中图分类号: TP391　文献标志码: A　文章编号: 2095-641X(2019)08-0018-06　DOI: 10.16543/j.2095-641x.electric.power.ict.2019.08.004
著录格式: 廖会敏 , 玄佳兴 , 甄平 , 等 . 泛在电力物联网信息安全综述 [J]. 电力信息与通信技术 , 2019, 17(8): 18-23.

泛在电力物联网信息安全综述

廖会敏[1,2],玄佳兴[1,2],甄平[1,2],李丽丽[1,2]
(1. 国网电子商务有限公司(国网雄安金融科技集团有限公司),北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室,北京 100053)

Overview of Information Security in Ubiquitous Power Internet of Things

LIAO Huimin[1,2], *XUAN Jiaxing*[1,2], *ZHEN Ping*[1,2], *LI Lili*[1,2]
(1. State Grid Electronic Commerce Co., Ltd., (State Grid Xiong'an Financial Technology Group Co., Ltd.), Beijing 100053, China; 2. Power Finance and E-commerce Laboratory, State Grid Corporation of China, Beijing 100053, China)

网络安全

摘要: 泛在电力物联网是能源互联网和泛在物联网在电力行业的具体实现形式和应用落地,其信息安全与互联网、物联网的信息安全相比,即有共性也有特性,主要面临的有访问控制、数据机密性和完整性、身份认证、隐私保护、可用性和不可抵赖性等信息安全问题。文章介绍了泛在电力物联网信息安全体系和感知层、网络层、平台层、应用层的信息安全,并分析了基础密码学和新型密码学技术在泛在电力物联网中的应用。

关键词: 泛在电力物联网; 信息安全; 密码学

Abstract: Ubiquitous Power Internet of Things (UPIoT) is the concrete realization form and application of the energy Internet and the ubiquitous Internet of Things in the power industry. Compared with the information security of the Internet and the Internet of Things, its information security has both commonalities and characteristics. It mainly faces such information security problems as access control, data confidentiality and integrity, identity authentication, privacy protection, availability and non-repudiation. This paper introduces the information security and information security of the perception layer, network layer, platform layer and application layer in the ubiquitous power Internet of Things, and analyses the application of basic cryptography and new cryptography technology in the ubiquitous power Internet of Things.

Key words: ubiquitous power Internet of things; information security; cryptography

0　引言

国家电网有限公司于 2019 年发布了《泛在电力物联网建设大纲》,泛在物联是在物联网的基础上,将其扩展和延伸到任何人、任何物、任何时间、任何地点之间的信息互联和交互,而泛在电力物联网是将电力的“发、输、变、配、用”中的用户、企业、设备、供应商、以及人和物连接起来的信息互联和交互[1]。

基金项目:国网电子商务有限公司(国网雄安金融科技集团有限公司)科技项目(5100/2019-72007B)。

狭义的信息安全是指保持信息的机密性、完整性、可用性,另外也可能包含其他的特性,如真实性、可核查性、抗抵赖和可靠性等[2]。广义的信息安全是将技术、管理、法规等相结合,保障网络系统的软件、硬件及系统中的信息受到保护,不因偶然或恶意攻击而受到威胁和破坏。在泛在电力物联网概念提出之前,信息安全在互联网、物联网的众多领域得到了广泛的应用[3],泛在电力物联网作为能源互联网和泛在物联网在电力行业的具体实现形式和应用落地,其信息安全与互联网、物联网的信息安全相比,

既有共性也有特性，主要面临的有访问控制、数据机密性和完整性、身份认证、隐私保护、可用性和不可抵赖性等信息安全问题[4]。

本文结合互联网信息安全、物联网信息安全和《泛在电力物联网建设大纲》，首先分析了泛在电力物联网建设过程中存在的主要信息安全需求，然后概述了泛在电力物联网的安全体系和4个层面的信息安全，最后介绍了密码学特别是新型密码学技术在泛在电力物联网中的应用。

