DIFFERENTIAL FAULT INTENSITY ANALYSIS
on PRESENT and LED Block Ciphers

Nahid Farhady Ghalaty, Bilgiday Yuce, Patrick Schaumont

ECE Department

Virginia Tech

COSADE 2015

This research was supported through NSF Grant 1441710, Grant 1115839, and through SRC.

Outline

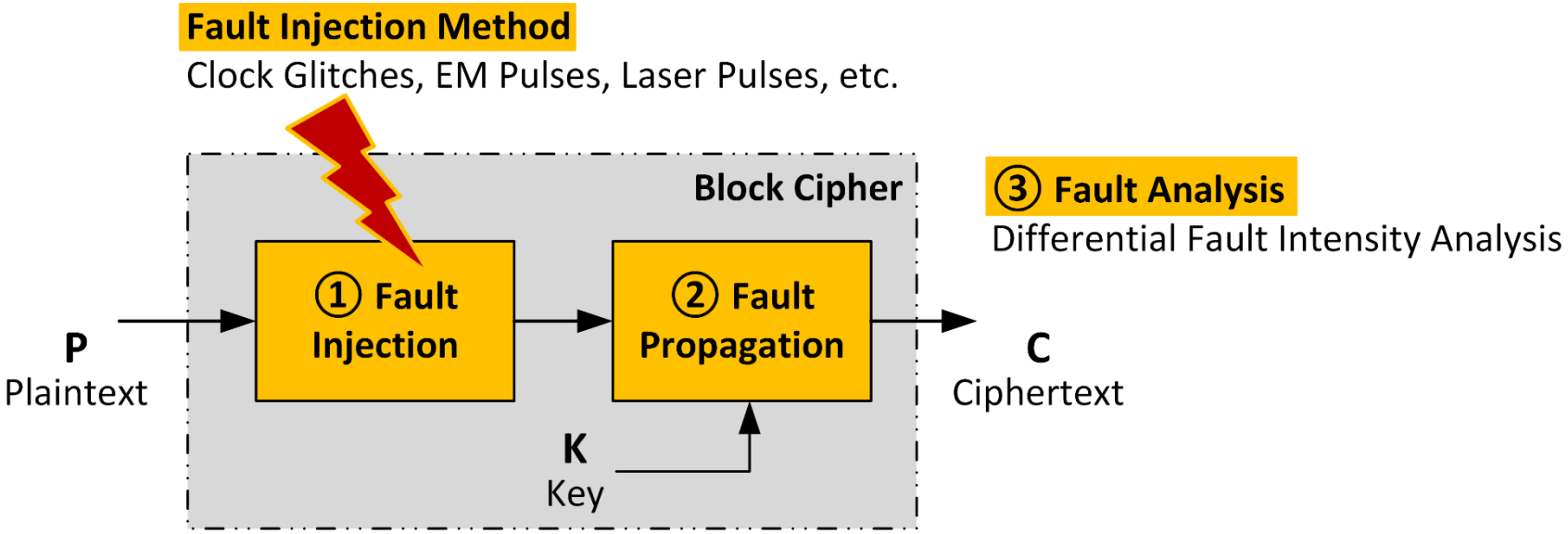
1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
   - Differential Fault Intensity Analysis (DFIA)
   - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

In a nutshell

- The basis of Differential Fault Intensity Analysis (DFIA) is biased (non-uniform) fault behavior.
- DFIA provides a feasible (cheap, general) biased fault model.
- DFIA works even we do not have high-capability fault injection equipment.

