Glitch modelling of FPGA device primitives for Side-Channel Attack Resilience

Keywords: Toggle count, lookup table, carry chain, interconnect, power analysis attack.

In today's advanced technological age, electronic devices have become an important medium to process, store, and transfer data information contained in them. With advent of portable devices such as smartphones and tablets, data processing and transfer are now increasingly exposed to malicious users who aim for data theft, corruption and privacy intrusion. Today's FPGA SoCs can be used to implement a scalable security scheme that extends all the way down to the IC level. They help deliver the full range of scalable security features such as, confidentiality, data integrity, authentication, and non-repudiation. In addition, such implementations ensure low power system operation in a small footprint. However, recently physical attacks such as side-channel analysis have put the focus back on implementation vulnerabilities that leak secret information into physical side-channels such as power, execution time etc.

Glitches are the spurious signal transitions, which occur due to unbalanced path delays at the inputs of a gate. Presence of glitches in a digital system increases the number of signal transitions, thereby increasing the dynamic power consumption of the system. Consequently, overall power consumption, a major design criteria of a digital system, is increased. Furthermore, glitches are shown to be a source of side-channel leakage and can be exploited to enhance the success rate of power analysis attacks against cryptographic applications even in presence of side-channel countermeasures. Therefore, elimination of glitches in digital systems implemented on hardware platforms, such as Field Programmable Gate Arrays (FPGAs), is imperative for low power and secure designs. In the proposed project, we focus to propose a methodology of selecting digital primitive blocks such as lookup tables, carry chains, etc so that unbalanced path delays of signals are eliminated. The information leakage through glitch has become increasingly important with merging of more logical resources in a configurable logic block (CLB) in the Xilinx Ultrascale architecture. Although the total length of local interconnect is reduced in this architecture, an additional stage of wider multiplexers and a longer 8-bit carry chain has been incorporated for faster arithmetic functions. However, from the security perspective, the information leakage of such technology modifications remains to be addressed. We aim to work on mitigation of glitch based information leakage for cryptographic and other secure implementations that employ Xilinx Ultrascale architecture for high device utilization at maximum possible performance.

In the proposed methodology, we aim to work on glitch propagation model that strictly depends on the implementation and the digital primitive blocks employed in a secure cryptographic implementation. One such model instance is to account glitches obtained from an XOR of two glitched signals (referred to as double glitch) that are input to a lookup table. Such glitch models have significant implications on security results. Depending upon the FPGA digital primitive used for a digital block, a double-glitch may count as twice a normal glitch, or a normal glitch, or may not count at all if the glitches cancel each other. Each of these affect the information leakage of the secret key that is embedded in the design.