Rasta

A cipher with low ANDdepth and few ANDs per bit

Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, Christian Rechberger

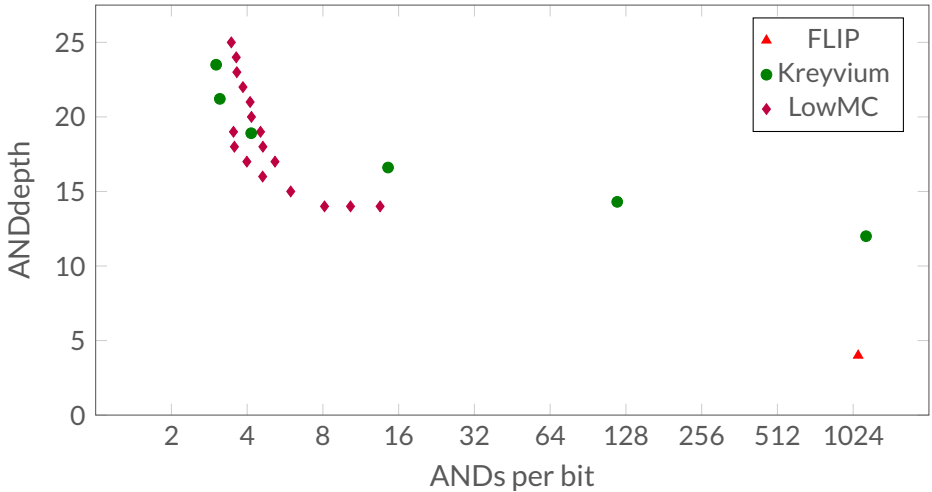
Crypto 2018

Motivation

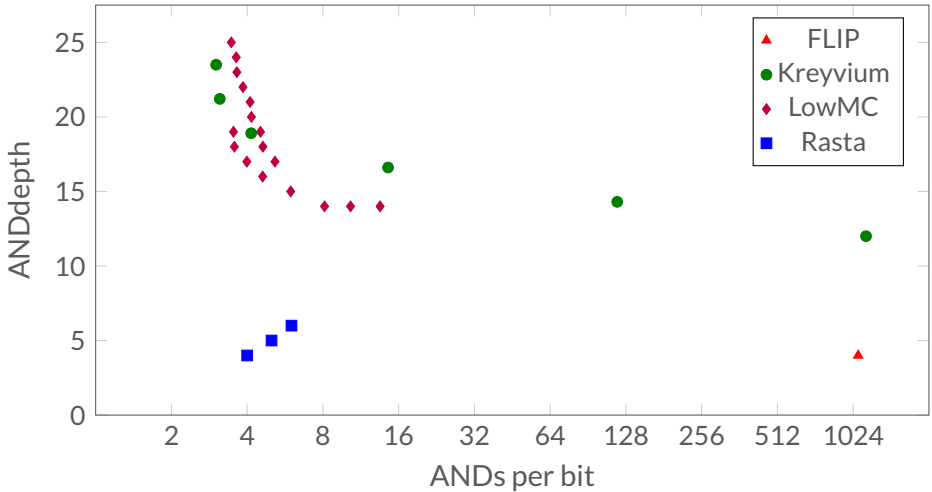
Motivation

- Several designs minimize number of multiplications
  - FLIP [MJSC16]
  - Kreyvium [CCFLNPS16]
  - LowMC [ARSTZ15]
  - MiMC [AGRRT16]
- New optimization goals enable/require new design strategies

Motivation


FLIP
Kreyvium
LowMC
ANDdepth
ANDs per bit
0
5
10
15
20
25
2
4
8
16
32
64
128
256
512
1024

