Current and Future Efforts in Benchmarking NIST LWC Ciphers

Sebastian Renner[1,2], Enrico Pozzobon[1,3], and Jürgen Mottok[1]

[1] OTH Regensburg, Germany
{sebastian1.renner, enrico.pozzobon, juergen.mottok}@othr.de
[2] Technical University of Munich, Germany
[3] University of West Bohemia, Czech Republic

Abstract. The National Institute of Standards and Technology (NIST) stated the performance of Software implementations as one criterion in the selection process of lightweight cryptography ciphers. We have already introduced a basic version of our benchmarking framework at the 3rd LWC Workshop at NIST. Since then, we have made some changes and added new features to this work. Especially the support of more platforms and the integration of a public website (lwc.las3.de) for publishing the latest results are worth to be noted. Through the webiste, we are able to offer a submission system for new and optimized implemenations on the one hand and can provide up-to-date statistics regarding our tests just upon their completion on the other hand. In this talk, we would like to explain how these new features have been integrated, show current results and discuss how the testing process and result presentation might be improved in order to maximize transparency. Moreover, we will introduce planned future additions to the framework, specifically in the domain of (power) traces collection and basic automated leakage evaluation. We aim for discussing the best and easiest way on how to facilitate side-channel and fault injection analysis to support the research and cipher selection process in these fields.