Post-quantum security: Power Analysis of NTRUEncrypt

Thomas Schamberger

Technical University of Munich
Munich
Germany

The possibility of a large scale quantum computer threatens the security of established public-key cryptography and therefore a transition to post-quantum secure cryptosystems is necessary. This transition process was officially initiated by the post-quantum contest of the National Institute of Standards and Technology (NIST). One promising candidate in this contest is the lattice based algorithm NTRUEncrypt [NTRU98]. Although, this algorithm has withstand mathematical analysis for almost 20 years, its vulnerability against side-channel attacks has to be explored in order to ensure secure implementations.

This work investigates the vulnerability of the polynomial multiplication of NTRUEncrypt against power analysis attacks. The published attacks in [Lee10, Wang13] are revisited for modern parameter sets. It is shown that the DPA attack of [Lee10] is still applicable while the SPA, described in [Wang13], is not valid anymore. The attack results are shown for an implementation on a 32-bit ARM Cortex-M4 microcontroller on the STM32F407G-DISC evaluation board of STMicroelectronics.

References

[NTRU98] Hoffstein *et al.* NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA, June 21–25, 1998.*

[Lee10] Lee *et al.* Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2010.*

[Wang13] Wang *et al.* Power Analysis Attacks and Countermeasures on NTRU-Based Wireless Body Area Networks. *TIIS, vol. 7, no. 5, pp. 10941107, 2013.*

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-13