Asynchronous S-Boxes

Designing Clockless First-Order Masked Functions

Mateus Simoes[1,2], Lilian Bossuet[1], Nicolas Bruneau[2], Vincent Grosso[1], Patrick Haddad[2] and Thomas Sarno[2]

[1] Laboratoire Hubert Curien, Saint-Etienne, France
{mateus.simoes,lilian.bossuet,vincent.grosso}@univ-st-etienne.fr
[2] STMicroelectronics, Rousset, France {nicolas.bruneau,patrick.haddad}@st.com

Abstract. Passive physical attacks represent a threat to microelectronics systems by exploiting leakages through side-channels, such as power consumption and electromagnetic radiation. In this context, masking is a sound countermeasure against side-channel attacks, which splits the secret data into several randomly uniform data, achieving independence between the data processing and the secret variable. However, a secure masking scheme requires additional implementation costs. Furthermore, glitches and early evaluation can temporally weaken a masked implementation in hardware, creating a potential source of exploitable leakages.
This work shows how to create register-free masking schemes that avoid the early evaluation effect with the help of the dual-rail logic. Moreover, we employ monotonic functions with the purpose of eliminating the occurrence of glitches in combinational circuits. Finally, we evaluate different 2-share masked implementations of the PRESENT and AES S-boxes in a noiseless scenario in order to detect potential first-order leakages and to determine data propagation profiles correlated to the secret variables.