אוניברסיטת חיפה
University of Haifa
جامعة حيفا

General information

University of Haifa
Prof. Orr Dunkelman
orrd@cs.haifa.ac.il
+972-4-828-8447

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

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Competencies

- *Design and Cryptanalysis of Symmetric-Key Primitives*
- *Proven track record in the design and analysis of lightweight schemes*
- *Development and Implementation of Real-Life software and hardware designs*

- *Current participation: PQCRYPTO (ICT-645622) and COST action CRYPTACUS (IC 1403)*
  - **Past participation in NESSIE (IST-1999-12324), ECRYPT (IST-2002-507932) , ECRYPT2 (ICT-2007-216676)**

- *Speaking both "Crypto" and "Security"*
- *Understanding "Market Needs" and Engineering aspects, as well as future directions in computing*

- *[Team includes Prof. Shay Gueron (Math dept. + Intel Corp.)]*