KU LEUVEN

Cosic

Fault Analysis of the ChaCha and Salsa Families of Stream Ciphers

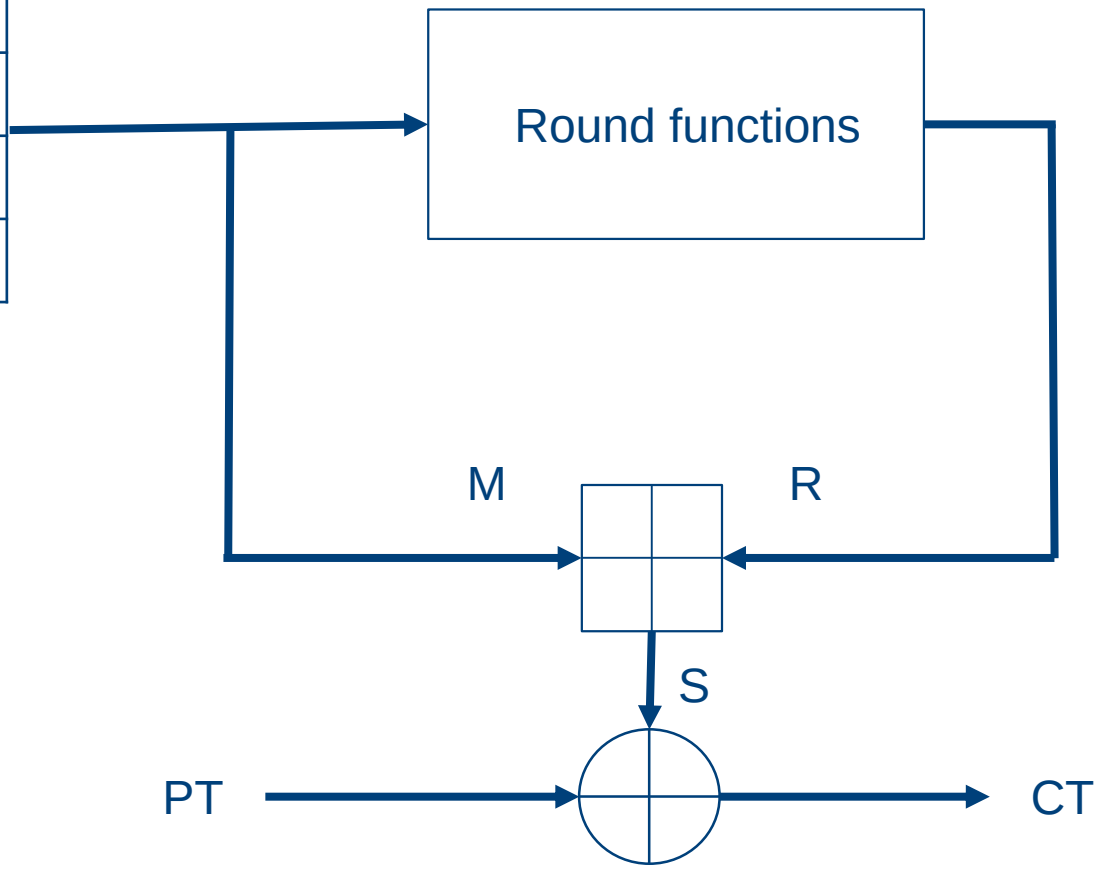
Arthur Beckers, Benedikt Gierlichs, Ingrid Verbauwhede

