基于 GPU 的 X25519/448 密钥协商算法的高速实现

董建阔[1,2,3], 郑昉昱[1,2], 林璟锵[1,2,3]

[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 中国 100093
[2] 中国科学院数据与通信保护研究教育中心 北京 中国 100093
[3] 中国科学院大学网络空间安全学院 北京 中国 100049

摘要 密钥协商算法目前被广泛运用于包括TLS/SSL在内的各种安全协议中, 以支持通信双方在不被保护的信道中建立共享秘密。特别是在 TLS 1.3 中, 为保证前向安全性(forward secrecy), 移除了利用静态 RSA 公钥加密算法进行密钥交换的方式, 仅保留 Diffie Hellman(DH)密钥协商算法, 并引入了一个新的密钥协商算法 X25519/448。相比于 TLS 1.3 其他两类 DH 密钥协商算法(有限域 DH 和基于 NIST-P 曲线的椭圆曲线 DH), X25519/448 的计算量更小且参数的选取过程公开, 更受产业界青睐。事实上, 包括 OpenSSH 在内的众多开源项目已经将 X25519/448 作为默认的密钥协商算法。虽然 X25519/448 的计算量相对较小, 但是在云计算、电子交易等大规模并发请求的场景下, 它所依赖的椭圆曲线点乘运算仍然是性能瓶颈。本文利用图形处理器(Graphics Processing Unit, GPU)针对 X25519/448 进行了多层次的性能优化, 同时考虑了可能的计时攻击威胁, 完成性能的最大化。所实现的 X25519/448 在桌面级 GPU GTX 1080 达到每秒 2860412/357944 次操作, 在嵌入式 GPU Tegra X2 上达到每秒 155459/17909 次操作, 性能远远超过 CPU、FPGA 和同类 GPU 平台实现。其中, Tegra X2 上的 X25519 实现分别是 ARM CPU 的 8.5 倍和 FPGA 的 13.2 倍, 体现了 GPU 在嵌入式密码计算领域的强大潜能。

关键词 Curve25519; Curve448; GPU; 密钥协商
中图法分类号 TP309.2 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2020.11.06

Implementing High-performance X25519/448 Key Agreement Scheme in General Purpose GPUs

DONG Jiankuo[1,2,3], ZHENG Fangyu[1,2], LIN Jingqiang[1,2,3]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Widely used in a large range of Internet security protocols such as TLS/SSL, the key exchange provides a method to establish a shared secret between two parties in unprotected channel. Especially in TLS 1.3, in order to ensure forward secrecy, the key exchange method using static RSA public key encryption algorithm is removed, only Diffie Hellman (DH) key agreement algorithm is retained, and a new key agreement algorithm X25519/448 is introduced. Compared with other two DH key agreement algorithms (finite field DH and elliptic curve DH based on NIST-P curve) in TLS 1.3, X25519/448 has less computation and the process of parameter selection is undisguised, which is more favored by the industry. In fact, many open source projects, including OpenSSH, have adopted X25519/448 as the default key exchange algorithm. Although X25519/448 has relatively small computational complexity, the point multiplication of elliptic curves in large-scale concurrent requests such as cloud computing and electronic transactions, is still a performance bottleneck. In this paper, the Graphics Processing Unit (GPU) is used to optimize the performance of X25519/448 at different levels. And in consideration of the possible threat of timing attack, we maximize the performance. The X25519/448 achieved 2860412/357944 ops/s on the desktop GPU GTX 1080 and 155459/17909 ops/s on the embedded GPU Tegra X2. The performance of the X25519/448 is far outstripped the CPU, FPGA and similar GPU platforms. Among them, the X25519 implementations on Tegra X2 is 8.5 times of ARM CPU and 13.2 times of FPGA, respectively, reflecting the strong potential of GPU in the field of embedded cryptographic computing.

通讯作者: 郑昉昱, 博士, 助理研究员, Email: zhengfangyu@iie.ac.cn。

本论文工作得到自然科学基金“通用计算平台的密钥保护技术研究”(No. 61772518)、自然科学基金“基于并行平台和人工智能加速器的高性能密码计算技术研究”(No. 61902392)和国家重点研发计划网络空间安全重点专项“基于国产密码算法的移动互联网密码服务支撑基础设施关键技术”(No. 2017YFB0802100)资助。
收稿日期: 2018-08-30; 修改日期: 2018-11-20; 定稿日期: 2020-09-22