Motivation

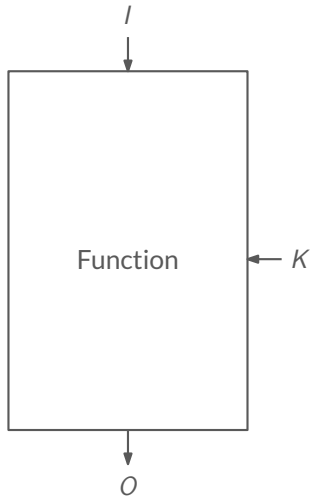

FLIP
Kreyvium
LowMC
Rasta
ANDdepth
0
5
10
15
20
25
2
4
8
16
32
64
128
256
512
1024
ANDs per bit

Challenges

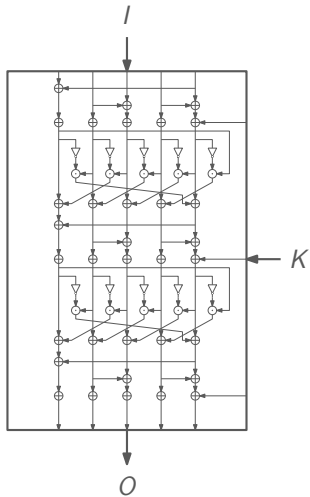
Challenges for Rasta

- How to minimize ANDdepth and ANDs per bit at the same time?
- Especially low ANDdepth seems challenging
- How to analyze the outcome?

Why do we have a high ANDdepth?



Why do we have a high ANDdepth?



Why do we have a high ANDdepth?

- Evaluated for varying inputs
- Part of the input potentially public
- Need high algebraic degree (ANDdepth) for protection
  - Against higher-order differentials, cube-like attacks, …
- $O_1 = I_1K_1K_3 + I_2I_3K_4 + I_1I_2K_2 + I_1I_2 + I_4K_1 + K_2$
- $O_1 = I_1I_2(K_2 + 1) + I_1K_1K_3 + I_2I_3K_4 + I_4K_1 + K_2$

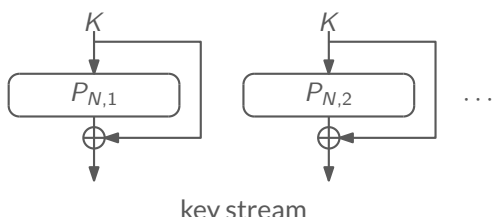
Why do we have a high ANDdepth?

- Evaluated for varying inputs
- Part of the input potentially public
- Need high algebraic degree (ANDdepth) for protection
  - Against higher-order differentials, cube-like attacks, …
- $O_1 = I_1K_1K_3 + I_2I_3K_4 + I_1I_2K_2 + I_1I_2 + I_4K_1 + K_2$
- $O_1 = I_1I_2(K_2 + 1) + I_1K_1K_3 + I_2I_3K_4 + I_4K_1 + K_2$

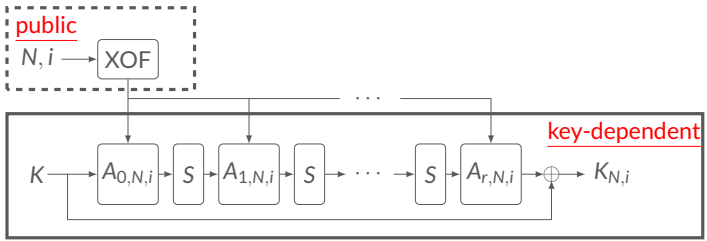
The Design

Rasta

- Stream cipher based on family of public permutations $P_{N,i}$
  - Each permutation evaluated once
  - Different permutations to generate key stream
  - Choice of permutation depends solely on public parameters
    - Public nonce N
    - Block counter i