CARDIS 2017

ChaCha/Salsa stream cipher

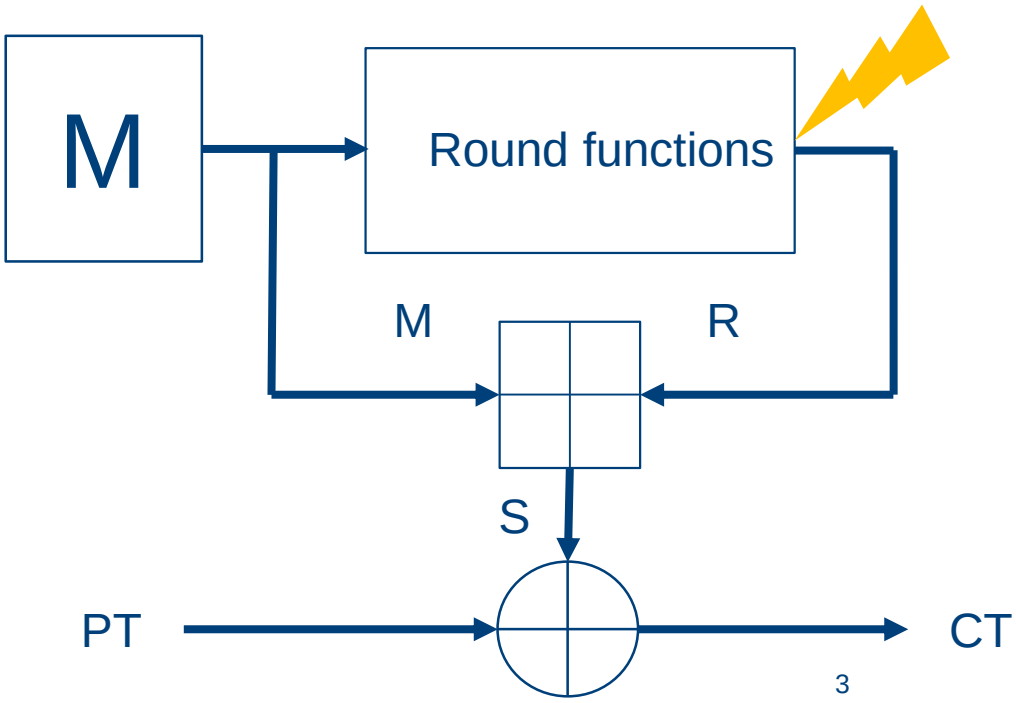
State matrix

C	C	C	C
K_1	K_2	K_3	K_4
K_5	K_6	K_7	K_8
CNT	CNT	N	N

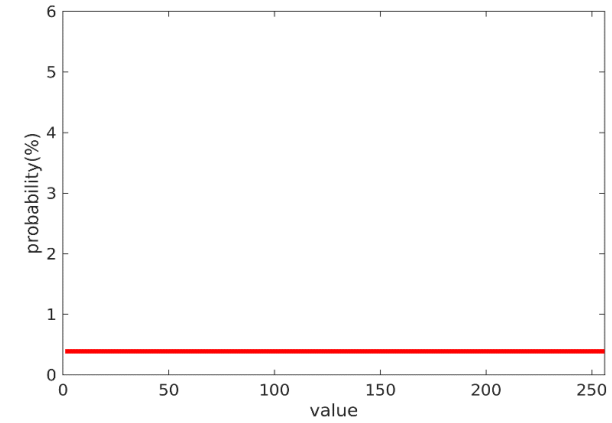


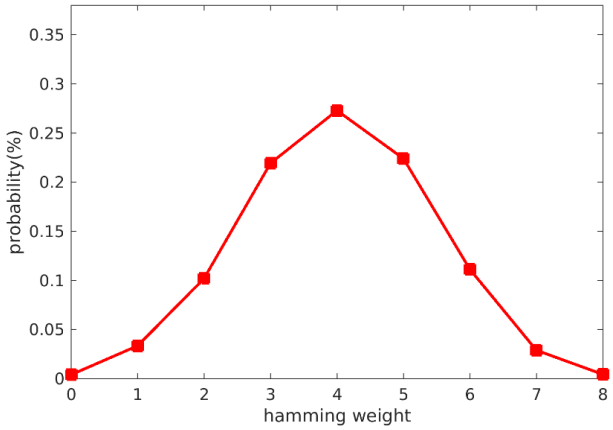
General attack structure

- Attack output of the round functions
- Injected faults influence the distribution of R
- Attacker can observe either:
  - S (known plaintext (PT) – ciphertext (CT))
  - CT with a constant but unknown PT



Distribution of R, S, CT



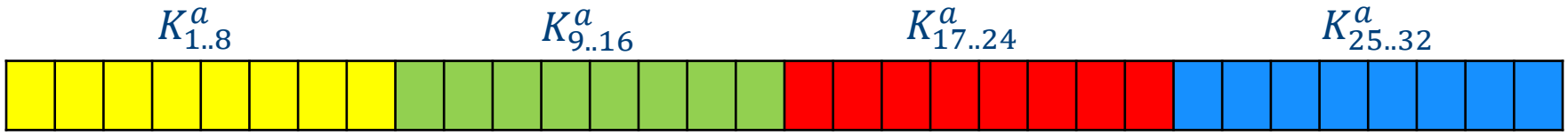


KU LEUVEN

General attack structure

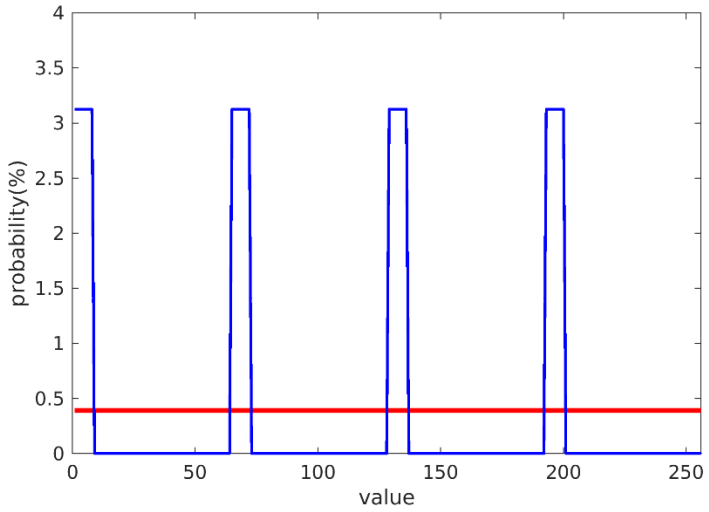
- Two fault models:
  - Stuck-at fault model
  - Biased fault model
- Verification of the attacks is done in simulation

