

Improved Differential Fault Analysis on CLEFIA

Junko Takahashi and Toshinori Fukunaga
NTT Information Sharing Platform Laboratories, JAPAN

FDTC 2008 Washington DC, USA
August 10

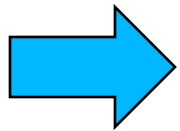


Outline

- Background
- Previous Study
 - Structure of CLEFIA
 - General DFA Method
 - Chen's Attack
- Proposed Attack
 - Attack Method
 - Simulation Results
- Conclusions

Background

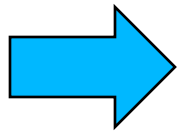
- CLEFIA - 128-bit block cipher developed by SONY Corporation in 2007.
 - Small implementation size and high speed utilizing characteristic structure
- Differential fault analysis (DFA) on CLEFIA was first proposed by Chen et al. in 2007.
 - Simply applied attack against DES to CLEFIA
 - 18 pairs needed to obtain 128-bit key



Can we develop more efficient attack using characteristic of CLEFIA structure ?

Background

- CLEFIA - 128-bit block cipher developed by SONY Corporation in 2007.
 - Small implementation size and high speed utilizing characteristic structure
- Differential fault analysis (DFA) on CLEFIA was first proposed by Chen et al. in 2007.
 - Simply applied attack against DES to CLEFIA
 - 18 pairs needed to obtain 128-bit key



Yes, we can !!



Result

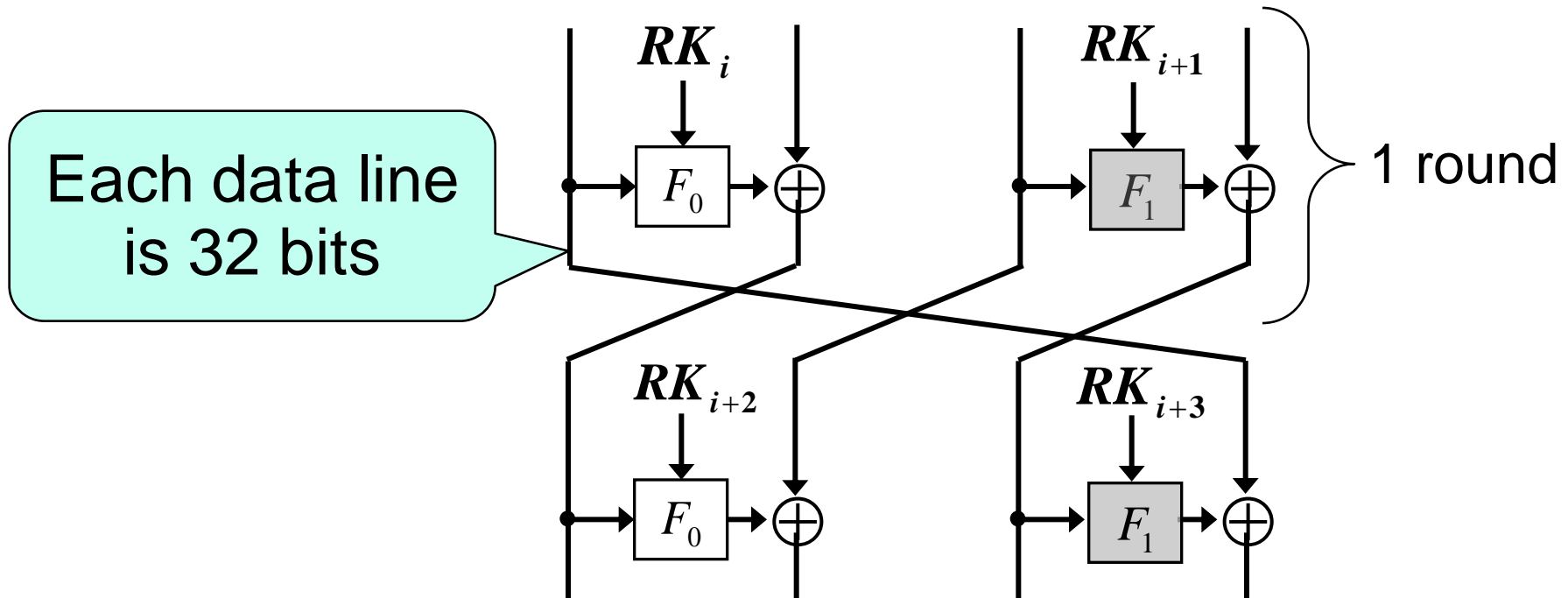
Comparison of attack efficiency for 128-bit key

	No. of pairs of correct & faulty ciphertexts	No. of fault injection points	Calculation time on Xeon 3GHz PC
Proposed attack	2	2	average 3 min
Chen's attack (in 2007)	18	6	< 1 sec

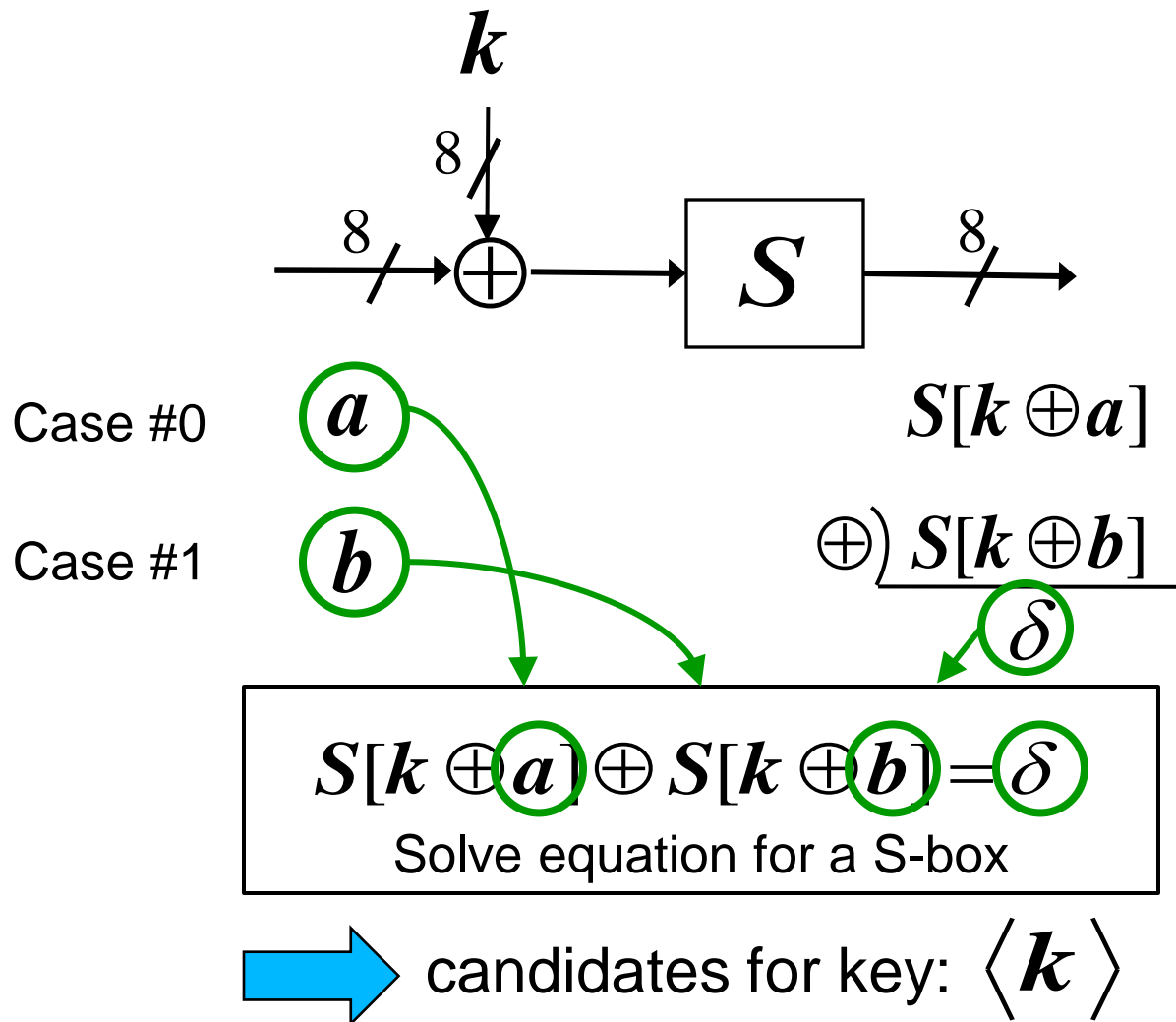
- Background
- Previous Study
 - Structure of CLEFIA
 - General DFA Method
 - Chen's Attack
- Proposed Attack
 - Attack Method
 - Simulation Results
- Conclusions

