Multiple Limited-Birthday Distinguishers and Applications

Jérémy Jean[1] María Naya-Plasencia[2] Thomas Peyrin[3]

[1]École Normale Supérieure, France

[2]SECRET Project-Team - INRIA Paris-Rocquencourt, France

[3]Nanyang Technological University, Singapore

SAC'2013 – August 16, 2013

Open-Key Distinguishers

Block-cipher $E \cong$ family of PRPs $E : \mathcal{K} \times \mathcal{D} \longrightarrow \mathcal{D}$.
Known-key model: introduced by Knudsen and Rijmen in [KR-A07]
Let Δ_{IN} and Δ_{OUT} two truncated differences.

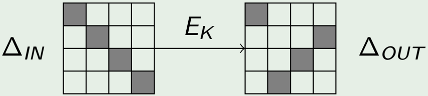
A Known-key Distinguisher

Let K a key and E_K the associated permutation.
Find (P, P') s.t. $P \oplus P' \in \Delta_{IN}$ and $E_K(P) \oplus E_K(P') \in \Delta_{OUT}$.

A Chosen-key Distinguisher

Find $K, (P, P')$ s.t. $P \oplus P' \in \Delta_{IN}$ and $E_K(P) \oplus E_K(P') \in \Delta_{OUT}$.

Example: AES

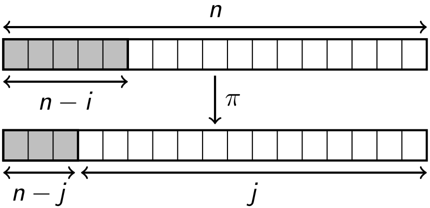


Limited Birthday Algorithm [GP-FSE10]

Conjecture: best generic algorithm to solve the LB problem.

Limited Birthday

What is the generic complexity for mapping i fixed-difference bits to j fixed-difference bits with a random n-bit permutation π?



Algorithm: sequential applications of the birthday algorithm.

Time complexity: $C(i, j)$ (assuming $i \leq j$)

$$\log_2 \left(C(i,j) \right) = \begin{cases} j/2, & \text{if: } j \leq 2(n-i), \\ i + j - n, & \text{if: } j > 2(n-i). \end{cases}$$

Our Contributions

- We add more than one valid truncated differences Δ_{IN} and Δ_{OUT}
- We consider this extended LB problem as Multiple Limited-Birthday
- We provide the best known algorithm to solve the MLB problem
- We apply it to several AES-like primitives

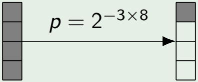
Intuitions (1/2)

Obs.: the gap between generic and distinguishing complexities is often big

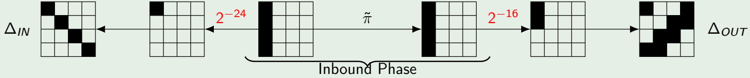
Rebound-based distinguishing algorithms

- Two phases: inbound (deterministic) and outbound (probabilistic)
- We do not elaborate on the inbound phase
- In the outbound, constrained truncated probabilistic transitions.
  $\Longrightarrow$ output positions can be **relaxed**

Probabilistic transition



LB Problem applied to AES



$P_{outbound} = 2^{-40}$

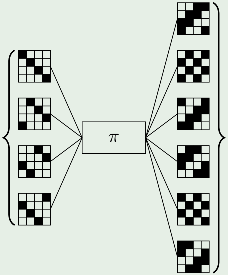
Intuitions (2/2)

Relaxation

- A $t \to c$ transition leads to $\binom{t}{c}$ possibilities
- The probability is $\binom{t}{c}$ higher

Example

$\binom{4}{1}$ Possible inputs



$\binom{4}{2}$ Possible outputs

$$P_{outbound} = 24 \times 2^{-40} \approx 2^{-35.4}$$

Generic Problem

Generic problem

- Relaxing the positions changes the generic algorithm (MLB)
- The algorithm due to [GP-FSE10] is not optimal
  $\Longrightarrow$ Need to commit to a fixed Δ_{IN} (or Δ_{OUT})
- We restric ourselves to:
  - geometries of square size $t \times t$ ($\texttt{AES}$: $t = 4$),
  - n_B active diagonals for Δ_{IN}
  - n_F active anti-diagonals for Δ_{OUT}

Let Δ_{IN} be the set of truncated patterns containing all the $\binom{t}{n_B}$ possible ways to choose n_B active diagonals among the t ones.
Let Δ_{OUT} defined similarly with n_F active anti-diagonals.

Multiple Limited Birthday (MLB)

Given F, Δ_{IN} and Δ_{OUT}, find a pair (m, m') of inputs to F such that $m \oplus m' \in \Delta_{IN}$ and $F(m) \oplus F(m') \in \Delta_{OUT}$.

