Innovative R&D by NTT

Cryptanalysis of Reduced NORX

initially discussed at ASK 2016

Nasour Bagheri (SRTTU, Iran),
Tao Huang (NTU, Singaopre),
Keting Jia (Tsinghua Univ., State Key Lab, China),
Florian Mendel (TUGraz, Austria),
Yu Sasaki (NTT, Japan)

FSE2016@Bochum 23/March/2016

Research Summary

NORX: one of 29 2nd round candidates in CAESAR

Previous: full (4R) distinguisher for permutation

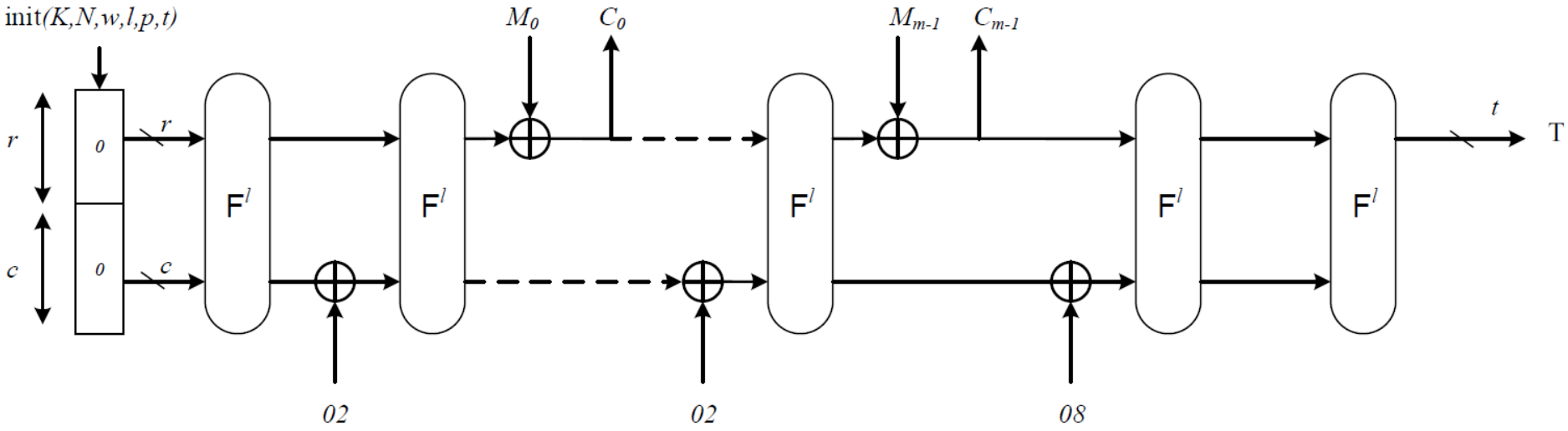
Ours: meaningful security notions for reduced rounds in the nonce-respect setting

Approach	Goal	Target	Rounds	Data	Time	Memory
Guess and determine	KR	NORX64	2/4	3	2^{234}	negl.
Guess and determine	KR	NORX32	2/4	3	2^{119}	negl.
Internal difference	KR	NORX64	2/4	74	$2^{232.8}$	2^{225}
Internal difference	KR	NORX32	2/4	158	$2^{124.3}$	2^{115}
Internal differential-linear	KD	NORX64	2/4	90	negl.	negl.

Introduction of NORX

- Sponge(duplex)-based AE designed by Aumasson, Jovanovic and Neves
  - NORXw (w=32,64):

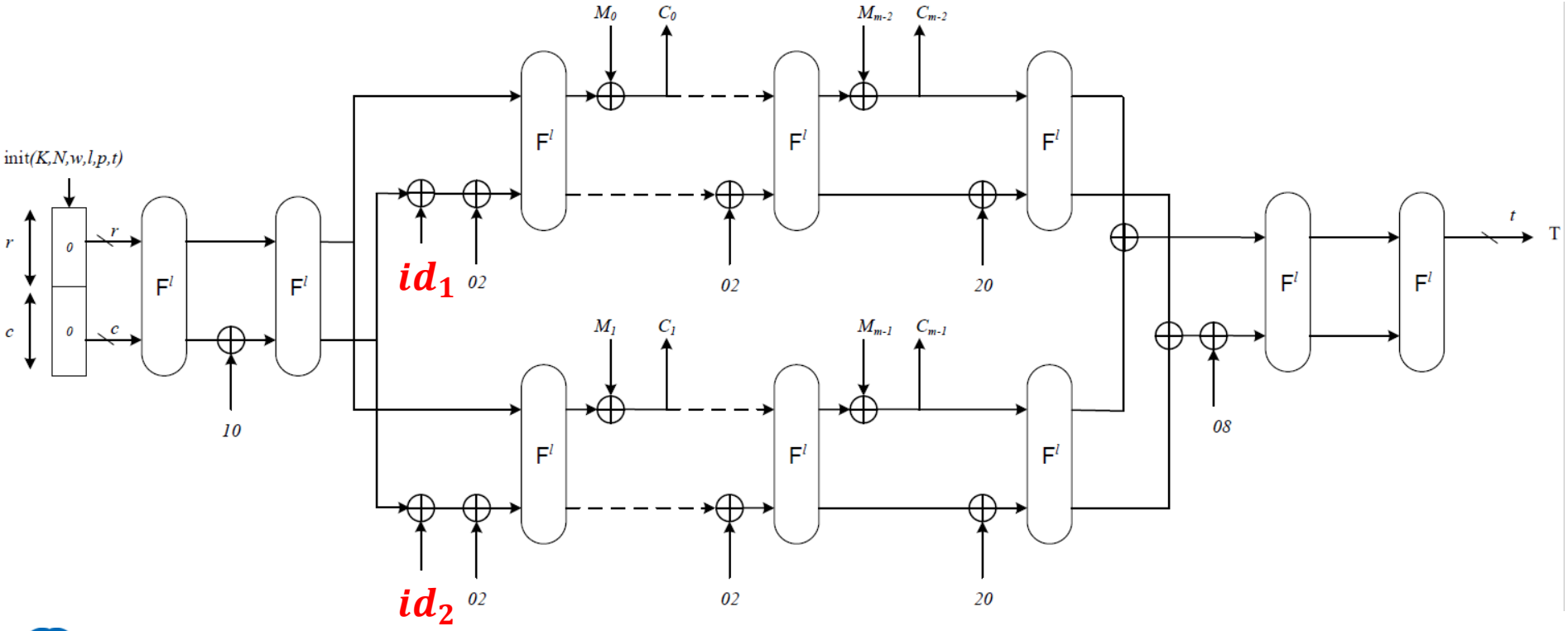
    $16w$-bit state, $12w$-bit rate, $4w$-bit capacity
  - $4w$-bit security in nonce-respect



