**Speeding-Up Elliptic Curve Cryptography**

**Algorithms**

Diana Maimuţ[](https://orcid.org/0000-0002-9541-5705) and Alexandru Cristian Matei [](https://orcid.org/0000-0001-9233-0573)

Advanced Technologies Institute

10 Dinu Vintilă, Bucharest, Romania

{diana.maimut,alexandru.matei}@dcti.ro

**Abstract.** During the last decades there has been an increasing interest in Elliptic curve cryptography (ECC) and, especially, the Elliptic Curve Digital Signature Algorithm (ECDSA) in practice. The rather recent developments of emergent technologies, such as blockchain and the Internet of Things (IoT), have motivated researchers and developers to construct new cryptographic hardware accelerators for ECDSA. Different types of optimizations (either platform dependent or algorithmic) were presented in the literature. In this context, we turn our attention to ECC and propose a new method for generating ECDSA moduli with a predetermined portion that allows one to double the speed of Barrett’s algorithm. Moreover, we take advantage of the advancements in the Artificial Intelligence (AI) field and bring forward an AI-based approach that enhances Schoof’s algorithm for finding the number of points on an elliptic curve in terms of implementation efficiency. Our results represent algorithmic speed-ups exceeding the current paradigm as we are also preoccupied by other particular security environments meeting the needs of governmental organizations.

**Keywords:** Elliptic curve, elliptic curve cryptography, ECDSA, artificial intelligence, Schoof’s algorithm, Barrett’s algorithm.

# 1 Introduction

Elliptic curve cryptographic (ECC) was initially proposed in [25,31] as an alternative to the already established public key cryptographic schemes. As a side note, the credit for the first use of elliptic curves in a cryptology related context is given to Lenstra for his factorization algorithm [28]. ECC has received an increasing amount of attention in time not only for the high level provable security offered, but especially due to a desired property concerning the implementation efficiency: the cryptographic keys are significantly shorter compared to, e.g., the case of RSA [34].

For more than a decade now, ECC has become a central piece for the Blockchain technology. To be more specific, the Elliptic Curve Digital Signature Algorithm (ECDSA) [22] is widely adopted in the construction of cryptocurrency and, implicitly, blockchains. Thus, there has been a justified hype with respect to efficient