Fault Analysis with Coupon Collector's Problem

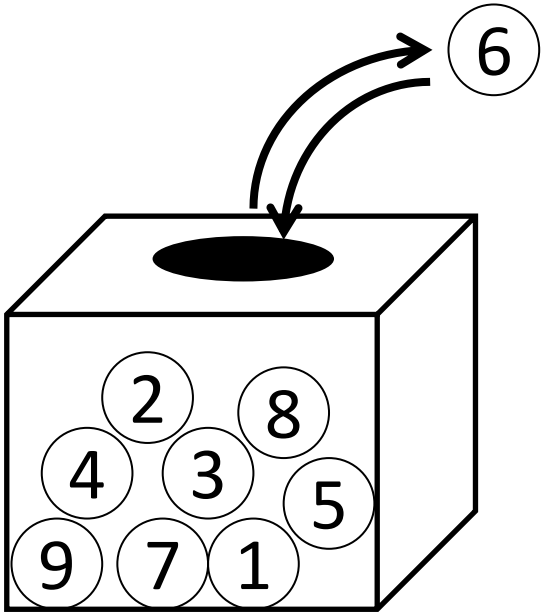
Yu Sasaki[1], Yang Li[2], Hikaru Sakamoto[2], and Kazuo Sakiyama[2]

1: NTT Corporation

2: University of Electro-Communications

Coupon Collector's Problem (CCP)

- Definition



For each coupon drawing event, 1 random coupon is obtained.

How many events are expected to complete all coupons?

$$n \ln(n)$$

- CCP can be applied to the fault attack.

Motivation

- Primary motivation

Motivation

- Primary motivation

fun !!