Parallel Mode in NORX

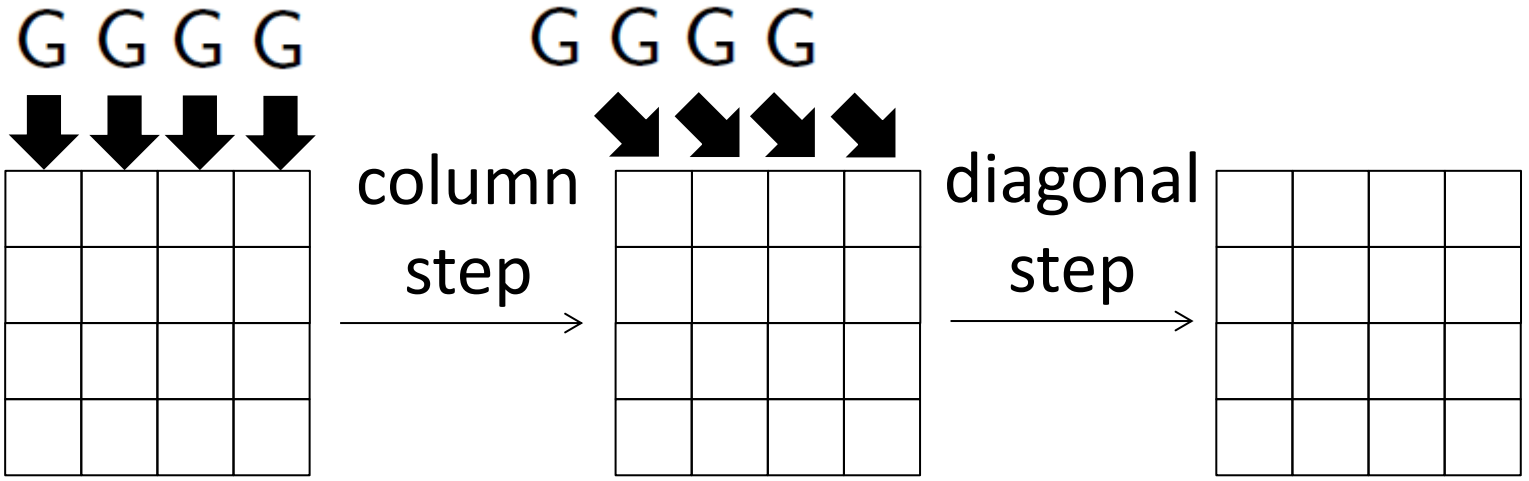
- NORX specifies a parallel mode.
  - Duplicate state then XORs different id numbers

(picture for 2 parallel lanes)

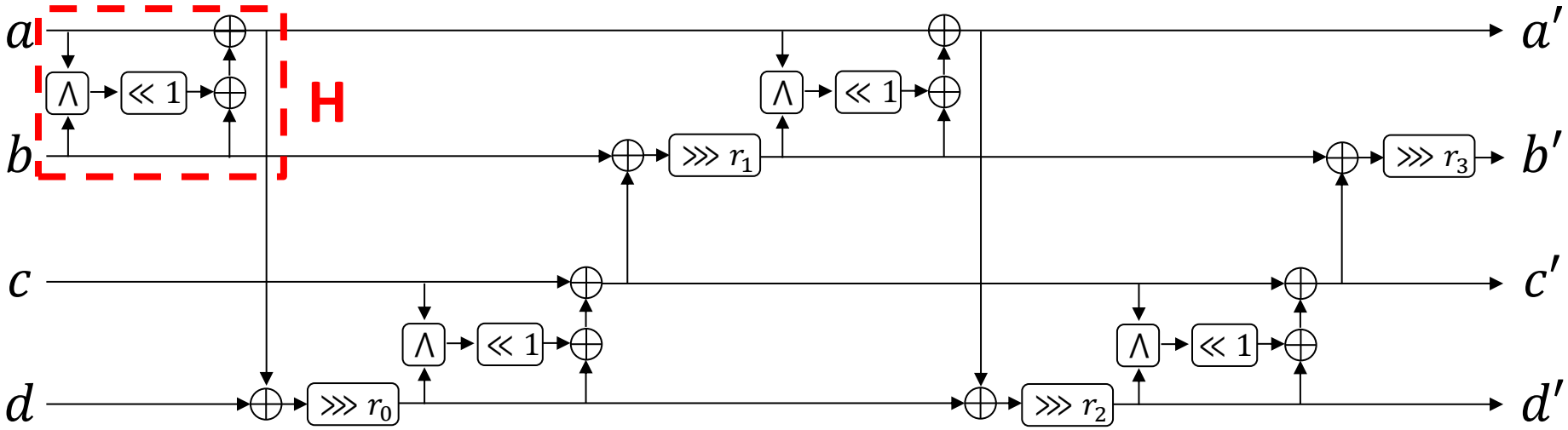


NORX Core Permutation **F**

- State is initialized by key and nonce
- Each round of **F** applies $4w$-bit permutation **G**.
  - Column Step: apply G in each of 4 columns
  - Diagonal Step: apply G in each of 4 diagonals
- **F** outputs the state after 4 (6) rounds.



