基于混合密码体制的配电网数据安全传输研究

付宇,肖小兵,张锐锋,郑友卓,刘安茳,何洪流,吴鹏,张洋,李前敏
贵州电网有限责任有限公司电力科学研究院，贵州省贵阳市，550002

Research on data security transmission scheme for distribution network based on hybrid cryptosystem

FU Yu, XIAO Xiaobing,ZHANG Ruifeng,ZHENG Youzhuo,LIU Anjiang,He Hongliu,Wu Peng,Zhang Yang,Li Qianmin
Electric Power Research Institute of Guizhou Power Grid Co., Ltd., Guiyang 550001, China

摘要：配电网络数据安全是其安全稳定运行的重要保障，为了确保配电网数据的安全，本文提出基于混合密码体制的配电网数据安全传输方案。该方案将 SM4 和 SM2 算法相结合提高了数据安全性；通过使用 SM4 算法对报文加密，获得了较高的加密效率；通过采用 SM2 算法加密 SM4 算法的秘钥，有效提高安全性，并降低存储空间。数值仿真结果表明，本方案可有效完成数据的加解密，与 RSA 算法相比加密速度快，内存消耗少。本方案可以提高数据传输的安全性、提高加密效率、降低内存开销，具有广阔的应用前景。

关键词：混合密码；配电网；SM4 算法；SM2 算法

Abstract: Distribution network data security is an important guarantee for its safe and stable operation. In order to ensure the security of distribution network data, this paper proposes a data transmission security scheme for distribution network based on hybrid cryptosystem. This solution combines the SM4 and SM2 algorithms to improve data security. By encrypting packets using the SM4 algorithm, a higher encryption efficiency is achieved. By using the SM2 algorithm to encrypt the secret key of the SM4 algorithm, the security is improved and the security is reduced. storage. The numerical simulation results show that this scheme can effectively complete the encryption and decryption of data. Compared with the RSA algorithm, the encryption speed is fast and the memory consumption is low. This solution can improve the security of data transmission, improve the encryption efficiency, reduce the memory overhead, and has broad application prospects.

Key words: Mixed password; Distribution network; SM4 algorithm; SM2 algorithm

1 引言

配电网络是保障电力系统安全可靠稳定运行的重要基础，如何确保配电网络的数据安全进而保障整个电力系统的可靠稳定成为了当前研究的热点[1-4]。近年来，随着现代化信息技术以及自动控制技术在社会生产生活中的广泛应用，以此为基础的智能配电网络成为了不少不法分子而已攻击的对象。智能化的配电网络借助现代信息技术实现了用户与企业间的双向信息流动。信息开放成为了一把双刃剑，其为电网与用户搭建的信息交换平台也成为了智能配电网所面临的一个巨大安全威胁[5-7]，如何确保配电网络的数据安全成为了目前的然就热点。

为了能够加强配电网的数据安全性，目前国内外研究人员提出了多种数据安全传输方案，主要分为两个方向：消息认证方案与秘钥管理方案。例如 2011 年 Fouda 等人提出使用 DES 认证方案进行消息认证[6]，通过 DES 算法对目标消息进行认证以确认是否来自合法用户发送，就是一种采用消息认证方案进行数据安全保护的方法。紧接着 Usman 等人在 2013 年对使用 DES 与 AES 等认证方案的加密方法进行了对比总结，指出了其加密简便但是存在安全性不高的特点[7]。而 2014 年 Hu 等人提出的动态秘钥分配方法则采用秘钥管理对目标数据进行安全传输与加解密操作[2]，同样达到了对配电网数据进行加密的目的。虽然这两种数据

安全传输方法都可以对目标数据进行加密以达到安全传输的目的，但是这些方案普遍单纯采用一种算法进行加密或者认证，虽然非常简便快捷地实现了数据加密的目的，但是存在着安全性不高的缺陷，系统依然易于受到攻击造成数据泄露。

近年来，混合密码体制获得了越来越多的关注，混合密码体制即采用多种加密方法相结合而不是单一的某种算法进行加密的方案[8-13]。例如 Mantoro T 等人将混合密码系统应用于邮件通信安全[8]，而 Kuppuswamy P 等人更是提出了将公钥密码与对称秘钥相结合的混合密码方案[9]，这些工作不但推动了混合密码体制的理论研究同时也拓展了其应用范围，为其在配电网络中应用提供了基础。