1 泛在电力物联网主要信息安全需求

1.1 身份认证

身份是区别于其他个体的一种标识，身份认证是对用户身份的确认技术，是确定通信过程中一端或通信的两端个体是谁的过程。主流的身份认证方式有3种：一是账号+口令、验证码的认证方式；二是基于PKI技术的数字证书认证方式；三是以生物识别、用户行为分析为主导的认证方式[5]。

身份认证可以实现泛在电力物联网用户安全接入电力系统，使用户合理地使用各种资源和数据，它是泛在电力物联网信息安全的第一道防线。身份认证技术可以用来解决泛在电力物联网访问者的物理身份和数字身份的一致性，是整个泛在电力物联网信息安全体系的基础。

1.2 访问控制

访问控制是在保障授权用户能获取所需资源的同时拒绝非授权用户对任何资源进行访问的安全控制机制，基于角色的权限访问控制（Role-Based Access Control，RBAC）是目前信息系统中最常用的访问控制方式。访问控制包括主体、客体和安全访问策略，分为认证和授权2个过程[6]。

泛在电力物联网用户在访问电力系统时，系统通过验证用户的口令或数字证书等对其身份进行鉴别，验证通过后赋予用户相应的角色，访问策略通过对用户的访问目的与预期目的比对后，用户可以获取到与其权限相对应的资源。

1.3 数据安全

数据安全包括数据的机密性、完整性和可用性，机密性强调数据在授权范围内使用，完整性强调数据的防篡改功能，可用性强调数据能按需使用[7]。

泛在电力物联网的核心是海量数据在电力系统的应用。海量数据在通信过程中，一方面要保障敏感数据的机密性，能安全地低达最终目的地；另一方面确保数据在传输的过程中没有被修改，若数据被非法篡改应能够识别和校验。此外，还需保障数据能够可靠、快速的传输。

1.4 隐私保护

隐私保护是为了使用户既能享受各种应用和服务，又能保证其隐私不被泄露和滥用[8]。隐私保护包含数据隐私保护、个人隐私保护和位置隐私保护。

泛在电力物联网将电力系统的人和物联系起来，产生共享数据，实现人和物的互联互动，在交互的过程中必然会产生大量的时间、位置、行为、参与者、目的等信息，这些信息可能包含了人或物的敏感信息，如果不能进行有效的保护，容易在信息交互或共享的过程中被攻击者截取。个人信息若被泄露，可能给个人的财物、生活甚至是人身安全带来风险，设备信息若被滥用可能影响正常的生产秩序，构成严重的安全威胁。

2 泛在电力物联网信息安全体系

从信息安全的角度看，泛在电力物联网是一个多网并存的异构融合网络，与互联网、物联网相比具有相同的安全问题，也有其特殊的安全问题。泛在电力物联网的体系结构大致分为4个层次：感知层、网络层、平台层和应用层[9]（见图1）。

2.1 感知层信息安全

感知层包括以智能电表、摄像头、RFID、实物ID、智能传感器、GPS设备等为代表的一种或多种融合的信息感知设备[10]。

1）感知层是泛在电力物联网信息的来源，保障感知层的信息安全是泛在电力物联网的基础。感知层主要的安全威胁有：利用安全漏洞，获得感知节点的身份信息；通过伪造或仿冒身份与其他节点通信，监听用户信息，发布虚假消息、发起DOS攻击[11]；对传输的信息进行拦截、篡改、伪造、重放，使得用户业务无法正常开展；同时通过扫描实物ID、定位传感器、追踪GPS设备，使接入泛在电力物联网的用户存在隐私泄露的风险。

2）感知层的信息安全可以通过加强传感网络机密性的安全控制而得到进一步的保障，例如在泛在电力物联网构建中选择射频识别系统，根据实际需求考虑是否选择有密码和认证功能的模块；个别传感网需要节点认证，确保非法节点不能接入，认证