G Function



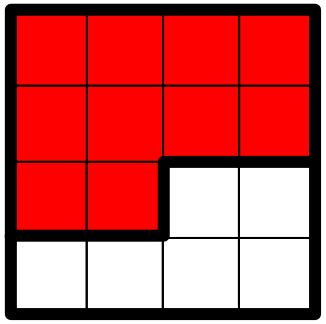
- Consists of OR, XOR, << 1 and >>> r_i.
- H is an approximation of addition $a \leftarrow a + b$.

Design Tweak in Version 2

NORX V1

$|r| = 10w$

$|c| = 6w$

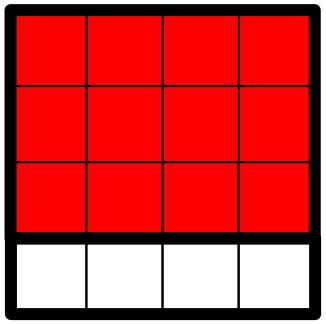


Security: $4w$ bits

NORX V2

$|r| = 12w$

$|c| = 4w$



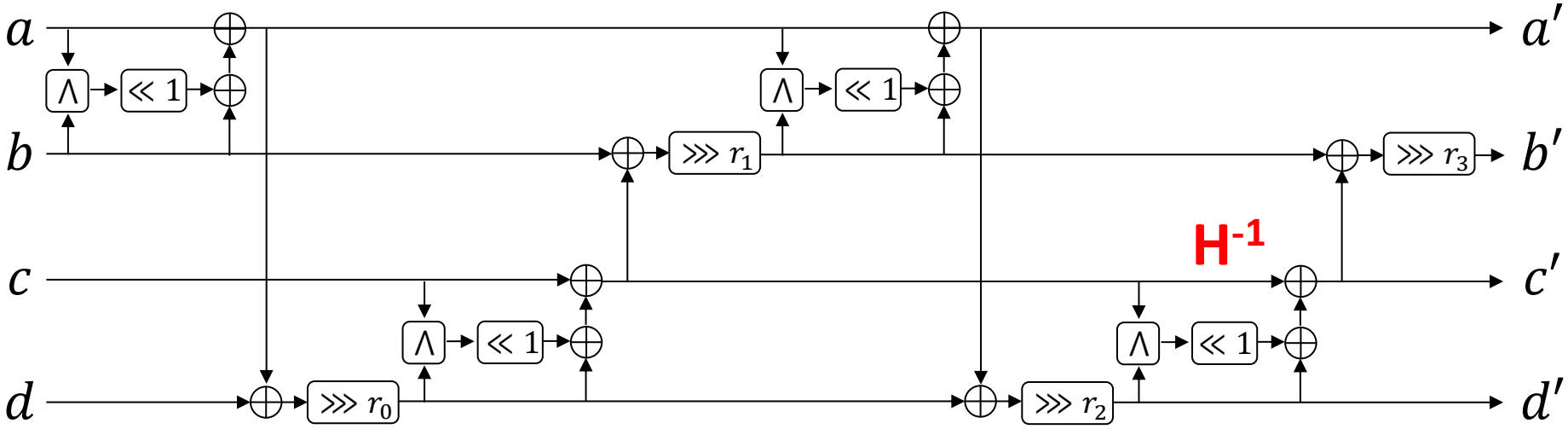
Security: $4w$ bits

Our initial motivation

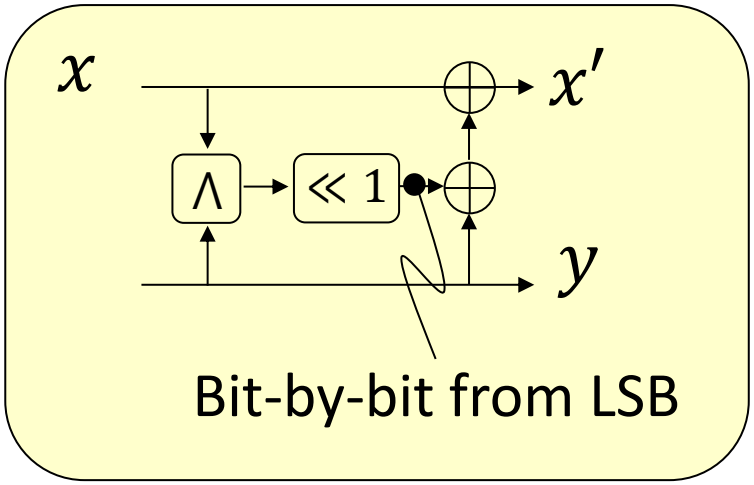
In version 2, recovering single bit of capacity immediately leads to key recovery attack.