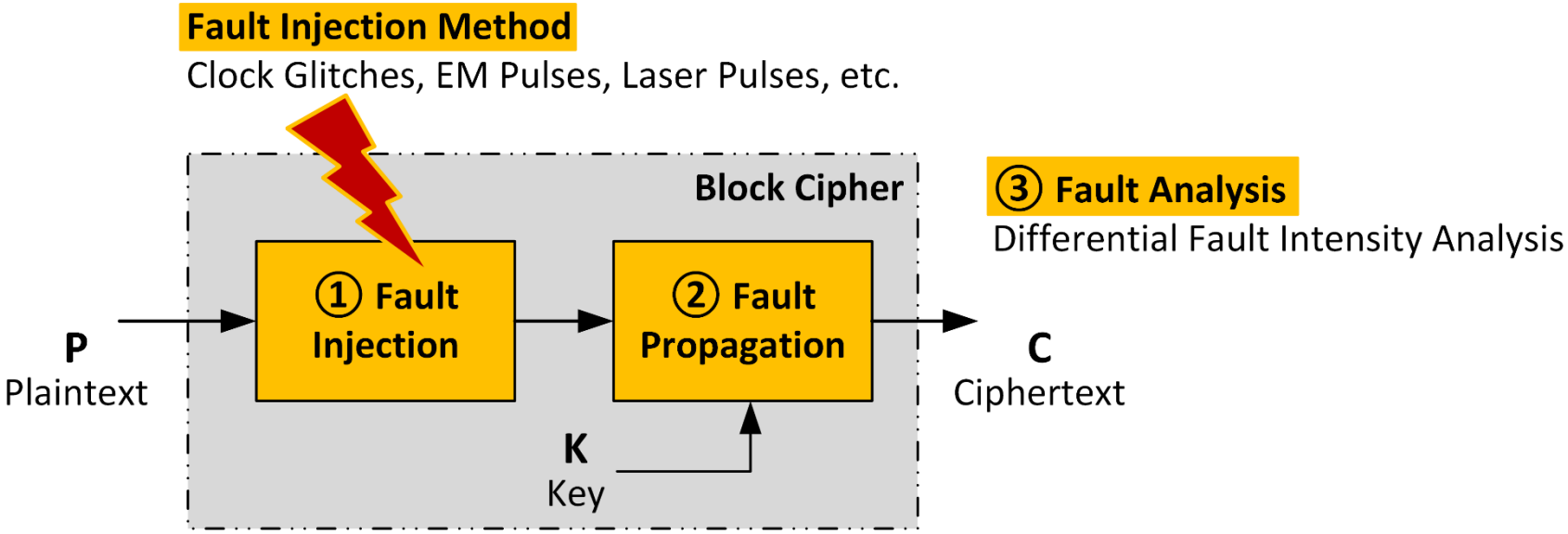
Fault Attack Requirements

- Fault Attacks:
  1. Injecting faults in cipher's state
  2. Observing the effects of the fault
  3. Analyzing the effects to retrieve the key



Fault Attack Requirements

- Fault analysis relies on fault model.
  - Fault model: Assumptions/Restrictions on the injected faults
- Attacker needs a feasible fault model.



Fault Attack Requirements

- Differential Fault Intensity Analysis (DFIA):
  1. How can we obtain biased faults?
     - With low-cost setups
     - With applicability to any fault injection method

     $\Longrightarrow$ A feasible fault model

Fault Attack Requirements

- Differential Fault Intensity Analysis (DFIA):
  1. How can we tune the injected faults?
     - With low-cost setups
     - With applicability to any fault injection method

     ⟹ A feasible fault model

  2. How can we exploit the biased faults?
     - Using side-channel analysis approach
     - Similar to Differential Power Analysis (DPA)

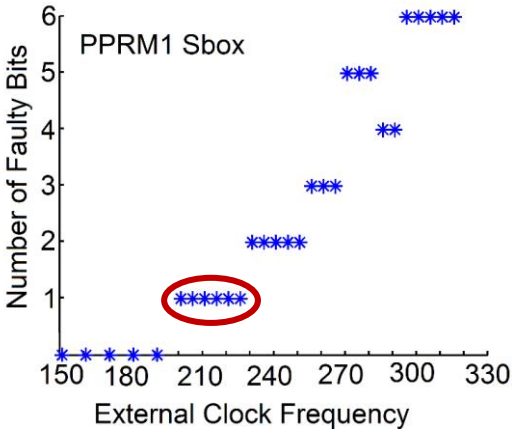
Outline

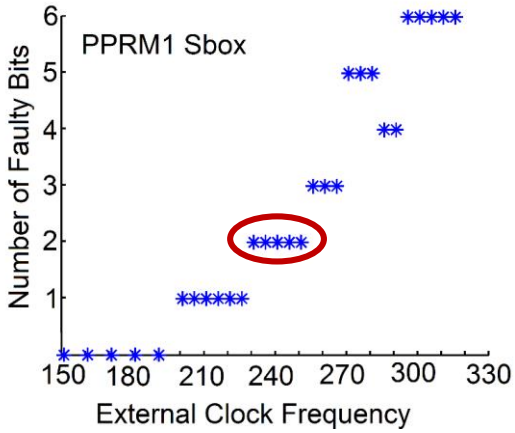
1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
    - Differential Fault Intensity Analysis (DFIA)
    - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