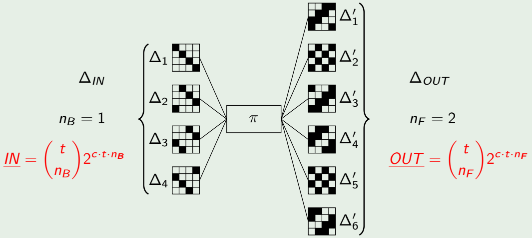
Lower Bounding the Generic Time Complexity

Lower bound on the time complexity T

- MLB with differences $(\Delta_{IN}, \Delta_{OUT})$ is at least as hard as LB on the equivalent parameters $(\underline{IN}, \underline{OUT})$
- Indeed, LB is made easier with less constraints and more possible input pairs

$$C(\underline{IN}, \underline{OUT}) \leq T$$

MLB Example $(t = 4, c = 8)$



Upper Bounding the Generic Time Complexity

Upper bound on the time complexity T

- A first algorithm to solve MLB is based on independent applications of the generic algorithm for LB
- Take one random input Δ_i of size $\overline{IN}$, and apply $LB(\overline{IN}, \underline{OUT})$ until one solution is found

$$T \leq \min\left\{ C(\overline{IN}, \underline{OUT}),\ C(\underline{IN}, \overline{OUT}) \right\}$$

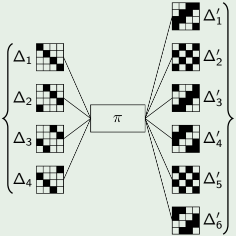
MLB Example ($t = 4, c = 8$)

Δ_{IN}

$n_B = 1$

$\underline{IN} = \binom{t}{n_B} 2^{c \cdot t \cdot n_B}$

$\overline{IN} = 2^{c \cdot t \cdot n_B}$



Δ_{OUT}

$n_F = 2$

$\underline{OUT} = \binom{t}{n_F} 2^{c \cdot t \cdot n_F}$

$\overline{OUT} = 2^{c \cdot t \cdot n_F}$

Improving the Generic Time Complexity

Bounds

$$C(\underline{IN}, \underline{OUT}) \leq T \leq \min\left\{C(\overline{IN}, \underline{OUT}),\ C(\underline{IN}, \overline{OUT})\right\}$$

Our algorithm

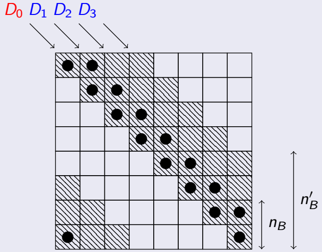
- Solves the generic MLB problem with time complexity T
- We conjecture its optimality
- In the sequel, we explain the forward direction
- We compare our time complexities to the lower bound $C(\underline{IN}, \underline{OUT})$

Data

Notes

- A random pair is a right pair with proba.
  $$P_{out} = \binom{t}{n_F} 2^{-t(t-n_F)c}$$
- We need (at least) P_{out}^{-1} pairs at the input
- $D_1, \ldots, D_{n'_B}$ assume 2^{ct} values
- D_0 assume $2^y < 2^{ct}$ values
- $n_B = 2,\ n'_B = 3$

Structure of Input Data



Number of Pairs

$$N_{pairs}(n'_B, y) \stackrel{\text{def}}{=} \binom{n'_B}{n_B}\binom{2^{n_B ct}}{2} 2^y\, 2^{(n'_B - n_B)tc} + \binom{n'_B}{n_B - 1}\binom{2^{y+(n_B-1)ct}}{2} 2^{(n'_B-(n_B-1))ct}$$

Then: Solve $\mathbf{N_{pairs}(n'_B, y)} = \mathbf{P_{out}^{-1}}$ to get (n'_B, y).

Online Phase

Online Phase

- Query the $2^{y+ctn'_B}$ outputs to the permutation π
- Sort them, and:
  - check for a valid output pattern
  - then, check for a valid input pattern

Time Complexity

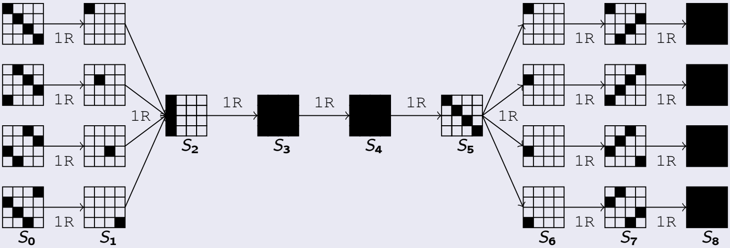
$$2^{y+ctn'_B} + 2^{2(y+ctn'_B)-1} P_{out} \approx 2^{y+ctn'_B}$$

Improvements: constant memory with collision-finding algorithms.

AES in the Known-Key Model

AES: 10 rounds, $t = 4$, $c = 8$.

