Higher-order cryptanalysis of LowMC

Christoph Dobraunig **Maria Eichlseder** **Florian Mendel**

Presentation by **Daniel Slamanig**

ICISC 2015

Overview

- The block cipher LowMC
  - "Explores corners of design space"
  - Optimized for evaluation with MPC, FHE & ZK
- Higher-order differential cryptanalysis
  - Exploit low algebraic degree of cipher
- Contribution: Key-recovery attacks on LowMC
  - Exploit LowMC's special S-box layer design
  - 9 / 11 rounds of LowMC-80
  - 9 / 12 rounds of LowMC-128

LowMC

Motivation: Ciphers for MPC and FHE

- Multi-Party Computation (MPC):
  - Jointly compute a function over private inputs
- Fully Homomorphic Encryption (FHE):
  - Evaluate function over encrypted input
- Zero-Knowledge Proofs (ZK):
  - Prove functional relation over undisclosed inputs

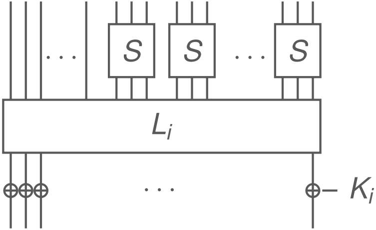
- Linear operations in function “almost free”
  ... at least compared to non-linear ones (multiplications)

- Suitable ciphers to evaluate with MPC, FHE & ZK?

LowMC

- Block cipher
- Presented at Eurocrypt 2015 [Alb+15] by
  Albrecht, Rechberger, Schneider, Tiessen, Zohner
- Design goals:
  - Low "Multiplicative Complexity" ('and'-gates, 'and'-depth)
  - Optimized for MPC, FHE & ZK
  - "Explore corners of the design space"

LowMC: Round function f



S-box layer f_S (m 3-bit S-boxes)

Linear layer f_L (random matrix)

Key addition f_K (linear key schedule)

- Incomplete S-box layer
- Small S-boxes (3-bit)
- Few rounds (10–12)
- Strong linear layer

LowMC: Parameters

	LowMC-80	LowMC-128
Key size k	80	128
Block size n	256	256
Log. data limit d	64	128
# Rounds r	11	12
# S-boxes m	49	63

Focus on LowMC-80

Higher-order differential attacks

Higher-order differential attacks

- "Higher-order": differences of differences of differences...
- "Algebraic cryptanalysis" based on Boolean function theory
- Exploit low algebraic degree of ciphers
- Introduced by Lai [Lai94], Knudsen [Knu94]
- Attack goals:
  - Distinguishers (Zero-sums, ...)
  - Key recovery (Cube attacks, ...)

Algebraic normal form of Boolean functions

Algebraic normal form (ANF)

- "xor of ands": $\bigoplus(\bigwedge x_i)$, often written $\sum(\prod x_i)$
- S-box of LowMC as vectorial ANF:

$$f\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=\begin{pmatrix}x_2x_3+x_1\\x_3x_1+x_1+x_2\\x_1x_2+x_1+x_2+x_3\end{pmatrix}$$

Algebraic degree (deg f)

- Polynomial degree of ANF
- S-box of LowMC: degree 2

“Deriving” a vectorial Boolean function

Derivative of $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ wrt. $a \in \mathbb{F}_2^n$

- $\frac{\mathrm{d}}{\mathrm{d}a} f(x) = f(x) + f(x+a)$
- Compare differential cryptanalysis!

***k*-th order derivative of *f* [Lai94]**

- basis $a_1, \ldots, a_k$ of vector space $V \leq \mathbb{F}_2^n$
- $\frac{\mathrm{d}}{\mathrm{d}a_1} \cdots \frac{\mathrm{d}}{\mathrm{d}a_k} f(x) = \frac{\mathrm{d}}{\mathrm{d}V} f(x) = \sum_{v \in V} f(x+v) = \sum_{w \in V+x} f(w)$

Zero-sum distinguisher

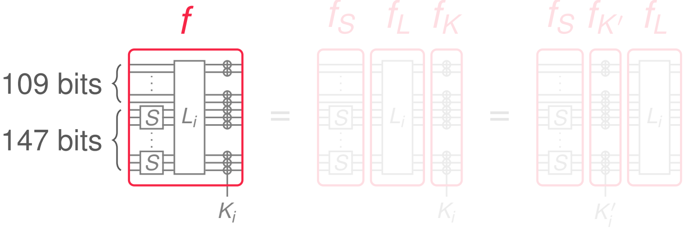
Observation: if $\deg(f) < d$ and $\dim V = d$, then

$$\sum_{w \in V+x} f(w) = \frac{\mathrm{d}}{\mathrm{d}a_1} \cdots \frac{\mathrm{d}}{\mathrm{d}a_d} f = 0$$