Structure of CLEFIA

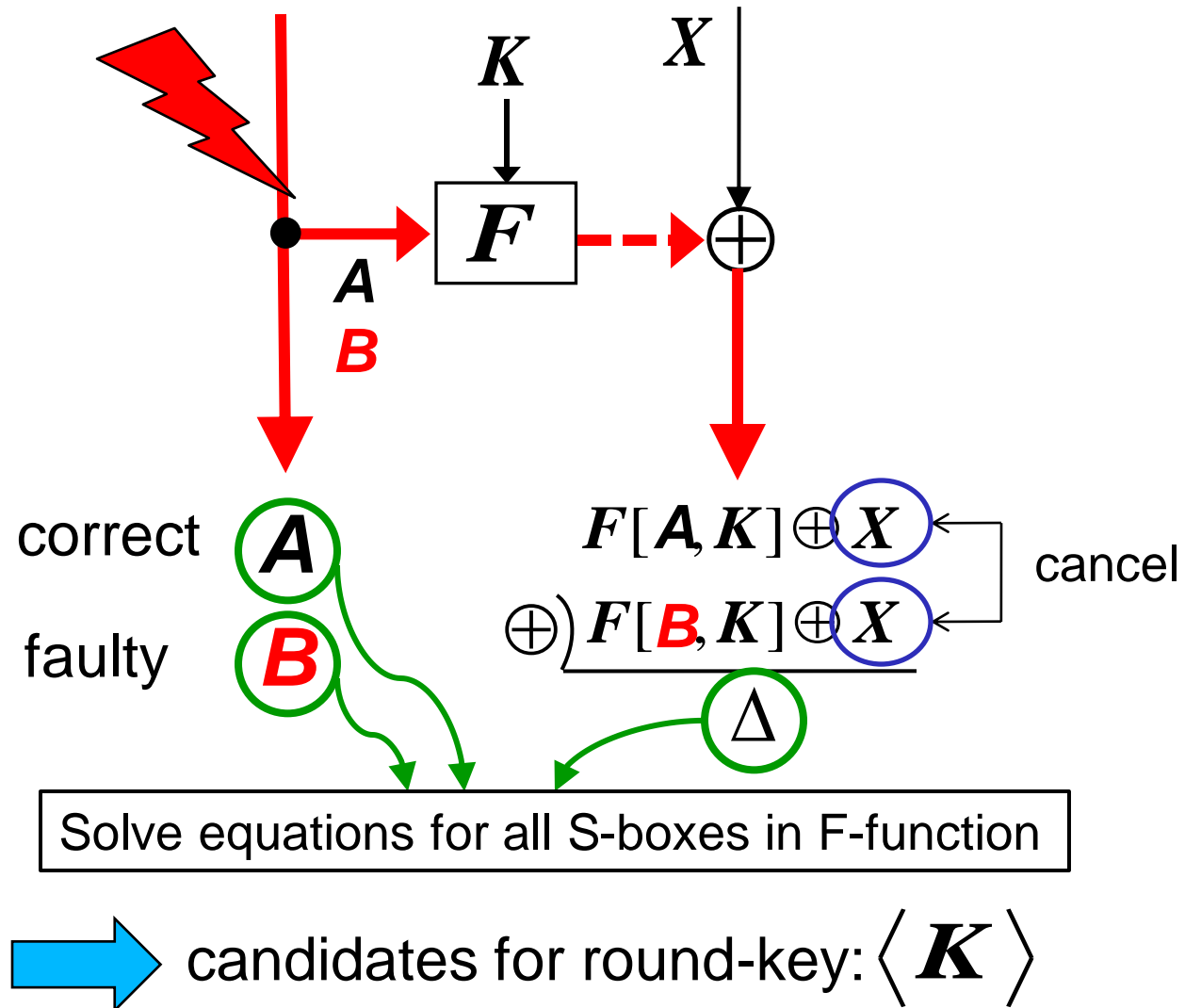
- 4-branch generalized Feistel network
- 18 rounds for 128-bit key



