密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(3): 290–310

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

密码应用安全专刊

密码应用安全技术研究及软件密码模块检测的讨论*

郑昉昱[1,2], 林璟锵[1,2,3,4], 魏 荣[1,2,3], 王琼霄[1,2,3]

1. 中国科学院 数据与通信保护研究教育中心, 北京 100093
2. 中国科学院 信息工程研究所 信息安全国家重点实验室, 北京 100093
3. 中国科学院大学 网络空间安全学院, 北京 100049
4. 中国科学技术大学 网络空间安全学院, 合肥 230026

通信作者: 林璟锵, E-mail: linjingqiang@iie.ac.cn

摘 要: 基于密码学原理的安全解决方案是网络空间安全研究的重要内容, 能够为信息系统提供各种必要安全保障. 然而, 许多现实事例表明, 在信息系统中完善地实施密码技术并非易事. 尤其是, 在现实系统中, 实现密码理论方案的运行假设和前提条件非常困难, 例如, 选用语义安全的协议、不可预测的随机数和攻击者不能访问的密钥等. 近年来, 学术界取得了大量相关技术研究成果, 包括安全问题和相应的解决方案 (本文称为密码应用安全技术研究). 另一方面, 密码模块检测一直都是密码技术实际应用的重要环节: 通过对密码模块的技术要求和检测, 确保能够正确有效地实现密码算法功能. 本文分析了当前密码应用安全技术研究和密码模块检测的安全要求, 揭示了二者在密码理论方案的实现安全方面的联系和差异. 然后, 本文总结了现有密码应用安全技术研究成果, 包括密码理论方案的选用、随机数发生器的设计和实现、密钥安全、密码计算的使用控制、密钥管理和 PKI 基础设施、以及应用功能密码协议的实现安全等方向. 最后, 基于现有密码应用安全技术研究成果, 本文讨论了软件密码实现的特殊性和具体实施的注意事项.

关键词: 密码应用; 密码模块; 密码模块检测; 软件密码实现

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000369

中文引用格式: 郑昉昱, 林璟锵, 魏荣, 王琼霄. 密码应用安全技术研究及软件密码模块检测的讨论[J]. 密码学报, 2020, 7(3): 290–310. [DOI: 10.13868/j.cnki.jcr.000369]

英文引用格式: ZHENG F Y, LIN J Q, WEI R, WANG Q X. Research progresses on security applications of cryptography and discussions on validation of software cryptographic modules[J]. Journal of Cryptologic Research, 2020, 7(3): 290–310. [DOI: 10.13868/j.cnki.jcr.000369]

Research Progresses on Security Applications of Cryptography and Discussions on Validation of Software Cryptographic Modules

ZHENG Fang-Yu[1,2], LIN Jing-Qiang[1,2,3,4], WEI Rong[1,2,3], WANG Qiong-Xiao[1,2,3]

1. Data Assurance and Commnications Security Research Center, Chinese Academy of Sciences, Bejing 100093, China

* 基金项目: 国家重点研发计划网络空间安全重点专项 (2017YFB0802100); 国家自然科学基金 (61772518, 61902392)
Foundation: National Key Research and Development Program of China (2017YFB0802100); National Natural Science Foundation of China (61772518, 61902392)
收稿日期: 2020-06-10 定稿日期: 2020-06-20