- Degree of a block cipher:
  - b-bit S-box has degree $d \leq b - 1$
  - r rounds of degree $d \rightarrow$ total degree $D \leq d^r$
- Zero-sum distinguisher:
  - Chosen plaintexts: $D + 1$-dimensional (affine) vector space V
    V is often a “cube”: $D + 1$ bits vary, rest constant
  - Ciphertexts will sum to 0

Application to LowMC

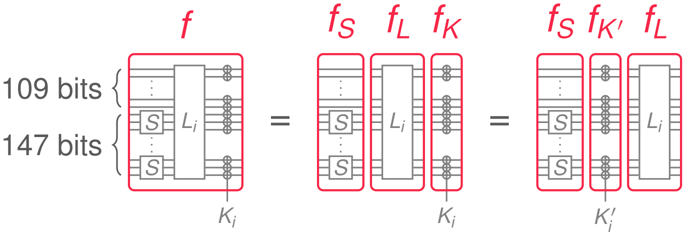
LowMC-80: Round function



Goal: Key recovery for 9 / 11 rounds of LowMC-80

- Need to recover $\approx$ 80 bits of any K_i or, equivalently, K'_i
- Data limit: $< 2^{64}$ queries

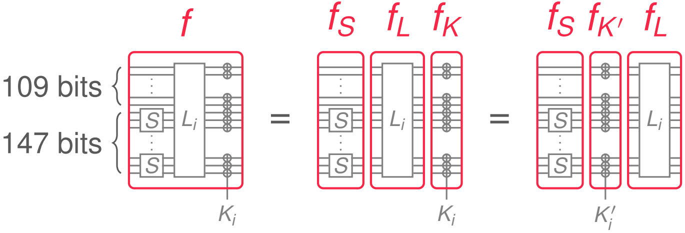
LowMC-80: Round function



Goal: Key recovery for 9 / 11 rounds of LowMC-80

- Need to recover ≈ 80 bits of any K_i or, equivalently, K_i'
- Data limit: $< 2^{64}$ queries

LowMC-80: Round function

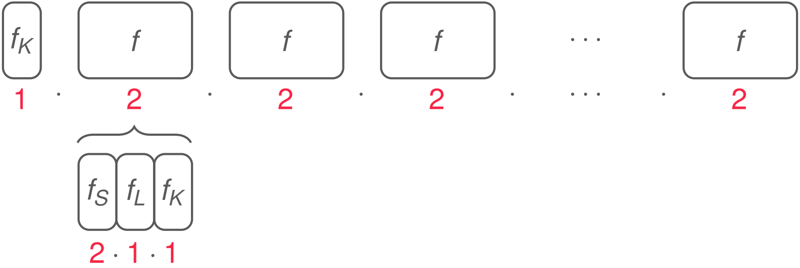


Goal: Key recovery for 9 / 11 rounds of LowMC-80

- Need to recover $\approx$ 80 bits of any K_i or, equivalently, K_i'
- Data limit: $< 2^{64}$ queries

LowMC-80: Algebraic degree (bounds)

11 rounds f of degree 2 (plus initial key-whitening):

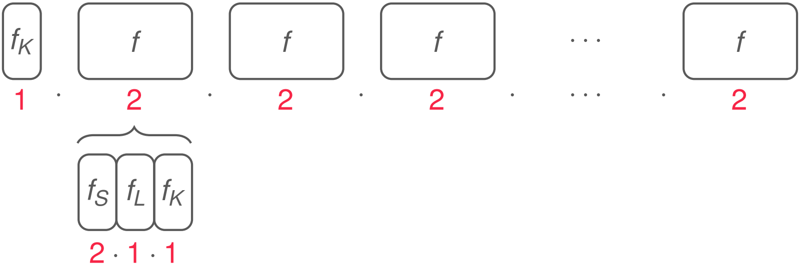


Bounds on degree:

Rounds r	1	2	3	4	5	6	7	8	9	10	11	12
LowMC-80	2	4	8	16	32	64	113	162	209	232	244	
LowMC-128	2	4	8	16	32	64	127	190	223	239	247	251

LowMC-80: Algebraic degree (bounds)

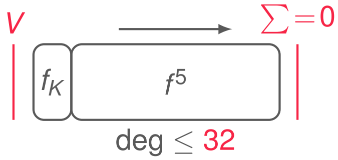
11 rounds f of degree 2 (plus initial key-whitening):



Bounds on degree:

Rounds r	1	2	3	4	5	6	7	8	9	10	11	12
LowMC-80	2	4	8	16	32	64	113	162	209	232	244	
LowMC-128	2	4	8	16	32	64	127	190	223	239	247	251

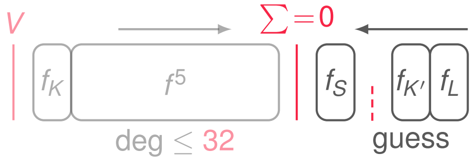
Zero-sum distinguisher for 5 rounds



1. For 5 forward rounds: V with 2^{33} chosen messages
   (due to query complexity limit 2^{64})

Complexity: 2^{33} queries, 2^{33} time

Key recovery for 6 rounds



2 Add 1 final round to recover key in 3-bit-chunks
Repeat for $\lceil \frac{80}{3} \rceil = 27$ S-boxes:

(a) Guess 3 key bits (of K')

(b) Compute backwards to S-box inputs

(c) Check if each S-box input bit sums to 0

Complexity: 2^{33} queries, 2^{33+0} time

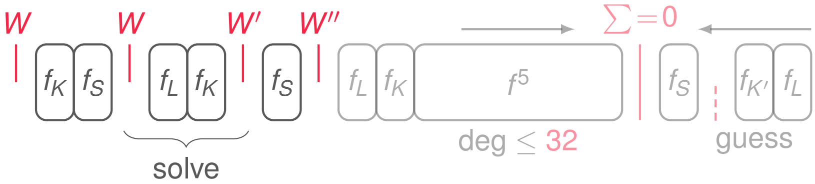
Key recovery for 7 rounds

3 Add 1 free initial round (f_S maps V to V)

- V is constant/zero except on 109 bits of identity part
- f_K and f_S map $V + c$ to some $V + c'$

Complexity: 2^{33} queries, 2^{33+0} time

Key recovery for 8 rounds

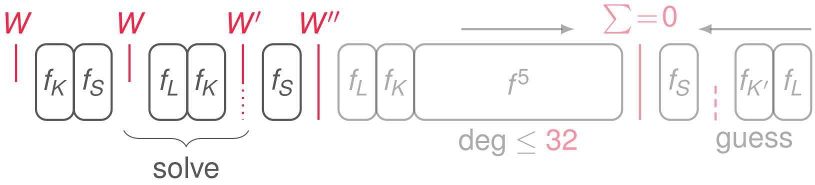


4 Add 1 initial round (construct W to bridge f_S in 2 rounds)

- 1st f_S easy, like **3**: W is 0 except on identity part (dim 109)
- 2nd f_S adds linear constraints to W to get W':
  - Force 3 bits per S-box to 0: $3 \cdot 49 = 147$ constraints
  - Guess 21 key bits to partially invert 1st f_S ($\rightarrow$ dim $11 + 21 = 32$)
  - $+1$ from selecting redundant constraints

Complexity: 2^{33} queries, 2^{33+21} time

Key recovery for 8 rounds

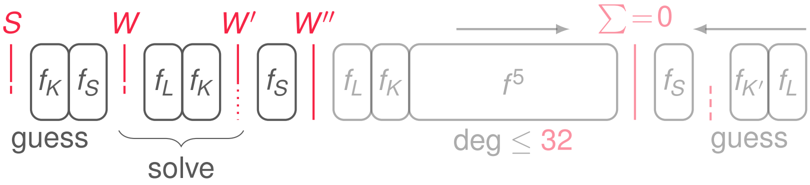


4 Add 1 initial round (construct W to bridge f_S in 2 rounds)

- 1st f_S easy, like 3: W is 0 except on identity part (dim 109)
- 2nd f_S adds linear constraints to W to get W':
  - Force 2 bits per S-box to 0: $2 \cdot 49 = 98$ constraints ($\rightarrow$ dim 11)
  - Guess 21 key bits to partially invert 1st f_S ($\rightarrow$ dim $11 + 21 = 32$)
  - $+1$ from selecting redundant constraints

