The long story of substitution boxes in embedded cyber-security

Sylvain Guilley

TELECOM-ParisTech, France

Substitution boxes (S-box) are vectorial Boolean functions with applications in many areas of cryptography, including iterated block ciphers. Their security requirements are varied, based on resistance to some known attacks. Therefore, multiple designs have been put forward over time, trying to be as close as optimal in fulfilling most constraints. For the sake of global block cipher efficiency, S-box have been thought to be as large as possible, in order to minimize the latency (= number of rounds) of the block cipher.

But then came additional complications with (cache) timing and side-channel attacks. Resisting to those attacks entails large overheads, that are better mitigated if the S-boxes are small (i.e., at the opposite of the design requirements from a cryptographic standpoint). We discuss the intricacies of requirements to implement S-boxes securely. Namely, we consider two logic styles: balanced and masked logic styles. We show the deep implications on the way to implement the S-boxes.