本文将国密 SM4 算法、SM2 算法和配电网数据传输相结合，提出了基于混合密码体制的配电网数据安全传输方案，在使用 SM4 算法对报文进行加密的情况下，进一步使用 SM2 算法对 SM4 算法产生的秘钥进行加密，它有效提高了数据传输的安全性，且降低了对系统内存的开销。通过数值仿真，分析并对比了该方案进行数据加密的可行性以及在加密速度和内存开销上的优越性。

2 研究方法与过程

2.1 研究方法

本文以混合加密算法为研究对象，以基于混合加密体制的配电网数据安全传输系统为研究目标，通过文献研究分析了当前智能配电网络中存在的数据传输安全问题，利用理论分析与数值仿真相结合设计并验证了基于混合密码体制的配电网数据安全传输方案。首先详细介绍了方案的理论基础，即国密 SM4 与 SM2 加密算法，随后在此基础上设计了基于混合密码体制的安全传输方案，最后通过定性分析与比较分析相结合的方法对方案进行了验证与分析。

2.2 研究过程

为了满足系统对于传输数据快速高效进行加解密操作，需要传输的目标数据采用国密 SM4 算法加密，其中 SM1 加密采用一次一密的加密方式，每一次生成的秘钥均不相同，数据通过 VPN 进行传输，发送方随机生成秘钥进行加密，随后使用国密 SM2 算法加密 SM4 的秘钥，简化对秘钥的交换与管理过程，实现数字签名。最后将经过加密的数据通过 VPN 传输给接收方。

国密 SM4 算法全称为 SM4 分组密码算法，是一种分组对称秘钥算法，该加密算法的明文、秘钥以及密文都是 16 个字节，其加解密使用的秘钥相同。采用 32 轮非线性迭代结构作为加密算法与秘钥扩展算法所使用的基础结构，解密过程只是使用顺序相反的轮秘钥，与加密过程结构类似[14-16]。

国密 SM4 算法将明文和密文都是由 4 个 32 比特字组成，SM4 算法的明文可以看做为，而其密文则可以看做为 $(Y_0,Y_1,Y_2,Y_3)\in(Z_2^{32})^4$ $(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$，而轮秘钥可以看做为 $rk_i\in Z_2^{32},i=0,1,2...31$，$R(A_0,A_1,A_2,A_3)=(A_3,A_2,A_1,A_0),A_i\in Z_2^{32},i=0,1,2,3$ 则可以看做是其反序变换 R。

国密 SM4 的加密过程一般由如下加密变换表示：

$$X_{i+4}=F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i),i=0,1,...31$$
$$(Y_0,Y_1,Y_2,Y_3)=R(X_{32},X_{33},X_{34}.X_{35})=(X_{35},X_{34},X_{33},X_{32})$$

该算法的加密和解密变换使用相同的结构，仅仅是两者对于轮秘钥的使用顺序相反。在加密过程中，轮秘钥的使用顺序为：$(rk_0,rk_1,...rk_{31})$；而在解密时则使用相反的轮秘钥顺序即：$(rk_{31},rk_{30},...rk_0)$。其加密使用的轮秘钥是由 128 比特的加密秘钥 $MK=(MK_0,MK_1,MK_2,MK_3)$ 生成的，这之中 $MK_i\in Z_2^{32}(i=0,1,2,3)$。

国密 SM4 加密算法具有诸多优点，其软硬件易于实现且运算速度快，但是其也存在着缺

陷，由于该算法的加解密过程使用同一套秘钥，一旦其秘钥发生泄漏就表示任何不法分子都是可以使用它对其进行破解。这很大程度上限制了他的应用。

国密 SM2 算法的全称是 SM2 椭圆曲线公钥密码算法，作为一种非对称秘钥算法，其加解密过程使用两套不同的秘钥，在加密操作中使用公共可见的公钥加密，而在解密时则使用不可见的私钥进行解密，并且即便是已知公钥的情况下在计算上对私钥进行求解也是不切实际的。发送者使用收方的公钥将待发送数据加密得到密文，而接收者则使用私钥对接收的密文数据解密还原出目标数据[17-18]。

国密 SM2 加密算法相对于其他非对称公钥加密使用更短的密钥串就实现了较为牢固的加密强度，同时由于其秘钥串更短因此其加密速度也更快。同时与 SM4 算法对比来说的话，SM2 算法在存储空间占用以及安全性上都具有很大优势，不过其算法也更为复杂使得其对于大块的报文数据加密效率低下。

