DPF-ECC: Accelerating Elliptic Curve Cryptography with Floating-Point Computing Power of GPUs

Lili Gao*†‡, Fangyu Zheng*†, Niall Emmart§, Jiankuo Dong*†‡, Jingqiang Lin*†‡, Charles Weems§
*State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
†School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
‡Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China
§College of Information and Computer Sciences, University of Massachusetts, Amherst, MA 01003-4610, USA

***Abstract*—Driven by artificial intelligence (AI) and computer vision industries, Graphics Processing Units (GPUs) are now rapidly achieving extraordinary computing power. In particular, the floating-point computing power, which is heavily relied on by graphics rendering and AI computation workload, is developing much faster in GPUs. Meanwhile, in many fields such as e-commerce and online finance, the demand for cryptographic operations for secure communications and authentication is also expanding.**

In this contribution, targeting the important cryptographic primitives widely used in TLS 1.3, etc., we implement Curve25519 and Edwards25519 with GPUs' floating-point computing power, where various performance optimization methods are customized for the target platform, including novel big-number representations combined with a new floating-point-based computing algorithm, efficient merged reduction strategies, and curve-level acceleration. This paper reports record-setting performance for the elliptic-curve method: on TITAN V, we respectively achieve 7.21 and 77.30 million operations per second of unknown and known point multiplication of Edwards25519, and 13.55 million operations per second of point multiplication of Curve25519. To the best of our knowledge, this contribution is the first to show that floating-point-based ECC implementations can outperform the integer-based ones by a huge margin. The experimental result in Tesla P100 achieves over double performance of the existing fastest integer work on the same platform, and the result in TITAN V sets a record for the throughput which is 4.43 times better than the second.

***Index Terms*—Elliptic Curve Cryptography; Graphics Processing Unit; Double Precision Floating-point**

I. Introduction

The proliferation of the Internet has given rise to financial, electronic commerce and other industries which serve huge-scale users. Used ubiquitously in security-sensitive applications of these industries, public key cryptosystems are fundamental to security. Elliptic Curve Cryptography (ECC) [1, 2], one of the mainstream asymmetric cryptographic algorithms, is widely used to guarantee transmission security, and privacy protection of users including key exchange, digital signature, etc. Thanks to its shorter key size and better performance, it is now replacing the prevailing RSA public key cryptography.

Since the Prism Gate broke out in 2013, one of ECC, Curve25519 which was designed by Daniel J. Bernstein in 2006 [3] has been gaining popularity in a wide range of protocols and software because of its outstanding efficiency and security. In 2016, RFC 7748 [4] released by the Internet Research Task Force (IRTF) recommended Curve25519 for an Elliptic Curve Diffie-Hellman (ECDH) protocol. Under a change of coordinates from Curve25519 to twisted Edwards curves [5], Edwards25519 is used in Edwards-Curve Digital Signature Algorithm (EdDSA, RFC 8032 [6]), which is designed to be faster than existing digital signature schemes without sacrificing security.

Curve25519/Edwards25519 are used in many prevailing cryptographic protocols and networks, such as TLS 1.3 [7], SSH [8], password-authenticated key exchange (e.g., RFC 8236 J-PAKE [9]). Software and protocols that have deployed Curve25519/Edwards25519 in recent years are listed in [10, 11] in detail.

A. Technical Challenges

In fact, ECC algorithms whose chief cryptographic primitive is point multiplication, are far more computationally expensive than symmetric algorithms, e.g., block ciphers and hash functions. Some of the protocols even require multiple operations of the ECC primitives, for example, J-PAKE requires 11 scalar multiplications in a single session.

The ECC algorithm is not only computationally intensive, but also urgently required. The requirements for and volume of cipher suites are expanding rapidly, straining the capabilities of existing devices. For example, Alipay set a record by processing up to 544,000 payment transactions per second in "Double-Eleven", the Chinese online "Black-Friday" in 2019. In each payment transaction, the sensitive information (e.g., buyer privacy) shall be encrypted by a key which is agreed between Alipay and buyer, buyer shall be authenticated and the deal shall be notarized via digital signatures. Both key

This work was partially supported by National Natural Science Foundation of China under Award No. 61902392, National Science Foundation (NSF) under Award No. CCF-1525754 and National Key R&D Program of China under Award No. 2017YFB0802100. *(Corresponding author: Fangyu Zheng, E-mail: zhengfangyu@iie.ac.cn.)*

1530-2075/20/$31.00 ©2020 IEEE
DOI 10.1109/IPDPS47924.2020.00058