# Discussing the Initialization of the Montgomery $kP$-Algorithm in the Light of SCA

Estuardo Alpirez Bock, Zoya Dyka and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

Side channel analysis (SCA) attacks have been a popular research topic in the last years. Parameters like power consumption, electromagnetic radiation and execution time of a cryptographic implementation can be analysed for identifying implementation details and based on this, extracting the private key. The Montgomery $kP$-algorithm using Lopez-Dahab projective coordinates [LD99] is an efficient method for performing the scalar multiplication in elliptic curve crypto-systems (ECC). This algorithm is a bitwise processing of the scalar $k$, which is the private key used for performing decryption in ECC. It is considered resistant against simple power analysis (SPA) since each key bit is processed by the same type, amount and sequence of operations, independently of the key bit's value. Nevertheless, its initialization phase affects this algorithm's robustness against SCA. We describe how the first iteration of the $kP$ processing loop reveals information about the key bit being processed, i.e. bit $k_{l-2}$.

Using simulated power traces, we demonstrate that the power profile of the processing of $k_{l-2}$ differs from the power profiles of the processing of all other key bits. Moreover, we demonstrate that this power profile differs significantly for the cases $k_{l-2} = 1$ and $k_{l-2} = 0$. This leads to an easy extraction of bit $k_{l-2}$ using SPA and exposes details of the implementation of the algorithm. This can be useful for the preparation of further attacks. As a countermeasure against this vulnerability, we propose a modification of the algorithm's initialization phase and of the processing of bit $k_{l-2}$. We show that with this modification, the power profiles of the processings of $k_{l-2} = 1$ and $k_{l-2} = 0$ look similar to each other and similar to the processing of all remaining bits of the key, i.e. the value of the key bit $k_{l-2}$ cannot be extracted using SPA.

Our proposed modifications increase the algorithm's robustness against SCA and even reduce the time needed for the initialization phase and for processing $k_{l-2}$. Compared to the original design, our new implementation needs only 0.12% additional area, while its energy consumption is almost the same, remaining by 2.09 $\mu$J. Thus, we achieved to increase the security of our implementation without any additional costs.

**Acknowledgement:** The research leading to these results has received funding from the European Commission's Horizon 2020 under grant agreement from project myAirCoach – No. 643607.

## 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.