Properties of Round Function

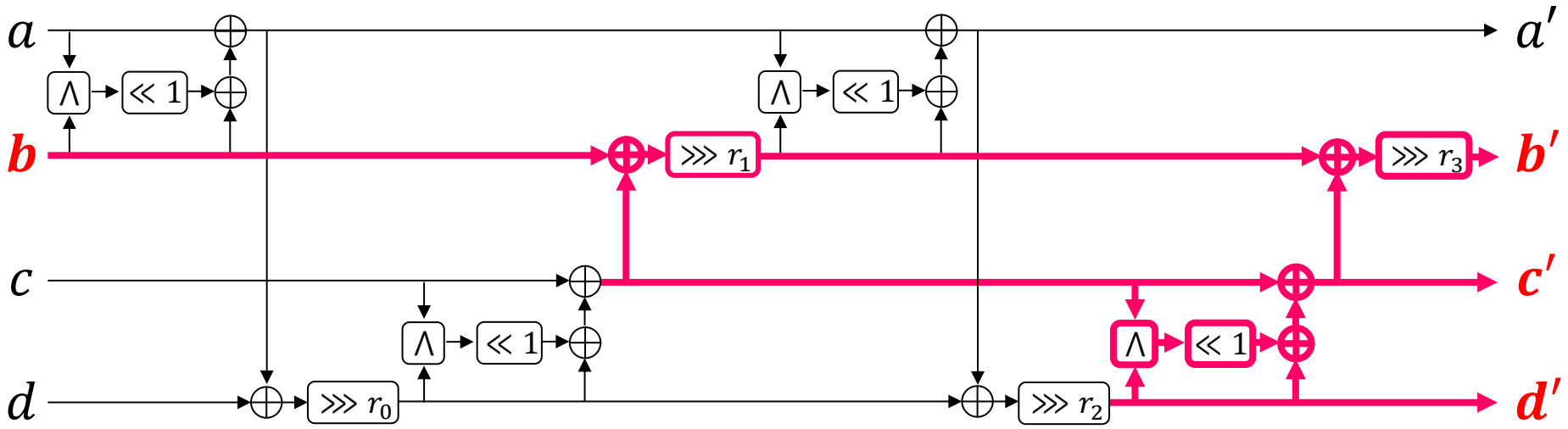
Inverting **G**



- Diffusion is weaker in backwards.
- **H**$^{-1}$ can be computed efficiently bit-by-bit.
- From given output, **G**$^{-1}$ can be computed efficiently.



Example: Elementary Property

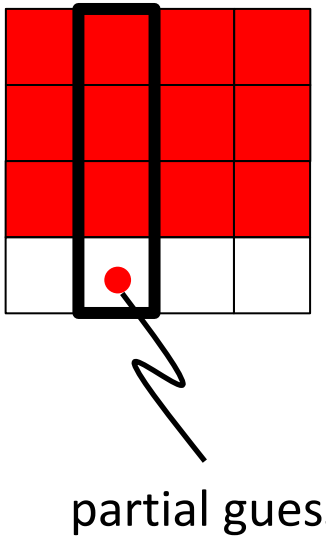


- b can be computed from given b', c', d' by G^{-1}
- c can be computed from given a', c', d' by G^{-1}

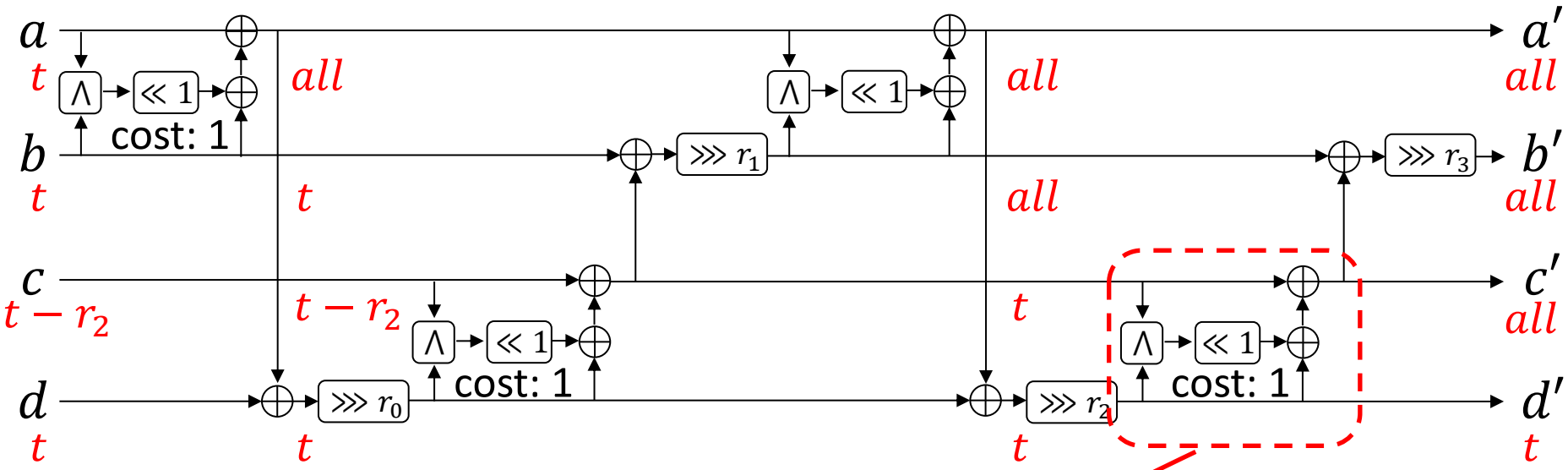
- Only those 2 properties from 3 known output words.
- Any other useful properties?

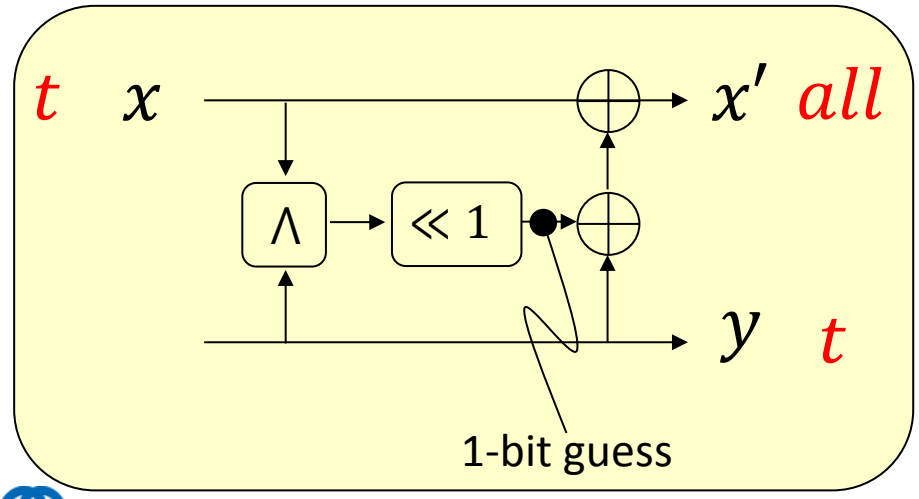
Property after Observing Key Stream

- From a key stream, in each column,
  - 3 words are known
  - 1 word is unknown
- Moreover, the attacker can guess some capacity bits of d'.
- Do analysis for any of one of a', b', c', d' is partially known and other 3 are fully known.



