Lightweight cipher implementations for resilience against side-channel analysis

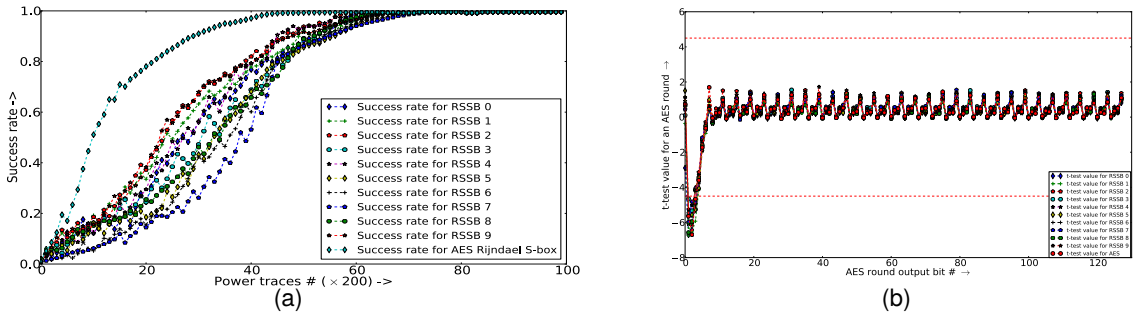
Bodhisatwa Mazumdar,
Discipline of Computer Science and Engineering, IIT Indore

Research Highlights

Our present research focuses on emerging aspects of hardware security, such as side-channel analysis of cryptographic implementations and logic synthesis techniques for improved resilience against such attacks.

The current research aims to propose implementations that thwart power-based side-channel analysis of lightweight block ciphers such as Simon and Hummingbird ciphers. Power analysis is one of the side-channel vulnerabilities that has been exploited by the cryptographic research community to extract secret information embedded in resource-constrained hardware devices. We have proposed construction of S-boxes and other block cipher primitives that have improved resilience against power analysis attacks. In this research, we model the cryptographic properties of S-boxes that determine its vulnerabilities against power based side-channel analysis. The synthesis model is used to create S-boxes that has improved resilience against power-based side-channel analysis. In Figure 1(a), we present a comparison of success rate of power analysis of the proposed class of S-boxes with that of a standard AES S-box. The plot shows that the number of queries required for the proposed class of S-boxes increased by $2X - 3X$ as compared to that of AES S-box. This imparts increased life-time of the session key that is embedded in the device. Further, as shown in Fig. 1(b), the information leakage at vulnerable points is reduced for the proposed class of S-boxes as compared to that of the AES S-box.

This work was published as "Construction of Rotation Symmetric S-Boxes with High Nonlinearity and Improved DPA Resistivity" in IEEE Transaction of Computers in January 2017.



(a) (b)

Figure 1: (a) Success rate of correlation power analysis attacks on the synthesized S-boxes and AES S-box shows improved resilience of proposed S-boxes as compared to AES S-box, (b) Welch's t-test plot on the synthesized S-boxes and AES S-box to determine vulnerable points during execution of the cipher.