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

![Graph showing the relationship between ANDs per bit and ANDdepth. The graph includes data points for FLIP, Kreyvium, and LowMC.]
Motivation

![Graph](image_url)

- **FLIP**
- **Kreyvium**
- **LowMC**
- **Rasta**
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 AND depth?
Why do we have a high AND depth?
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, ...

\[ O_1 = I_1 K_1 K_3 + I_2 I_3 K_4 + I_1 I_2 K_2 + I_1 I_2 + I_4 K_1 + K_2 \]

\[ O_1 = I_1 I_2 (K_2 + 1) + I_1 K_1 K_3 + I_2 I_3 K_4 + I_4 K_1 + K_2 \]
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, ...

\[
O_1 = l_1K_1K_3 + l_2l_3K_4 + I_1l_2K_2 + l_1l_2 + l_4K_1 + K_2
\]

\[
O_1 = l_1l_2(K_2 + 1) + l_1K_1K_3 + l_2l_3K_4 + l_4K_1 + K_2
\]
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 $i$

![Diagram of Rasta stream cipher](image)
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 $\chi$ [Dae95] as non-linear function $S$
- 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

\[ \log_2(\text{probability}) \]

- 128-bit, \( r = 2 \)
- 128-bit, \( r = 4 \)
- 128-bit, \( r = 6 \)
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

$\log_2(\text{maximum different monomials})$

- $\text{key and block size } k \text{ (bits)}$
- $\text{depth } r = 6$
- $\text{depth } r = 5$
- $\text{depth } r = 4$
- $\text{depth } r = 3$
- $\text{depth } r = 2$
# Instances of Rasta

<table>
<thead>
<tr>
<th>Security level</th>
<th>Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td>80-bit</td>
<td>$2^{21.2}$</td>
</tr>
<tr>
<td>128-bit</td>
<td>$2^{33.2}$</td>
</tr>
<tr>
<td>256-bit</td>
<td>$2^{65.2}$</td>
</tr>
</tbody>
</table>
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

![Graph showing key and block size (k bits) vs. rounds (r) for Rasta and Agrasta.](image-url)
Agrasta: More aggressive parameters

<table>
<thead>
<tr>
<th>Security level</th>
<th>Rounds</th>
<th>Block size</th>
</tr>
</thead>
<tbody>
<tr>
<td>80-bit</td>
<td>4</td>
<td>81</td>
</tr>
<tr>
<td>128-bit</td>
<td>4</td>
<td>129</td>
</tr>
<tr>
<td>256-bit</td>
<td>5</td>
<td>257</td>
</tr>
</tbody>
</table>
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

MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity
ASIACRYPT 2016

Ciphers for MPC and FHE
EUROCRYPT 2015

Stream Ciphers: A Practical Solution for Efficient Homomorphic-Cipherertext Compression
FSE 2016
Bibliography II

[Dae95] J. Daemen, 
Cipher and hash function design – Strategies based on linear and differential cryptanalysis,

Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts
EUROCRYPT 2016