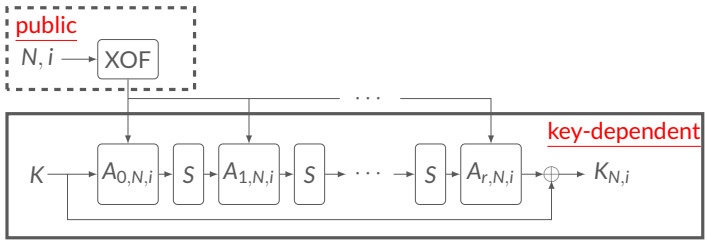


Rasta



- Seed extendable output function (XOF) with public values
  - "Randomly" generates invertible matrices $M_{j,N,i}$
  - "Randomly" generates round constants $c_{j,N,i}$
  - To get affine layer $A_{j,N,i}(x) = M_{j,N,i} \cdot x \oplus c_{j,N,i}$
- Use of χ [Dae95] as non-linear function S

Rasta



- High-level idea to make relevant computations of the cipher independent of the key was first used in Flip [MJSC16]
- XOF does not influence relevant AND metric

Design Rationale

- Changing affine layers against
  - Differential and impossible-differential attacks
  - Cube and higher-order differential attacks
  - Integral attacks
- Block size, key size $\gg$ security level against
  - Attacks based on linear approximations
  - Attacks targeting polynomial system of equations

Choosing parameters

- Parameterizable problem regarding
  - Block size
  - Number of rounds
- Rasta
  - Base parameters on bounds and arguments
  - Conservative approach
- Agrasta
  - Aggressive parameter set of Rasta design strategy
  - Base parameters on best known attacks
  - Challenge for cryptanalysts

Choosing parameters

- Parameterizable problem regarding
  - Block size
  - Number of rounds
- Rasta
  - Base parameters on bounds and arguments
  - Conservative approach
- Agrasta
  - Aggressive parameter set of Rasta design strategy
  - Base parameters on best known attacks
  - Challenge for cryptanalysts

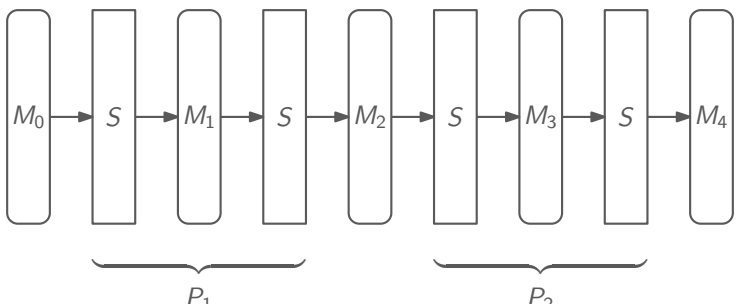
Choosing parameters

- Parameterizable problem regarding
  - Block size
  - Number of rounds
- Rasta
  - Base parameters on bounds and arguments
  - Conservative approach
- Agrasta
  - Aggressive parameter set of Rasta design strategy
  - Base parameters on best known attacks
  - Challenge for cryptanalysts