Inversion from Full a', b', c' and Partial d'





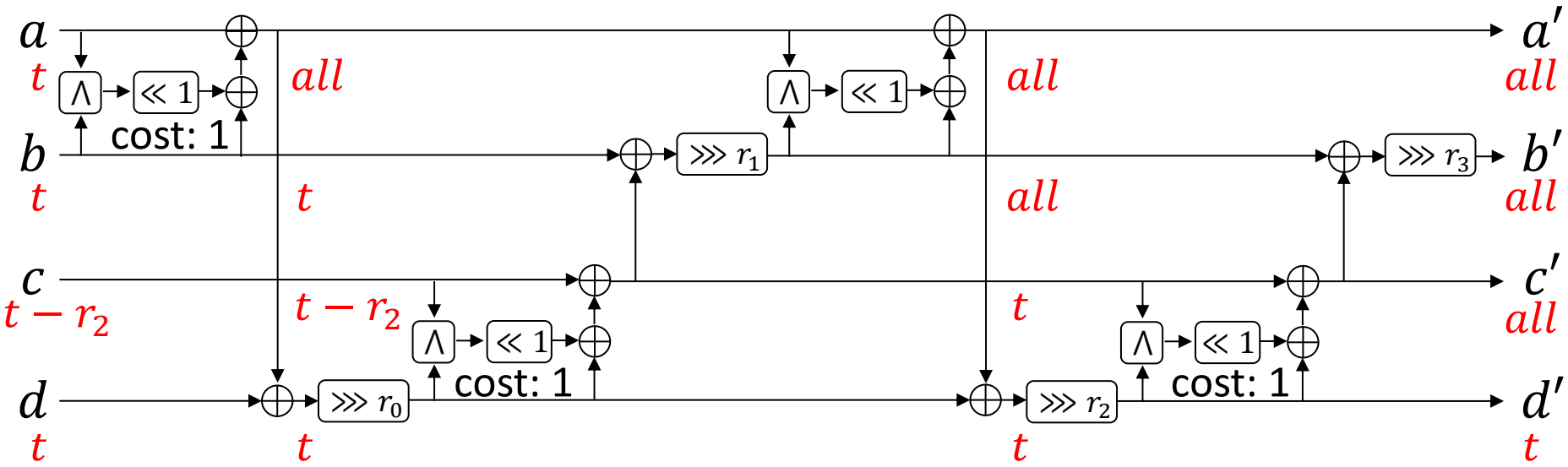
If t bits start from LSB:

t bits of x are computed without any guess.

Otherwise:

1-bit guess is required (cost 1)

Inversion from Full a', b', c' and Partial d'



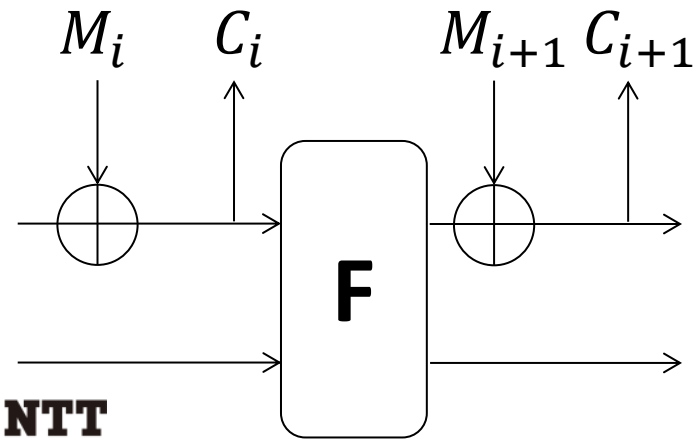
Property 4. Suppose that a', b', c' are fully known and t bits of d' are known. Then, t bits of a, t bits of b, $t - r_2$ bits of c, and t bits of d can be computed with a cost of 3-bit guess. Moreover, the guess is reduced to 1-bit when t consecutive bits of d' start from the LSB.

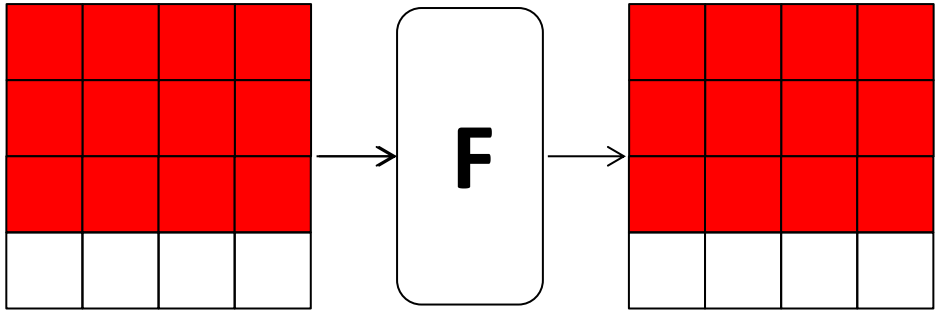
9 properties and extensions are shown in the paper.