Motivation

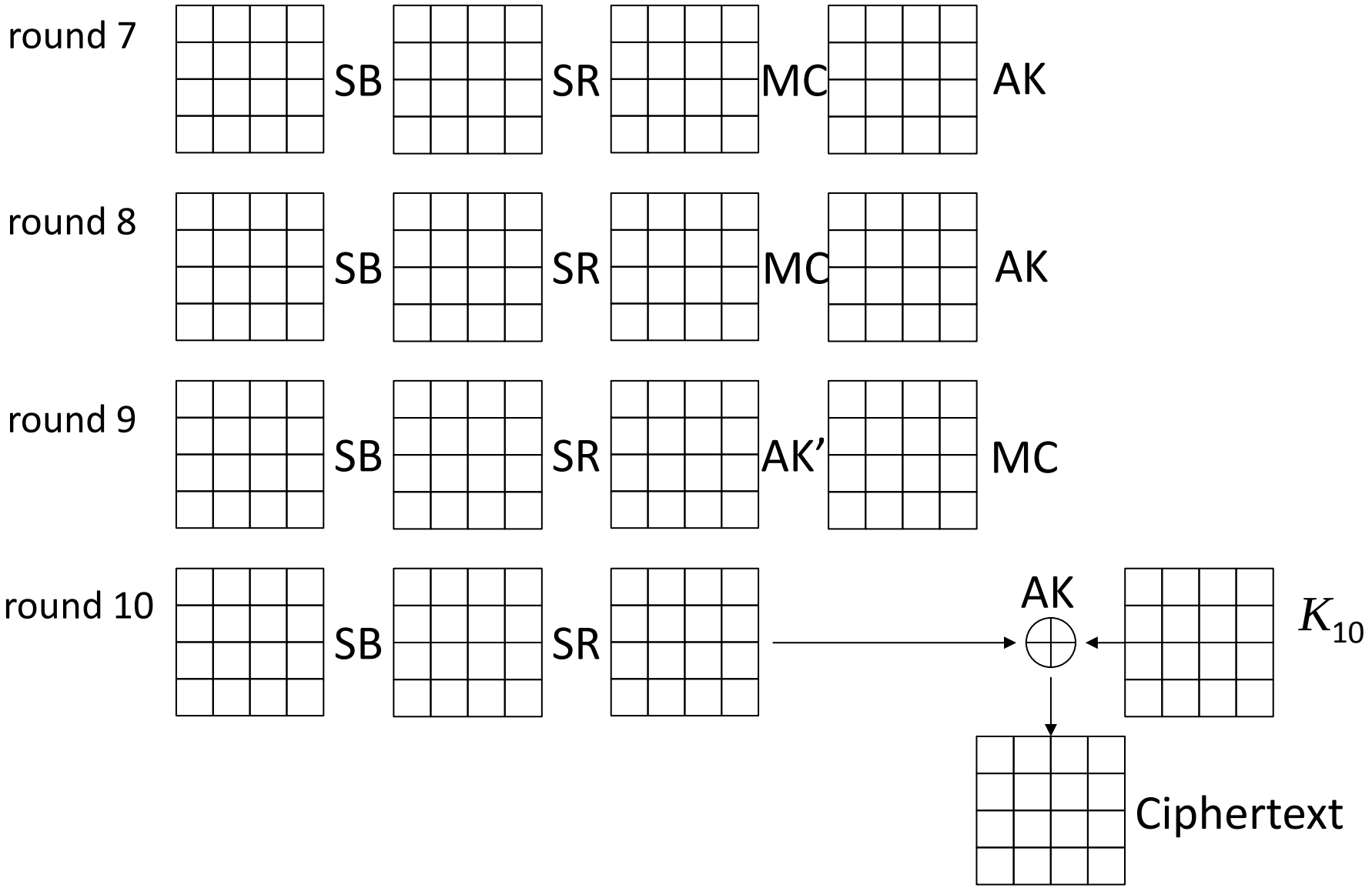
- Primary motivation