- Splitting up R:

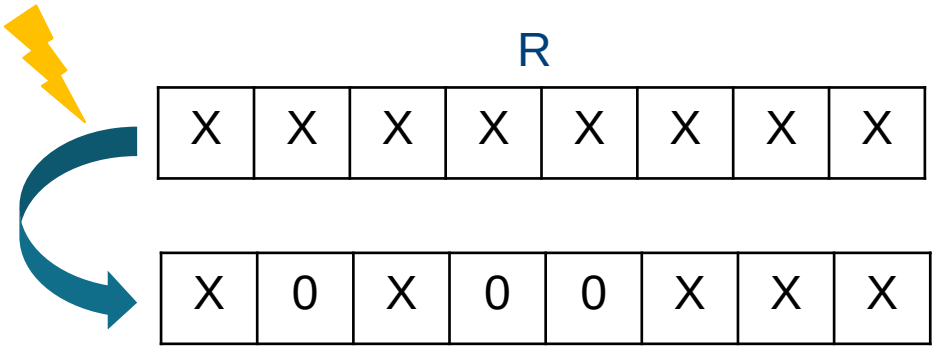


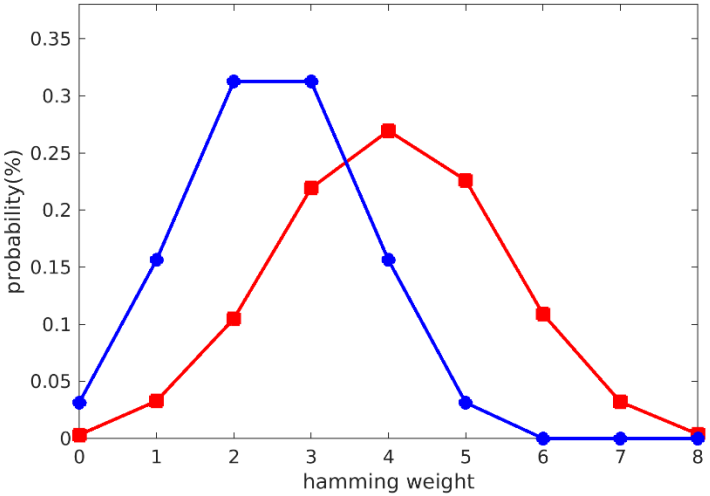
Stuck at fault model

- Some bits of R set to fixed 0 or 1
- Stuck bits location is constant



Example: 3 bits out of 8 stuck at 0



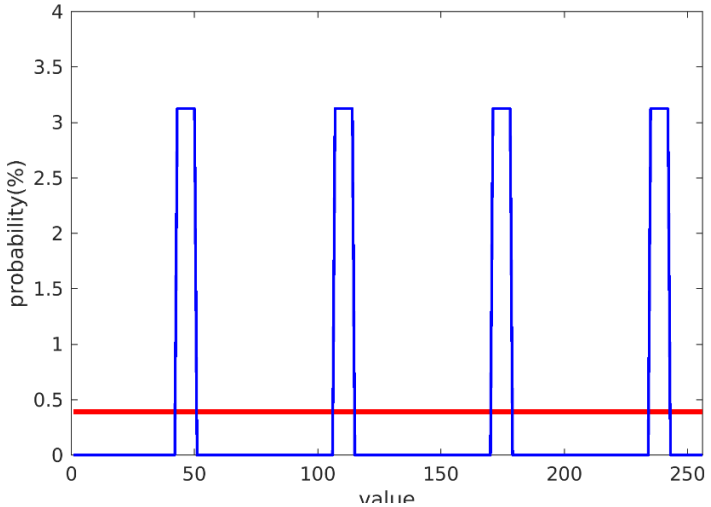


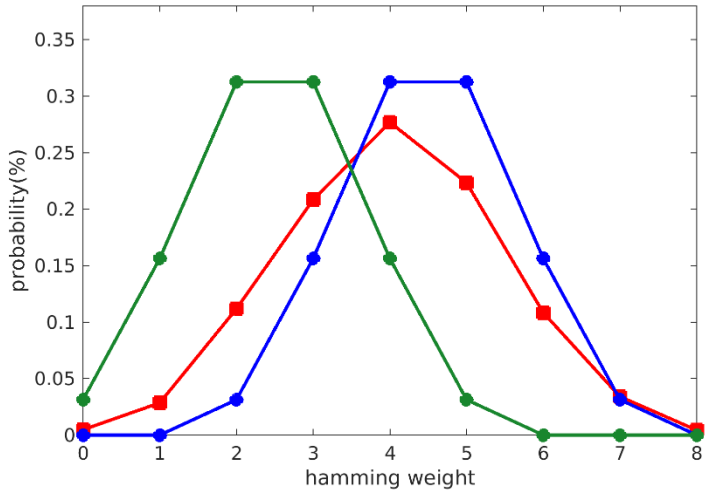
Stuck at exploitation

- At position S: $R' = R \boxplus M \boxminus M'$
- At position CT: $R' = R \boxplus M \oplus PT \oplus PT' \boxminus M'$

- The keyspace reduction criteria are deterministic:
  - Check the Hammingweight distribution
  - Check the stuck positions on bit level

