GLITCH-FREE IMPLEMENTATION OF MASKING IN MODERN FPGAS

Amir Moradi and Oliver Mischke

Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
{moradi, mischke}@crypto.rub.de

Due to the propagation of the glitches in combinational circuits side-channel leakage of the masked S-boxes realized in hardware is a known issue. Our contribution in this paper is to adopt a masked AES S-box circuit according to the FPGA resources in order to avoid the glitches. Our design is suitable for the 5, 6, and 7 FPGA series of Xilinx although our practical investigations are performed using a Virtex-5 chip. In short, compared to the original design synthesized by automatic tools while requiring the same area (slice count) our design reduces power consumption, critical path delay, and more importantly the side-channel leakage. In our practical investigations we could not recover any first-order leakage of our design using up to 50 million traces. However, since the targeted S-box realizes a first-order boolean masking, the second-order leakage could be revealed using around 25 million measurements.