密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2021, 8(4): 680–683

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

国产商用公钥密码专栏

国产商用公钥密码专栏序言 (中英文)

翁 健[1], 黄欣沂[2], 何德彪[3]

1. 暨南大学, 广州 510632
2. 福建师范大学 计算机与网络空间安全学院, 福州 350117
3. 武汉大学 国家网络安全学院, 武汉 430072

通信作者: 黄欣沂, E-mail: xyhuang@fjnu.edu.cn

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000469

中文引用格式: 翁健, 黄欣沂, 何德彪. 国产商用公钥密码专栏序言 (中英文)[J]. 密码学报, 2021, 8(4): 680–683. [DOI: 10.13868/j.cnki.jcr.000469]

英文引用格式: WENG J, HUANG X Y, HE D B. Preface of special column on SM public-key cryptography[J]. Journal of Cryptologic Research, 2021, 8(4): 680–683. [DOI: 10.13868/j.cnki.jcr.000469]

Preface of Special Column on SM Public-Key Cryptography

WENG Jian[1], HUANG Xin-Yi[2], HE De-Biao[3]

1. Jinan University, Guangzhou 510632, China
2. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
3. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Corresponding author: HUANG Xin-Yi, E-mail: xyhuang@fjnu.edu.cn

密码是国家的重要战略资源, 直接关系国家政治安全、经济安全、国防安全和信息安全. 根据 2020 年 1 月 1 日正式施行的《中华人民共和国密码法》, 密码分为核心密码、普通密码和商用密码. 核心密码、普通密码用于保护国家秘密信息, 属于国家秘密; 商用密码用于保护不属于国家秘密的信息, 公民、法人和其他组织可以依法使用商用密码保护网络与信息安全. 由国家密码管理局组织, 我国自主设计的基于椭圆曲线公钥密码算法 SM2、密码杂凑算法 SM3、分组密码算法 SM4、序列密码算法祖冲之 (ZUC)、标识密码算法 SM9 等商用密码已成为国家标准, 有效保障了国家网络与信息安全.

虽然国产商用密码实现了 “从无到有” 的跨越式发展, 但其设计初衷是满足网络与信息系统的共性基础安全需求. 随着信息化进程不断推进, 越来越多的敏感服务开始陆续上线, 衍生出渗漏免疫、匿名认证、双盲认证、多人共享、不可诽谤等新型安全需求, 亟需依托已有的国产商用密码, 开展功能型密码的研究, 为网络与信息系统继续提供有效的安全服务.

本期《密码学报》组织 “国产商用公钥密码” 专栏, 主要针对国产商用密码中的 SM2、SM9 等公钥密码算法, 根据网络与信息系统的新型安全需求, 结合其发展现状, 小规模地展示我国学者近期在该领域的研究进展. 本专栏共收录 4 篇论文, 分别简介如下:

收稿日期: 2021-08-15 定稿日期: 2021-08-20

论文《SM2 密码算法密钥渗漏分析》, 针对国产商用密码算法使用过程中易遭受一系列不同动机的分析和攻击问题, 选取 SM2 数字签名算法和公钥加密算法作为分析对象, 提出两种高效难检测的密钥渗漏攻击: (1) 针对 SM2 数字签名算法, 密钥渗漏攻击者能够根据两个连续的数字签名成功还原完整签名私钥; (2) 针对 SM2 公钥加密算法, 密钥渗漏攻击者可根据当前的密文成功预测下一次加密的会话密钥, 从而具备解密密文的能力. 因此, SM2 面临的密钥渗漏威胁比目前已知的通用攻击更严重. 针对发现的高效攻击, 本文探讨了适用于 SM2 的抗密钥渗漏技术, 保障 SM2 数字签名算法和 SM2 公钥加密算法的安全性.

论文《基于 SM2 的多接收方公钥加密方案》, 针对网络与信息系统单发送者—多接收者的数据安全共享需求, 基于 SM2 公钥加密算法提出一种随机数可重用的多接收方公钥加密方案, 并在随机预言机模型下证明方案满足 IND-CCA 安全性. 此方案能够在多用户开放网络环境保护数据隐私, 所使用的随机数重用技术能够有效减少发送方计算量, 极大地提高加密算法效率.

论文《基于 SM2 数字签名算法的环签名方案》, 针对网络与信息系统的匿名认证和国产自主化需求, 基于 SM2 数字签名算法提出环签名方案、可链接环签名方案以及两种变型, 并证明环签名方案满足正确性、不可伪造性和无条件匿名性, 可链接环签名方案满足正确性、不可伪造性、无条件匿名性、可链接性和不可诽谤性, 最后通过性能评估说明几种方案的通信量和计算量均与环成员数量呈线性关系.

论文《基于 SM9 标识密码算法的环签名方案》, 针对标识体系环签名具有匿名保护和避免繁琐公钥证书管理的特点, 基于 SM9 标识数字签名算法构造一种基于标识的环签名方案, 此方案与 SM9 的用户签名密钥生成方式具有一致性, 并在随机谕言机模型下证明此方案具有不可伪造性和匿名性, 最后通过效率分析说明了方案的签名计算开销和通信代价比现有方案少, 具有更强的实用性.

希望本专栏能够让更多国内学者关注国产商用密码的分析与设计.

