Efficient implementation of unified ECC accelerators based on the Karatsuba multiplication method

Dan Klann[1], Ievgen Kabin[1], Zoya Dyka[1], and Peter Langendoerfer[1, 2]

[1] IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany
{klann,kabin,dyka,langendoerfer}@ihp-microelectronics.com

[2] BTU Cottbus-Senftenberg
Cottbus, Germany
peter.langendoerfer@b-tu.de

32st Crypto Day, 15. January 2020

Modern communication systems rely heavily on cryptography to ensure authenticity, confidentiality and integrity of exchanged messages. Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic approach and is used in a various fields of application. ECC is one of the commonly used standard methods for sharing secret keys, for signing messages and for authentication. In this paper we present our ASIC implementation of a design supporting four different NIST Elliptic Curves 186-4 (2015). The design supports two B-curves over $GF(2^n)$ (B-233, B-283) and two P-curves over $GF(p)$ (P-224, P-256). Sharing the hardware components – bus, multiplier and registers – reduces the area of the kP accelerator significantly. The core component that enables this type of a combined design is our unified multiplier used for both types of finite fields. As far as we know it is the first time that the 4-segment Karatsuba multiplication method [Date-2005] is used for multiplication of elements of $GF(2^n)$ as well as of elements of $GF(p)$. Compared to the classical multiplication method that needs 16 partial product calculations the 4-segment Karatsuba multiplication method needs to calculate only 9 partial products. The calculation of each partial product requires a single clock cycle in our implementation. We implemented the writing of inputs to the field multiplier and reading the field product in parallel to the calculation of the partial products. Thus, the applying the 4-segment Karatsuba multiplication method decreases the calculation time of a field product by about $\frac{(16-9)}{16} \cdot 100\% = 44\%$.

ACKNOWLEDGMENT

This research has been funded by the Federal Ministry of Education and Research of Germany under grant number 03ZZ0527A.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-24

References

Federal Information Processing Standard (FIPS) 186-4 (2015). Digital Signature Standard; Request for Comments on the NIST-Recommended Elliptic Curves.