Guess-and-Determine Attacks

Overview

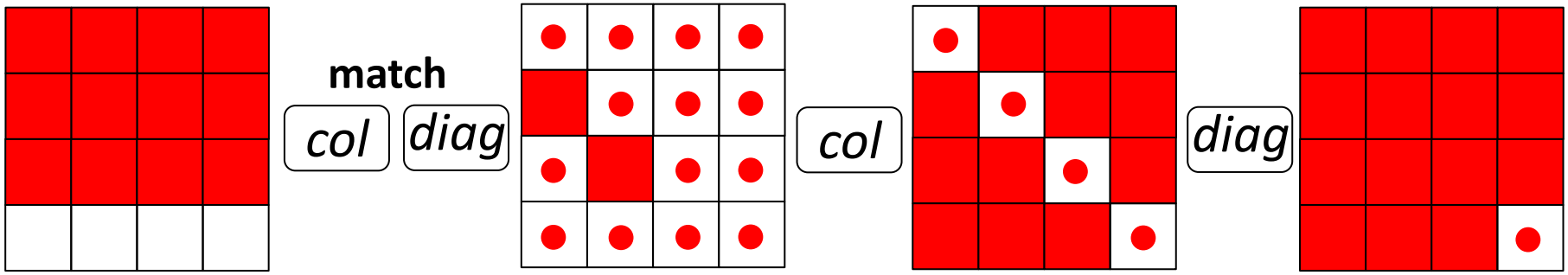
- It can work in both serial and parallel modes.
- Overall framework looks similar to guess-and-determine attack against FIDES [DJ15].
  - Observe key stream in two consecutive blocks
  - Guess unknown values
  - Matching the data through **F**





Guess and Determine

- Guess capacity values and propagate the knowledge in backwards for 1.5 rounds with Properties presented.
- Similarly propagate the input value in forwards for 0.5 rounds.
- No bits can be matched directly.



Tracing Linearity

- We trace the linearity of several bits.
- Each bit is classified into 3 categories
  - known(k), linearly represented (l), unknown(u)

Forward pattern			
lllllllllllllll	lllllllllllllll	lllllll11111111	lllllllllllllll
nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnln
nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnl
lllllllllllllll	lllllll11111111	lllllllllllllll	lllllllllllllll
Backward pattern			
nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnn1111111k	kkkkkkkkkkkkkkk
nnnnnnnnnnnnnnn	nnnnnnn1kkkkkkk	kkkkkkkkkkkkk111	lllllllllllllll
nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnn	nnnnnnnnnnnnnnl
nnnnnnnnnnnnnnn	nnnnnnn11111111	lllllllllllllll	lllllllllllllll

- We developed a tool for the match over linear relation.