AES: Known-Key Distinguisher for 8R



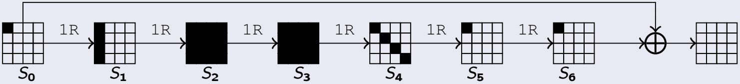
Details

- Super-SBox technique [GP-FSE10]: $\mathcal{S}_2 \to \mathcal{S}_5 = 1$ operation on av.
- Total cost: $2^{24}/4 \cdot 2^{24}/4 = 2^{44}$ computations (prev: 2^{48}).
- Lower bound for generic complexity: 2^{61} computations.

Collision on 6-Round AES in Davies-Meyer Mode

Reduced AES: 6 rounds, $t = 4$, $c = 8$.

AES: 6-Round Collision in DM



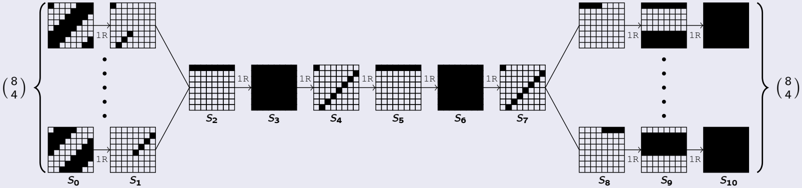
Details

- Technique from [DFJ-INDO12]: $\mathcal{S}_1 \to \mathcal{S}_6 = 1$ operation on av.
- Total cost: $2^{24} \times 2^8 = 2^{32}$ computations (position constrained).
- Lower bound for generic complexity: 2^{64} computations.

Improved Distinguisher of `Whirlpool` CF

`Whirlpool`: 10 rounds, $t = 8$, $c = 8$.
Compression Function (CF): $h(H, M) = E_H(M) \oplus M \oplus H$.

`Whirlpool`: 10-Round Truncated Characteristic



Details

- Inbound from [LMRRS-09]: $\mathcal{S}_2 \rightarrow \mathcal{S}_7 = 2^{64}$ computations on av.
- Cost outbound: $2^{32}/\binom{8}{4} \times 2^{32}/\binom{8}{4} = 2^{51.74}$ computations.
- Total cost: $2^{64} \times 2^{51.74} = 2^{115.74}$ computations
- Lower bound for generic complexity: 2^{125} computations.
- Previous: 2^{176} computations – Ideal: 2^{384}.

Conclusion

- New generic problem for permutations: Multiple Limited-Birthday.
- Lower and upper bounds.
- Best known algorithm to solve the MLB problem.
- Applications to `AES` (proceedings):
  - 8R known-key distinguisher in 2^{44} computations.
  - 8R chosen-key distinguisher in $2^{13.4}$ computations.
  - 6R collision attack in DM in 2^{32} computations.
- Applications to `Whirlpool` (proceedings):
  - 10R CF distinguisher in $2^{115.74}$ computations.
  - 7.5R CF collision attack in 2^{176} computations.
  - 5.5R HF collision attack in 2^{176} computations.
- More in the extended version: `LED`, `Grøstl`, `ECHO`, `PHOTON`.

Conclusion

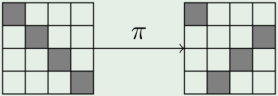
- New generic problem for permutations: Multiple Limited-Birthday.
- Lower and upper bounds.
- Best known algorithm to solve the MLB problem.
- Applications to AES (proceedings):
  - 8R known-key distinguisher in 2^{44} computations.
  - 8R chosen-key distinguisher in $2^{13.4}$ computations.
  - 6R collision attack in DM in 2^{32} computations.
- Applications to Whirlpool (proceedings):
  - 10R CF distinguisher in $2^{115.74}$ computations.
  - 7.5R CF collision attack in 2^{176} computations.
  - 5.5R HF collision attack in 2^{176} computations.
- More in the extended version: LED, Grøstl, ECHO, PHOTON.

Thank you!

