Threshold Implementations and Their Applications

Begül Bilgin

COSIC, KU Leuven, Belgium

With the increase of small pervasive devices, the strength of the ongoing algorithm against side channel attacks becomes important. There are many countermeasures proposed against such attacks, however many of them fail to achieve the required security on hardware because of glitches. Threshold implementation is a method based on multi party computation and secret sharing that can be applied in a wide range of algorithms with low cost and provides first order side channel attack security even in a glitchy environment. In my talk, I will briefly describe Threshold Implementations and their applications on some well known algorithm and give a discussion on how this knowledge can be used while designing a new symmetric algorithm.

Kasteelpark Arenberg 10, bus 2446, 3001, Heverlee, Belgium
begul.bilgin@esat.kuleuven.be