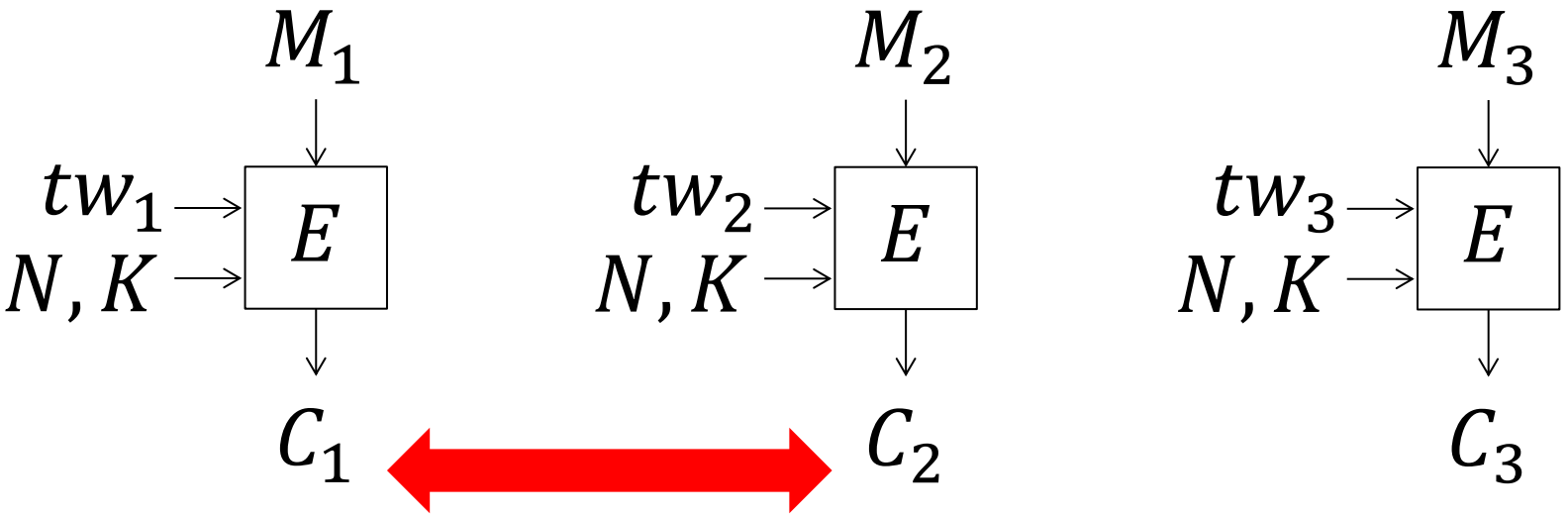
Innovative R&D by NTT

Internal Differential Attacks

- 2-round key recovery
- 2-round practical key stream distinguisher

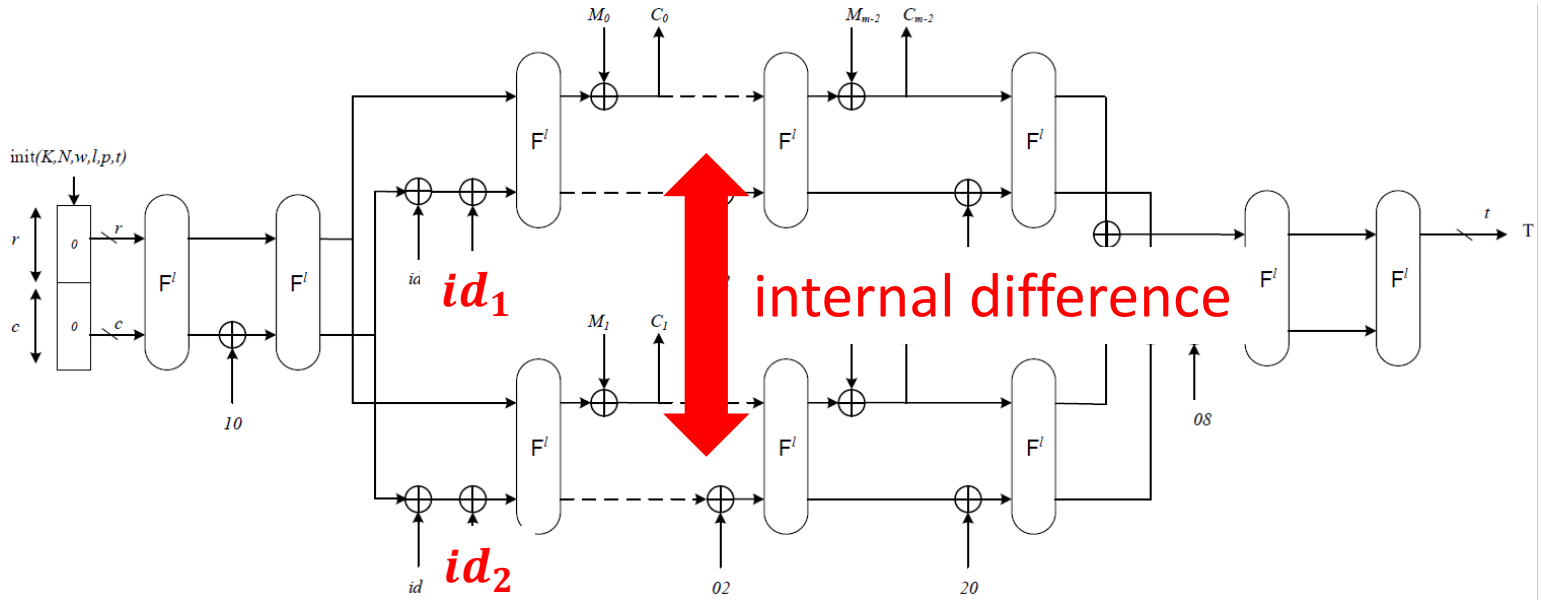
Differential Attack for Nonce-Respect

- Differential attack is generally hard to apply in nonce-respect.
- Jean-Sasaki-Wang exploited difference between two blocks in the analysis on Silver (fully parallelized tweakable BC based AE)



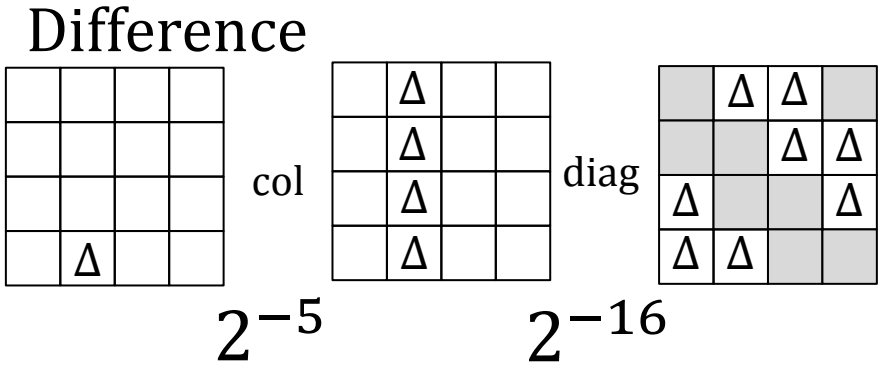
Differential Attack for Nonce-Respect

- Sponge is serial, no internal difference exists.
- NORX supports the parallel mode.
- Small Hamming weight of the lane id (counter) allows to consider difference between lanes.



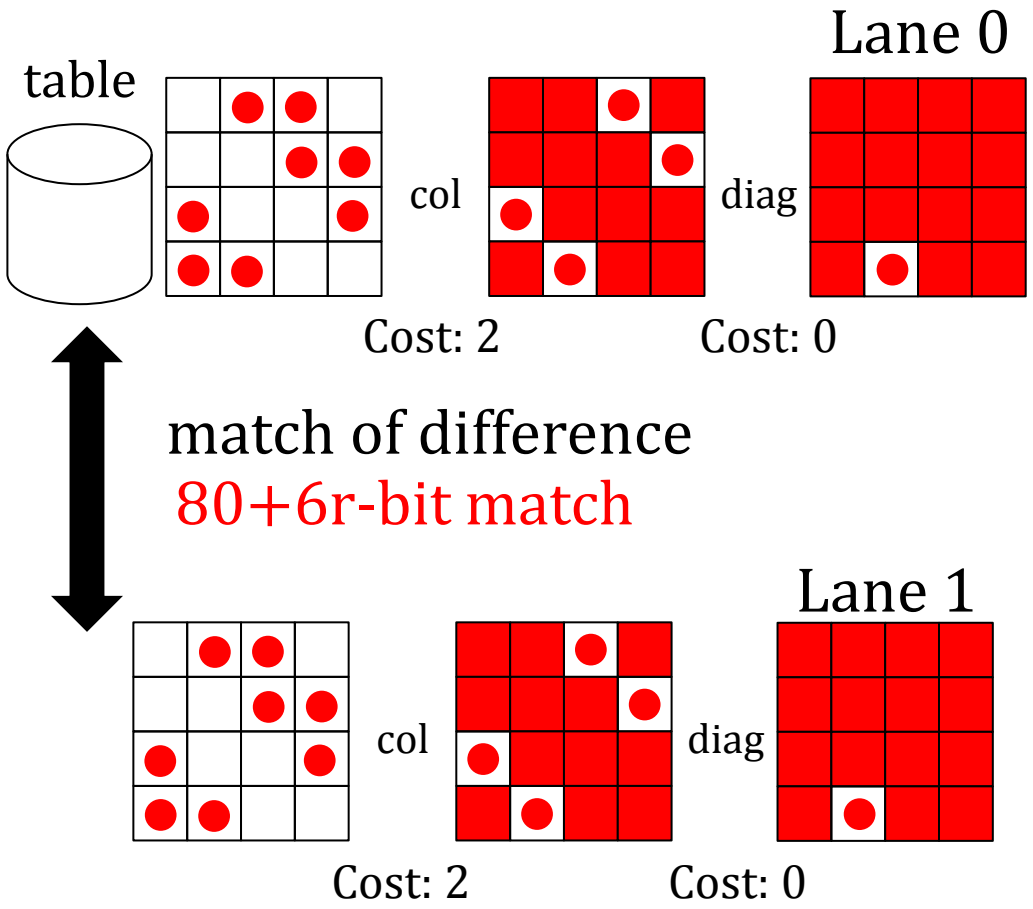
Internal Differential Propagation

- 1-round internal differential propagation
- 1-round backward computation for key recovery
- Lane IDs are injected to 2^{nd} column, 4^{th} row
- Experimentally found the best characteristic (and then differential) for 1R



