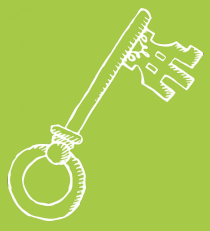


Misuse Attacks on Lightweight Ciphers

Advisor: **Maria Eichlseder**

Motivation

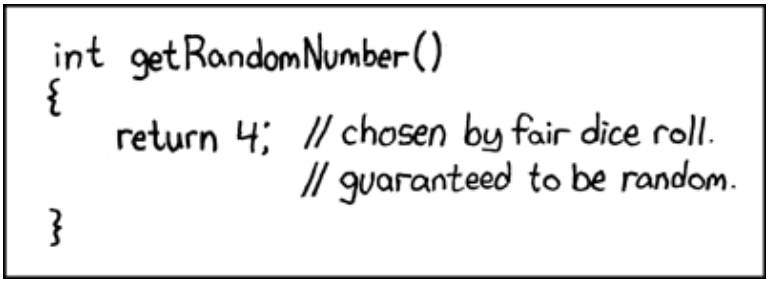
NIST is currently running a competition for algorithms to be considered for *lightweight cryptographic standards*, and has selected 32 round-2 candidate ciphers in September 2019. These candidates are now being scrutinized by the cryptographic community. They need to be categorized, analyzed, and compared.

All candidates are nonce-based authenticated encryption schemes: In addition to the secret key K and the plaintext message M, these schemes also require an additional input, the *nonce ("number-only-used-once")* N. This nonce must be a unique value for every plaintext that is never reused for the same secret key. It is usually chosen as a random number, or a message counter or address. If the nonce is reused, the security of the cipher is partially compromised.

Your task in this project is to investigate *how wrong things go when things go wrong*: How much can an attacker learn if the nonce is *misused* and the same nonce is repeated?

Goals and Tasks

- Get to know lightweight crypto candidates
- Understand the problems of nonce reuse
- Describe/implement attacks you find
- Summarize your findings



Literature

- National Institute of Standards and Technology (NIST)
  Lightweight Cryptography Standardization Process
  https://csrc.nist.gov/projects/lightweight-cryptography 2019
- S. Vaudenay and D. Vizár
  Can Caesar Beat Galois? – Robustness of CAESAR Candidates Against Nonce Reusing and High Data Complexity Attacks
  ACNS 2018
  https://doi.org/10.1007/978-3-319-93387-0_25

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 cryptography

Advisor / Contact

maria.eichlseder@iaik.tugraz.at