

Almost the Right Key: Wrong-Key Behavior in Key Recovery Attacks

Advisor: **Nedžma Mušović**

Motivation

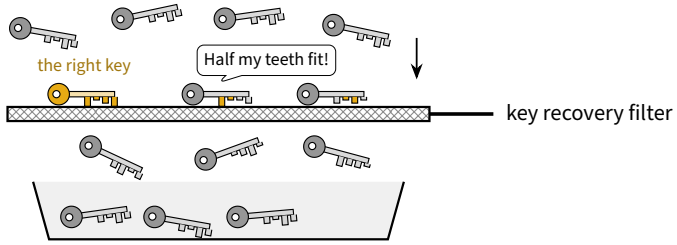
How do you break a cipher whose key is far too long to guess? You attack it piece by piece: guess a small part of the key, use it to decrypt the last rounds, and look for an identified pattern that should only appear when your guess is right. Repeat this for every candidate, and the right key should stand out from the crowd.

But how do we know it really stands out? To estimate the complexity of such attacks, cryptanalysts commonly assume that decrypting with a wrong guess behaves like applying a random permutation. This heuristic keeps the analysis tractable, but it is not always accurate: a wrong guess still decrypts with the real cipher, and many wrong guesses are not entirely wrong. These *partially correct* keys may slip through the attack's filter far more often than expected, and if they do, attacks are weaker than they claim to be.

In this thesis, you will put this assumption to the test. You will implement a real key recovery attack on a lightweight block cipher, check how wrong keys actually behave, and find out when the theory holds and when partially correct keys break it.

Goals and Tasks

- Get familiar with block ciphers, statistical key recovery attacks, and the assumptions behind them
- Implement a round-reduced block cipher and a key recovery attack on it
- Measure how wrong keys, and partially correct keys in particular, behave and compare this to the standard predictions



Literature

- T. Ashur, T. Beyne, and V. Rijmen
  Revisiting the Wrong-Key-Randomization Hypothesis
  J. Cryptol. 2020
  doi:10.1007/S00145-020-09343-2
- T. Beyne et al.
  What to Guess in Key-Recovery Attacks?
  IACR ePrint Report 2026/1897 2026

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in block ciphers and cryptanalysis
- Programming (C or Python)

Advisor Contact

nedzma.musovic@tugraz.at