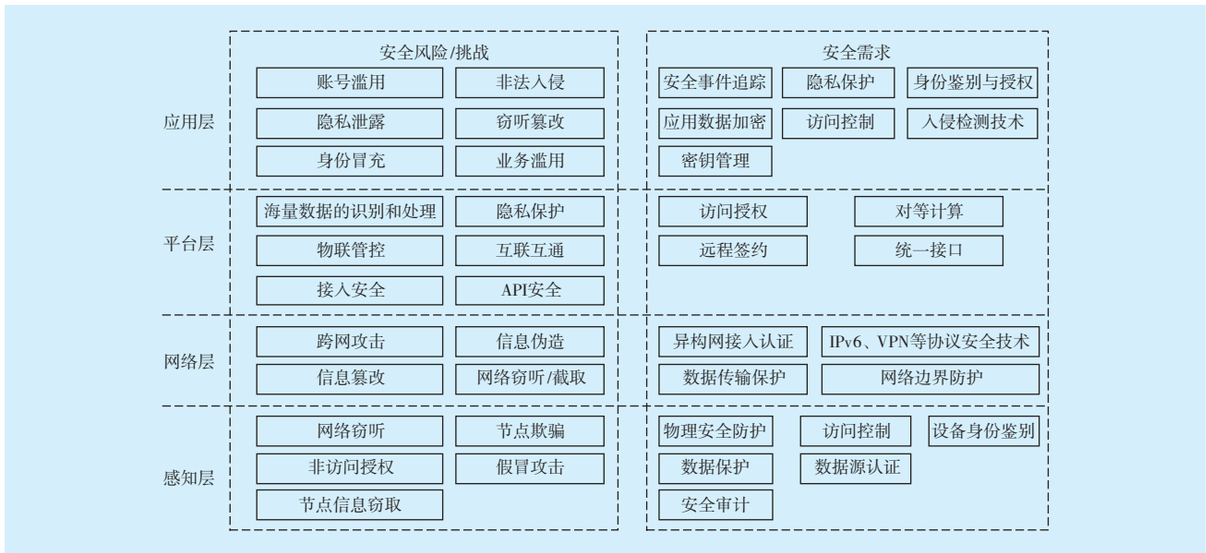

图 1 泛在电力物联网安全体系结构

Fig.1 Security architecture of ubiquitous power Internet of things

性可以通过数字证书解决；此外，还要提高传感器网络中的拓扑控制等技术，强化传感器网络的密钥管理[12,13]。

2.2 网络层信息安全

网络层是泛在电力物联网信息的传输层，主要将感知层采集到的信息安全可靠地传输到应用层以便进一步的处理和操作。

1）网络层传输距离远，通信范围广，传输途径经过各种不同的网络，会面临严重的安全威胁：①由于网络协议自身的缺陷，有些物联网的协议在设计之初，可能就只适合在物联网内部或是局域网之间使用；②拒绝服务攻击，如电网接入的终端数量巨大，防御能力薄弱，在攻击情况下容易造成网络冲突和拥塞；③攻击者在攻破电力物联网网络的通信后，窃取用户隐私及敏感信息造成隐私泄露[14]。

2）网络层的安全应对措施可从几个方面展开：①在网络层安装防火墙，给内部网络和外部网络之间提供一个安全屏障；②采用 SSL/TSL 协议的安全机制，对感知层传输过来的信息进行加密处理，然后再对信息进行传输，保障信息在传输过程中的安全；③采用轻量级算法，加快跨网认证，提高传输效率，才能有效地减少破坏者的攻击，从而保护信息的传输安全。

2.3 平台层信息安全

平台层是连接网络层和应用层的桥梁，平台层的意义就是把可以通用的软件功能模块化，避免重复开发。

1）平台层安全主要保障信息在计算、存储、传输过程中的安全，平台层必须采用适当的安全策略来保证泛在电力物联网中信息的机密性、完整性、可用性和不可抵赖性，此外还要保障接入安全及 API 安全。

