# EC-ECC: Accelerating Elliptic Curve Cryptography for Edge Computing on Embedded GPU TX2

JIANKUO DONG, School of Computer Science, Nanjing University of Posts and Telecommunications, China
FANGYU ZHENG*, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
JINGQIANG LIN, School of Cyber Security, University of Science and Technology of China, China
ZHE LIU, College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China
FU XIAO, School of Computer Science, Nanjing University of Posts and Telecommunications, China
GUANG FAN, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China

Driven by artificial intelligence and computer vision industries, Graphics Processing Units (GPUs) are now rapidly achieving extraordinary computing power. In particular, the NVIDIA Tegra K1/X1/X2 embedded GPU platforms, which are also treated as edge computing devices, are now widely used in embedded environments such as mobile phones, game consoles and vehicle-mounted systems to support high-dimension display, auto-pilot, etc. Meanwhile, with the rise of the Internet of Things (IoT), the demand for cryptographic operations for secure communications and authentications between edge computing nodes and IoT devices is also expanding. In this contribution, instead of the conventional implementations based on FPGA, ASIC and ARM CPUs, we provide an alternative solution for cryptographic implementation on embedded GPU devices. Targeting the new cipher suite added in TLS 1.3, we implement Edwards25519/448 and Curve25519/448 on an edge computing platform, embedded GPU NVIDIA Tegra X2, where various performance optimizations are customized for the target platform, including a novel parallel method for the register-limited embedded GPUs. With about 15 watts of power consumption, it can provide 210k/31k ops/s of Curve25519/448 scalar multiplication, 834k/123k ops/s of fixed-point Edwards25519/448 scalar multiplication, and 150k/22k ops/s of unknown-point one, which are respectively the primitives and main workloads of key agreement, signature generation and verification of TLS 1.3 protocol. Our implementations achieve 8 to 26 times speedup of OpenSSL running in the very powerful ARM CPU of the same platform and outperform the state-of-the-art implementations in FPGA by a wide margin with better power efficiency.

CCS Concepts: • **Security and privacy → Digital signatures**.

*Fangyu Zheng is the corresponding author.

This work is supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803400, in part by CCF-Tencent Open Fund under Grant RAGR20210130 and RAGR20210131, in part by National Natural Science Foundation of China under Grant 61902392 and 62132008, and in part by Open Project of National Engineering Laboratory for Mobile Internet System and Application Security.
Authors' addresses: Jiankuo Dong, djiankuo@njupt.edu.cn, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, JiangSu, China; Fangyu Zheng, zhengfangyu@iie.ac.cn, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; Jingqiang Lin, linjq@ustc.edu.cn, School of Cyber Security, University of Science and Technology of China, Hefei, China; Zhe Liu, zhe.liu@nuaa.edu.cn, College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China; Fu Xiao, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, JiangSu, China; Guang Fan, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.


Manuscript submitted to ACM