abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In this work we re-visit the question of building cryptographic primitives that remain secure even when queried on inputs that depend on the secret key. This was investigated by Black, Rogaway, and Shrimpton in the context of randomized encryption schemes and in the random oracle model. We extend the investigation to deterministic symmetric schemes (such as PRFs and block ciphers) and to the standard model. We term this notion "security against key-dependent-input attack", or KDI-security for short. Our motivation for studying KDI security is the existence of significant real-world implementations of deterministic encryption (in the context of storage encryption) that actually rely on their building blocks to be KDI secure.

We consider many natural constructions for PRFs, ciphers, tweakable ciphers and randomized encryption, and examine them with respect to their KDI security. We exhibit inherent limitations of this notion and show many natural constructions that fail to be KDI secure in the standard model, including some schemes that have been proven in the random oracle model. On the positive side, we demonstrate examples where some measure of KDI security can be provably achieved (in particular, we show such examples in the standard model).

Joint work with Hugo Krawczyk