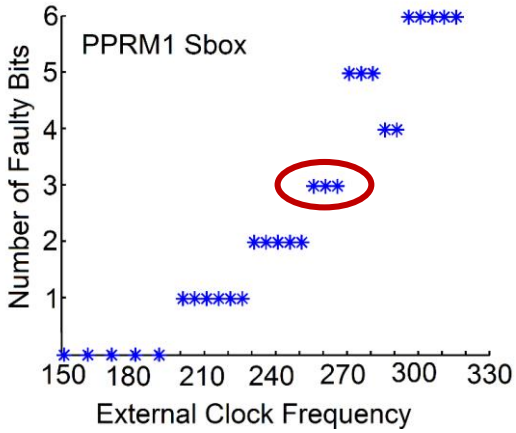
Observation I

- # of Faults vs. External Clock Frequency

Clock-glitching (Ghalaty et al. FDTC'14)







f_1 = 210 MHz

Faults = 1

f_1 = 240 MHz

Faults = 2

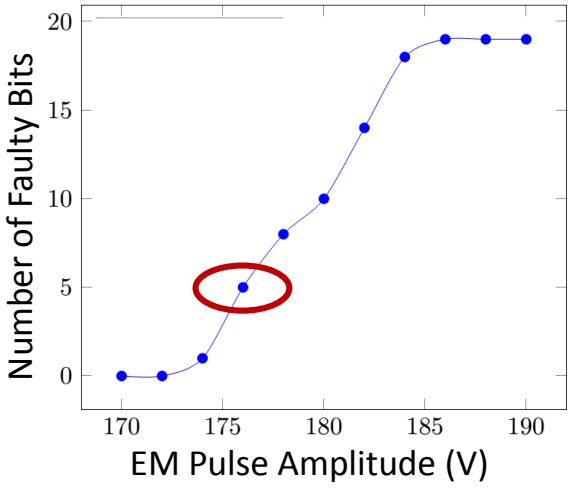
f_1 = 270 MHz

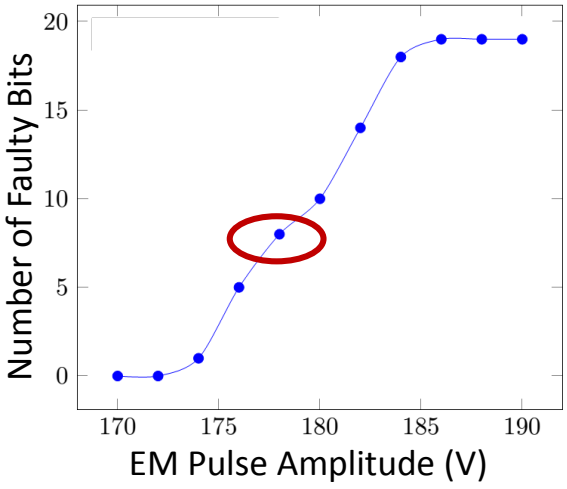
Faults = 3

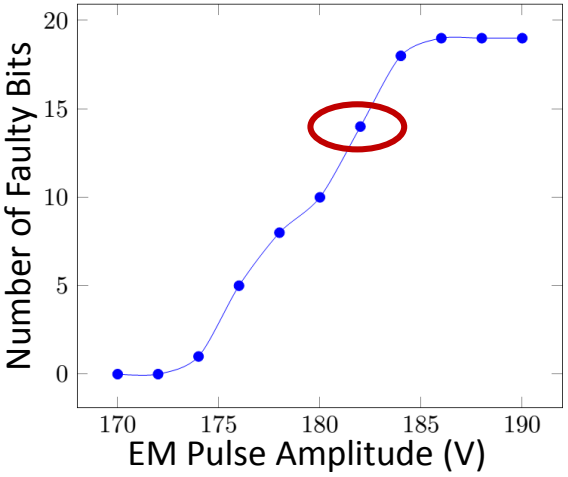
Observation II

- # of Faults vs. EM Pulse Amplitude

Electromagnetic (EM) Pulses (Moro et al. FDTC'13)







V_{pulse} = 176 V

Faults = 5

V_{pulse} = 178 V

Faults = 8

V_{pulse} = 182 V

Faults = 13

Creating Biased Faults

- How can we inject biased faults?
  - By varying the fault intensity
- Fault Intensity:
  - The strength of the applied stress on the attacked device

Fault Injection Method	Fault Intensity
Clock-glitching	Clock frequency
EM Pulses	Pulse voltage

Creating Biased Faults (cont.)