fun !!

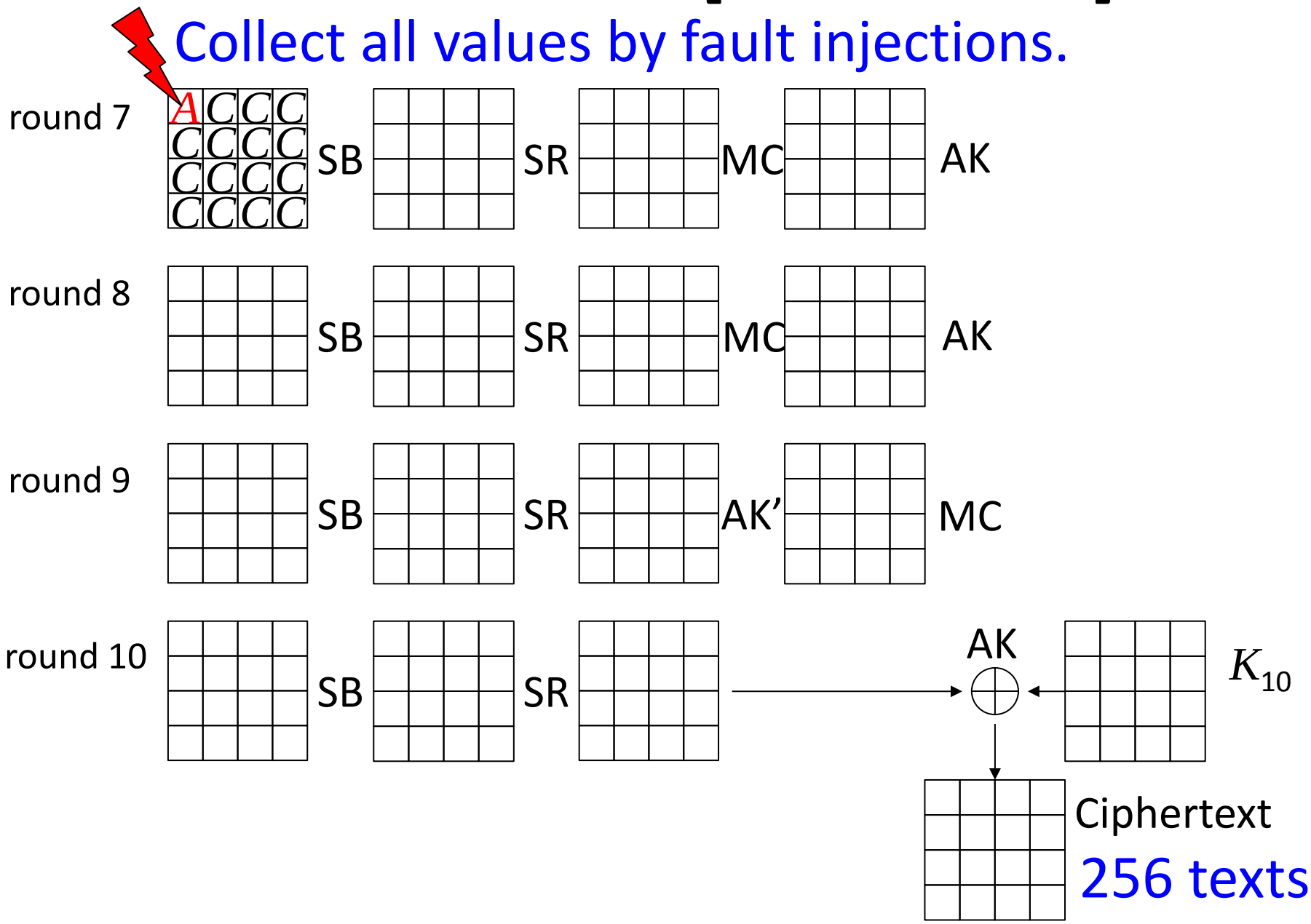
- Byproduct:

