TX-RSA: A High Performance RSA Implementation Scheme on NVIDIA Tegra X2

Jiankuo Dong[1,2], Guang Fan[3,5], Fangyu Zheng[3,5(✉)], Jingqiang Lin[4], and Fu Xiao[1]

[1] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
[2] Guangxi Key Laboratory of Cryptography and Information Security, Guilin, China
[3] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
zhengfangyu@iie.ac.cn
[4] School of Cyber Security, University of Science and Technology of China, Hefei, China
[5] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China

Abstract. Driven by computer vision and autopilot industries, embedded graphics processing units (GPUs) are now rapidly achieving extraordinary computing power, such NVIDIA Tegra K1/X1/X2, which are widely used in embedded environments such as mobile phones, game console and vehicle-mounted systems. Such performance advantages give embedded GPUs the possibility of accelerating cryptography that also requires high-density computing. In this paper, we implement TX-RSA in embedded GPU platforms, i.e., NVIDIA TX2, to accelerate the most prevailing public-key cryptosystem, RSA. Various optimization methods are employed to promote the efficiency, including multi-threaded Montgomery multiplication and CRT implementation on the resource-constricted embedded GPUs. Within 20 W of power consumption, TX-RSA can deliver 6,423 ops/s of RSA encryption and 131,324 ops/s of RSA decryption, which outperforms implementations in the desktop GPUs and embedded CPUs in the perspective of performance-to-power ratio.

Keywords: RSA · CUDA · Embedded GPU

1 Introduction

With the rapid development of all kinds of network services, a huge number of transactions are generated in electronic commerce, digital publishing, software

This work was partially supported by National Natural Science Foundation of China under Award No. 61902392 and Guangxi Key Laboratory of Cryptography and Information Security (No. CIS202120).

Z. Liu et al. (Eds.): WASA 2021, LNCS 12938, pp. 210–222, 2021.
https://doi.org/10.1007/978-3-030-86130-8_17