为了进一步对加密方案进行研究，首先给出目标系统的数据传输设计。整体方案采用 T/S（终端/服务器）架构，设计的方案中可以接入两种不同类型的业务，分别为串口和网口，在密文条件下两种业务的速率分别为 50Kbps 和 5Mbps。系统部署方案如下图所示：

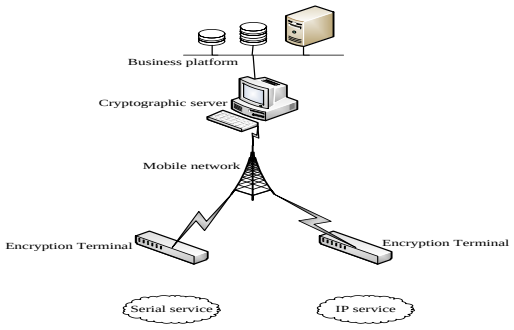


Fig.1 Data encryption scheme deployment of intelligent distribution network

终端安全防护装置内部集成 GPRS 无线拨号模块，配电终端通过串口同安全防护装置进行数据传输。其拓扑示意图如图所示：

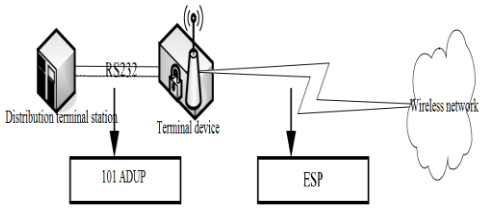


Fig.2 Deployment topology between distribution terminals and protective devices

配电终端通过串口的方式同安全防护装置连接，业务数据类型为 101 规约数据，使用带有拨号功能的 VPN 设备作为终端装置，且其需要和前置机建立起 TCP 长连接。如果终端装置拨号成功同时 TCP 长连接也顺利建立，则此时的业务数据传输过程示意图如下图所示：

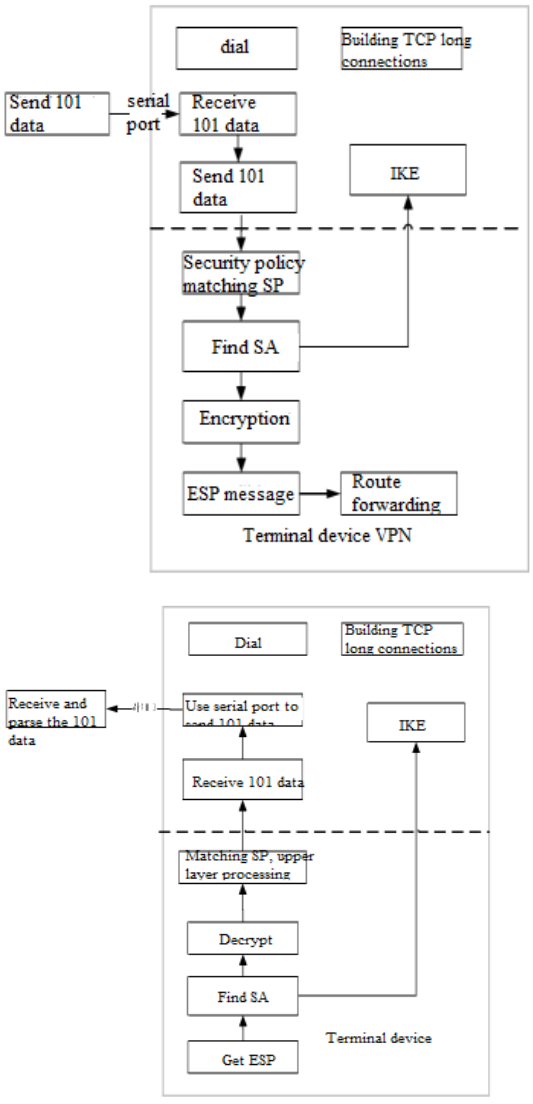


Fig.3 Schematic diagram of service data transfer process

安全防护装置通过串口对 101 规约的数据进行接收，同时将其经过 TCP 连接传送出去。系统会根据 SP 匹配查询出对应的 SA，将数据加密后发送。安全防护装置在接收到 ESP 包后，查找 SA，随后对数据解密并且将数据包交给更上层进行处理。而 TCP 在收到 101 规约数据后，将其通过串口传输给配电终端。