  Assumption for the fault injection can be more realistic (noise is acceptable).

The Last 4 Rounds of AES

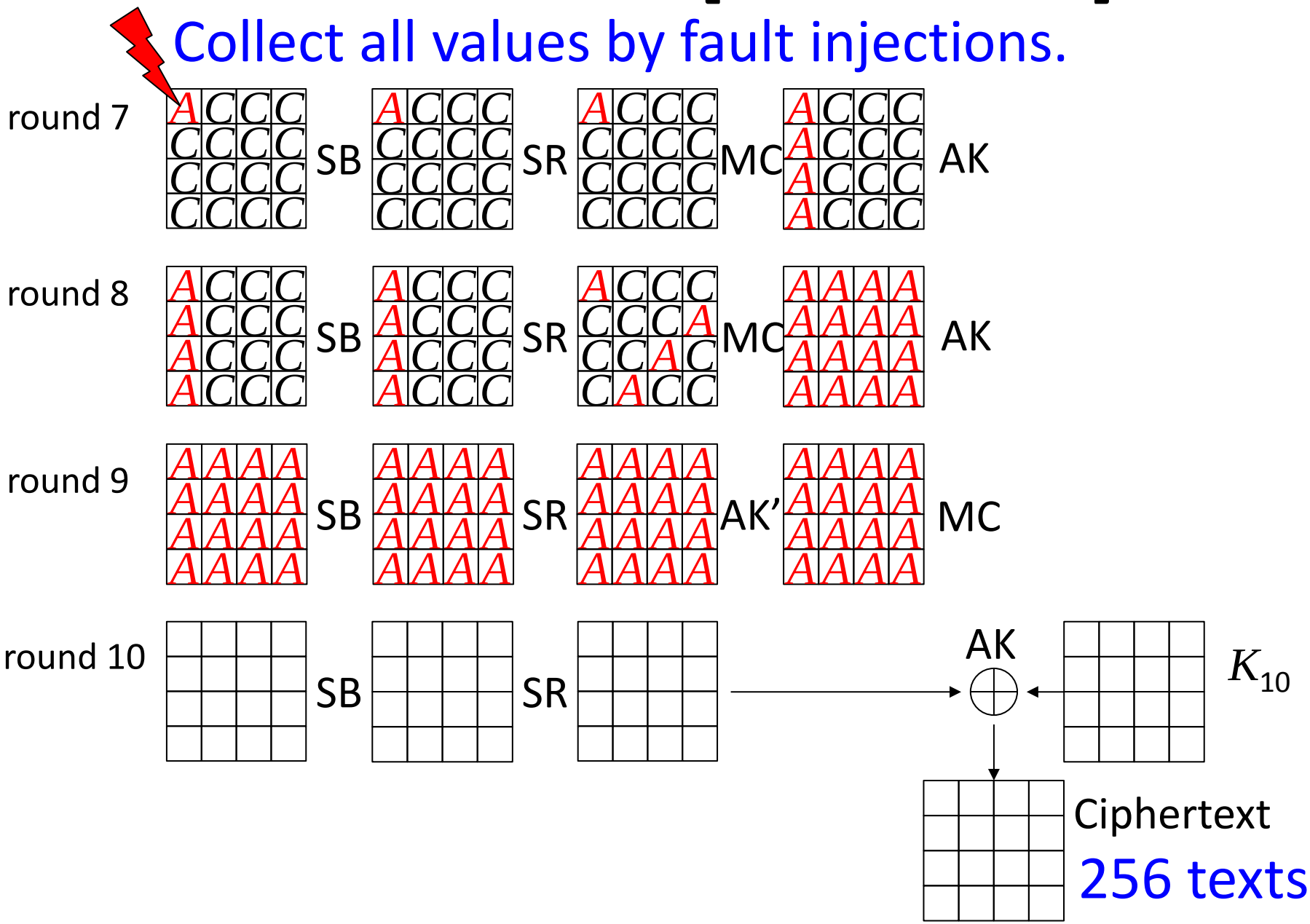


SQUARE DFA [PhanYin06]

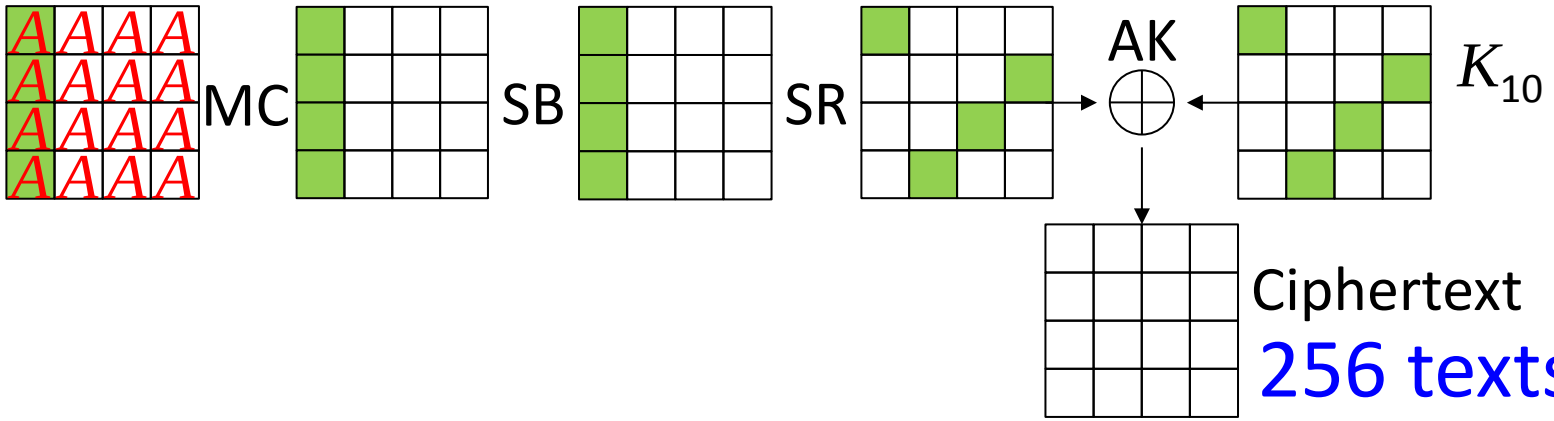


SQUARE DFA [PhanYin06]

Collect all values by fault injections.



SQUARE DFA [PhanYin06]



