USF NEXUS INITIATIVE 2019 AWARD RECIPIENT

Mehran Mozaffari Kermani
Active Side-Channel Attacks and Countermeasures for Lightweight Cryptography

The goal of this one-year award, hosted at Sabanci University in Turkey, is to explore a paradigm shift in scrutinizing lightweight cryptography with respect to side-channel attacks for highly-constrained devices and hardware/software usage models including, but not limited to, implantable medical devices, smart nano-sensors, and smart fabrics. Throughout this project, we plan to investigate the contrast between legacy and lightweight cryptography with respect to attack immunity without compromising usability, energy-efficacy, and resistance to implementation attacks. We also plan to initiate grants to explore these opportunities beyond the award.

Partnership:

Erkay Savas, Ph.D.
Sabanci University (Istanbul, Turkey)

UNIVERSITY OF SOUTH FLORIDA
A PREEMINENT RESEARCH UNIVERSITY