Key-Dependent Message Security in the Standard Model

Dennis Hofheinz (CWI, Amsterdam)

What and why?

- Key-dependent message (KDM) security
- As IND, but with **special** encryption oracle
  - Real game: $O(F) = ENC_{SK}(F(SK))$
  - Random game: $O(F) = ENC_{SK}(random)$
- Security: no adv. can distinguish real/rand
- **Useful**: formal link, encrypt your hard drive
- **Our focus**: symmetric setting and CPA

What is known?

- Black, Shrimpton, Rogaway 2002:

$$ENC_{SK}(M) = (R, H(SK||R) + M)$$

- KDM-CPA in RO model, but RO **essential**
- **Only*** provable construction known!

* except for straightforward but uninteresting solutions:

  - schemes with secret key longer than total volume of messages ever encrypted (then privacy amplification techniques work)
  - “hey, look how easy the proof now is”-style interactive non-standard computational assumptions beyond intuition

What do we have?

- **Stateful** encryption assuming PRNG only

  $ENC_{SK_i}(M)$:

  1.) pick UHF h

  2.) cond := $h(SK_i)$

  3.) $(SK_{i+1}, pad) := PRNG(cond)$

  4.) C := (h, pad + M)

- **Weak** stateful KDM-CPA (i.e., $M=M(SK_i)$)