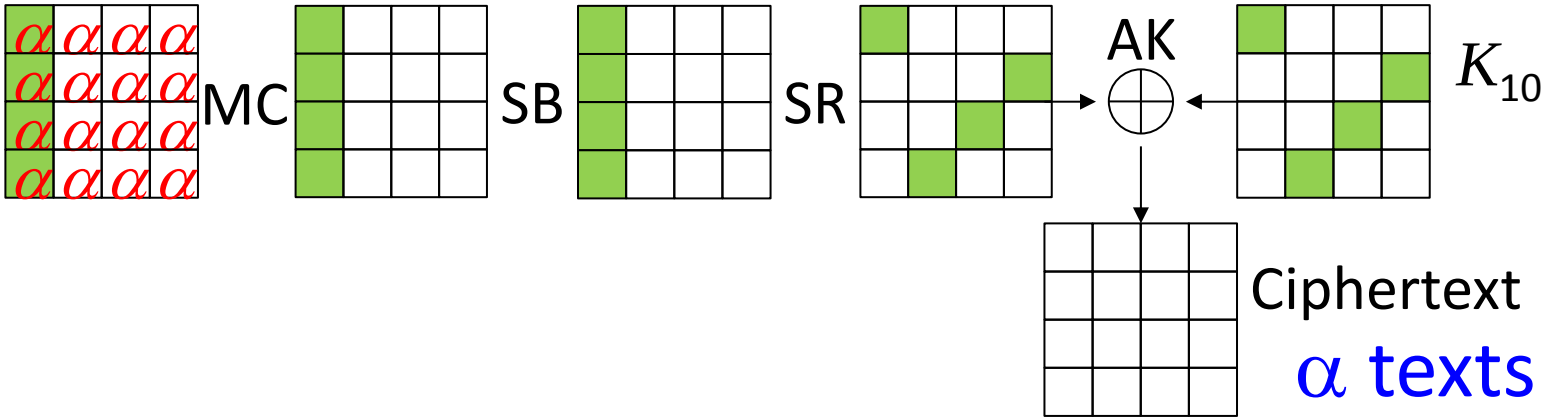
The key K_{10} is guessed column by column.

Each guess is a right key candidate with prob.:

$$\left(\prod_{i=0}^{255} \frac{(256-i)}{256}\right)^4$$

The correct key is recovered.

Improved SQUARE DFA [Kim11]



256 values are not necessary. α values are enough.

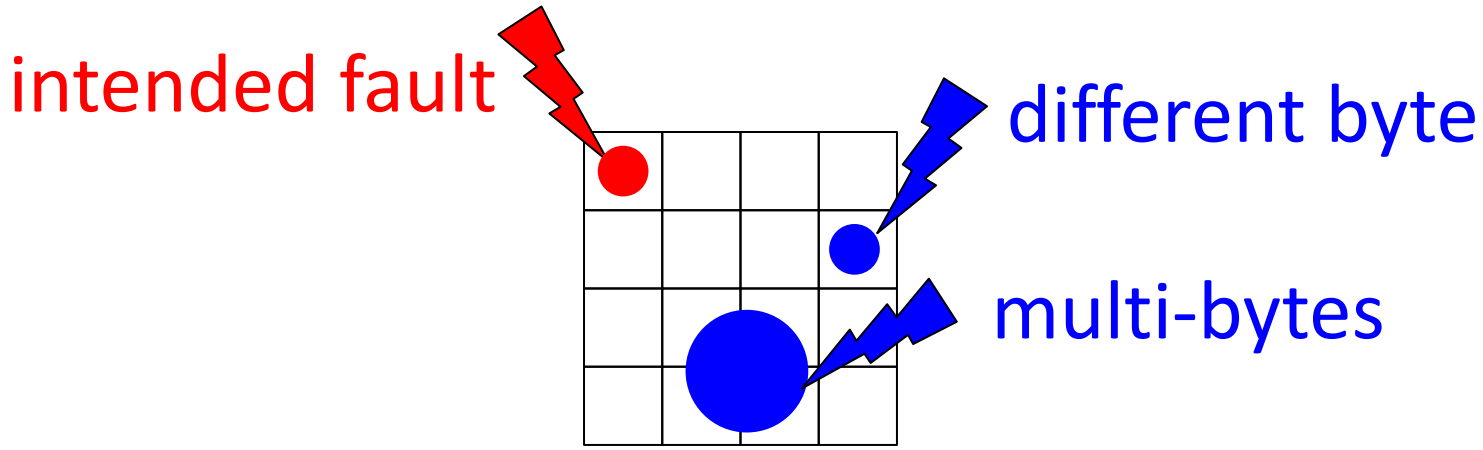
Each guess is a right key candidate with prob:

$$\left(\prod_{i=0}^{\alpha-1}\frac{(256-i)}{256}\right)^4$$

The probability is smaller than 2^{-32} for $\alpha = 45$.

