The LowMC Cipher Breaking Challenge

Christian Rechberger, Hadi Soleimany, Tyge Tiessen
Security of modern IT Systems

- User
- Secure System
- Communication Protocol
- AES, SHA-3
Security of modern IT Systems

User

Secure System

KEM/DEM, PKI, ...

AES, SHA-3
Security of modern IT Systems

User

Secure System

MPC, FHE, SNARKS, Masked impl., PQ-Signatures

AES, SHA-3
Security of modern IT Systems

User

Secure System

MPC, FHE, SNARKS, Masked impl., PQ-Signatures

?? (Multiplications matter much more)
Security of modern IT Systems

User

Secure System

MPC, FHE, SNARKS, Masked impl., PQ-Signatures

LowMC, MiMC, Kreyvium, FLIP, ...
LowMC

By

Martin Albrecht (RHUL)
Christian Rechberger (TUG, DTU)
Thomas Schneider (TUD)
Michael Zohner (TUD)
Tyge Tiessen (DTU),

LowMC v1 published at Eurocrypt 2015
Round transformation

\[ S_0(\mathcal{A}, \mathcal{B}, \mathcal{C}) = \mathcal{A} \oplus \mathcal{B}\mathcal{C} \]
\[ S_1(\mathcal{A}, \mathcal{B}, \mathcal{C}) = \mathcal{A} \oplus \mathcal{B} \oplus \mathcal{A}\mathcal{C} \]
\[ S_2(\mathcal{A}, \mathcal{B}, \mathcal{C}) = \mathcal{A} \oplus \mathcal{B} \oplus \mathcal{C} \oplus \mathcal{A}\mathcal{B} \]
Design space

Size
  – n: Block size
  – m: Number of Sboxes

Security
  – k: Key size (allowed time complexity)
  – d: allowed data complexity

r: Number of rounds is function of (n,m,k,d)
Challenges for Three Use-Cases
LowMC Challenge I

PQ-Signature use-case: \[\text{minimizes } m \times r\]

Parameters: \(n=256, \ k=256, \ m=1, \ d=1\)

- How fast can you break \(r = 243\) rounds?
- Can you break \(r = 380\) rounds?
LowMC Challenge II

FHE/MPC use-case: minimizes r

Parameters: n=256, k=128, m=85, d=1
• How fast can you break r=5 rounds?
• Can you break r=8 rounds?

Parameters: n=256, k=128, m=85, d=128
• How fast can you break r=11 rounds?
• Can you break r=14 rounds?
LowMC Challenge III

MPC use-case: minimize $m*r/n$

Parameters: $n=1024, k=128, m=1, d=128$

• How fast can you break $r=600$ rounds?
• Can you break $r=901$ rounds?
Details

• Start: Now!
• Deadline: Nov 1\textsuperscript{st}, 2017.
• Prices are gifts from Austria, Germany, Denmark, UK, Iran.
• More details on [https://github.com/lowmc](https://github.com/lowmc) incl. affine-layer matrices and vectors for direct download