Profiling Side-Channel Attack on HQC Polynomial Multiplication Using Machine Learning Methods

Tomas Rabas

Department of Digital Design on Faculty of Information Technology

CTU in Prague, Czech Republic

Abstract

The Hamming Quasi-Cyclic (HQC) cryptosystem was selected for standardization in the 4th round of the NIST post-quantum standardization competition targeting public-key encryption and key-establishment algorithms. We will describe profiling power side-channel attack on a HQC cryptosystem exploiting power consumption leakage during polynomial multiplication in the beginning of the decryption. The attack scheme is based on generic methods such as Welch's ANOVA test or multilayer perceptron with a grid-search algorithm used for the hyperparameter tuning. We will present results of a practical evaluation on a chosen targets using ChipWhisperer platform and describe countermeasures and their efficiency with respect to security.