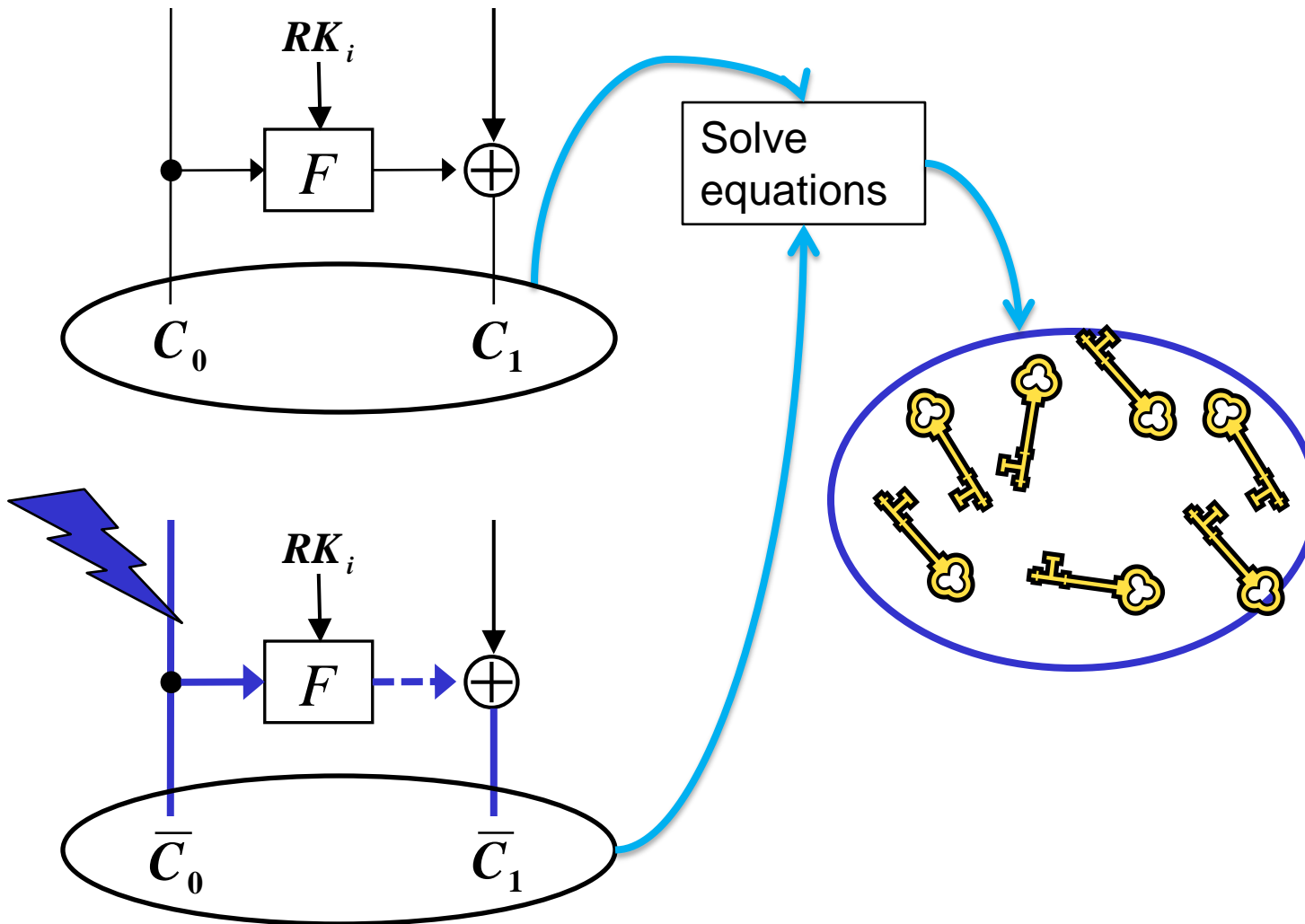
General DFA on a S-box



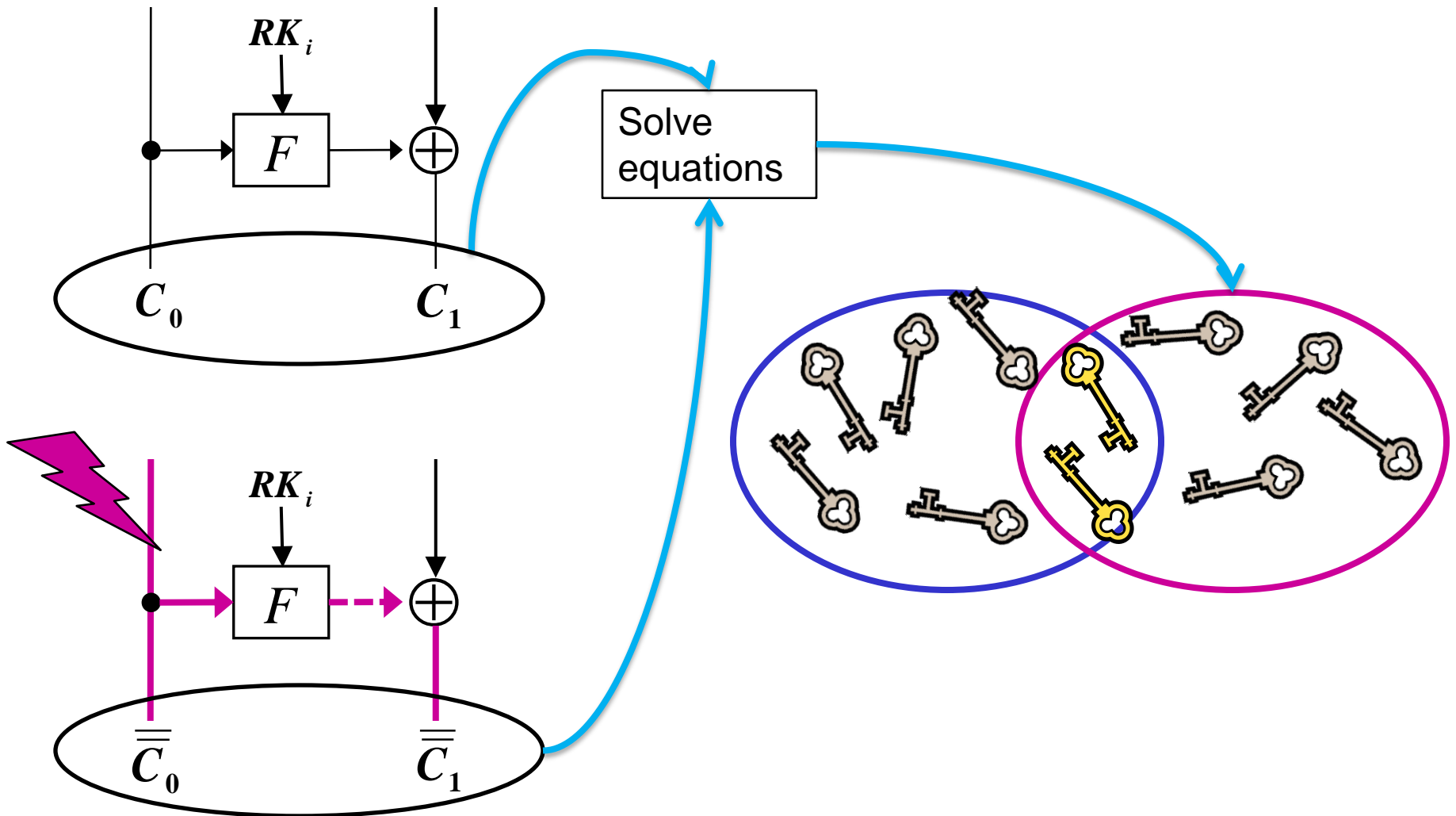
General DFA on Feistel Structure



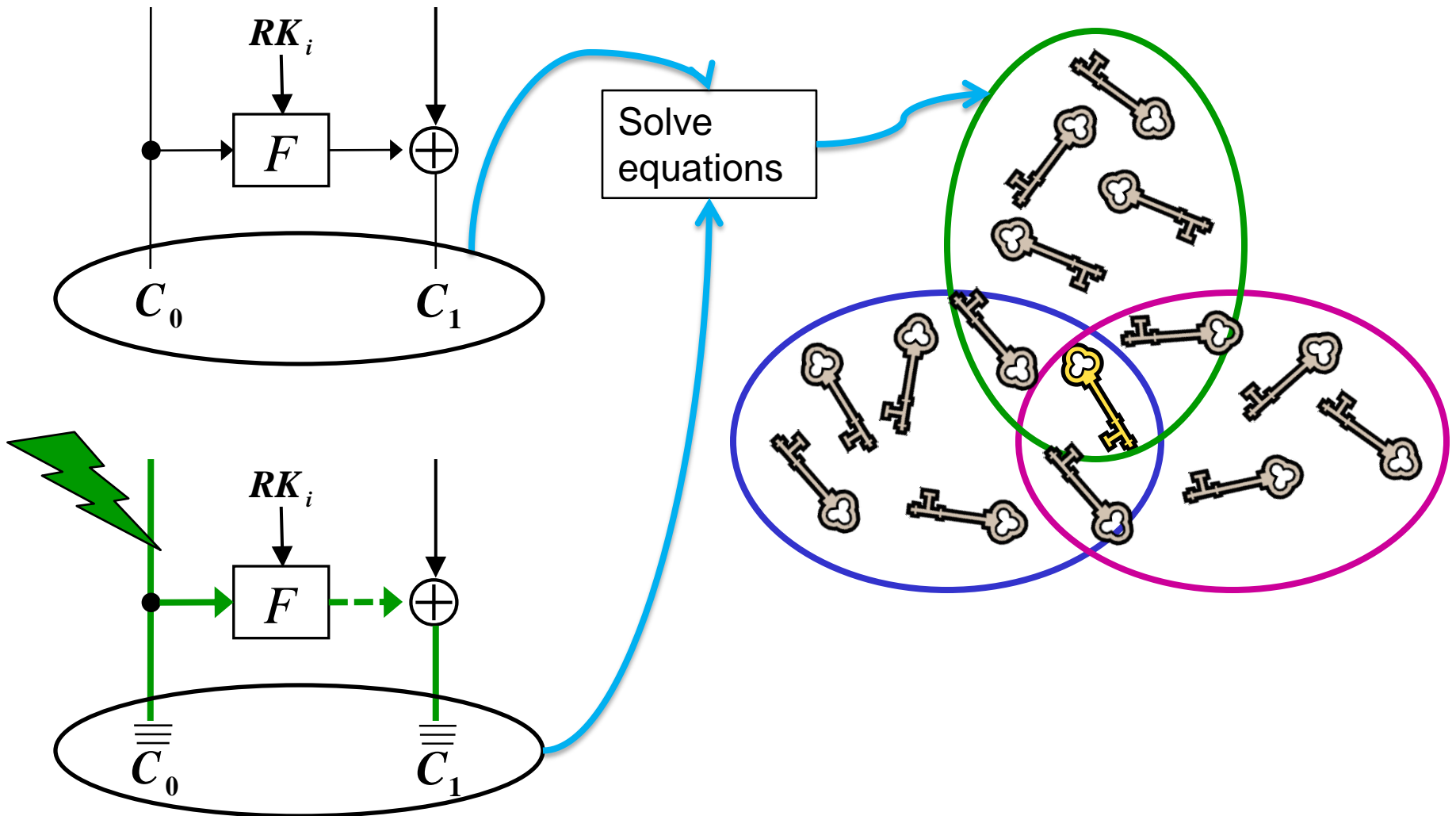
Chen's Attack (2007)



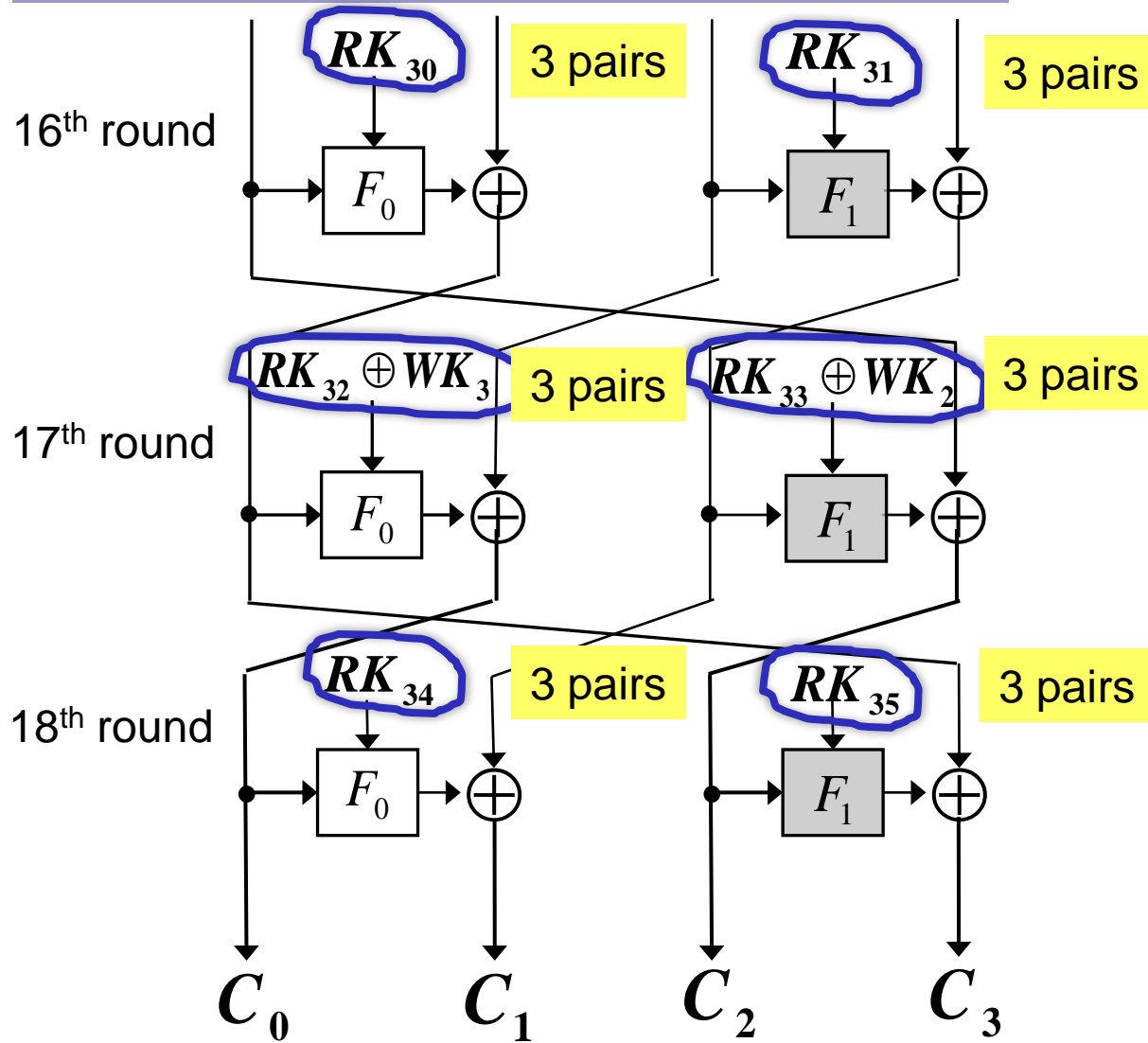
Chen's Attack (2007)



Chen's Attack (2007)



Chen's Attack (2007)



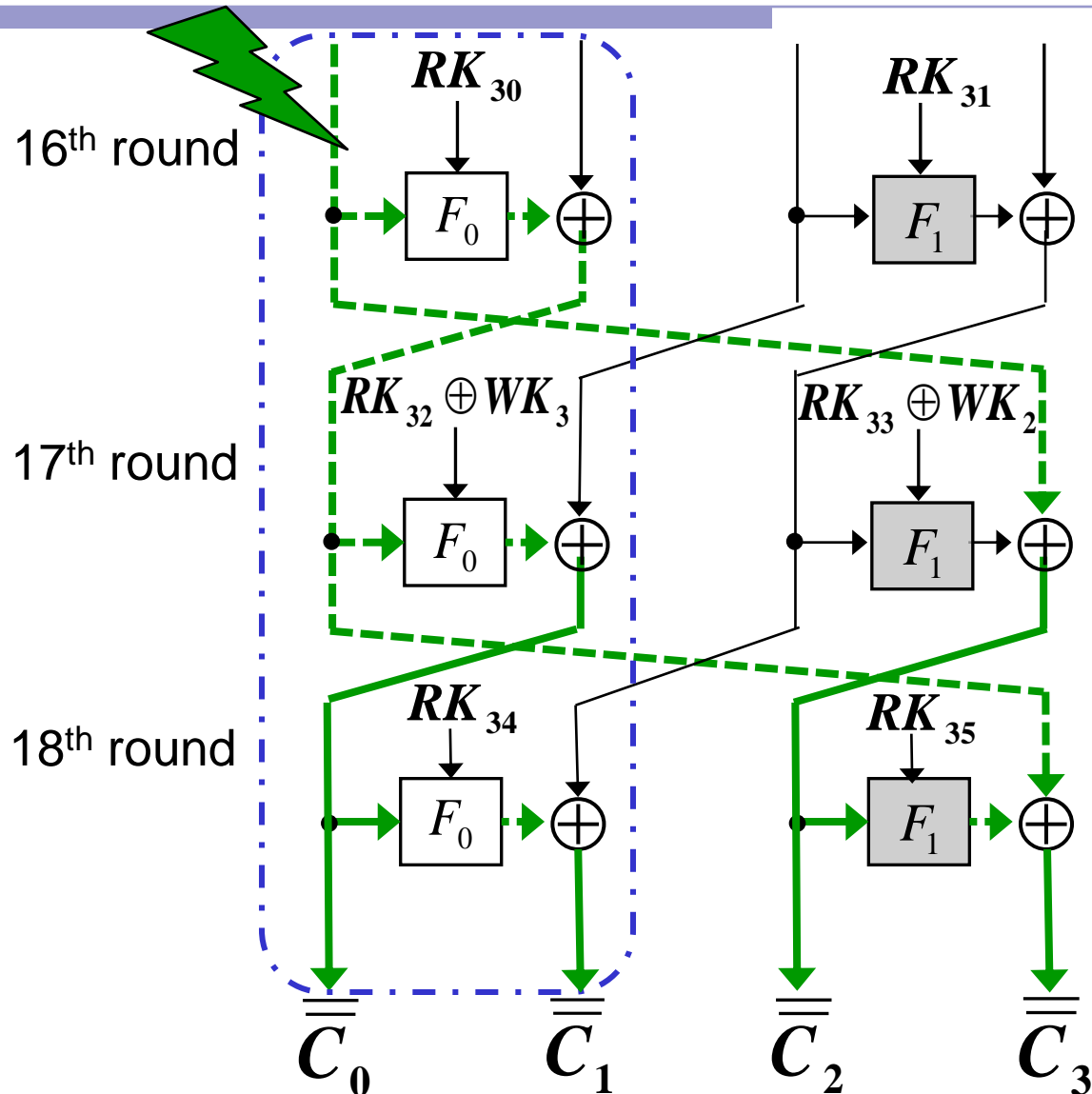
A total of
18 pairs
are needed

- Background
- Previous Study
 - Structure of CLEFIA
 - General DFA Method
 - Chen's Attack
- **Proposed Attack**
 - Attack Method
 - Simulation Results
- Conclusions