2）平台层的安全可以根据应用的需求，对所有接入的设备和应用提供双向验证机制，进行身份鉴别和授权管理，确保接入的终端设备与传输的信息安全可靠；加强 API 调用的访问控制，防止未授权的访问，调用 API 接口前进行用户的鉴别，验证用户凭据和用户身份，防止篡改和重放攻击；对敏感数据加密防范数据被篡改[15]。

2.4 应用层信息安全

在泛在电力物联网发展过程中，大量的数据涉及到个人隐私，如用电数据、用户行为等。同时随着感知定位技术的发展，人们可以快速、精准地获知自己的位置，位置服务在给用户带来便利的同时也为心怀叵测者提供了攻击机会。

1）应用层通过对平台层传输过来的信息进行分析处理，为最终用户提供丰富的服务，如智能电网、电力交易、企业运营、电商平台等。应用层对平台层传输来的信息进行相应的处理后，可能再次通过平台层反馈给网络层和感知层。

2）应用层安全主要保障各类应用在用户使用过程中的安全，包括对用户的身份鉴别、访问控制、应用漏洞管理、外部攻击防护、隐私保护等。应用访问时进行强制认证和业务权限控制，应尽可能采用双因素身份验证机制，加强权限管理、端口控制和敏感信息访问等，防范应用本身漏洞而导致的数据被盗取或系统攻击[16]。

3 密码学技术的应用

密码学是信息安全的核心技术和基础支撑[17]。密码作为保护网络与信息安全的重要手段，在身份认证、安全隔离、信息加密、完整性保护和抗抵赖等方面发挥着不可替代的重要作用，能够有效保障泛在电力物联网网络系统的安全运行。

3.1 基础密码技术的应用

基础密码算法和技术包括对称密码、非对称密码、单向散列函数、数字签名、消息认证码和随机数生成算法。

1）对称密码是指加密和解密密钥是相同的，如SM4算法。

2）非对称加密也称公钥加密，含有一对密钥，用私钥进行解密和签名，再用配对的公钥进行加密和验签，公钥是公开的，而私钥是保密的，如SM2、SM9算法。

3）单向散列函数也称哈希函数、消息摘要算法等，能把任意长的输入消息串转变成固定长的输出串，输出值称为“散列值”或“消息摘要”，如SM3算法。

4）数字签名是签名者使用非对称算法的私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

5）消息认证码是一种确认消息完整性并进行认证的技术，消息认证码的输入包括任意长度的消息和一个发送者与接收者之间的共享密钥，它可以输出固定长度的数据，这个数据称为MAC值。

6）随机数生成算法并不能解决信息安全问题，但它承担了密钥生成、生成初始化向量、生成随机数据、抗重放攻击等功能，在密码学中占有重要的地位。

基础密码技术用于泛在电力物联网中的信息安全，提供信息的机密性、完整性、抗抵赖等服务，泛在电力物联网信息安全面临的威胁和对应的基础密码技术如图2所示。

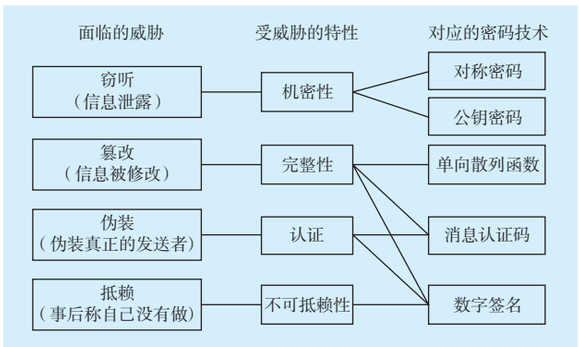

图2 泛在电力物联网信息安全面临的威胁和对应的基础密码技术

Fig.2 Threats to information security and corresponding cryptographic basic technology

