟随原始报文发送到智能配电网通信系统上。

2) 作为报文接收方的智能电子设备实现验证过程。接收方首先根据所接收到的报文源地址判断报文来源于哪个智能电子设备，并在智能配电网密钥管理中心找到该智能电子设备对应的公钥，进而用公钥对附加在原始报文后面的数字签名(以密文形式出现)进行解密，得到解密值；进而用事先约定好的哈希函数对所接收到的报文进行哈希运算，得到哈希值，将哈希值与上述的解密值进行比较，若一致，则可判断该报文来自于真实的智能电子设备，同时，报文信息内容完全由作为发送方的智能电子设备负责；若不一致，则说明该报文内容已被篡改或不是由真实的智能电子设备发出。

4　算例与分析

构造如图 3 所示的智能配电网报文安全测试平台，智能电子设备通过以太网方式接入到以太网交换机中，从而各个智能电子设备可以通过智能配电网通信总线进行信息交互。

除了用于模拟报文发送方和接收方的正常智能电子设备，还有模拟恶意第三方的工控机也接入到通信总线中，恶意第三方一直监听整个智能配电网总线的报文流动情况，并可以拦截报文并进一步发动伪造报文或是篡改报文等网络攻击。

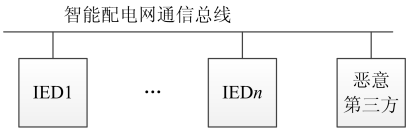

图 3 含恶意第三方的配电网实验平台

Fig. 3 Distribution network test platform containing malicious third party

4.1 算例

以某智能配电网的通信系统的遥测报文为例，对基于 ECC 采用数字签名方法的配电网报文进行验证。

报文采用当前电力通信系统应用最广泛的 IEC61850 格式，具体报文数据用十六进制表示如图 4 所示，其中， 01 0c cd 01 01 ff 是报文源地址；00 50 c2 4f 95 c2 是报文目的地址，类型符号采用与 IEC61850 的 GOOSE 报文一样的类型符 88 b8，方便以后的智能电网信息统一化；报文长度为 81(143Byte)。由于该智能配电网实际应用中没有采

用对时机制，因此，报文中时间选项空缺，剩下的报文都是 APDU 内容，表征配电网的遥测量。

```
0000  01 0c cd 01 01 ff 00 50 c2 4f 95 c2 88 b8 00 81
0010  00 03 00 00 00 00 61 77 80 17 47 54 4e 45 54 43
0020  54 52 4c 2f 4c 4c 4e 30 24 47 4f 24 47 63 62 30
0030  31 81 02 0f a0 82 1e 47 54 4e 45 54 43 54 52 4c
0040  2f 4c 4c 4e 30 24 47 4f 4f 53 45 5f 6f 75 74 70
0050  75 74 73 5f 31 83 01 31 84 08 41 cd b4 da 08 99
0060  22 1f 85 01 01 86 02 01 ea 87 01 00 88 01 01 89
0070  01 00 8a 01 06 ab 18 84 02 06 80 84 02 06 80 84
0080  02 06 80 84 02 06 80 84 02 06 80 84 02 06 80
```

图 4 智能配电网报文具体内容

Fig. 4 Packet content of smart distribution network

对该报文采用 ECC 数字签名方法，采用 SECP256K1 作为 ECC 曲线，具体算法为 SHA256 和椭圆曲线。数字签名对应的私钥(发送方自身的私钥)为 7a 01 52 fb 87 48 bb 4c 8b 93 c5 2b 18 18 ba 8b 0b 93 96 bb 1f 62 ef 82 f5 be 20 1a 3b 1d c4 7c，公钥(对接收方公开的公钥)为 04 0c a7 09 c6 80 4b 64 cd d9 7e 21 dd 7a a5 23 dc b0 77 d7 85 ab 73 e2 83 7d c6 ba b3 c7 e1 7f 25 2b d2 54 9d fa e9 07 8b 30 90 0e 70 06 6e ac c4 54 0c 30 06 71 cc c4 08 14 b1 e4 a7 04 16 5d e7。

