شانزدهمین کنفرانس بین المللی انجمن رمز ایران

۶ و ۷ شهریور ۱۳۹۸

دانشگاه فردوسی مشهد

انجمن رمز ایران
Iranian Society of Cryptology

دانشگاه فردوسی مشهد

Workshop

Invariant Attacks

Prof. Gregor Leander
Ruhr University Bochum (Germany)

Abstract

Invariant attacks are attacks on symmetric primitives, in particular block ciphers. Those (non-linear) invariant attacks are generalizations of invariant subspace attacks and have been applied to a couple of lightweight ciphers in recent years. In this workshop, I will explain (i) how invariant attacks work, (ii) how they can be detected and (iii) how, as a designer, one can ensure resistance against those attacks. Besides the theoretical background, I will focus on the algorithmic aspects as well.

Duration: 4 h

Time: Tuesday August 27, 2019

مرکز منطقه‌ای اطلاع‌رسانی علوم و فناوری

IEEE IRAN SECTION

ISC
Islamic World Science Citation Center

Sponsored and Indexed by
CIVILICA
We Respect the Science

مشهد، میدان آزادی، پردیس دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر
تلفن: ۰۵۱-۳۸۸۰۶۱۲۶   نمابر: ۰۵۱-۳۸۸۰۷۱۸۱
http://iscisc2019.um.ac.ir   2019@isc.org.ir