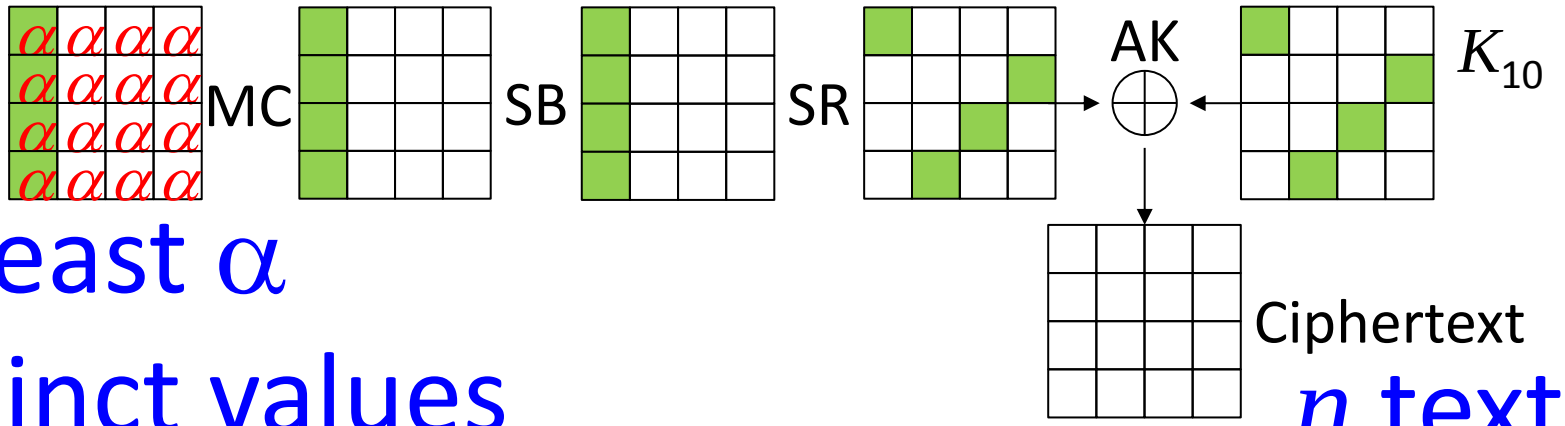
Noisy Fault Model

- Previous SQUARE DFAs assume that unintended fault never occurs.
- But, in practice, noise is obtained.



We can still recover the key !!

Our Attacks



At least α distinct values

n texts

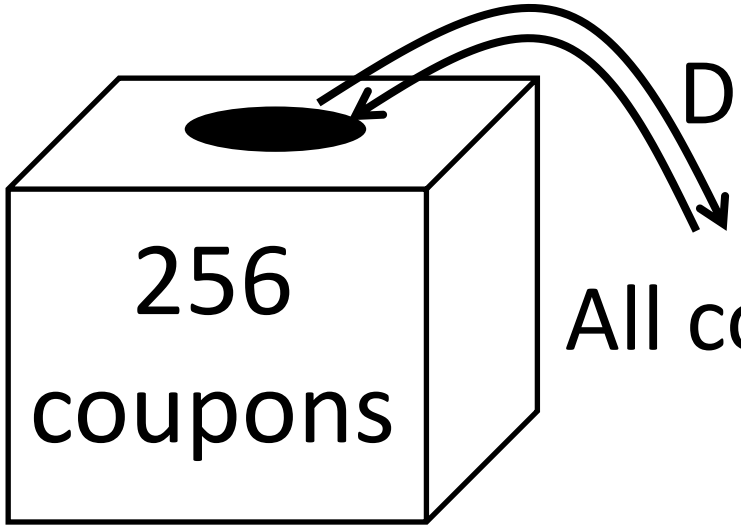
- α: the number of distinct fault values
- n: the total number of texts to be analyzed

For the correct guess at least α distinct values appear, otherwise, the guess is wrong.

What's the probability?

Probability Estimation with CCP

- Suppose that α = 256. Each guess is a right key candidate if all 256 values are completed after n trials.