发送方通过自身的私钥对该报文进行数字签名，得到的数字签名结果为：30 46 02 21 00 e5 cf 00 da e1 26 35 52 93 93 6e e5 32 94 93 f4 40 bb 31 cc 6e 63 34 3d 48 2e 25 7c d1 3d b0 06 02 21 00 ba 82 f1 2c 9b e8 7d 77 46 f2 6b b6 3a d4 70 b1 d2 b4 91 ba 73 84 b4 91 d4 8f d9 90 72 b5 18 60。将该结果添加到统一报文格式的帧校验域，实现报文的数字签名以防止报文被篡改或伪造。

接收方采用相应的数字签名方法，基于与发送方私钥对应的公钥，对所接受的报文进行数字签名验算，比较计算得到的帧校验域与从接收到的报文的帧校验域是否一致，如果不一致，说明所收到的报文并非来自于发送方的真实报文，丢弃该报文。

进行安全性分析。采用数字签名后，接收方若计算得到验证码一致，首先可判断报文内容没有遭受篡改，报文内容遭受篡改则无法得到一致的验证码；其次，通过公钥属于哪个智能电子设备可以确定报文的发送方，从而确认了报文来源的有效性；最重要的是，由于发送方自身拥有私钥而且对外保密，没有该私钥不可能得到具有一致性的数字签名验证码，因此，该报文可确定来自于发送方，即发送方需对所发的报文信息负责，具有不可抵赖性。

需要注意的是，采用数字签名的配电网报文虽然具有上述的安全性，但不具备机密性，需要保密的配电网报文需要对报文内容自身采用加解密等密码技术实现。另外，上述数字签名方法没有考虑重放攻击的情况，可以通过在报文中加入时间戳或同步信号等方法实现。

4.2 效率分析

为验证椭圆曲线算法在配电网通信中的效率，本文在不同性能的智能电子设备平台下对椭圆曲线算法进行算法耗时测试，分别采用型号为 AM35x cortex-A8 的 ARM 芯片和型号为 C6652 的 DSP 芯片，对本文算法进行耗时测试，两种芯片的主频都为 600 M。

算法耗时结果如表 1 所示，从实测延时可知，当前较为先进的控制器芯片，对本文所提的算法都能有较好的运算速度，所需的算法耗时都在毫秒等级，能满足智能配电网一般信息交换的实时性要求。对于椭圆曲线数字签名算法而言，发送方所用的算法耗时比接收方的算法耗时稍微大，主要是由椭圆曲线公钥加密算法特点决定，但两者之间的耗时差别也比较接近。

表 1 不同控制器芯片的 ECC 数字签名算法耗时

Table 1 Time-consuming of different controllers for ECC digital signature

芯片类型	AM35x cortex-A8	C6652
发送方耗时/ms	71.98	25.18
接收端耗时/ms	77.42	28.63

同时注意到，不同处理器的芯片结构对安全算法的耗时影响很大，算例中的两种控制器的主频虽然相同，但是由于芯片结构并不相同，测试结果表明中基于 DSP 芯片的算法总耗时约为 53.81ms，远小于基于 ARM 芯片的算法总耗时 149.4 ms。因此，在配电网报文安全算法的实际应用中，选择合适类型的处理器对减少安全算法耗时也具有重要意义。

5 结论

智能配电网报文的完整性、有效性以及不可抵赖性，是智能配电网信息安全的重要组成部分，本文在分析智能配电网信息安全性基础上，采用基于椭圆曲线的公钥机制对智能配电网报文进行数字签名，具体介绍了智能配电网应用中的实现方法。通过算例进行了算法的安全性分析，嵌入式控制器的算法耗时测试证明该算法能满足智能配电网的实时性要求。

参考文献

[1] 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.

[2] 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.

[3] ERICSSON G N. Cyber security and power system communication essential parts of a smart grid infrastructure[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1501-1507.

