Efficient and Power Analysis Resistant Implementation of the Montgomery kP-Algorithm

Estuardo Alpirez Bock, Zoya Dyka and Peter Langendoerfer

System dept.
IHP
Frankfurt (Oder), Germany

Cryptographic algorithms implemented in hardware are devices that generate, besides the processing results, additional data which is linked to the calculation. Some of this data, for example the power consumption or electromagnetic radiation, can be measured, saved and analysed for attacking the implementation with the goal to extract the cryptographic key. Such attacks are known as side channel analysis attacks. The Montgomery kP-algorithm based on [LD99] is an efficient method for performing the elliptic curve point multiplication, which is the basic operation in elliptic curve crypto-systems (ECC). With this algorithm, each bit of the key k is processed in the same way, i. e. the number of the performed mathematical operations and their sequence are independent of the processed bit value. ECC hardware implementations using this algorithm are robust against simple power analysis attacks, but not against differential power analysis (DPA) attacks.

In this work we present a method for a time and energy optimized implementation of the Montgomery kP-algorithm. Our two implemented kP-designs are resistant against a horizontal DPA attack using the *difference-of-means* test.

In our implementation not only the type, number and sequence of mathematical operations are the same for each key bit, but we also take their energy consumption into account. The processing of each bit of the key in the Montgomery kP-algorithm consists of 6 multiplications, 5 squarings and 3 additions. The number of multiplications defines the shortest possible number of clock cycles needed for processing one key bit. This minimal number can be achieved only if all other operations are performed parallel to the multiplications. Our area-optimized multipliers need 9 clock cycles in our first and 6 clock cycles in our second ECC designs to calculate the product of two 233 bit long elements of $GF(2^{233})$. All other operations, including the writing of data to registers, are performed in our new designs parallel to the multiplications and are regularly performed during the bit processing time. This way, the calculation time and energy consumption of our implemented ECC designs were reduced, while their resistance against DPA attacks was increased.

We performed the horizontal DPA attack using the difference-of-means test against our two implementations and against our old ECC design, which is a straight forward implementation of the Montgomery kP-algorithm. The old ECC design delivered 57 key-candidates. Four of these candidates were extracted with a correctness of about 90%; one candidate was extracted with 100% correctness. The first of our new implementations delivered only 54 key-candidates and none of them was extracted with a correctness higher than 70%. The second implementation delivered only 36 key-candidates, from which none was extracted with a correctness higher than 76%. Our fastest ECC design has the area of 0.3 mm^2 (IHP 130nm technology) and consumes only 1.61 μJ for the performance of a complete kP-operation.

References

[LD99] Julio Lopez and Ricardo Dahab. Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. *Proceedings of the First International Workshop CHES*, Springer, 1999.