Update on the LowMC/Picnic cryptanalysis competition

Christian Rechberger, TU Graz

LowMC

Special-purpose cryptographic permuation/cipher

- very few AND gates

Picnic

Signature scheme based on ‘MPC-in-the-head’

- Recently advanced to round 3 of NIST PQC process
- Only hardness assumption is security of LowMC in a very constrained setting

LowMC Cryptanalysis challenge

Total sponsoring is 50k€ from Microsoft + donation from IOV42

Attacker only knows a single pt/ct pair

- In case of full nonlinear layer
  - Who has the fastest attack on 2 / 3 / 4 rounds?
- In case of partial nonlinear layer
  - Who has the fastest attack on n/s * (0.8 / 1 / 1.2) rounds?

Winners of 1st round

The team

Subhadeep Banik (EPFL)
Khashayar Barooti (EPFL)
F. Betül Durak (Bosch Research)
Serge Vaudenay (EPFL)

describing a 2-round attack, and an attack on n/s * 0.8 rounds both with the lowest time complexities. **Winning 4k€!**

Paper here: https://lowmcchallenge.github.io/

2nd round of LowMC challenge

- Sponsoring: 50k USD by Microsoft plus donation from IOV42

- Full nonlinear layers
  - Submitters of the fastest attack on 2 rounds win EUR 2k
  - Submitters of the fastest attack on 3 rounds win EUR 3k
  - Submitters of the fastest attack on 4 rounds win EUR 4k

- Partial nonlinear layers
  - Submitters of the fastest attack on floor(n/s)*0.8 rounds win EUR 2k
  - Submitters of the fastest attack on floor(n/s)*1.0 rounds win EUR 3k
  - Submitters of the fastest attack on floor(n/s)*1.2 rounds win EUR 4k.

- Bonus prize for interesting property or technique: 4k.
- Up for grabs in the 2nd round: 22k

Tentative schedule and rules

- In case of similar results, earlier submission counts!
- Verifiability is important. Submissions are expected to be public.

- Deadline: Dec 1st, i.e. the week before Asiacrypt 2020.
- Overall duration: around 2 years, money that is not spent remains in the pot and is part of the following rounds.
- More infos:
  https://lowmcchallenge.github.io/ and
  lowmc-challenge@iaik.tugraz.at

Update on the LowMC/Picnic cryptanalysis competition

Christian Rechberger, TU Graz