[4] 黄梦婕, 青布工. 基于 HMAC 算法的远程电力监控通信安全策略[J]. 电力系统保护与控制, 2011, 39(19): 79-82.
HUANG Mengjie, XU Bugong. Cyber security strategies based on HMAC[J]. Power System Protection and Control, 2011, 39(19): 79-82.

[5] KIM M, METZNER J. A key exchange method for intelligent electronic devices in distribution automation[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1458-1463.

[6] 杨洪涛, 汝雁飞, 盛立健, 等. 基于OpenSSL的配网终端遥控加密测试软件的实现[J]. 电力系统自动化, 2012, 36(18): 77-81.
YANG Hongtao, RU Yanfei, SHENG Lijian, et al. Implementation of remote control encryption test software in the distribution network terminal based on OpenSSL[J]. Automation of Electric Power Systems, 2012, 36(18): 77-81.

[7] 徐显秋. 配电网信息采集系统数据通路复用及安全加密的研究[J]. 重庆科技学院学报(自然科学版), 2013, 15(5): 63-68.
XU Xianqiu. Research on data path reused and security encryption of information collection system for distribution network[J]. Journal of Chongqing University of Science and Technology (Natural Science Edition), 2013, 15(5): 63-68.

[8] 王智东, 王钢, 黎永昌,等. 基于微型加密算法的IEC61850-9-2LE 报文加密方法[J]. 电力系统自动化, 2016, 40(4): 121-127.
WANG Zhidong, WANG Gang, LI Yongchang, et al. An encryption method for IEC 61850-9-2LE packet based on tiny encryption algorithm[J]. Automation of Electric Power Systems, 2016, 40(4): 121-127.

[9] 王智东, 王钢, 许志恒, 等. 一种改进的 GOOSE 报文 HMAC 认证方法[J]. 电网技术, 2015, 39(12): 3627-3633.
WANG Zhidong, WANG Gang, XU Zhiheng, et al. An HMAC based authenticated method for GOOSE packets[J]. Power System Technology, 2015, 39(12): 3627-3633.

[10] 赵银春. 配电网安全防护系统[D]. 成都: 电子科技大学, 2013.

[11] 汪强, 徐小兰, 张剑. 一种新的智能变电站通信业务安全隔离技术的研究[J]. 电力系统保护与控制, 2015, 43(13): 139-144.
WANG Qiang, XU Xiaolan, ZHANG Jian. A new method of smart substation communication service security isolation technology[J]. Power System Protection and Control, 2015, 43(13): 139-144.

[12] 姚强. 基于数字签名的智能配电网通信安全方法[J]. 电子技术与软件工程, 2015(12): 222-223.
YAO Qiang. Intelligent distribution network security communication method based on digital signature[J]. Electronic Technology & Software Engineering, 2015(12): 222-223.

[13] 杨慧. 基于椭圆曲线的公钥密码系统及其在数字签名中的应用[D]. 西安: 西安电子科技大学, 2007.
YANG Hui. Public-key cryptosystem based on conic curve and its application in digital signature[D]. Xi'an: Xidian University, 2007.

[14] STAMP M. 信息安全原理与实践[M]. 2 版. 张戈, 译. 北京: 清华大学出版社, 2013.

[15] 王国才, 柯福送, 王芳. 基于椭圆曲线的三方口令认证密钥交换协议[J]. 计算机工程, 2012, 38(6): 153-155.
WANG Guocai, KE Fusong, WANG Fang. Conic curve-based password authenticated key exchange protocol for three-party[J]. Computer Engineering, 2012, 38(6): 153-155.

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

收稿日期：2017-02-20；　修回日期：2017-05-12

作者简介：

肖小兵(1986—)，男，硕士，工程师，主要研究方向为配电相关领域；

徐长宝(1977—)，男，硕士，教高，主要研究方向为电力系统自动化；

林呈辉(1983—)，男，硕士，高工，主要研究方向为电力系统自动化。

(编辑　张爱琴)