TU Graz

SCIENCE
PASSION
TECHNOLOGY

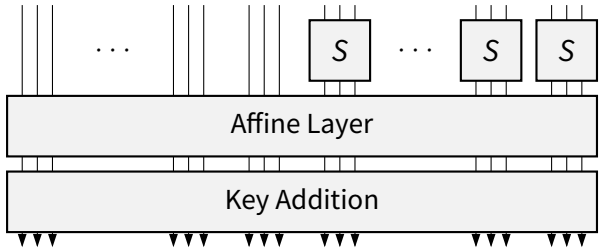
Incentives for LowMC-Cryptanalysis in the Low-Data Scenario

Christian Rechberger, Eurocrypt 2020 Rump Session

12.05.2020

LowMC

- LowMC first cipher design aiming directly a minimiying AND gates, Eurocrypt 2015
- VERY flexible instantiations possible



- A very interesting use-case: Picnic Signature scheme

Low-Data 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
- Focus on round numbers providing security in this specific scenario
- Nine 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