Is ASCON the best choice regarding the Side-channel Analysis?

Matúš Olekšák, Vojtěch Miškovský
Czech Technical University in Prague, CZ

Abstract

Since Internet of Things (IoT) is becoming widely used, it is required to ensure data are transmitted securely. IoT devices typically do not have much computation power and are battery-powered. This implies the need for lightweight encryption standard. Recently, the National Institute of Standards and Technology (NIST) found new standard for lightweight encryption. One of the requirements for the upcoming standard was resistance against side-channel attacks, since they are one of the main threats for embedded devices. For this reason, it is necessary to analyze the finalists, whether they are certainly resistant to side-channel attacks. Main contribution of this research is the discovery of possible side-channel attacks on the following finalists.