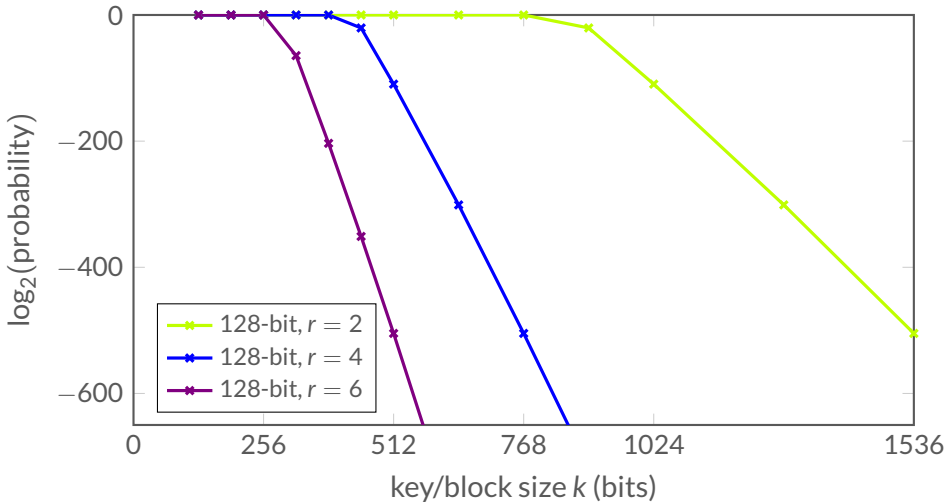
The Road to Rasta

Linear approximations

Bound probability that good approximations exist



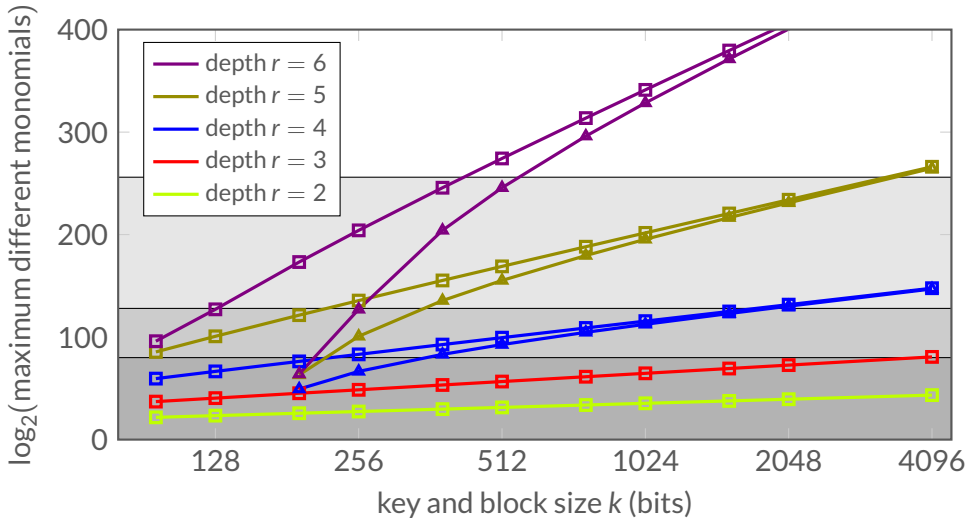
Probability of good approximations



Solving non-linear multivariate polynomial equations

- General problem of solving non-linear systems of m equations with k unknowns
- Limiting the degree limits possible number of different monomials
- Increase k to prevent trivial linearization

Maximum number of different monomials



Instances of Rasta

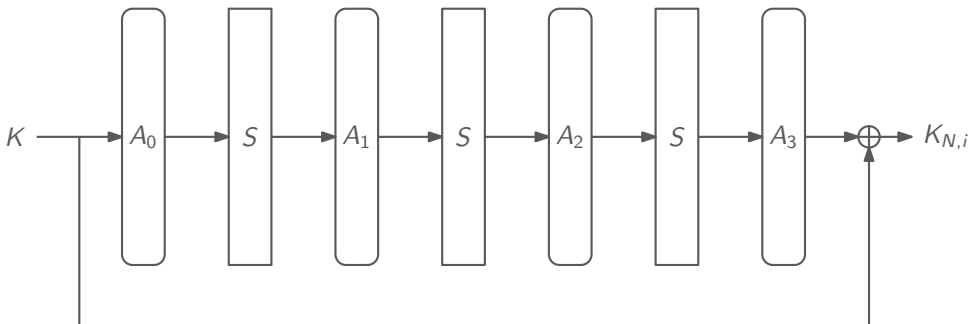
Security level	Rounds				
	2	3	4	5	6
80-bit	$2^{21.2}$	2^{12}	327	327	219
128-bit	$2^{33.2}$	2^{18}	1 877	525	351
256-bit	$2^{65.2}$	2^{34}	$2^{18.8}$	3 545	703

The Road to Agrasta (Cryptanalysis)