3.2 新型密码技术的应用

新型密码技术主要是基于基础密码学，探索具有更多特性的密码技术，包括同态加密、白盒密码、门限密码、区块链、量子密码等。

1）同态加密。同态加密源于隐私同态，是在不解密密文的情况下直接对密文进行操作，同态加密使得人们对加密数据的比较、检索和分析等操作成为可能[18]。泛在电力物联网利用“大云物移智”等技术，大量的数据存储在云端，同态加密可应用于泛在电力物联网云平台，处理加密数据，在保障数据安全存储的同时又保护了数据的隐私。

2）白盒密码。白盒密码是能抵御白盒攻击的加密技术，它的核心思想是将密钥和原来的加密算法进行混淆[19]，目的是为了保护在白盒环境下密钥的安全性，从而在白盒环境下安全地进行加解密操作。白盒密码的一种具体实现形式，是在加密过程中进行一些改动设计，引入查找表的概念，其中混淆可以是密钥和查找表的混淆等。白盒密码可应用在泛在电力物联网智能终端和云平台。在智能终端采用白盒密码，可保护感知层密钥安全及设备安全；可对云平台上的软件使用白盒密码，保证在云平台进行数据的加解密运算时，用户的敏感信息不会被泄露。

3）门限密码。门限密码是以秘密共享方案为基础，将密钥在多个成员中共享，在密钥计算如解密、签名时各成员利用持有的密钥份额进行分别计算，通过合成后得到最终的计算结果[20]。基于门限密码的方案，可以开发协同计算的软件密码模块，模块以

SDK 的形态集成到泛在电力物联网各种业务场景的移动终端 APP 中，有效解决了传统 UKey 无法运用于移动终端的问题；门限密码的方案也可结合盲签名、环签名、群签名等手段实现一些数字签名场景的用户隐私保护。

4）区块链。区块链的核心是密码学，区块链是分布式数据存储、点对点传输、共识机制、加密算法等密码学和计算机技术的新型应用模式。区块链技术能够打通不同组织之间的信息通道，能更好地实现泛在电力物联网电力系统主链与各省侧链间的信息互通，以及国家电网有限公司内外部的信息互通。区块链采用分布式账本技术，通过在网络成员间共享、复制和同步的事务记录建立数字记录，可以有效解决泛在电力物联网建设过程中面临的数据融通、设备安全、个人隐私、架构僵化和多主体协同等问题 [21]。

5）量子密码。量子密码与经典密码不同，它依赖于物理学原理，采用“一次一密”，即每次向对方传送一个密钥时，这个密钥是随机的，而且要求安全地分发。如果被外界探测到，这次密钥将被作废，所以说量子密码是无条件安全的。利用量子物理原理，人们设计出了在理论上可以满足“一次一密“的加密要求，即量子密钥分发。利用量子密码技术，可建立泛在电力物联网密码服务平台，实现密钥的安全分发和保密通信，有效地解决基础密码体系中密钥生成和分发过程中的安全难题 [22]。