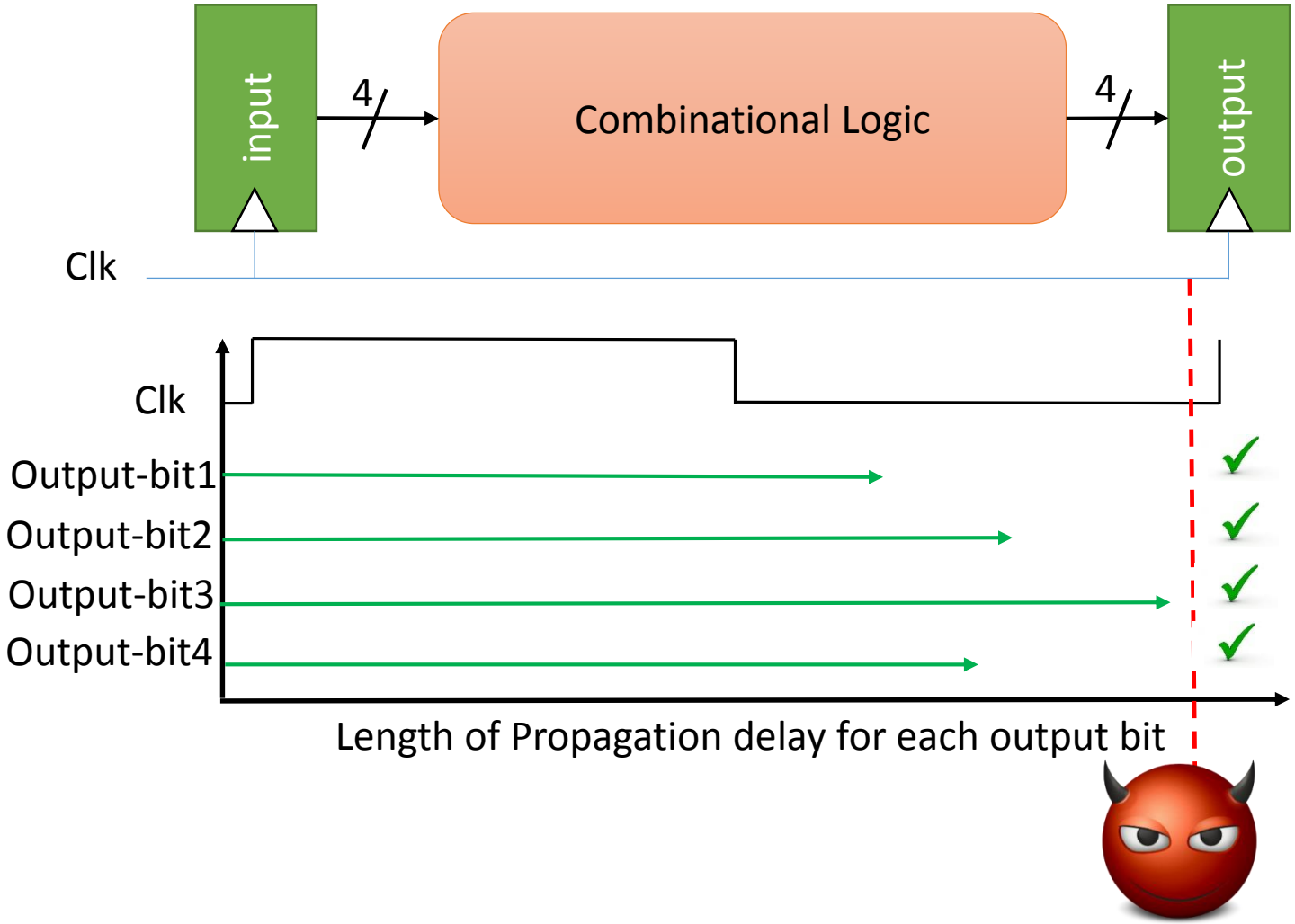
- How can we inject biased faults?
  - By varying the fault intensity
- Fault Intensity:
  - The strength of the applied stress on the attacked device