1-Round Key Recovery

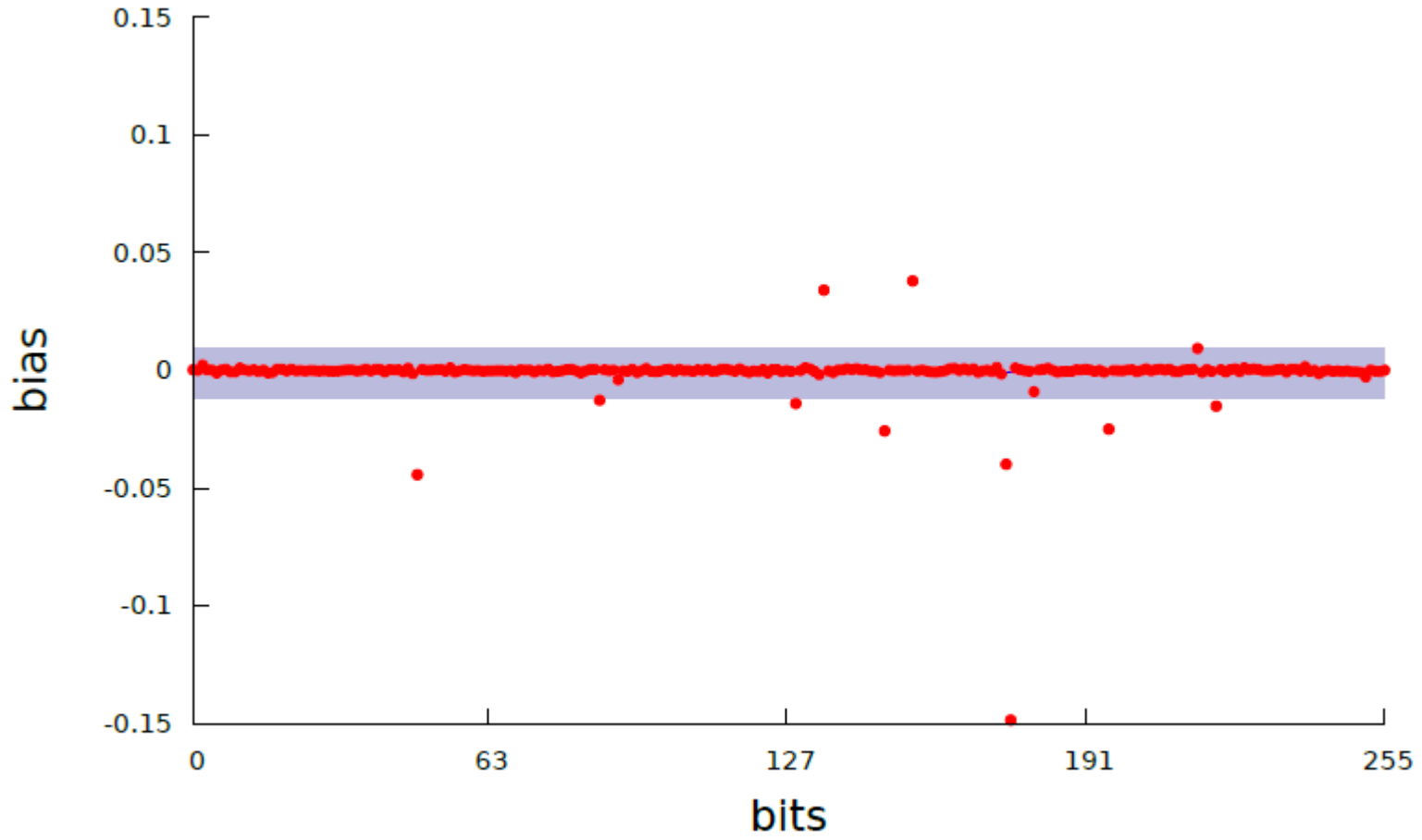
- Guess secret value (capacity) of 2 lanes.
- In classical DC, secret (key) is identical in two values in a pair.
- Here, capacity values are different in two lanes.
- We introduce MitM like matching procedure to make the complexity low.



Internal Differential Linear

- Internal differential version of differential-linear attacks
- For the fixed difference, some bits do (or do not) have difference more likely than other bits.
- We verified bias of output difference experimentally instead of theoretically building differential-linear characteristic.

Bias in the Key Stream after 2+α Rounds



Success Prob. is 97.7% by observing 90 message blocks.

Concluding Remarks

- We studied meaningful security notions of reduced NORX in the nonce-respect setting.
- Parallel mode is not exactly the same as serial mode. Further investigation seems useful.

Approach	Goal	Target	Rounds	Data	Time	Memory
Guess and determine	KR	NORX64	2/4	3	2^{234}	negl.
Guess and determine	KR	NORX32	2/4	3	2^{119}	negl.
Internal difference	KR	NORX64	2/4	74	$2^{232.8}$	2^{225}
Internal difference	KR	NORX32	2/4	158	$2^{124.3}$	2^{115}
Internal differential-linear	KD	NORX64	2/4	90	negl.	negl.

Thank You Four Your Attention !!

NTT