DPF-ECC: A Framework for Efficient ECC With Double Precision Floating-Point Computing Power

Lili Gao, Fangyu Zheng, Rong Wei, Jiankuo Dong, Niall Emmart, Yuan Ma, Jingqiang Lin, *Senior Member, IEEE*, and Charles Weems, *Senior Member, IEEE*

***Abstract*— Used ubiquitously in a huge amount of security protocols or applications, elliptic curve cryptography (ECC) is one of the most important cryptographic primitives, featuring efficiency and short key size compared with other public-key cryptosystems such as DSA and RSA. However, as a computation-intensive public-key cryptographic primitive, ECC arithmetic is still the bottleneck that restrains the overall performance of the end applications. In this paper, instead of the conventional and straightforward integer-based methods, we present a general framework to accelerate ECC schemes over prime field, called DPF-ECC, that deeply exploits double precision floating-point (DPF) computing power. The DPF-ECC framework finely manages each bit of the DPF numbers and minimizes the overhead brought by additional data format conversion, by making use of the DPF representation, the rounding operations, and fused multiply-add instruction supported by the IEEE 754 floating point standard. We also conduct two comprehensive case studies on Crandall primes and Solinas primes to demonstrate how the DPF-ECC framework is applied to the prevailing ECC schemes. To evaluate the proposed DPF-ECC framework in the real world, leveraging the floating-point computing power of GPUs, we implement Curve25519/448 and Edwards25519/448, the popular ECC schemes widely used in TLS 1.3, SSH, etc. The experimental result in Tesla P100 achieves a record-setting performance that outperforms the existing fastest integer work with 2x to 3x throughput. With dependency only on the very commonly supported IEEE 754 floating point standard, DPF-ECC framework can be a very competent and promising candidate for ECC implementation in most of general-purpose platforms.**

***Index Terms*— Elliptic curve cryptography, floating-point arithmetic, graphics processing unit.**

Manuscript received March 2, 2021; revised May 27, 2021; accepted June 30, 2021. Date of publication July 21, 2021; date of current version August 17, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61902392, in part by the National Science Foundation (NSF) under Grant CCF-1525754, and in part by the National Key Research and Development Program of China under Grant 2017YFB0802100. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Debdeep Mukhopadhyay. *(Corresponding author: Fangyu Zheng.)*

Lili Gao, Fangyu Zheng, Rong Wei, and Yuan Ma are with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China, also with the School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China, and also with the Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China (e-mail: zhengfangyu@iie.ac.cn).

Jiankuo Dong is with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210049, China.

Niall Emmart and Charles Weems are with the College of Information and Computer Sciences, University of Massachusetts Amherst, Amherst, MA 01003, USA.

Jingqiang Lin is with the School of Cyber Security, University of Science and Technology of China, Hefei, Anhui 230026, China.

Digital Object Identifier 10.1109/TIFS.2021.3098987

I. Introduction

THE proliferation of the Internet has given rise to software distribution, e-commerce, and other industries that serve huge-scale users. Used ubiquitously in security-sensitive applications of these industries, public-key cryptosystems have been indispensable in cybersecurity. Elliptic Curve Cryptography (ECC) [1], [2], widely used in key management and digital signatures for privacy protection and secure communications over the Internet, has gradually become the cornerstone of the public-key cryptosystems. ECC provides more computationally efficiency and greater security per bit increase in key size than RSA. In recent years, a growing number of security protocols have introduced cryptographic primitives based on elliptic curve groups. At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which uses ECC for digital signature and key agreement. The NIST standardized the Elliptic Curve Digital Signature Algorithm (ECDSA) in [3] for verifying the authenticity of digital messages or documents. In 2016 and 2017, RFC7748 [4] and RFC8032 [5] released by the Internet Engineering Task Force (IETF) recommended Curve25519/448 and Edwards25519/448 for an Elliptic Curve Diffie-Hellman (ECDH) protocol and the Edwards-curve Digital Signature Algorithm (EdDSA). Curve25519/448 and Edwards25519/448 are the most prevalent ECC schemes and are widely used in many protocols such as TLS 1.3 [6] and SSH [7], [8]. ECC-based schemes have been applied ubiquitously in numerous Internet security protocols and applications, which are of great importance.

A. Motivations

1) Urgent Demands for Cryptographic Services: In fact, ECC algorithms whose chief cryptographic primitive is point multiplication (PM), 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 [9] requires 11 point multiplications in a single session.

The ECC algorithm is not only computationally intensive but also urgently required. For example, Alipay set a record by processing up to 583,000 payment transactions per second on "Double-Eleven", the Chinese online "Black-Friday" in 2020 [10]. In each payment transaction, the sensitive information (e.g., buyer privacy) shall be encrypted by a key which is agreed between Alipay and buyer, the buyer shall be authenticated and the deal shall be notarized via