Complexity: 2^{33} queries, 2^{33+21} time

Key recovery for 8 rounds

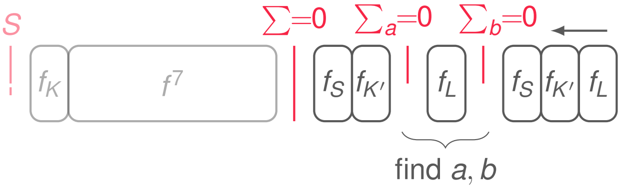


4 Add 1 initial round (construct W to bridge f_S in 2 rounds)

- 1st f_S easy, like 3: W is 0 except on identity part (dim 109)
- 2nd f_S adds linear constraints to W to get W':
  - Force 2 bits per S-box to 0: $2 \cdot 49 = 98$ constraints ($\rightarrow$ dim 11)
  - Guess 21 key bits to partially invert 1st f_S ($\rightarrow$ dim $11 + 21 = 32$)
  - $+1$ from selecting redundant constraints

Complexity: 2^{33} queries, 2^{33+21} time

Key recovery for 9 rounds

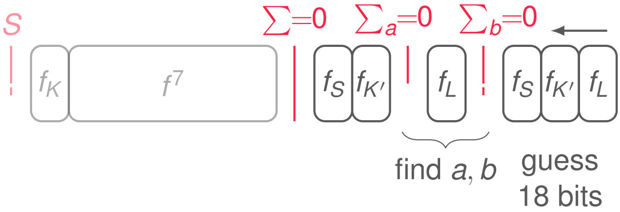


5 Add 1 final round (extend 0-sum with linear mask a, b)

- Partial 0-sum on 109 bits after $f_S, f_{K'}$
- 1-bit check: if $\forall x : \langle a, x\rangle + \langle b, f_L(x)\rangle = 0$, then $\sum_b = \langle b, \sum\rangle = 0$
- b covers 6 S-boxes $\rightarrow$ guess 18 key bits, win 1 bit information
- Repeat with 18 sets $S \times$ 4 masks a, b to recover full key

Complexity: $2^{33+\log 18} \approx 2^{37.2}$ queries, $2^{54+\log 18} \approx 2^{58.2}$ time

Key recovery for 9 rounds



5 Add 1 final round (extend 0-sum with linear mask a, b)

- Partial 0-sum on 109 bits after $f_S, f_{K'}$
- 1-bit check: if $\forall x : \langle a, x\rangle + \langle b, f_L(x)\rangle = 0$, then $\sum_b = \langle b, \sum\rangle = 0$
- b covers 6 S-boxes $\rightarrow$ guess 18 key bits, win 1 bit information
- Repeat with 18 sets $S \times$ 4 masks a, b to recover full key

Complexity: $2^{33+\log 18} \approx 2^{37.2}$ queries, $2^{54+\log 18} \approx 2^{58.2}$ time

Interpolation attacks by Dinur et al.

- Results by Dinur et al. [Din+15]:
  - Key recovery phase can be improved significantly with optimized interpolation attacks
  - LowMC-80: 10 / 11 rounds in 2^{57}
  - LowMC-128: 12 / 12 rounds in 2^{118}
  - Even better attacks for weak instances
- Check out their presentation at Asiacrypt 2015!

Conclusion

- LowMC explores corners of the design space
- Our results:
  - LowMC-80: Key recovery for 9 / 11 rounds ($\approx 2^{58.2}$)
  - LowMC-128: Key recovery for 9 / 12 rounds ($\approx 2^{72}$)
  - Up to 10 rounds of other LowMC variants
- Exploited properties of LowMC:
  - Partial S-box layer (the larger the identity part, the better)
  - Low degree per round
  - Small S-boxes

Bibliography

[Alb+15] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner
Ciphers for MPC and FHE
Advances in Cryptology – EUROCRYPT 2015

[Din+15] I. Dinur, Y. Liu, W. Meier, and Q. Wang
Optimized Interpolation Attacks on LowMC
Advances in Cryptology – ASIACRYPT 2015

[Knu94] L. R. Knudsen
Truncated and Higher Order Differentials
Fast Software Encryption – FSE 1994

[Lai94] X. Lai
Higher Order Derivatives and Differential Cryptanalysis
Communications and Cryptography 1994