Example of the LB on AES

Example: AES, one cell = 8 bits

$i = 96$

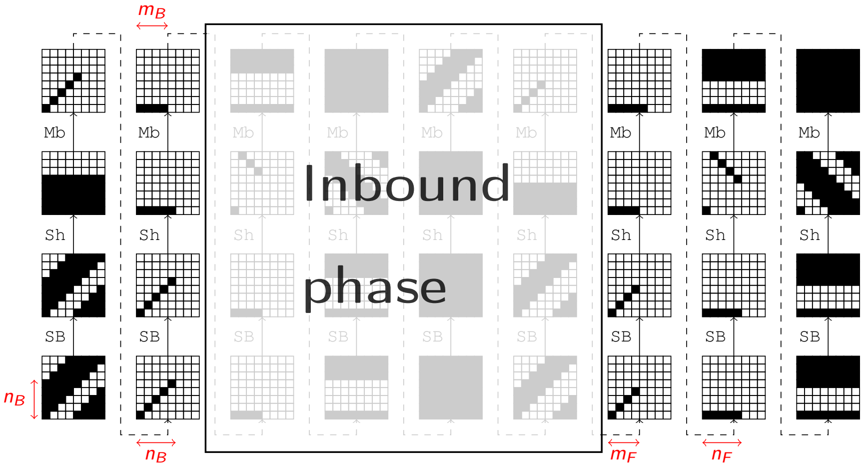


$j = 96$

Application of the algorithm

1. $n = 128$, $i = n - 32 = 96$, $j = n - 32 = 96$
2. Attacking π is as hard as π^{-1} ($i = j$)
3. With one structure of 2^{32} messages:
    - collision on 64 bits by the Birthday Paradox
    - $96 - 64 = 32$ non-colliding bits
4. Repeat **Step 3** 2^{32} times (randomize value of non-active bits)
5. Collision on 96 bits with 2^{64} messages and 2^{64} computations

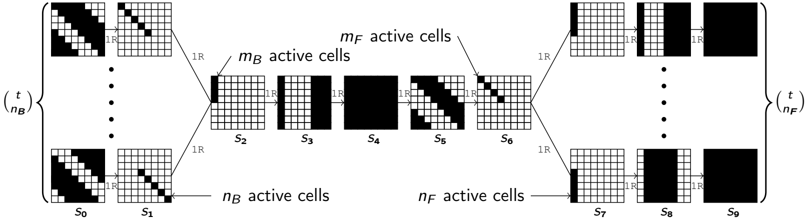
Example: AES-Like Permutation with $t = 8$



Outbound probability

$$2^{-c(2t-n_B-n_F)}$$

MLB on This Example



Outbound probability

$$\binom{t}{n_B}\binom{t}{n_F}2^{-c(2t-n_B-n_F)}$$

Some Time Complexities and Bounds

Bounds

$$C(\underline{IN}, \underline{OUT}) \leq T \leq \min\left\{C(\overline{IN}, \underline{OUT}),\ C(\underline{IN}, \overline{OUT})\right\}$$

Time Complexity: Examples

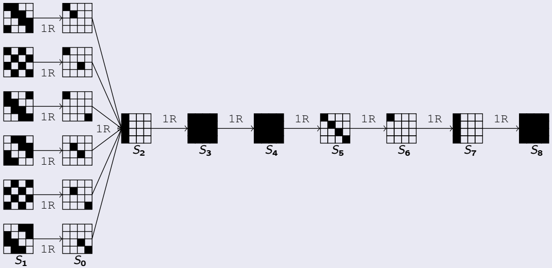
(t, c, n_B, n_F)	$C(\underline{IN}, \underline{OUT})$	T	$C(\overline{IN}, \underline{OUT})$
$(8, 8, 1, 1)$	2^{379}	$2^{379.7}$	2^{382}
$(8, 8, 1, 2)$	$2^{313.2}$	$2^{314.2}$	$2^{316.2}$
$(8, 8, 2, 2)$	$2^{248.4}$	$2^{250.6}$	$2^{253.2}$
$(8, 8, 1, 3)$	$2^{248.2}$	$2^{249.7}$	$2^{251.2}$
$(4, 8, 1, 1)$	2^{61}	$2^{62.6}$	2^{63}
$(4, 4, 1, 1)$	2^{29}	$2^{30.6}$	2^{31}

Note: $C(\overline{IN}, \underline{OUT}) = \binom{t}{n_B} C(\underline{IN}, \underline{OUT})$.

AES in the Chosen-Key Model

AES: 10 rounds, $t = 4$, $c = 8$.

AES: Chosen-Key Distinguisher for 8R



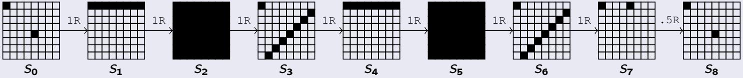
Details

- Technique from [DFJ-INDO12] $\mathcal{S}_2 \rightarrow \mathcal{S}_8 = 1$ operation on av.
- Total cost: $2^{16-\log_2 \binom{4}{2}} = 2^{13.4}$ computations (prev: 2^{24}).
- Lower bound for generic complexity: $2^{31.7}$ computations.

Improved Collision Attack for `Whirlpool` CF

`Whirlpool`: 10 rounds, $t = 8$, $c = 8$.

`Whirlpool`: 7.5-Round Truncated Characteristic



Details

- Same inbound from [LMRRS-09].
- We let one more active byte in S_0 and S_7.
- Gain factor: $2^8 \times 2^8 \times 2^{-8} = 2^8$.
- Total cost: 2^{176} computations (prev: 2^{184}).
- Same technique for the 5.5-Round collision attack on the HF.
- Generic complexity: 2^{256} computations.