After Key guess





Example: 2 out of 4 bits stuck

Ex. 1

1	0	0	0
1	1	0	0
0	1	0	0
0	0	0	0

Ex. 2

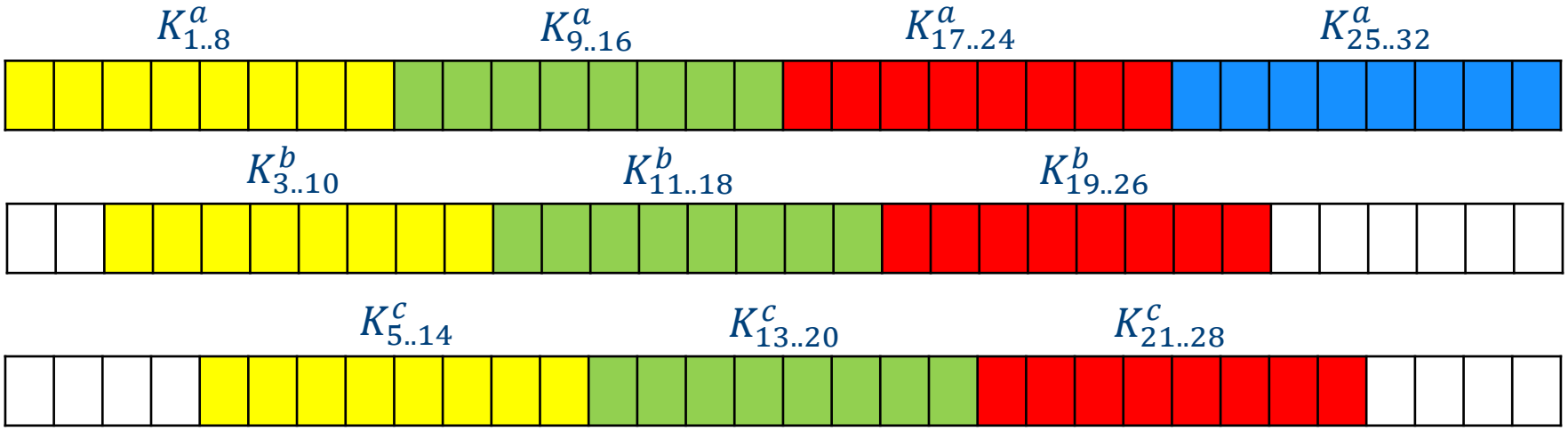
0	1	0	1
0	1	1	0
0	1	0	0
1	1	0	0

Ex. 3

1	0	1	1
0	1	1	0
0	0	0	1
0	1	0	0

KU LEUVEN

Stuck at exploitation

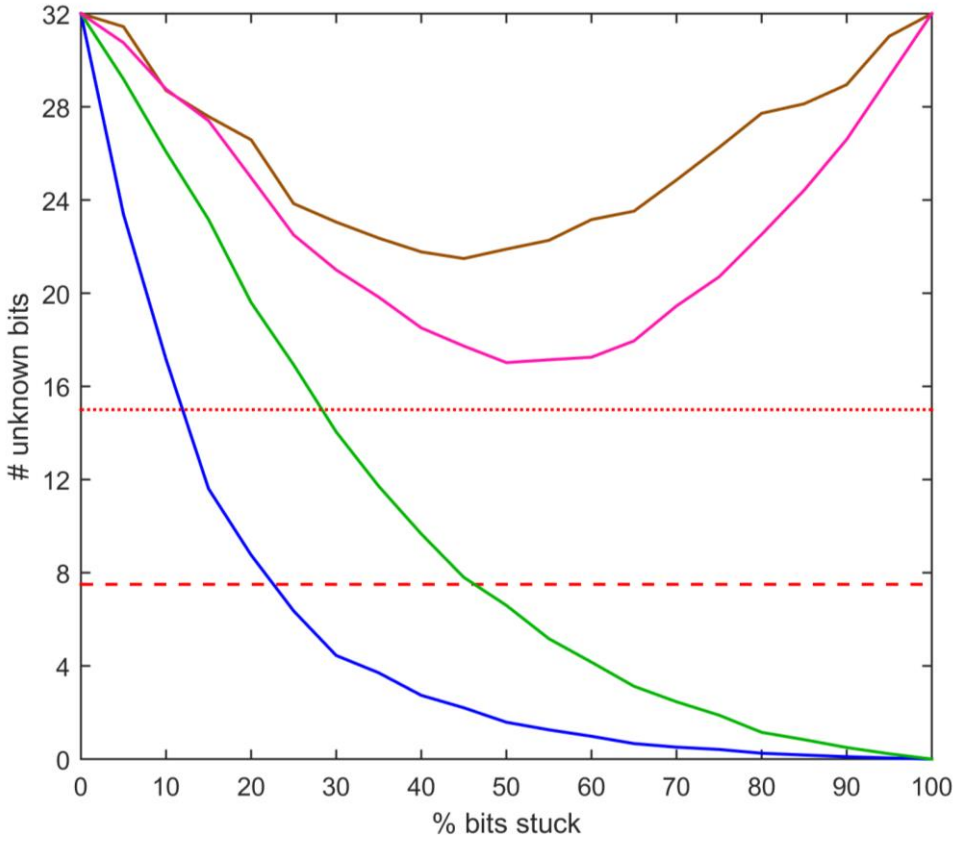


Keyspace reduction: calculate the intersection of K^a, K^b, K^c