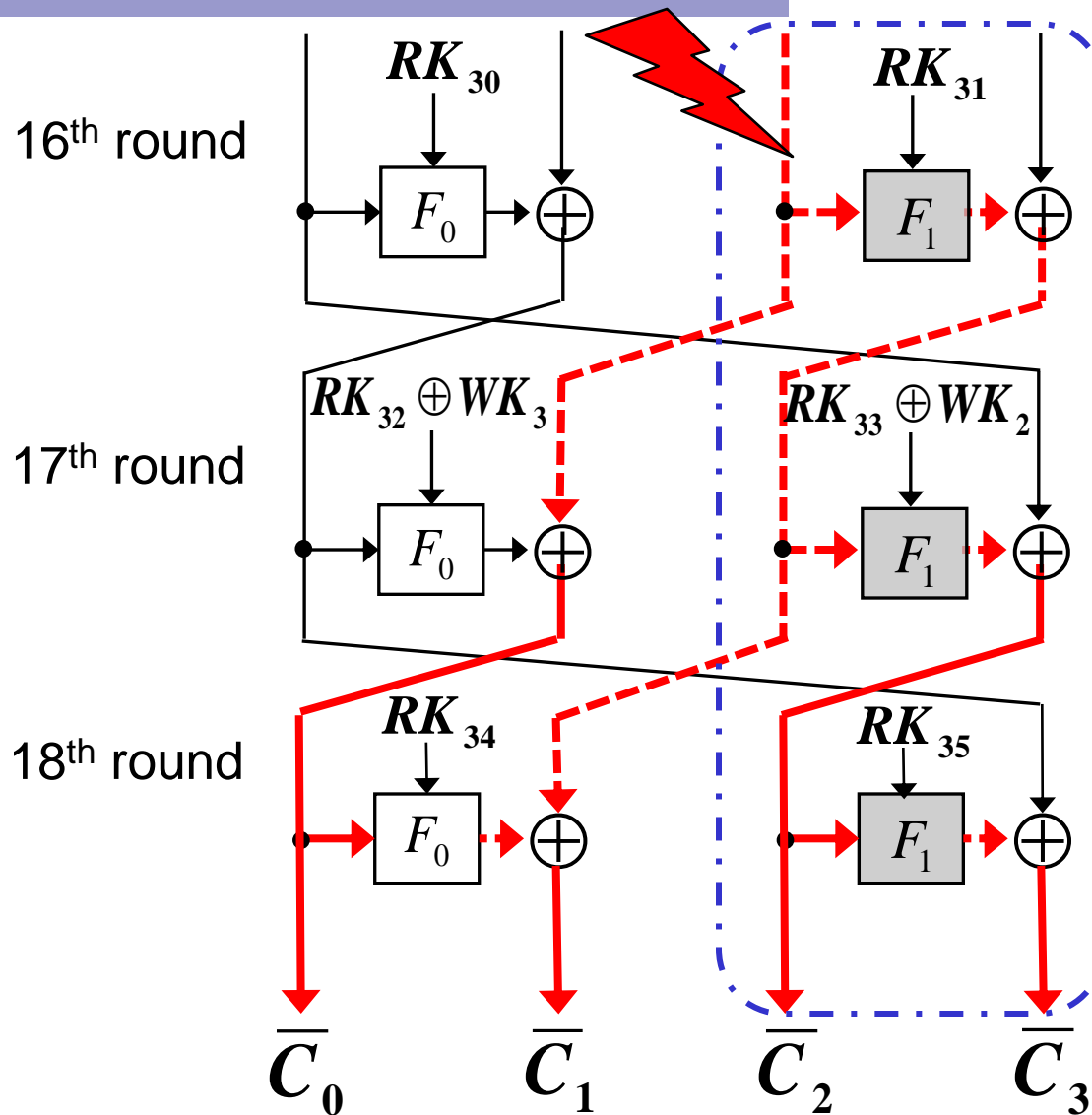
Key Point of Proposed Attack

- Utilize 4-branch structure with 32-bit data lines
 - We can obtain 6 round keys by utilizing the fault propagation of two fault injections.
 - The space of candidates for round key is small and we can obtain a 128-bit key within a practical time.