硬件上对于终端安全防护装置，本设计采用集成有 SM1、SM2、SM3、SM4 等加密算法的安全加密芯片。这样做的目的是满足系统公号上的低要求同时由于芯片直接集成于终端 PCB 上，大大提高了系统的可靠性。由于在主站一侧需要处理大量数据，设计使用额外的硬件网关来达到数据保护的目的。使用 FPGA+ARM 的方式实现加解密算法，这样可以提高系统的速度，同时避免修改主站程序。

在软件上则是通过建立 VPN 隧道的方式对数据进行加密。当前最常使用的用于建立 VPN 隧道的有 IPSec VPN 和 SSL VPN 这两种方式，两者分别基于网络层和应用层。安全防护装置的软件系统可以划分为如下模块：

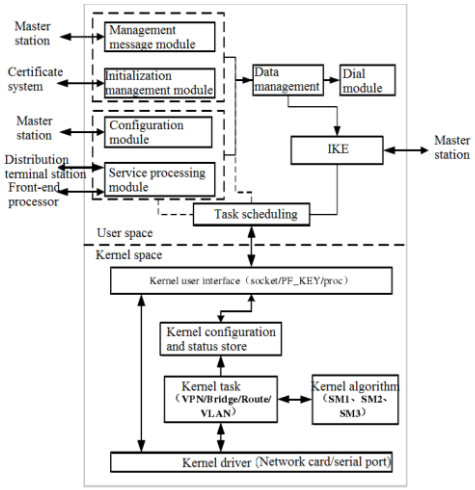
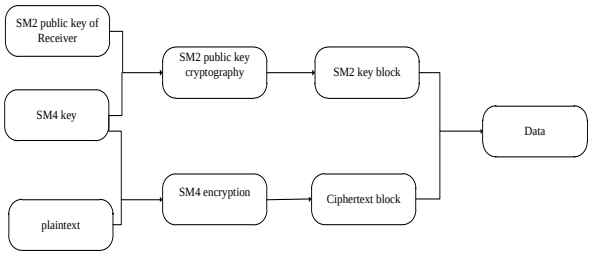


Fig.4 Module partition of software system for terminal security protection device

混合加密算法的加密流程为：假设 A 是数据发送方，B 为接收方（B 的公钥为 PublicB，私钥为 PrivateB），K 作为用于 SM4 加密的会话秘钥（AB 两者知道对方的 SM2 公钥），使用这种混合密码体制传输数据需要经过以下步骤，流程图如图所示：



FFig.5 Schematic diagram of data transmission process in mixed cipher system

- 发送方 A 生成随机的用于 SM4 算法加解密操作的秘钥 Key；
- A 从加密服务器得到到公开的接收方 SM2 公钥 PublicB；
- A 使用 SM4 的秘钥 Key 通过 SM4 算法对明文数据进行加密得到密文块 CipherData；
- A 使用接收方的公钥 PublicB 通过 SM2 算法将秘钥 Key 进行加密得到秘钥块 CipherKey；
- A 将秘钥块以及密文块打包一起作为数据发送；

接收方在接收到发送方发送的加密密文后，需要对其进行解密，其解密过程流程图如下图所示：

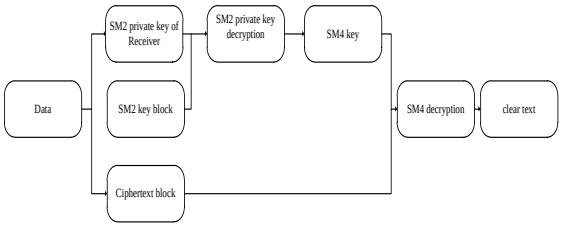


Fig.6 Mixed encryption and decryption algorithm flow chart

- 接收方 B 将接收的数据 Cipher 分为两个部分，密文块 CipherData 以及秘钥块 CipherKey；
- B 使用 SM2 算法私钥 PrivateB 对 CipherKey 进行 SM2 算法解密得到 SM4 秘钥 Key；
- B 使用得到的 SM4 秘钥对密文块采用 SM4 算法进行解密得到明文数据 Data。