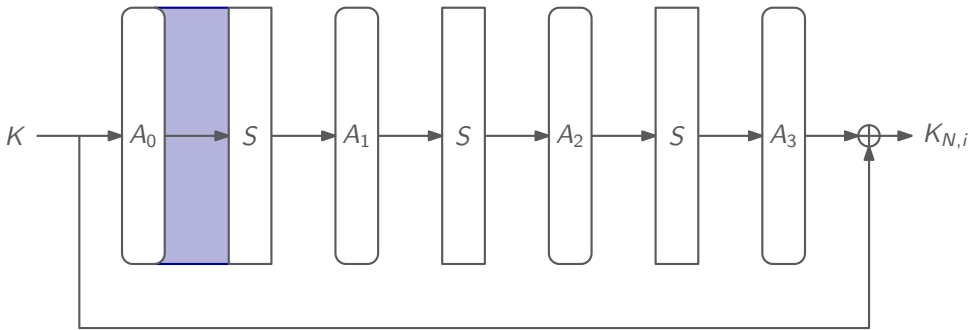
Cryptanalysis

- SAT solver
  - Exhaustive search performs better for more than 1 round
- Experiments with toy versions
  - No obvious outliers
  - Various dedicated attacks
    - For various versions of SAS
    - Variants of 2-round Rasta where block size $\approx$ security level
    - Variants of 3-round Rasta where block size $\approx$ security level

