Incentives for LowMC-Cryptanalysis in the Low-Data Scenario

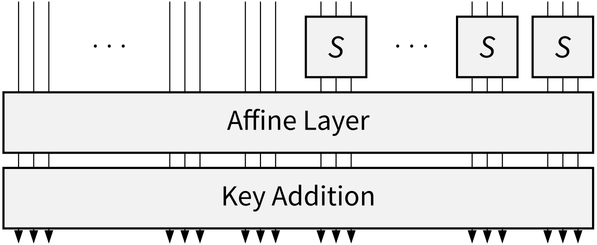
Christian Rechberger, Eurocrypt 2020 Rump Session

12.05.2020

> https://lowmcchallenge.github.io/

LowMC

- First cipher design aiming directly a minimizing AND gates, Eurocrypt 2015
- VERY flexible instantiations possible, lots of cryptanalysis[ARS+16; DEM15; DKP+19; DLMW15; RST18]



- A very interesting use-case: Picnic Signature scheme

Low-Data (single PT/CT pair) Scenario

- LowMC in the context of Picnic [CDG+19]
  - Post-quantum signature scheme
  - Round-2 submission of NIST PQC
  - Attacker only knows a single (plaintext, ciphertext) pair
- Nine interesting instantiations
  - LowMC with block size N in $\{128, 192, 256\}$
  - Number of S-boxes s in $\{1, 10, \mathit{full}\}$
  - Key size is the same as block size

Existing Analysis of LowMC with single PT/CT pair

- Survey paper [GKRS20]
- Attack goal is full key recovery
- Classical differential and linear attacks not possible
- Attacks considered so far:
  - Various Gröbner bases approaches
  - MiTM, guess-and-determine attacks [DF16]
  - Coding theory [Zaj17]

The LowMC Cryptanalysis Challenge: First Round until August 2020

Sponsoring: 50k USD by Microsoft, more sponsors upcoming

- 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.
- 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.
- Bonus prize for interesting property or technique: 4k.
- Total: 22k in first round

Tentative schedule and rules

- In case of similar results, earlier submission counts!
- Verifiability is important
- Submissions are expected to be public
- Deadline of first round: August 10, i.e. one week before Crypto 2020.
- Overall duration: around 2 years, money that is not spent remains in the pot and is part of the following rounds, next one tentatively ending end of 2020.
- More infos: `https://lowmcchallenge.github.io/` and lowmc-challenge@iaik.tugraz.at

References I

[ARS+16] Martin Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. **Ciphers for MPC and FHE.** Cryptology ePrint Archive, Report 2016/687. https://eprint.iacr.org/2016/687. 2016.

[CDG+19] Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Valdimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, and Greg Zaverucha. **The Picnic Signature Scheme Design Document (version 2).** 2019. URL: https://github.com/microsoft/Picnic/blob/master/spec/design-v2.0.pdf.

[DEM15] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. **Higher-Order Cryptanalysis of LowMC.** ICISC 2015. Vol. 9558. 2015, pp. 87–101. URL: https://doi.org/10.1007/978-3-319-30840-1%5C_6.

[DF16] Patrick Derbez and Pierre-Alain Fouque. **Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks.** CRYPTO (2). Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 157–184.

References II

[DKP+19] Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. **Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC.** EUROCRYPT 2019. Vol. 11476. LNCS. 2019, pp. 343–372. URL: https://doi.org/10.1007/978-3-030-17653-2%5C_12.

[DLMW15] Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang. **Optimized Interpolation Attacks on LowMC.** ASIACRYPT 2015. Vol. 9453. LNCS. 2015, pp. 535–560. URL: https://doi.org/10.1007/978-3-662-48800-3%5C_22.

[GKRS20] Lorenzo Grassi, Daniel Kales, Christian Rechberger, and Markus Schofnegger. **Survey of Key-Recovery Attacks on LowMC in a Single Plaintext/Ciphertext Scenario.** https://lowmcchallenge.github.io/. 2020.

References III

[RST18] Christian Rechberger, Hadi Soleimany, and Tyge Tiessen. **Cryptanalysis of Low-Data Instances of Full LowMCv2.** IACR Trans. Symmetric Cryptol. 2018.3 (2018), pp. 163–181. URL: https://doi.org/10.13154/tosc.v2018.i3.163-181.

[Zaj17] Pavol Zajac. **Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity.** Des. Codes Cryptogr. 82.1-2 (2017), pp. 43–56. DOI: 10.1007/s10623-016-0256-x. URL: https://doi.org/10.1007/s10623-016-0256-x.