同态加密、白盒密码等新型密码技术可以解决泛在电力网中数据处理安全、白盒攻击、隐私保护、密钥分发等安全问题，它们之间的对应关系如图 3 所示。

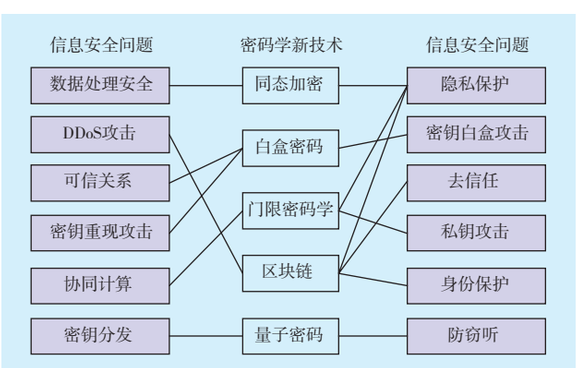

图 3 新型密码技术解决的信息安全问题

Fig.3 Information security problem solved by new cryptography technology

4 结语

随着国家电网有限公司泛在电力物联网建设大纲的落地，未来几年，建设和发展泛在电力物联网必将成为热点。泛在电力物联网的推广和运用，一方面将显著提高国家电网有限公司经济效益和电网系统运行效率；另一方面也对公民、企业，甚至是国家的信息安全和隐私保护等提出了严峻的挑战。有关部门应该未雨绸缪，尽早规划和研究泛在电力物联网 4 个层次的信息安全问题，利用传统密码学和新型密码学技术，为泛在电力物联网的安全运行和安全防护保驾护航。

参考文献：

[1] 国网互联网部. 泛在电力物联网建设大纲(节选)[J]. 华北电业, 2019, 35(3): 20-29.

[2] 李艳杰. GB/T 22080—2008《信息安全管理体系 要求》解析 解析系列五: GB/T22080—2008信息安全管理体系 要求 附录 A. 11—A. 15解析[J]. 中国标准导报, 2013, 22(1): 18-22.

[3] 郭建伟, 燕娜, 陈佳宇, 等. 智慧城市(物联网)信息安全建设研究[J]. 通信技术, 2017, 50(11): 2594-2599.
GUO Jianwei, YAN Na, CHEN Jiayu, et al. Smart city(IoT) InfoSec construction[J]. Communications Technology, 2017, 50(11): 2594-2599.

[4] 胡奥婷. 基于云存储环境的数据机密性及完整性机制研究[D]. 南京: 东南大学, 2018.

[5] 李小燕. 网络可信身份认证技术演变史及发展趋势研究[J]. 网络空间安全, 2018, 9(11): 6-11, 18.
LI Xiaoyan. Study on evolution history and development trend of network trusted identity authentication technology[J]. Cyberspace Security, 2018, 9(11): 6-11, 18.

[6] 任占胜. 数据访问权限控制方法的研究与实现[D]. 合肥: 安徽工业大学, 2016.

[7] 曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016, 53(10): 2137-2151.
CAO Zhenfu, DONG Xiaolei, ZHOU Jun, et al. Research advances on bigdata security and privacy preserving[J]. Journal of Computer Research and Development, 2016, 53(10): 2137-2151.

[8] 刘雅辉, 张铁赢, 靳小龙, 等. 大数据时代的个人隐私保护[J]. 计算机研究与发展, 2015, 52(1): 229-247.
LIU Yahui, ZHANG Tieying, JIN Xiaolong, et al. Personal privacy protection in the era of bigdata[J]. Journal of Computer Research and Development, 2015, 52(1): 229-247.

网络安全

[9] 张亚健, 杨挺, 孟广雨. 泛在电力物联网在智能配电系统应用综述及展望[J]. 电力建设, 2019, 40(6): 1-12.
ZHANG Yajian, YANG Ting, MENG Guangyu. Review and prospect of ubiquitous power internet of things in smart distribution system[J]. Electric Power Construction, 2019, 40(6): 1-12.

[10] 邓鹏程, 谢俭. 电力物联网统一信息感知模型研究[J]. 湖南电力, 2014, 34(3): 4-7.
DENG Pengcheng, XIE Jian. Research on an unified information perception mode for power system internet of things[J]. Hunan Electric Power, 2014, 34(3): 4-7.

[11] 陈春霖, 屠正伟, 郭靓. 国家电网公司网络与信息安全态势感知的实践[J]. 电力信息与通信技术, 2017, 15(6): 3-8.
CHEN Chunlin, TU Zhengwei, GUO Liang. Practice of network and information security situation awareness in SGCC[J]. Electric Power Information and Communication Technology, 2017, 15(6): 3-8.