3 研究结果与讨论

3.1 研究结果

为了验证所提方案的可行性与有效性，我们对其进行了仿真验证。采用同方 THD86 芯片作为仿真平台，对所提混合加密机制进行加

解密验证，CPU 工作频率为 16MHz。首先对其进行了可行性验证，如下表所示为对一段数据进行加密的中间密文数据：

Table.1 Data tables in the process of mixed cipher encryption

Data name	Length	Data
Data	16	0133456769ABCEFFEDCBE9876443210
Key	16	D521DA1F76283DG55FBOCCHF726685AA
PublicB	64	3613AZA687Z69B5E67C4191467847DZ4 B9F293A661Z32CB2F784F1232DDCC098 C0025DF427C3A7E96KWDE39E112817D9 B4FA32EDA469245Z313D1D310AAADC6D
PrivateB	32	9EA52SE361FDD07D85ZC9A0F7AC923FE 618GFC3ED46291D411Z84C57897F5F56
CipherData	16	220062E842D70327809078A338EFCC93
CipherKey	112	70D635444E67EDF43C1GC16J5ZA125F5 90E155DZ679DZ00065225749Z61E83Z8 E14C7LCDZ2E101D5CA993A1FF0Z85FCH 7F6FZE4155EDAF115Z5F1ZZZDF2373EF 3A4680282ZA9592111867211D980E37E 58FDZ10787CCFAE470BD06570FF21A60 5F66D1F4A9C007CFA7A4D24491F5F041
Cipher	128	220062E842D70327879078A338EFCC93 70D615446B67UDF56C1DCK605BF185F5 90E355DB679DB00065225749B61E83B8 E14N7BCDB3E106D5CF993A13F0B85FCB 7F6RBE4155EDAF115B5F1BBBDF2373EF 3W4680282BA2522111867911D970E31D 58KDB19787CCFAE170BDO6579FF21C60 5F26D1F4X9C007CFA7A4D24491F5F041

如上表 1 所示，混合密码算法可以完成对目标数据的加解密过程，实现方便可行，这表明所提方案是可行的。

为了验证所提方案的有效性，即可以有效完成配电网对于数据安全性的要求，我们对其进行性能验证。混合加密的目的主要是保护 SM4 算法产生的秘钥。而目前广泛采用的保护随机秘钥的算法是 RSA 算法，我们在同方 THD86 芯片上对 SM2 算法以及 RSA 算法性能进行仿真对比，芯片频率 16MHz，协处理器 32M，对比结果如下表所示：

Table.2 Comparison of SM2 and RSA algorithms

Algorithm	Encrypt (ms/time)	Decrypt (ms/time)
1024-bit RSA	65.1	17.4
256-bit SM2	52.5	94.1

通过如上表 2 的数据显示，SM2 算法相对于 RSA 算法在内存空间以及加密速度上都更具有优势。其加密时的速度要优于 RSA 算法，但解密速度要慢与 RSA。SM2 的秘钥长度为 256 位，远远小于 RSA 的 1024 位长度，这极大降低了存储要求。

3.2 讨论

通过以上的仿真结果表明，采用 SM4 和 SM2 算法相结合的混合加密方法可以有效实现配电网络数据的加解密。这也进而证明了混合加密体制应用于配电网数据安全传输的可行性，由于在加密过程中采用了两层加密体制即在 SM4 对报文进行加密后继续使用 SM2 算法对 SM4 的秘钥进行加密所以可以获得更高的安全性能。在在未来的实际应用中可以根据系统特点选择性地采用其他更有效的加密算法相结合的混合加密方案而不仅仅局限于 SM4 与 SM2 算法的组合。另一个方面通过 SM2 算法与 RSA 算法的对比发现，SM2 算法相对于 RSA 算法[7]算具有更快的加密速度与更少的内存需求。同时由于 SM2 算法基于椭圆曲线生成秘钥，这保证了其算法相对于 RSA 算法具有更好的安全性。这种采用多种不同加密算法相结合的理念可以运用于多个领域，例如云端数据加密，信息的安全传输等。

虽然以上结果表明了所提方案的可行性与有效性，但是依然存在一些不足之处。例如文章证实了所提方案的可行性，但是并没有对其在各种非法攻击下的安全性做定量分析。其次对比了其与 RSA 算法的性能，但是没有进一步分析两者在相同条件下的定量对比。这些不足都需要进一步工作进行深入研究与探讨。