Number of faults needed (99,9% sure to fill the bins)

# non-stuck bits	1	2	3	4	5	6	7
# faults	11	29	67	149	326	702	1500

Results stuck at attack



S

S (with key reduction)

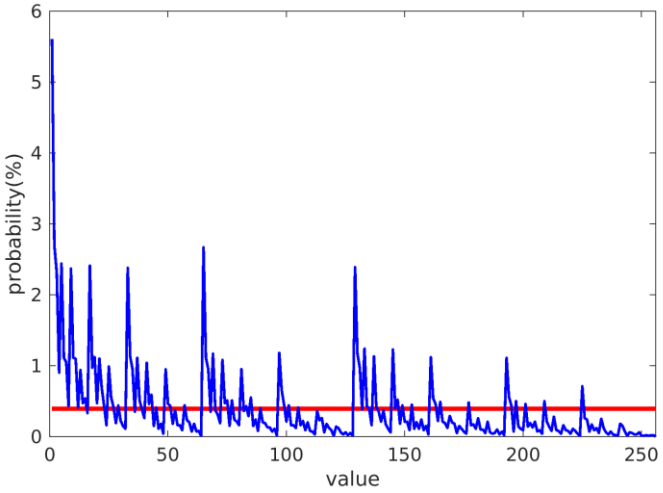
CT

CT (with key reduction)

KU LEUVEN

Biased fault model

- Bias introduced at bit level
- Bias is constant, but unknown
- HW of $R_{faulted}$ is still a binomial distribution

