密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(5): 595–604

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

支持国密算法的 JavaScript 通用密码库的实现*

魏 荣[1,2,3], 郑昉昱[1,2], 林璟锵[3,4]

1. 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
2. 中国科学院 数据与通信保护研究教育中心, 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: 郑昉昱, E-mail: zhengfangyu@iie.ac.cn

摘 要: 随着近年来 Web 应用的大量普及及其安全问题的频发, 用 JavaScript 进行一些密码运算的需求也随之而来. 相比传统外插硬件外加驱动的密码计算模式, 用 JavaScript 实现密码算法具有跨平台、免安装、兼容性好的优点. 我们基于一款用 JavaScript 编写的国际密码算法库, 加入了国密 SM2、SM3 和 SM4 算法, 并使用固定基的 comb 方法对椭圆曲线固定点的标量乘进行了优化, 使密钥生成和签名速度提升了一倍以上. 在保证运算速度的同时, 我们也尽量保持了代码量的最小化, 以减小流量消耗和下载时长. 我们在 Chrome、Firefox、Opera 和 Maxthon 浏览器中进行了验证和性能评估, 在 Firefox 上, SM2 签名算法性能达到了每秒生成 100 对密钥, 签名 95 次, 验签 40 次, SM3 算法速度达到了 69.75 Mbps, SM4 算法速度达到了 110.97 Mbps.

关键词: Web 应用; JavaScript; 国密算法; 标量乘; 密码库

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000392

中文引用格式: 魏荣, 郑昉昱, 林璟锵. 支持国密算法的 JavaScript 通用密码库的实现[J]. 密码学报, 2020, 7(5): 595–604. [DOI: 10.13868/j.cnki.jcr.000392]

英文引用格式: WEI R, ZHENG F Y, LIN J Q. Implementation of a general-purpose cryptography library supporting domestic algorithm with JavaScript[J]. Journal of Cryptologic Research, 2020, 7(5): 595–604. [DOI: 10.13868/j.cnki.jcr.000392]

Implementation of a General-purpose Cryptography Library Supporting Domestic Algorithm with JavaScript

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

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. Data Assurance and Communications Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
3. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
4. School of Cyber Security, University of Science and Technology of China, Hefei 230026, China

Corresponding author: ZHENG Fang-Yu, E-mail: zhengfangyu@iie.ac.cn

* 基金项目: 国家重点研发计划 (2017YFB0802100); 国家自然科学基金 (61772518)
Foundation: National Key Research and Development Program of China (2017YFB0802100); National Natural Science Foundation of China (61772518)
收稿日期: 2019-06-25 定稿日期: 2019-08-27