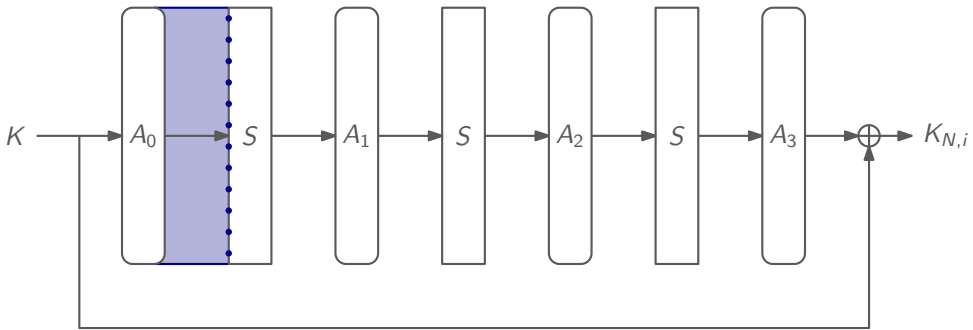
Sketch of 3-round analysis



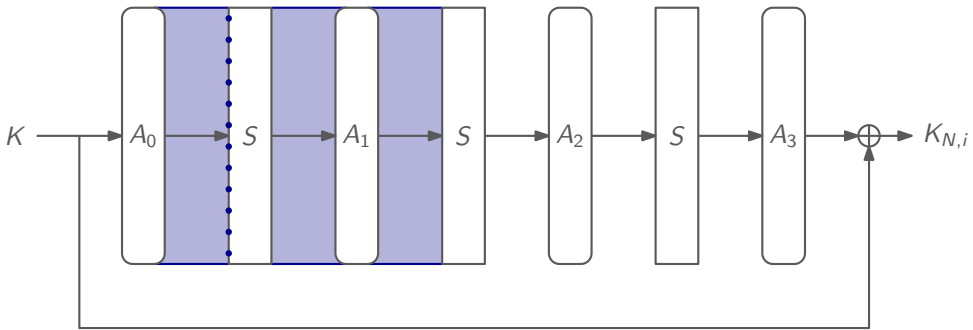
Sketch of 3-round analysis



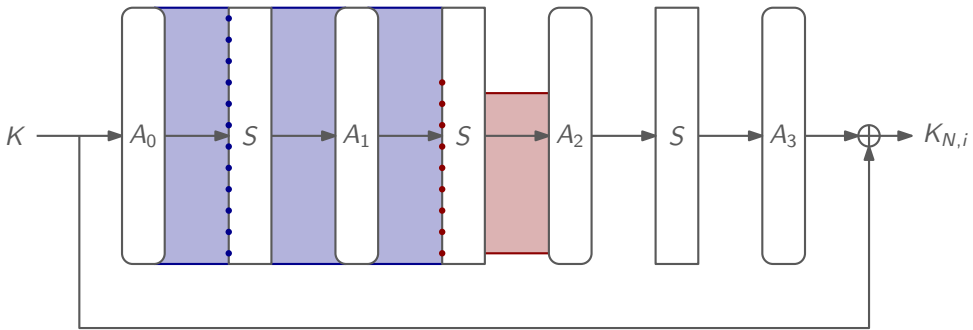
Sketch of 3-round analysis



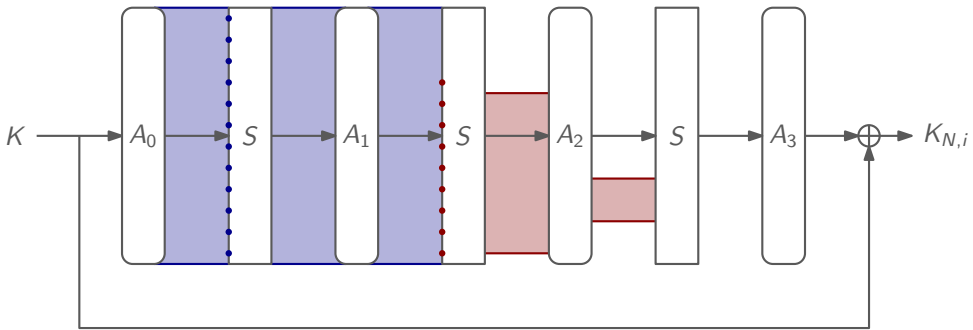
Sketch of 3-round analysis



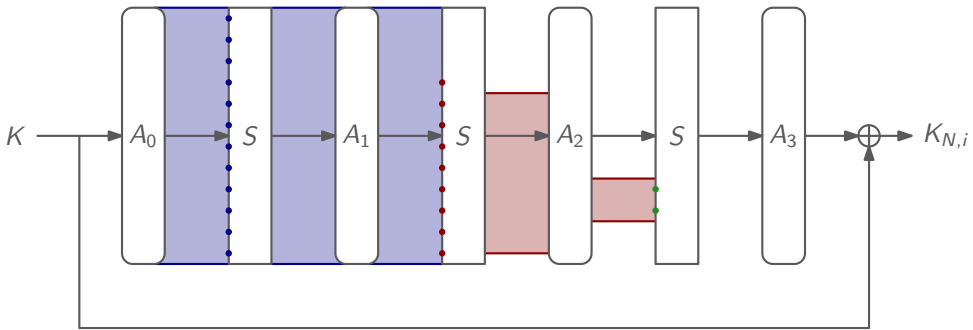
Sketch of 3-round analysis



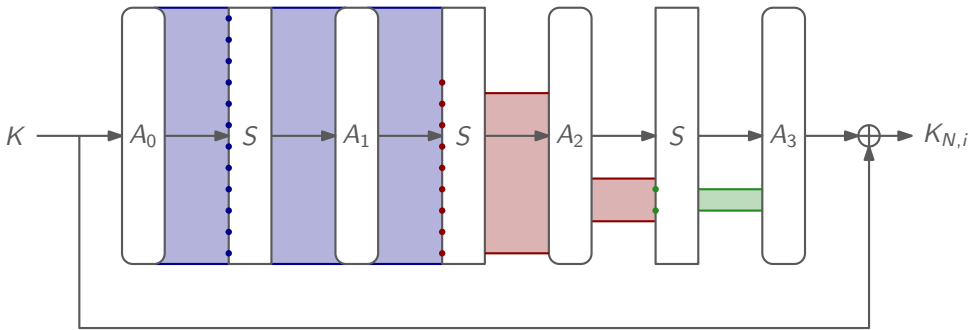
Sketch of 3-round analysis



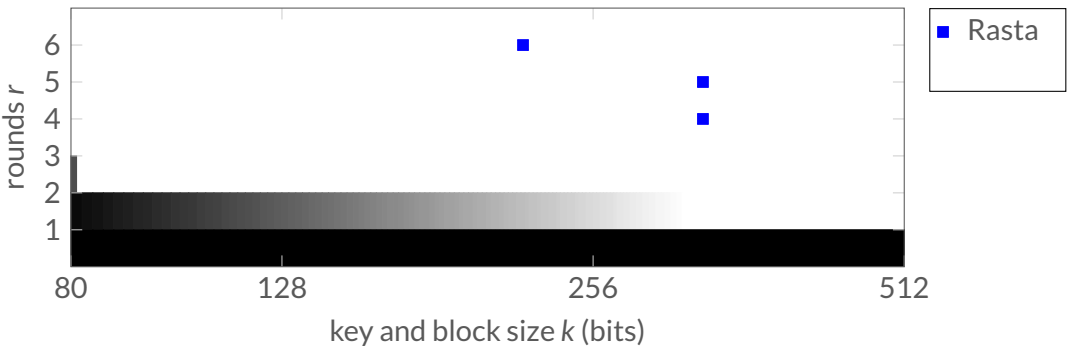
Sketch of 3-round analysis



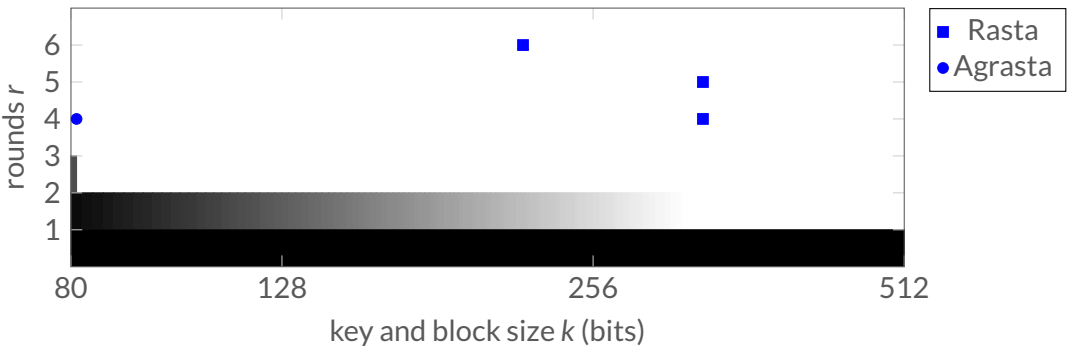
Sketch of 3-round analysis



Cryptanalysis of instances with 80-bit security



Cryptanalysis of instances with 80-bit security



Agrasta: More agressive parameters

Security level	Rounds	Block size
80-bit	4	81
128-bit	4	129
256-bit	5	257

Conclusion

Conclusion

- Rasta: conservative, based on bounds and arguments
- Agrasta: more aggressive, based on attacks
- New design approach
- Even conservative versions competitive in benchmark (HElib)
- Huge gap between known attacks and bounds

Bibliography I

[AGRRT16] M. R. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen
MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity
ASIACRYPT 2016

[ARSTZ15] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner
Ciphers for MPC and FHE
EUROCRYPT 2015

[CCFLNPS16] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. Naya-Plasencia, P. Paillier, and R. Sirdey
Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression
FSE 2016

Bibliography II

[Dae95] J. Daemen,
Cipher and hash function design – Strategies based on linear and differential cryptanalysis,
http://jda.noekeon.org/JDA_Thesis_1995.pdf,
PhD thesis, Katholieke Universiteit Leuven, 1995.

[MJSC16] P. Méaux, A. Journault, F.-X. Standaert, and C. Carlet
Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts
EUROCRYPT 2016