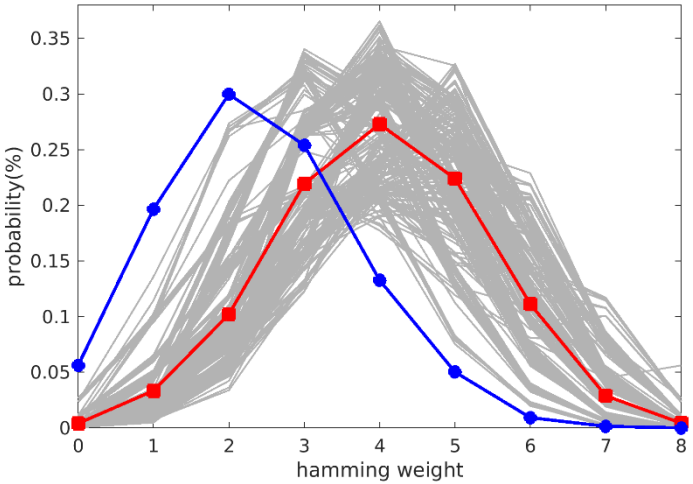


- P(X=0) = P(X=1) = 0.5

R

0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5

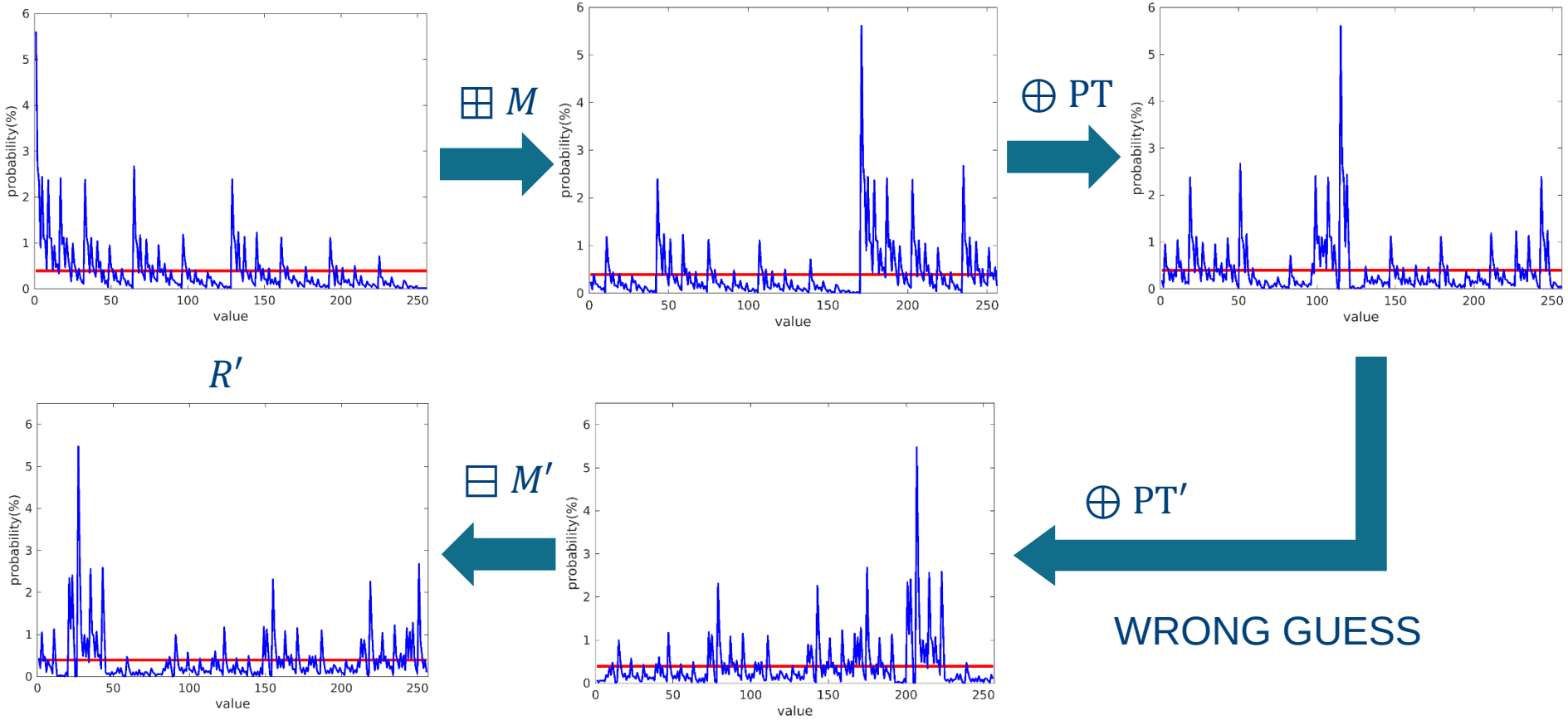
0.7	0.7	0.7	0.7	0.7	0.7	0.7	0.7



KU LEUVEN

Impact modular addition/ XOR

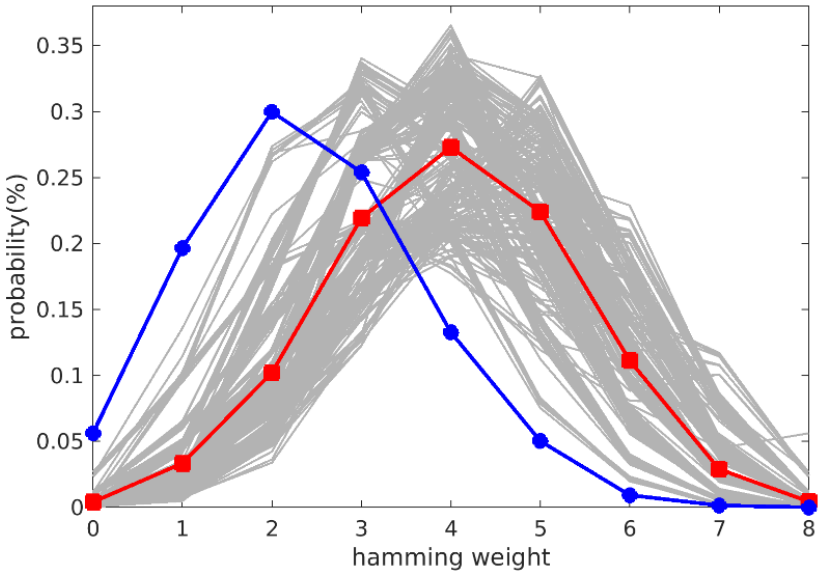
$$R' = R \boxplus M \oplus PT \oplus PT' \boxminus M'$$