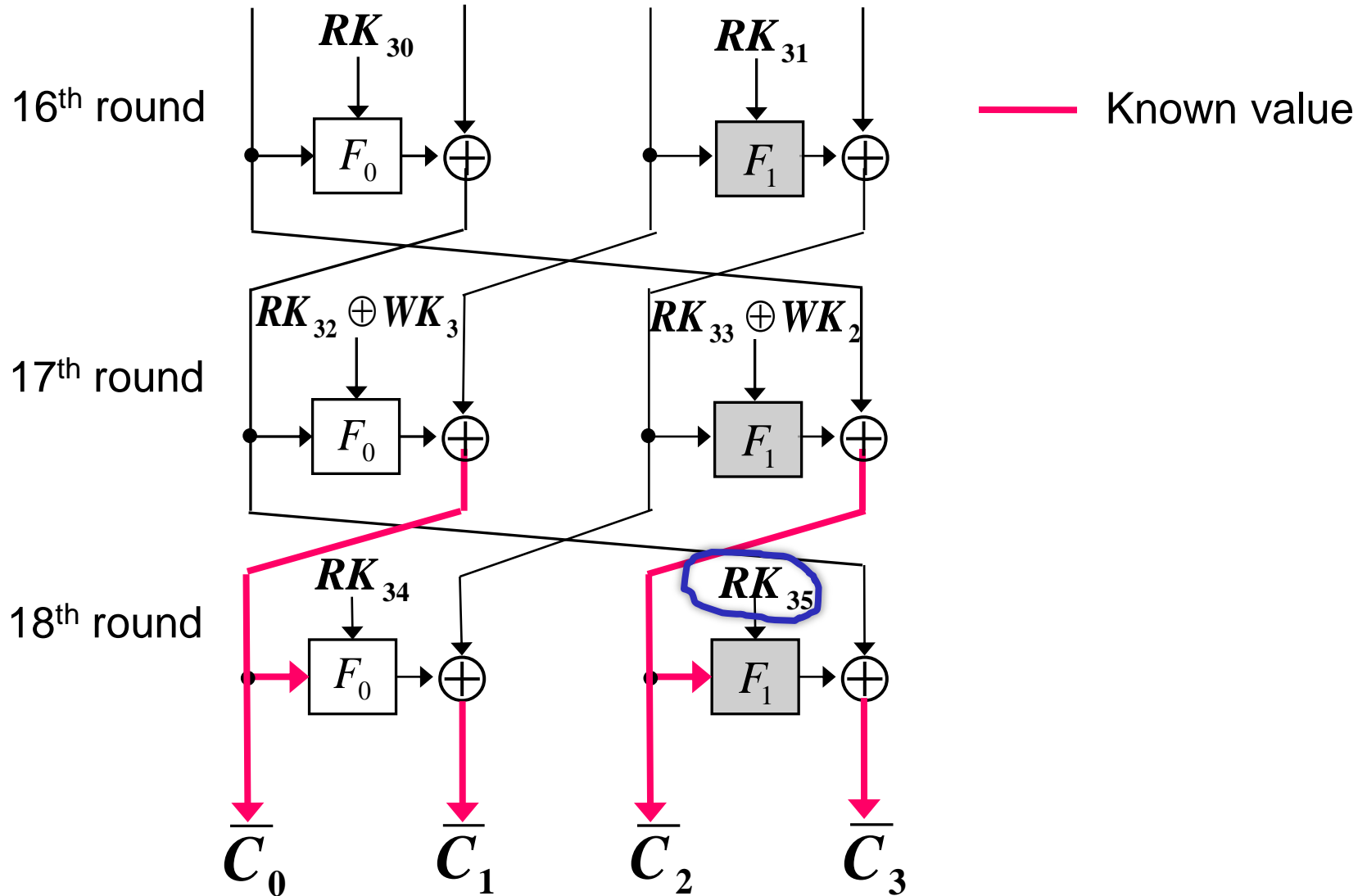
Fault Propagation



Fault Propagation

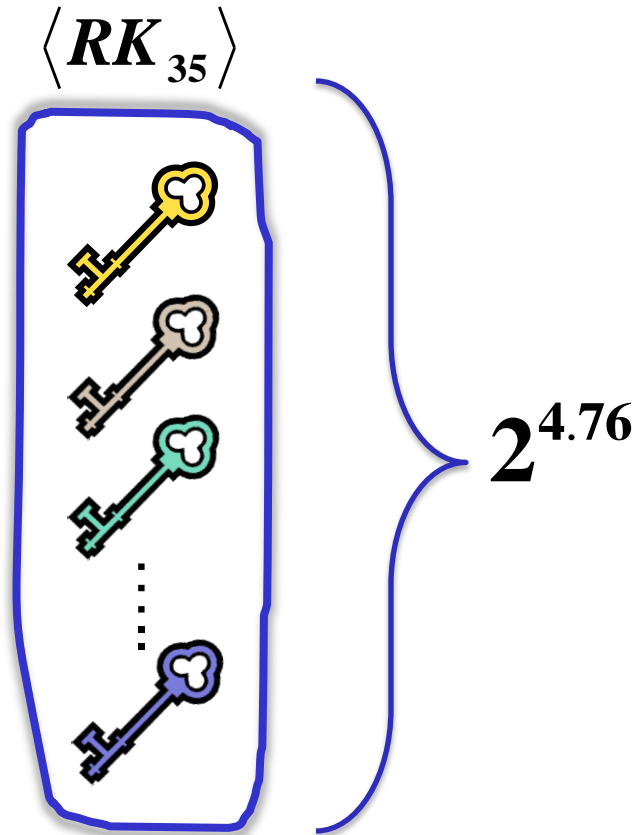


Step1: Obtain $\langle RK_{35} \rangle$



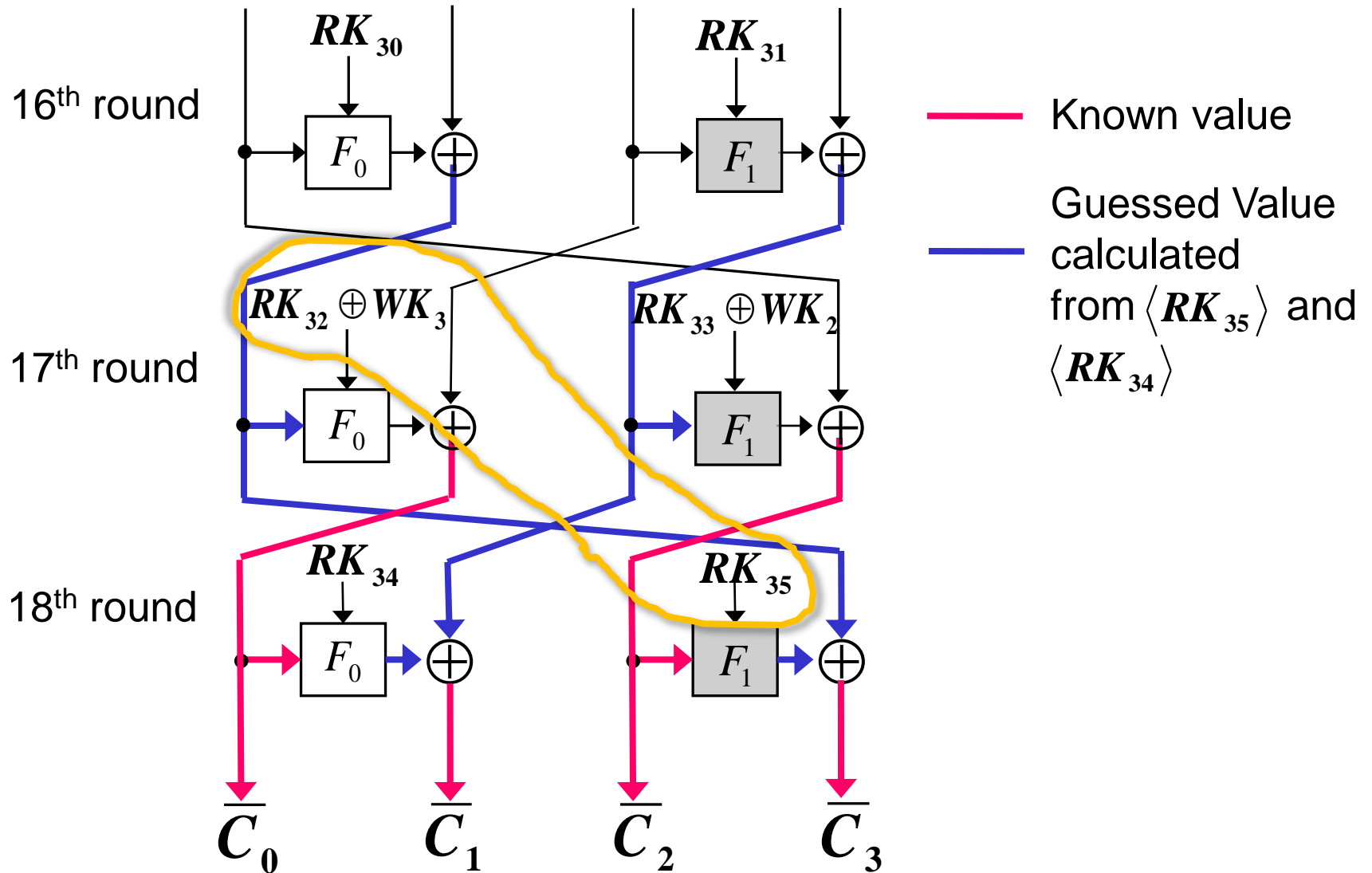
Step1: Obtain $\langle RK_{35} \rangle$ (2)

- Average space of candidate for RK_{35} is $2^{4.76}$



- Also obtain candidates for RK_{34}

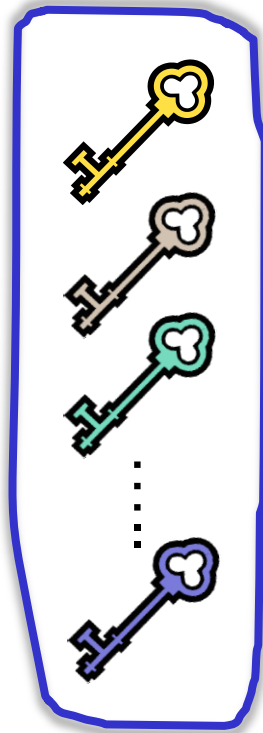
Step2: Obtain $\langle RK_{35}, RK_{32} \oplus WK_3 \rangle$



Step2: Obtain $\langle RK_{35}, RK_{32} \oplus WK_3 \rangle$ (2)

- Solve equation using candidates for RK_{35}

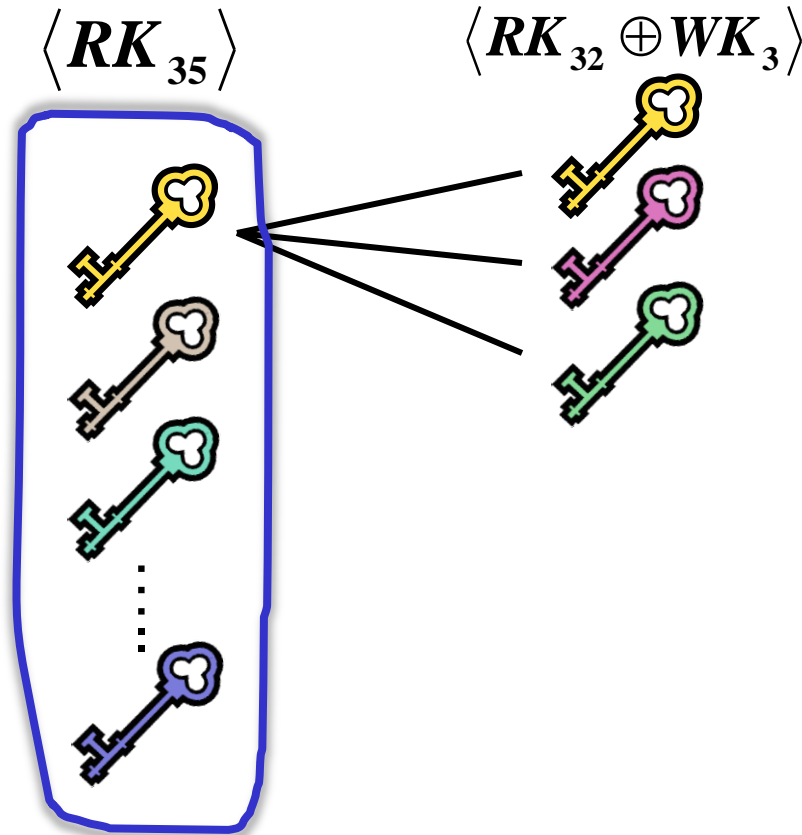
$\langle RK_{35} \rangle$



$\langle RK_{32} \oplus WK_3 \rangle$

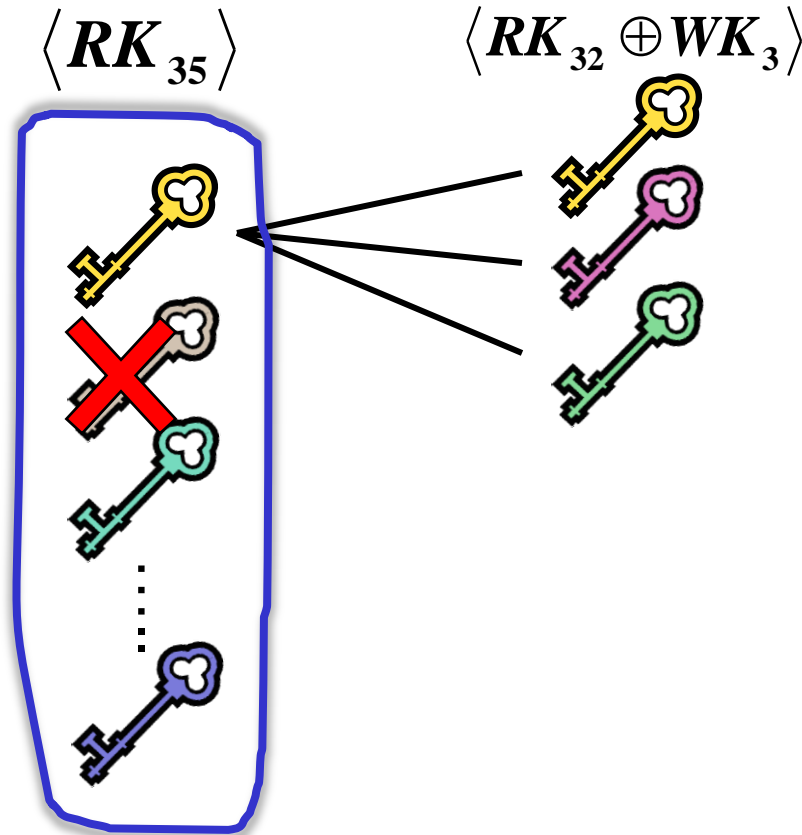
Step2: Obtain $\langle RK_{35}, RK_{32} \oplus WK_3 \rangle$ (2)

- Obtain candidates for combination ($RK_{35}, RK_{32} \oplus WK_3$)