4 结论

本文将国密 SM2 和 SM4 算法应用于智能配电网络的数据安全加密方案，提出了一种基于混合密码体制的配电网络数据安全传输方案。

通过模拟一段目标明文数据的传输验证了基于混合密码体制加密方案的可行性，并将 SM2 算法与 RSA 算法进行性能对比分析。数值仿真结果表明：采用混合密码体制的配电网络数据传输方案可以实现对目标数据的安全传输，完成数据的加解密操作。进一步 SM2 与 RSA 两种算法的性能对比结果表明，采用国密 SM2 算法可以获得更快的加密速度，同时降低了对系统内存的要求。因此，基于混合密码体制的配电网数据安全传输方案在获取高安全性的同时提高了加密效率并降低了系统内存开销，从而有利于推广混合密码体制在配电网络安全传输领域的应用。

参 考 文 献

[1] Giani, Annarita, et al. "Smart Grid Data Integrity Attacks." *IEEE Transactions on Smart Grid* 4.3(2013):1244-1253.

[2] Hu, Bin, and H. Gharavi. "Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkle Tree 4-Way Handshaking." *IEEE Transactions on Smart Grid* 5.2(2014):550-558.

[3] Bou-Harb, E., et al. "Communication security for smart grid distribution networks." *IEEE Communications Magazine* 51.1(2013):42-49.

[4] Khurana, Himanshu, et al. "Smart-grid security issues." *IEEE Security & Privacy Magazine* 8.1(2010):81-85.

[5] Park, Je Hong, M. Kim, and D. Kwon. "Security Weakness in the Smart Grid Key Distribution Scheme Proposed by Xia and Wang." *IEEE Transactions on Smart Grid* 4.3(2013):1613-1614.

[6] Fouda, Mostafa M., et al. "A Lightweight Message Authentication Scheme for Smart Grid Communications." *IEEE Transactions on Smart Grid* 2.4(2011):675-685.

[7] Usman, Ahmad, and Sajjad Haider Shami. "Evolution of communication technologies for smart grid applications." *Renewable and Sustainable Energy Reviews* 19 (2013): 191-199.

[8] Mantoro, Teddy, and A. Zakariya. "Securing E-mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices." *Telkomnika*10.4(2012):807-814.

[9] Kuppuswamy, Prakash, and Saeed QY Al-Khalidi. "Hybrid encryption/decryption technique using new public key and symmetric key algorithm." *International Journal of Information and Computer Security* 6.4 (2014): 372-382.

[10] Shehzad, Danish, et al. "A Novel Hybrid Encryption Scheme to Ensure Hadoop Based Cloud Data Security." *International Journal of Computer Science and Information Security* 14.4 (2016): 480-484.

[11] Song, Je-Ho, and Woo-Choun Lee. "The Design of Hybrid Cryptosystem for Smart Card." *Journal of the Korea Academia-Industrial cooperation Society*12.5 (2011): 2322-2326.

[12] Kaipa, Adi Narayana Reddy, et al. "A Hybrid Cryptosystem using Variable Length Sub Key Groups and Byte Substitution." *Journal of Computer Science* 10.2 (2014): 251-255.

[13] Gao, Na-na, Zhan-Cai Li, and Qin Wang. "A Reconfigurable Architecture for High-Speed Implementations of DES, 3DES and AES." *Acta Electronica Sinica* 34.8 (2006): 1386-1390.

[14] Hu, Xiangdong, H. Xu, and K. Han. "Design and Implementation of Secure Nodes in the Based-Internet-of-Things Intelligent Household. "*Journal of Computer & Communications* 02.7(2014):1-7.

[15] WANG, Chen-guang, Shu-shan QIAO, and Yong HEI. "Design of Low Complexity SM4 Block Cipher IP Core [J]." *Science Technology and Engineering* 2 (2013): 018-022.

[16] Yu, Siyang, et al. "A VLSI implementation of an SM4 algorithm resistant to power analysis." *Journal of Intelligent & Fuzzy Systems* 31.2 (2016): 795-803.

[17] NIE, Yi-xin, Bin-bin LIU, and Wei REN. "The Implementation and Evaluation of SM2 Algorithm in Java." *Netinfo Security* 8 (2013): 007-013.

[18] CHEN, Wen-qing, and Yan ZHU. "Research and application of SM2 digital signature algorithm in power line switch controller." *Journal of Electric Power Science and Technology* 3 (2015): 020-026.

付宇(1983-)，男，贵州六盘水，硕士研究生，高级工程师，研究方向为智能配电网与自动化技术研究。