Cryptography is an important strategic resource of a country, which is directly related to national security including political, economic, national defense, and information security. The Cryptography Law of the People's Republic of China has been inplemented since January 1, 2020. Accordingly, cryptography is classified into core, common, and SM cryptographies. The core and common cryptographies are used to protect national classified information (i.e. state secrets), and the SM cryptography is to protect other information but not state secrets. Citizens, legal persons, and other organizations may use the SM cryptography to protect network and information security lawfully. Organized by the State Cryptography Administration, Chinese independent SM crypto algorithms (e.g. elliptic curve public key cryptography SM2, cryptography hash algorithm SM3, block cipher algorithm SM4, stream cipher algorithm ZUC, and identity-based cryptography algorithm SM9) have become the national standard, effectively guaranteeing the national network and information security.

While SM crypto algorithms have achieved a leapfrogging development from scratch, their original intention is to meet the basic security requirements of network and information systems (NIS). With the continuous advancement of the informatization process, more and more sensitive services are provided online. This has derived various security requirements such as leakage immunity, anonymous authentication, double-blind authentication, sharing among multiple users, and non-slanderability. It is urgent to carry out the research on functional cryptographies from existing SM crypto algorithms, such that providing continuous and effective security services for NIS.

This special column titled "SM Public-Key Cryptography", organized by Journal of Cryptologic Research, mainly focuses on public-key cryptography algorithms such as SM2 and SM9 in Chinese SM cryptography, aiming at collecting state-of-the-art research progress of Chinese scholars in this field, according to the new security requirements of networks and information systems, and combined with its development status. This special column includes four papers, they are briefly summarized as follows.

The paper titled "Key Exfiltration on SM2 Cryptographic Algorithms" discusses the vulnerability of SM crypto algorithms to various cryptoanalyses and attacks with different motivations. This paper primarily investigates the security of the SM2 cryptographic algorithms against key exfiltration attacks and proposes two effective while undetectable attacks on the signature and public-key encryption scheme of the SM2. The first attack is on the SM2 signature scheme, which enables the attacker to recover the secret key from two successive signatures. The second attack is on the SM2 public-key encryption scheme, which enables the attacker to successfully predicate the current session key from the previous ciphertext hence to recover the plaintext. The attacks show that the impact of key exfiltration attacks on the SM2 cryptographic algorithms could be much more effective than other known attacks. Further discussion on effective approaches to enhance the security of SM2 encryption and signature schemes against the proposed key exfiltration attacks is presented.

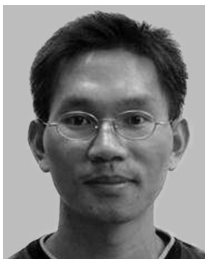
The paper titled "SM2-Based Multi-Recipient Public-Key Encryption" focuses on the secure data sharing requirement among one sender and multiple receivers in NIS. This paper proposes a randomness re-using multi-recipient public-key encryption (RR-MRPKE) scheme based on SM2 encryption scheme, and proves that it is IND-CCA secure (in the sense of MRPKE) in the random oracle model. The proposed scheme provides data privacy in open networks, and the employing technology of randomness re-using can effectively reduce the amount of computation and improve the encryption efficiency.

The paper titled "Ring Signature Schemes Based on SM2 Digital Signature Algorithm" considers the requirements of anonymity authentication and Chinese independence in NIS. This paper proposes a ring signature scheme and a linkable ring signature scheme based on SM2 digital signature algorithm, as well as two variations of SM2 linkable ring signature scheme. It is shown that, SM2 ring signature scheme satisfies correctness, unforgeability, and unconditional anonymity. SM2 linkable ring signature scheme is with correctness, unforgeability, unconditional anonymity, linkability, and non-slanderability. The final efficiency analysis demonstrates that the communication costs and computation costs of these designed schemes are respectively linear with the number of ring members.

The paper titled "An Identity-Based Ring Signature Scheme for SM9 Algorithm" finds that the identity-based cryptographic system owns anonymity protection and avoids the complex public key certificate management. This paper constructs an identity-based ring signature scheme based on SM9 signature scheme, which has the consistence of the user private key generation algorithm to the SM9 signature scheme. Moreover, this paper proves that the proposed ring signature scheme satisfies the unforgeability and anonymity under the random oracle model. The final efficiency analysis shows that the proposed scheme is with less computation costs and communication overheads than existing schemes, and hence owns the stronger utility.

Hope this special issue may attract more researchers to focus on the cryptoanalysis and design of SM crypto algorithms.

作者信息



翁健(1976–), 博士, 教授, 博士生导师. 主要研究领域为密码学与信息安全.
cryptjweng@gmail.com

WENG Jian (1976–), Ph.D., Professor, Doctoral Tutor. Main research covers cryptography and information security.
cryptjweng@gmail.com

黄欣沂 (1981–), 江苏仪征人, 博士, 教授, 博士生导师. 主要研究领域为公钥密码学.
xyhuang@fjnu.edu.cn

HUANG Xin-Yi (1981–), Ph.D., Professor, Doctoral Tutor. Main research covers public-key cryptography.
xyhuang@fjnu.edu.cn

何德彪 (1980–), 山东阳谷人, 博士, 教授, 博士生导师. 主要研究领域为公钥密码学、网络与信息安全.
hedebiao@163.com

HE De-Biao (1980–), Ph.D., Professor, Doctoral Tutor. Main research covers public-key cryptography, network and information security.
hedebiao@163.com