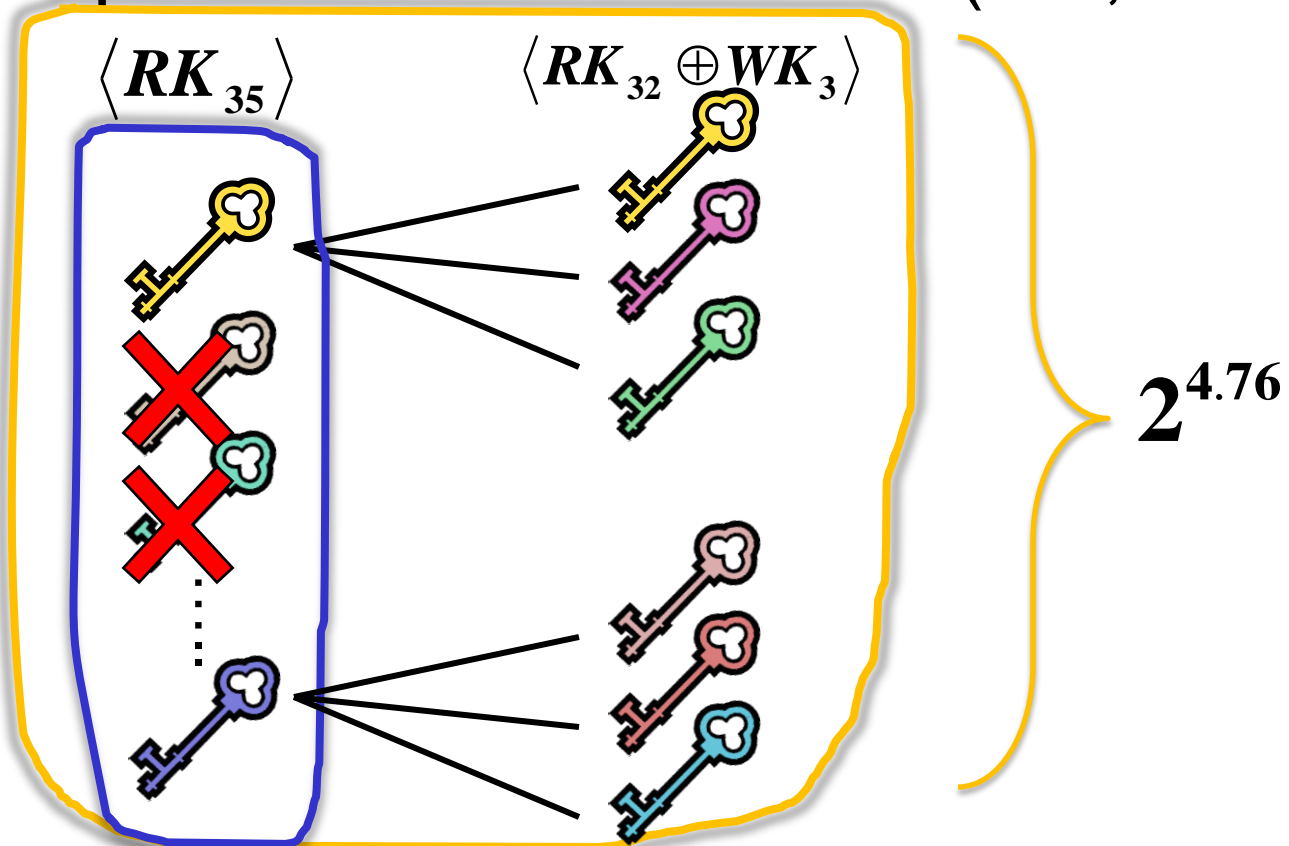
Step2: Obtain $\langle RK_{35}, RK_{32} \oplus WK_3 \rangle$ (3)

- Some candidates for RK_{35} is rejected.



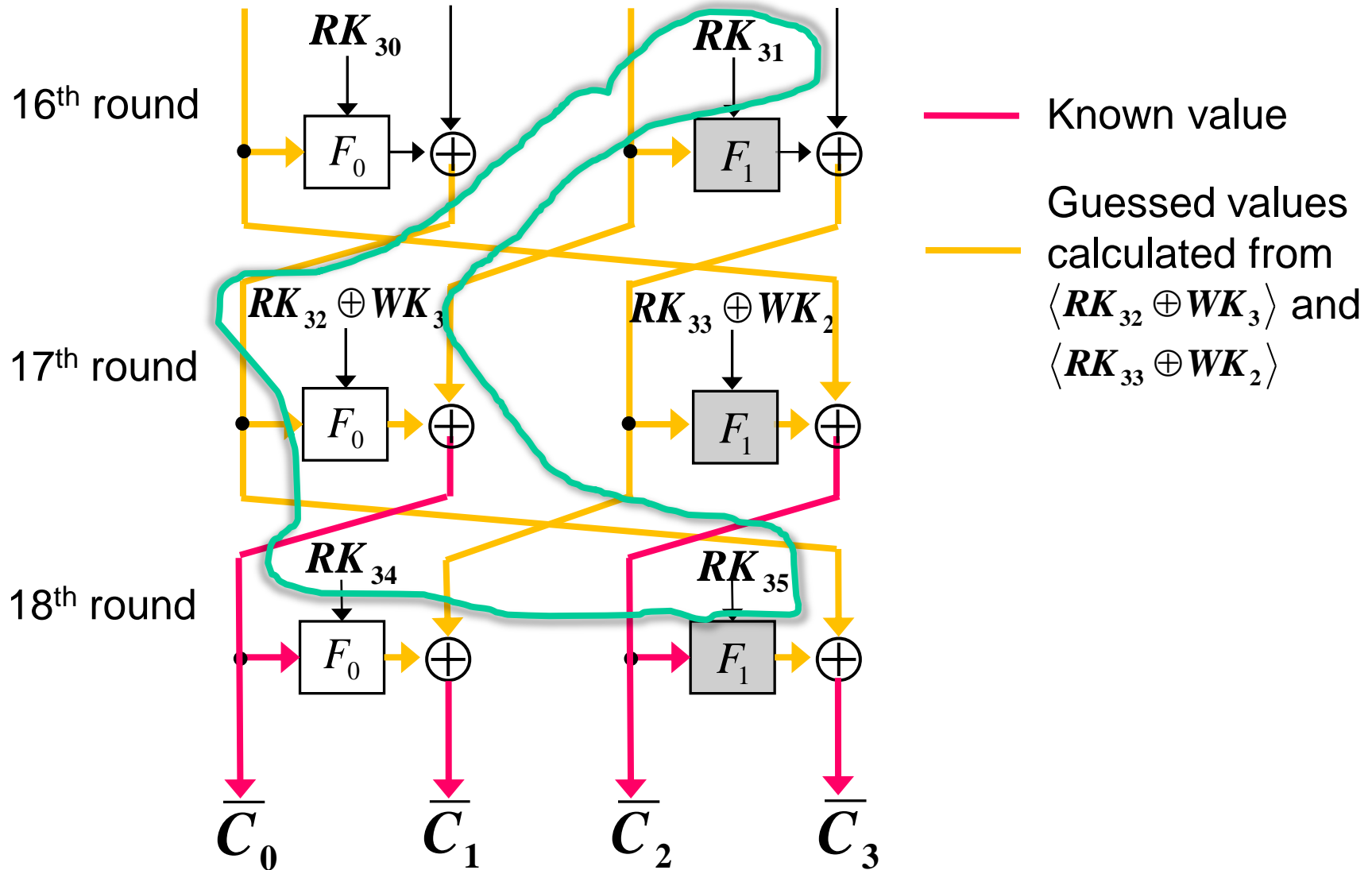
Step2: Obtain $\langle RK_{35}, RK_{32} \oplus WK_3 \rangle$ (4)

- Average space of candidates for $(RK_{35}, RK_{32} \oplus WK_3)$ is $2^{4.76}$



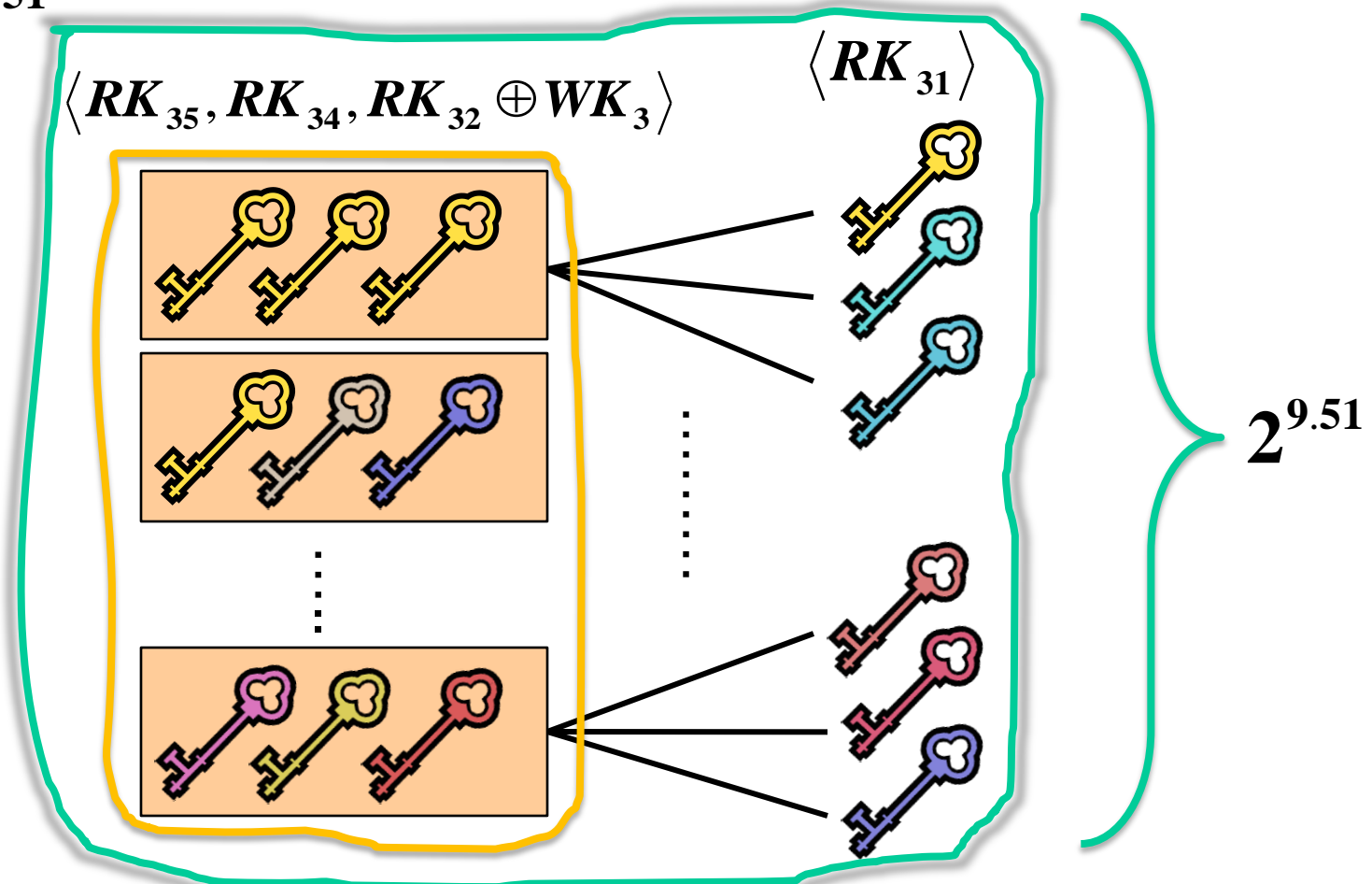
- Also obtain candidates for $(RK_{34}, RK_{33} \oplus WK_2)$

