Ben-Gurion University of the Negev

General information

Company name: Ben Gurion Univ. of the Negev
Contact name: Dr. Yossi OREN
Email: yos at bgu.ac.il
Telephone number: +972-8-647-9344
Webpage: https://iss.oy.ne.ro

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ **Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography**	Y
○ **Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices**	Y
○ Authenticated encrypted token research for mobile payment solution	N
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	N
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	N
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	N

Ben-Gurion University of the Negev

Competencies

- ***BGU** is a public research university with over 20,000 students, nationally designated center of excellence in cyber security*
- ***BGU** is a coordinator and partner in over 40 FP funded projects (CIG, ITN, IAPP, IRSES & IF) and MCAs in FP7 and H2020*
- ***My competencies**: Side-channel attacks in unexpected places, constraint solvers for sec., low-power crypto for RFID tags*
- ***Other researchers in BGU**: cryptographic theory (secure distributed computation), IoT sec., malware lab, network sec.*