

## **Trade-off between area and speed for projective Edwards Elliptic Curves Crypto-system over GF (p) using parallel hardware designs and architectures**

### **ABSTRACT**

Elliptic Curves Crypto-system (ECC) has been widely involved in many security applications. ECC computations suffer the long time inversion operation when applied using usual affine coordinates which affects the performance of ECC. Moreover, while the majority of previous researches focused on addressing the performance of ECC, other factors that play crucial role in building efficient ECC design for different security applications have not been intensively investigated, such as area, system utilization, resources-consuming, AT, and AT2 cost factors. Our research proposes several designs and architectures for Edwards ECC over GF (p) using projective coordinates ( $X/Z^2$   $Y/Z^2$ ). All our proposed designs apply ECC computations with no inversion operation. To improve the performance even further, our research utilizes the inherent parallelism in elliptic curves computations by applying arithmetic operations for ECC in parallel. Our results show that the performance for the proposed 5-PM design overcomes designs using the known projective coordinates as well as the affine coordinates, since it achieves the shortest time delay. Furthermore, the other proposed designs provide an attractive trade-off between mentioned factors by varying the degree of parallelism for ECC computational schemes. Although this trade-off compromises the performance of ECC, the other factors were enhanced progressively. This helps to select the most suitable ECC design for several elliptic curves applications according to their requirements and available resources. The 2-PM design obtains the best system utilization results and AT cost with less area in comparison with designs using a higher degree of parallelism.

**Keyword:** Area; Elliptic curves cryptography; Parallel hardware design; Point doubling operation; Projective coordinates; Resources; System utilization