Step3: Obtain $\langle RK_{35}, RK_{34}, RK_{32} \oplus WK_3, RK_{31} \rangle$



Step3: Obtain $\langle RK_{35}, RK_{34}, RK_{32} \oplus WK_3, RK_{31} \rangle$ (2)

- Average candidate space for $(RK_{35}, RK_{34}, RK_{32} \oplus WK_3, RK_{31})$ is $2^{9.51}$



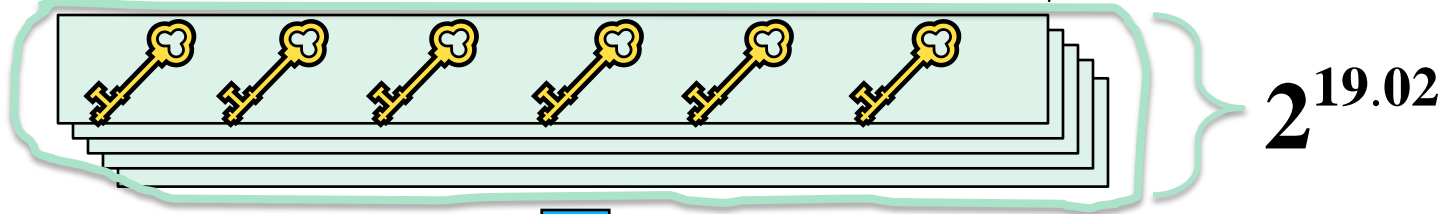
Total Brute-Force Search Space

- Average candidate space for $(RK_{35}, RK_{34}, RK_{32} \oplus WK_3, RK_{31})$ is $2^{9.51}$
- Also, average candidate space for $(RK_{35}, RK_{34}, RK_{33} \oplus WK_2, RK_{30})$ is also $2^{9.51}$
- Therefore, the total average space is $2^{19.02}$

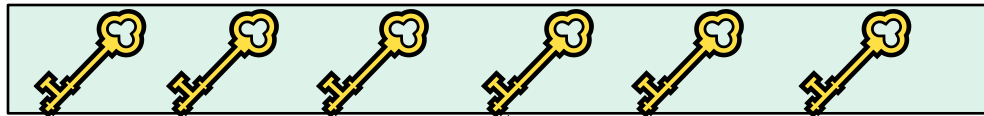
We need average a 19.02-bit brute-force search to obtain 128-bit key !

Step4: Recover Original Key

$$\langle RK_{35}, RK_{34}, RK_{32} \oplus WK_3, RK_{33} \oplus WK_2, RK_{31}, RK_{30} \rangle$$

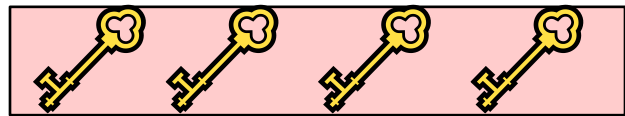


Choose one



Apply inverse DoubleSwap function

$RK_{35}, RK_{34}, RK_{32}, RK_{33}$

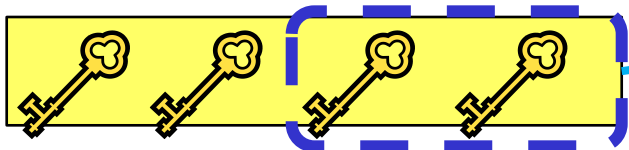


WK_2, WK_3



Calculate inverse key scheduling algorithm

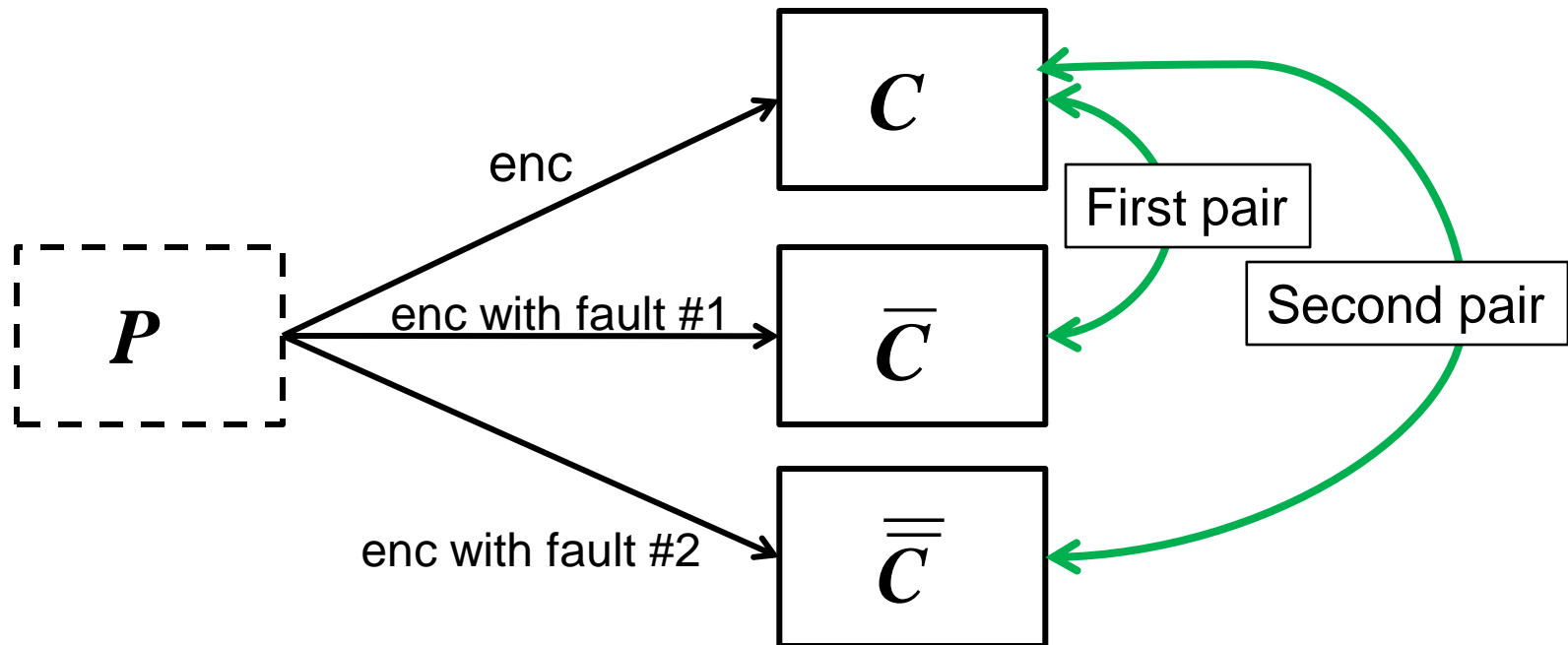
Candidate of the original key



If they are equal, the candidate of the original key is correct !

Attack Conditions (1)

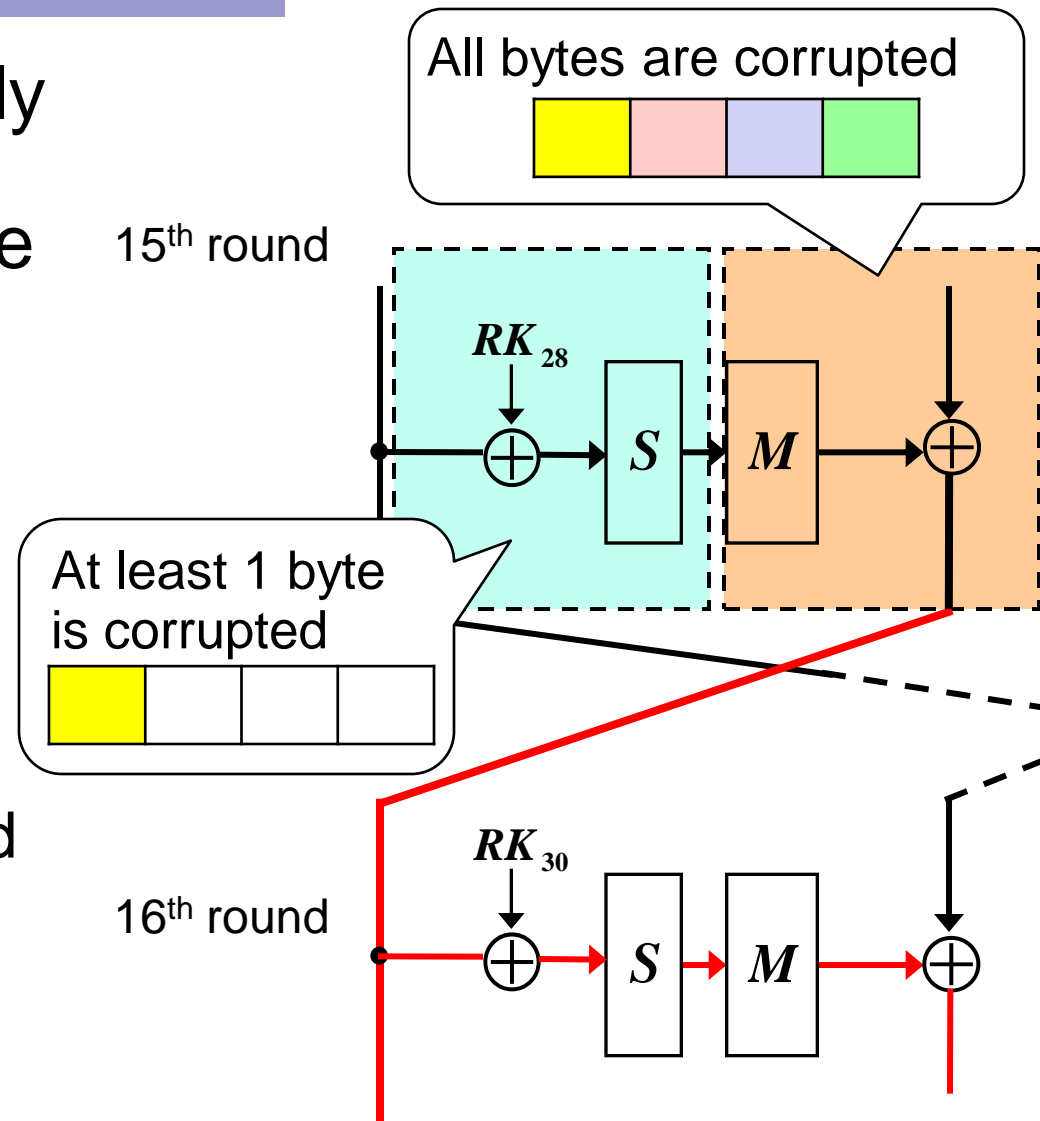
- Attacker can obtain two pairs of correct and faulty ciphertexts.
 - He does not need to know the value of the plaintext.