[12] 胡祥义, 徐冠宁, 杜丽萍. 基于轻量级加密技术建立物联网感知层信息安全的解决方案[J]. 网络安全技术与应用, 2013, 13(3): 9-12.
HU Xiangyi, XU Guanning, DU Liping. The perception layer information security scheme for internet of things based on lightweight crypraphy[J]. Net Security Technologies and Application, 2013, 13(3): 9-12.

[13] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1): 40-53.
WU Chuankun. An overview on the security techniques and challenges of the internet of things[J]. Journal of Cryptologic Research, 2015, 2(1): 40-53.

[14] 曾鸣, 王雨晴, 李明珠, 等. 泛在电力物联网体系架构及实施方案初探[J]. 智慧电力, 2019, 47(4): 1-7, 58.
ZENG Ming, WANG Yuqing, LI Mingzhu, et al. Preliminary study on the architecture and implementation plan of widespread power internet of things[J]. Smart Power, 2019, 47(4): 1-7, 58.

[15] 李自清. 基于网络的数据库敏感数据加密模型研究[J]. 计算机测量与控制, 2017, 25(5): 184-187, 191.
LI Ziqing. Research of database sensitive data encryption model based on web[J]. Computer Measurement & Control, 2017, 25(5): 184-187, 191.

[16] 陶启茜, 马金兰. CDMA用户信息加密关键技术研究与实现方案探讨[J]. 电信科学, 2013, 29(S2): 38-42.

[17] 冉冉, 李峰, 王欣柳, 等. 一种面向隐私保护的电力大数据脱敏方案及应用研究[J]. 网络空间安全, 2018, 9(1): 105-113.
RAN Ran, LI Feng, WANG Xinliu, et al. A method of data desensitization for privacy protection in electric power industry and its application[J]. Cyberspace Security, 2018, 9(1): 105-113.

[18] 李宗育, 桂小林, 顾迎捷, 等. 同态加密技术及其在云计算隐私保护中的应用[J]. 软件学报, 2018, 29(7): 1830-1851.
LI Zongyu, GUI Xiaolin, GU Yingjie, et al. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing[J]. Journal of Software, 2018, 29(7): 1830-1851.

[19] 林婷婷, 来学嘉. 白盒密码研究[J]. 密码学报, 2015, 2(3): 258-267.
LIN Tingting, LAI Xuejia. Research on white-box cryptography[J]. Journal of Cryptologic Research, 2015, 2(3): 258-267.

[20] 尚铭, 马原, 林璟锵, 等. SM2椭圆曲线门限密码算法[J]. 密码学报, 2014, 1(2): 155-166.
SHANG Ming, MA Yuan, LIN Jingqiang, et al. A threshold scheme for SM2 elliptic curve cryptographic algorithm[J]. Journal of Cryptologic Research, 2014, 1(2): 155-166.

[21] 赵曰浩, 彭克, 徐丙垠, 等. 能源区块链应用工程现状与展望[J]. 电力系统自动化, 2019, 43(7): 14-24, 58.
ZHAO Yuehao, PENG Ke, XU Bingyin, et al. Status and prospect of pilot project of energy blockchain[J]. Automation of Electric Power Systems, 2019, 43(7): 14-24, 58.

[22] 王栋, 李国春, 俞学豪, 等. 基于量子保密通信的国产密码服务云平台建设思路[J]. 电信科学, 2018, 34(7): 171-178.
WANG Dong, LI Guochun, YU Xuehao, et al. Construction contemplation of cloud platform for domestic password service based on quantum secret communication[J]. Telecommunications Science, 2018, 34(7): 171-178.

编辑　张钦芝
收稿日期：2019-05-20


廖会敏

作者简介：

廖会敏(1983–),男,高级工程师,从事密码学、信息安全、物联网等方面的研究工作,121356097@qq.com;

玄佳兴(1990–),男,工程师,从事区块链、电力信息化等方面的研究工作;

甄平(1987–),男,博士,从事密码学、区块链、物联网等方面的研究工作;

李丽丽(1983–),女,高级工程师,从事电力信息化研究工作。

网络安全