Scalable FPGA Hardware Models for Modular Multiplication Using AMNS Representation

Louis Noyez[1], Fangan Yssouf Dosso[1], Nadia El Mrabet[1], Olivier Potin[1], and Pascal Véron[2]

[1] Mines Saint-Etienne, CEA-LETI, Centre CMP, F-13541 Gardanne France
[2] Laboratoire Imath, Université de Toulon

Abstract

Modular arithmetic using large integers is the core of the most common public-key cryptography algorithms. If the implementation of modular arithmetic can be computationally costly, we can use alternative representations of large integers to accelerate operations.The Adapted Modular Number Systems (AMNS) representation is a polynomial representation of numbers which performs parallel computations during modular operations. This work describes a generic and scalable FPGA implementation of the AMNS arithmetic based on the AMNS generation process developed in [2]. The hardware models fit the AMNS parameters and provide optimization options in terms of FPGA resource cost, number of cycles or maximum clock frequency. We compare our results with FPGA implementations of the modular multiplication using a classical integer representation [1, 3]. Our fastest implementation performs a 256-bit modular multiplication in 210ns at 200MHz.

References

1. Chaouch, A., Didier, L.S., Dosso, F.Y., El Mrabet, N., Bouallegue, B., Ouni, B.: Two hardware implementations for modular multiplication in the AMNS: Sequential and semi-parallel **58**, 102770. https://doi.org/10.1016/j.jisa.2021.102770, {https://linkinghub.elsevier.com/retrieve/pii/S2214212621000193}
2. Didier, L.S., Dosso, F.Y., Véron, P.: Efficient modular operations using the adapted modular number system. Journal of Cryptographic Engineering (Jan 2020). https://doi.org/10.1007/s13389-019-00221-7, https://hal.archives-ouvertes.fr/hal-02486345
3. Mrabet, A., El-Mrabet, N., Lashermes, R., Rigaud, J.B., Bouallegue, B., Mesnager, S., Machhout, M.: High-performance elliptic curve cryptography by using the CIOS method for modular multiplication. In: Cuppens, F., Cuppens, N., Lanet, J.L., Legay, A. (eds.) Risks and Security of Internet and Systems, vol. 10158, pp. 185–198. Springer International Publishing. https://doi.org/10.1007/978-3-319-54876-0˙15, {http://link.springer.com/10.1007/978-3-319-54876-0_15}