Attack Conditions (2)

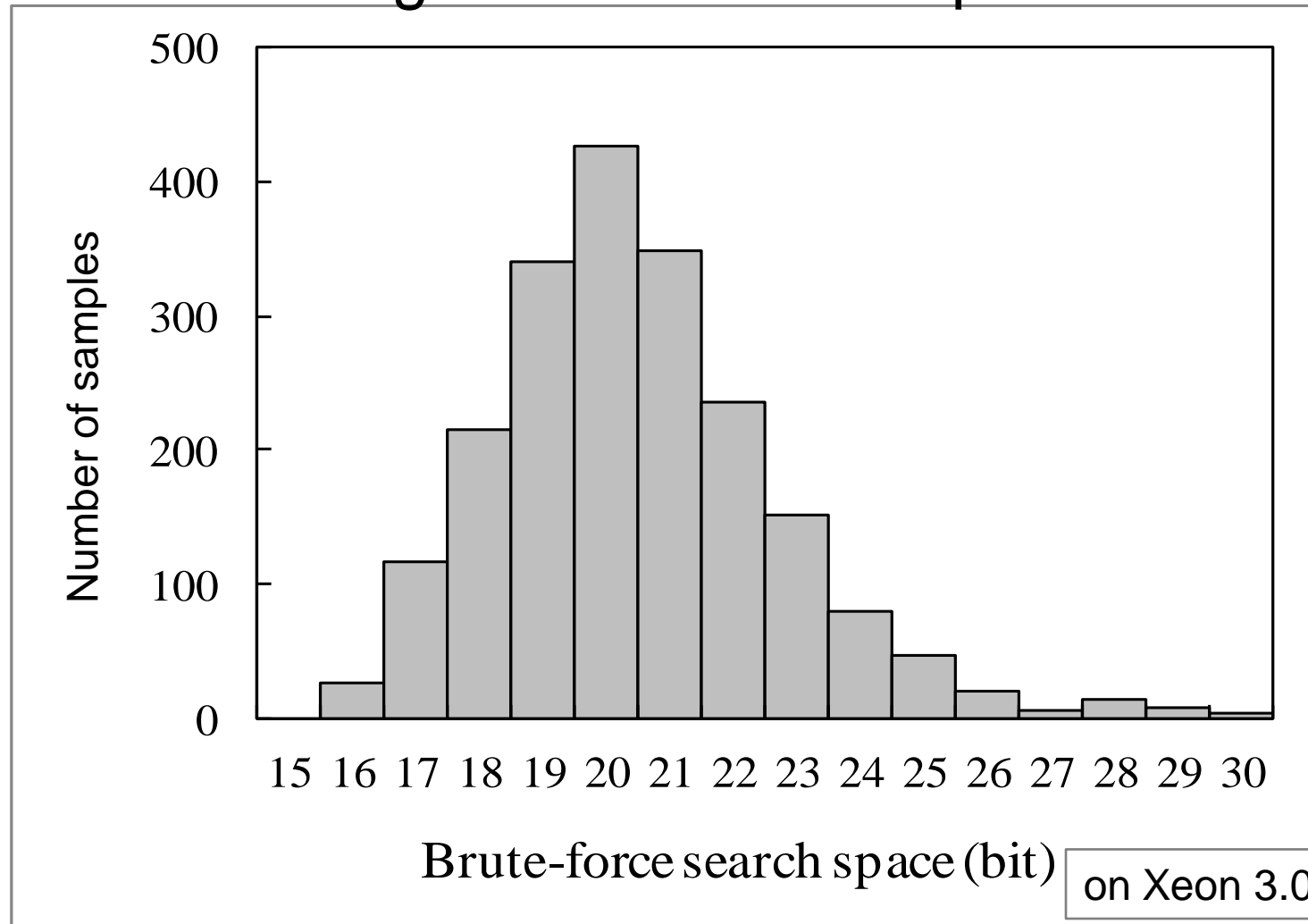
- Attacker must randomly corrupt a total of 4-bytes of the input in the 16th round.

- He does not need to know value of faults.
- He can choose the convenient ways of fault injection depended on devices.



Simulation Results (B-F Space)

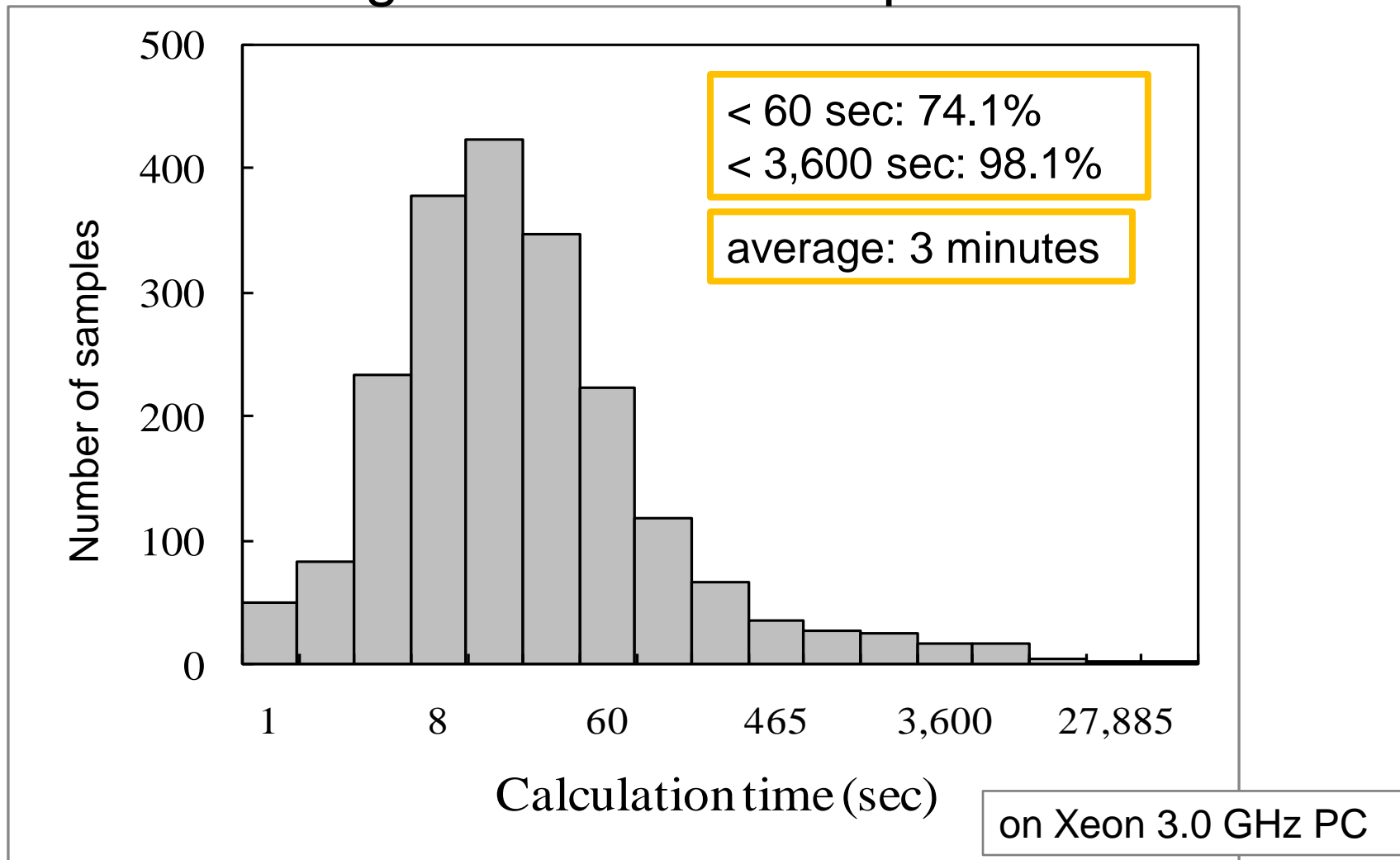
Histogram for 2000 samples



on Xeon 3.0 GHz PC

Simulation Results (Time)

Histogram for 2000 samples



- Background
- Previous Study
 - Structure of CLEFIA
 - General DFA Method
 - Chen's Attack
- Proposed Attack
 - Attack Method
 - Simulation Results
- Conclusions

Conclusion

- Developed efficient DFA on CLEFIA using its 4-branch structure with 32-bit data lines
 - Requires 2 pairs of correct and faulty ciphertexts
 - Average calculation time to obtain 128-bit key is about 3 minutes