KU LEUVEN

Distinguishers

- Requirement: work on unknown amount of bias
- SEI = $\sum_{i=0}^{N} \left[\frac{\#\left((HW_j)_{j=1}^{n} = i \right)}{n} - \Pr(i, N, 0.5) \right]^2$
- T-test = $\left| \frac{\mu - \bar{x}}{\sqrt{\frac{\sigma^2 + s^2}{n}}} \right|$
- T-test gives better results



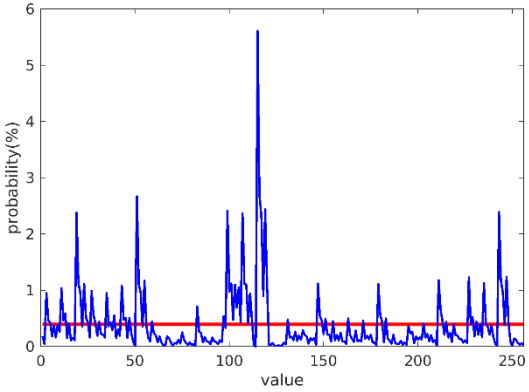
KU LEUVEN

False positives due to XOR

$$R' = R \boxplus M \oplus PT \oplus PT' \boxminus M'$$

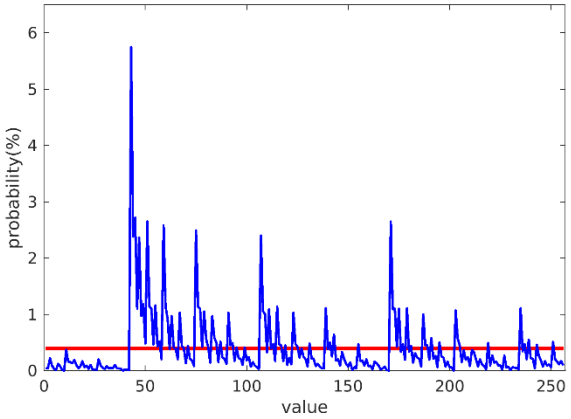
$PT \oplus PT' = 0$

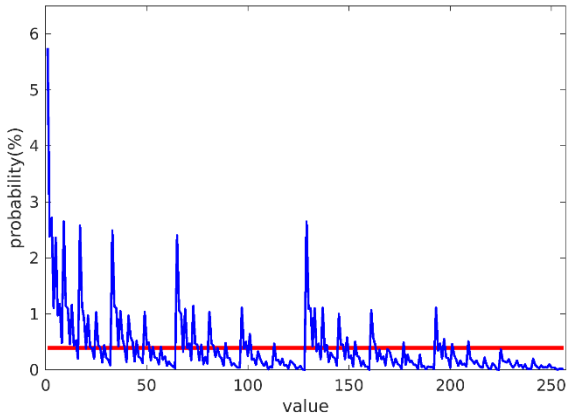
$PT \oplus PT' = 2^n/2$

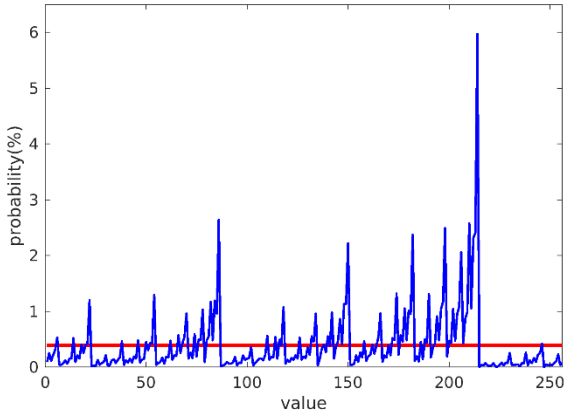


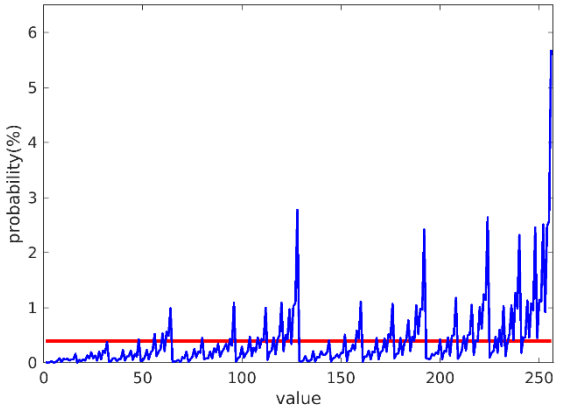