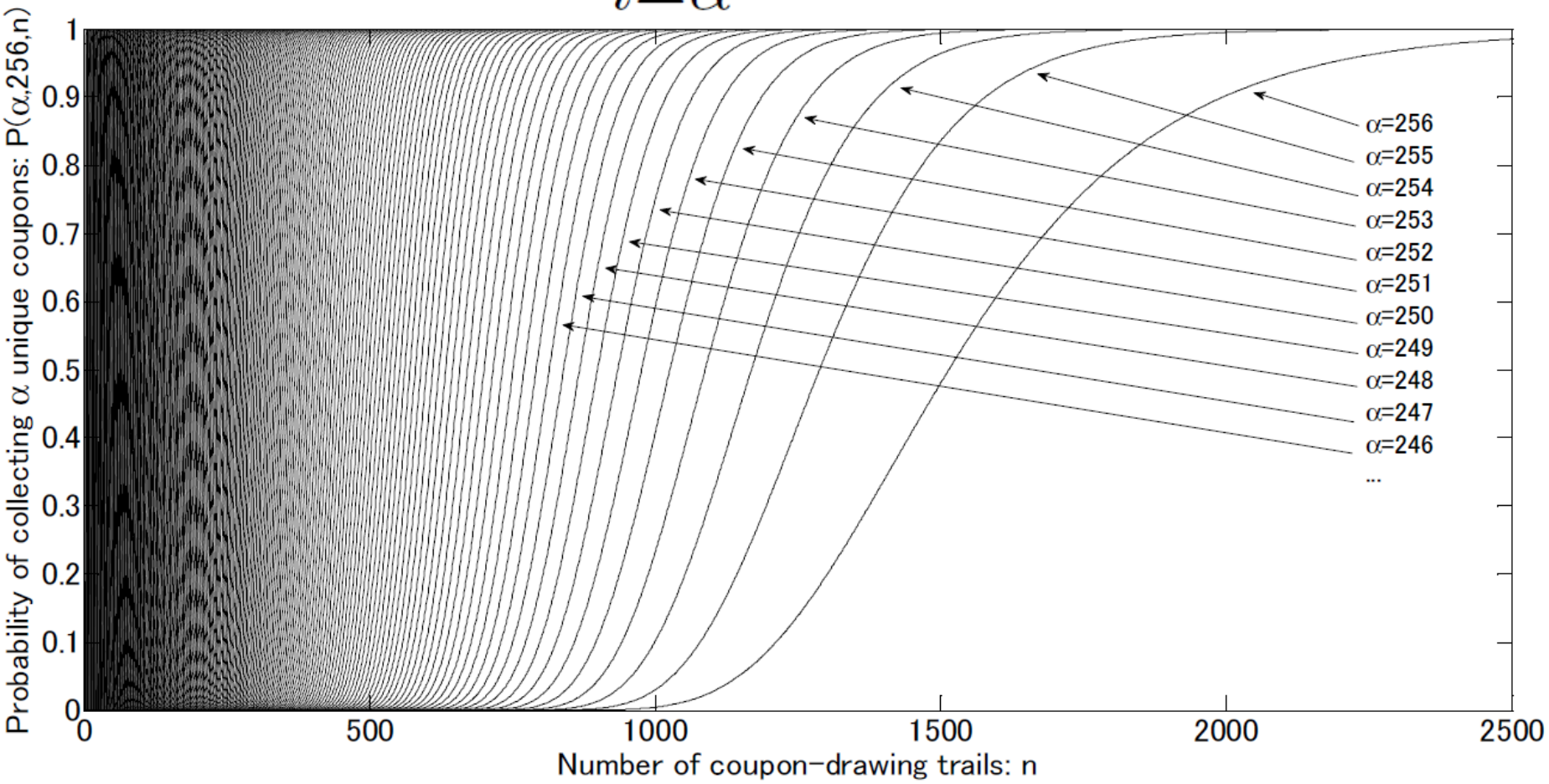
Draw a coupon n times.

All coupons are completed ?

- equivalent to the CCP. Pr=2^{-1} even if n=1553.
- For α < 256, it becomes a variant of the CCP.

Probability Estimation with CCP

$$\binom{\beta}{\alpha}\binom{\alpha}{1}\sum_{i=\alpha}^{n}\frac{Q(\alpha-1,i-1)}{\beta^{i}}$$



Conclusion

- We generalized the SQUARE DFA so that the noisy fault injection can be accepted.
- We did the probability estimation with the coupon collector's problem.
- The paper will appear at FC2013.

Thank you for your attention !!