Researchers at the University of South Florida have come up with a lightweight countermeasure against leakage power analysis (LPA) attacks.

The correlation between the power consumption and processed data can be exploited by a malicious attacker with side-channel attacks (SCAs) to obtain the stored critical information. Since the leakage mechanisms in the common differential power analysis (DPA) and the LPA attacks are quite different, DPA-resistant cryptographic circuits may still be vulnerable against LPA attacks. There is, therefore, a strong need for effective countermeasures against LPA attacks.

To perform a successful LPA attack, the attacker must mitigate the measurement noise by lowering the operating frequency of the cryptographic circuit. In this innovative countermeasure by our researchers, when an LPA attack is sensed by the proposed security adaptive (SA) voltage converter, a discharging resistor starts sinking redundant current to alter the signature of the power dissipation. Under an LPA attack, if the clock frequency is lower than the active critical frequency and higher than the idle critical frequency, some amount of redundant current flow through the discharging resistor to scramble the inserted power noise. This makes it difficult for the attacker to extract out meaningful information. The measurement-to-disclose (MTD) value of a cryptographic circuit that employs the proposed countermeasure is enhanced over 6145 times as compared with the MTD value of a conventional cryptographic circuit that has no countermeasure.

The proposed countermeasures are one of the very first countermeasures against LPA attacks. This is also an adaptive countermeasure which is quite new in the field.

ADVANTAGES:

- One of the very first countermeasures against LPA attacks
- Low overhead, lightweight
- MTD can be enhanced over 6145 times against LPA attacks

An Innovative Lightweight Countermeasure Against Leakage Power Analysis (LPA) Attacks

Architecture of the Proposed Security Adaptive (SA) Voltage Converter