$PT \oplus PT' = 2^n/2\text{-}1$

$PT \oplus PT' = 2^n$



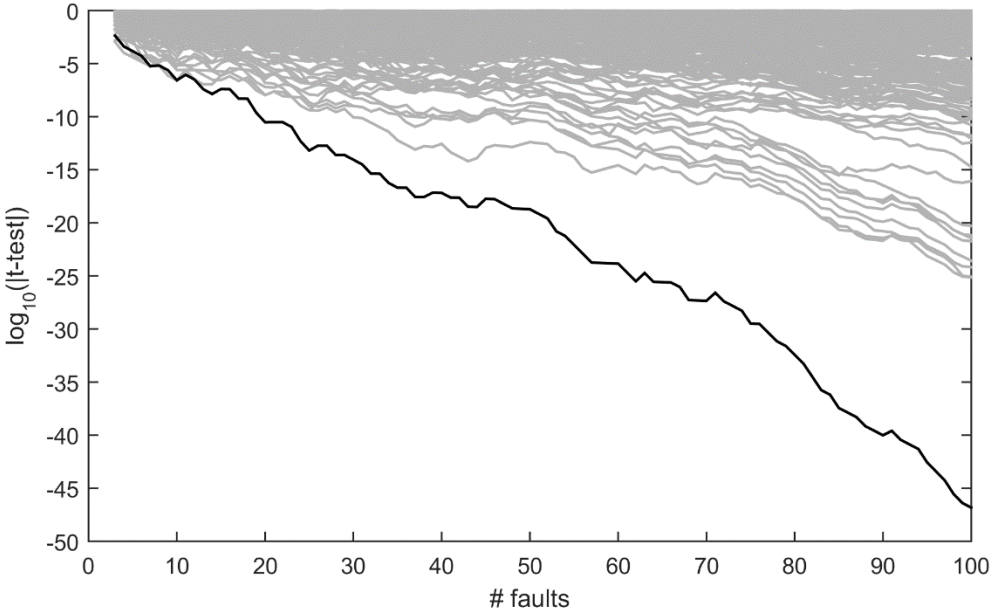




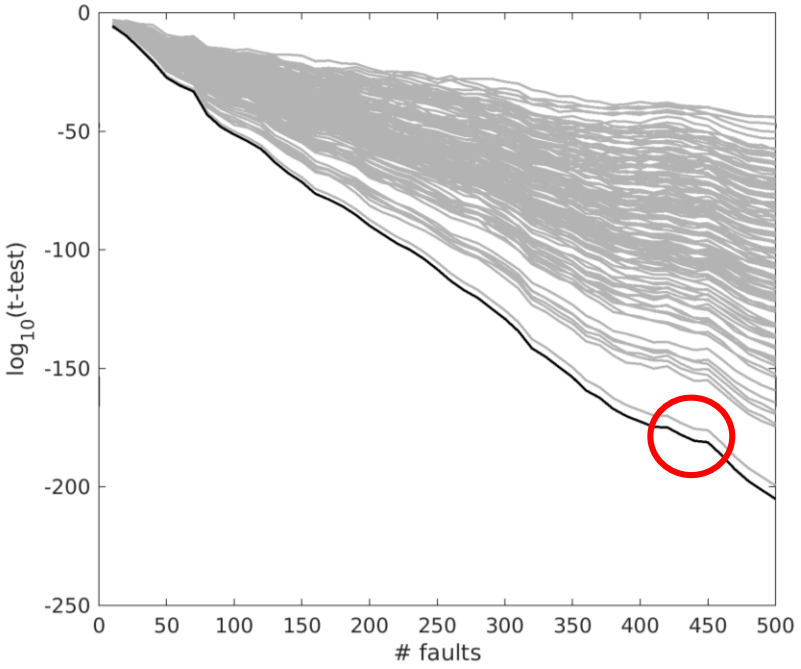


Results biased fault models

At position S



At position CT



BIAS	50%	55%	60%	65%	70%	75%	80%	85%	90%	95%	100%
#faults: S	/	400	115	50	27	11	7	5	5	5	/
#faults: CT	/	1356	420	158	100	77	65	63	78	134	/

Summary

- Presented two fault attacks on ChaCha structure
  - Attacking S position feasible both biased and stuck at fault model
  - Attacking CT position only feasible with biased fault model

- When designing countermeasures against fault attacks you might want to check the distribution of R

Questions?