Fault Injection Method	Fault Intensity
Clock-glitching	Clock frequency
EM Pulses	Pulse voltage

- Biased (Non-uniform) Fault Behavior:
  - Number of Faults ~ Fault Intensity
  - Small change in Fault Intensity → Small change in Faulty Value

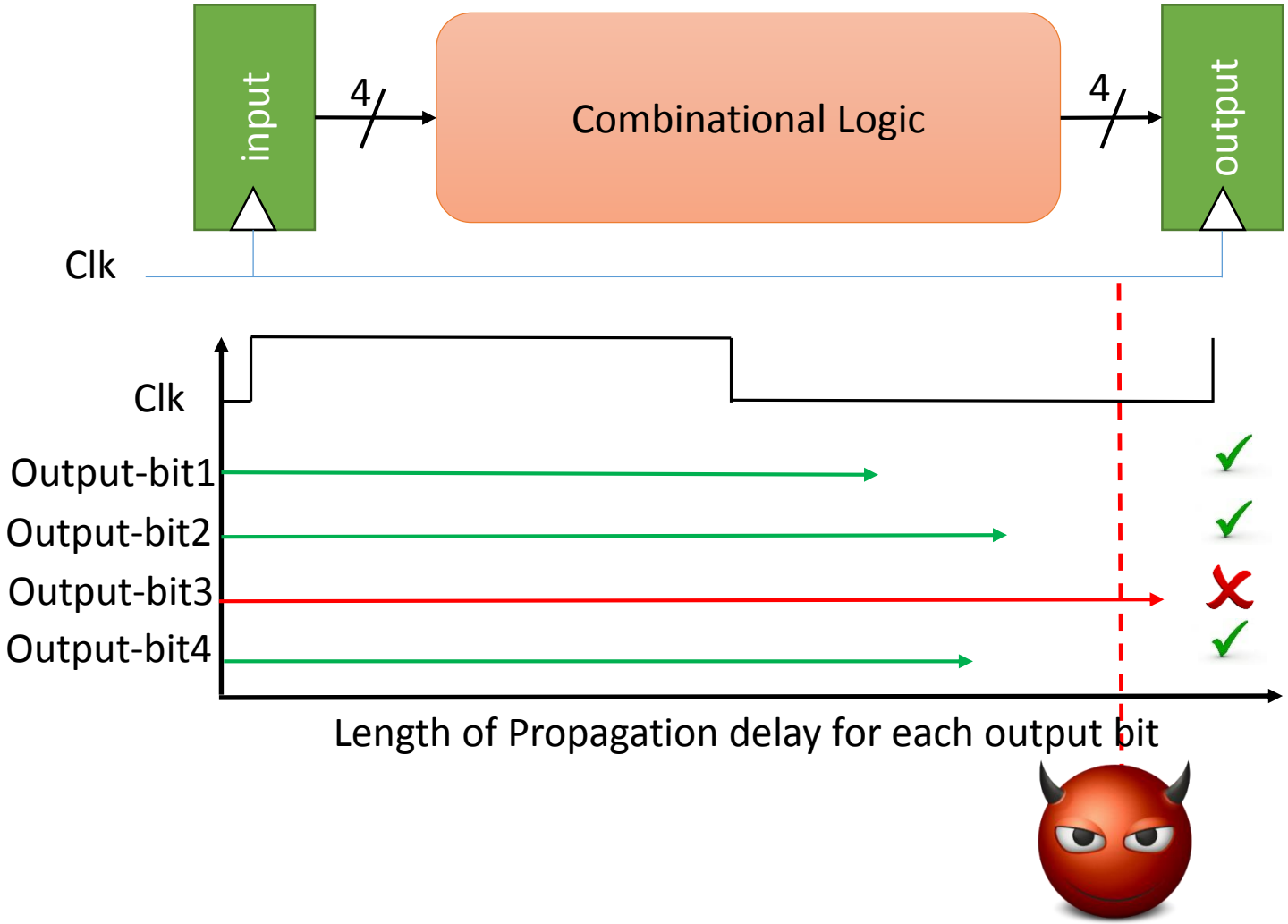
A Fault Mechanism

- Setup Time Violation:



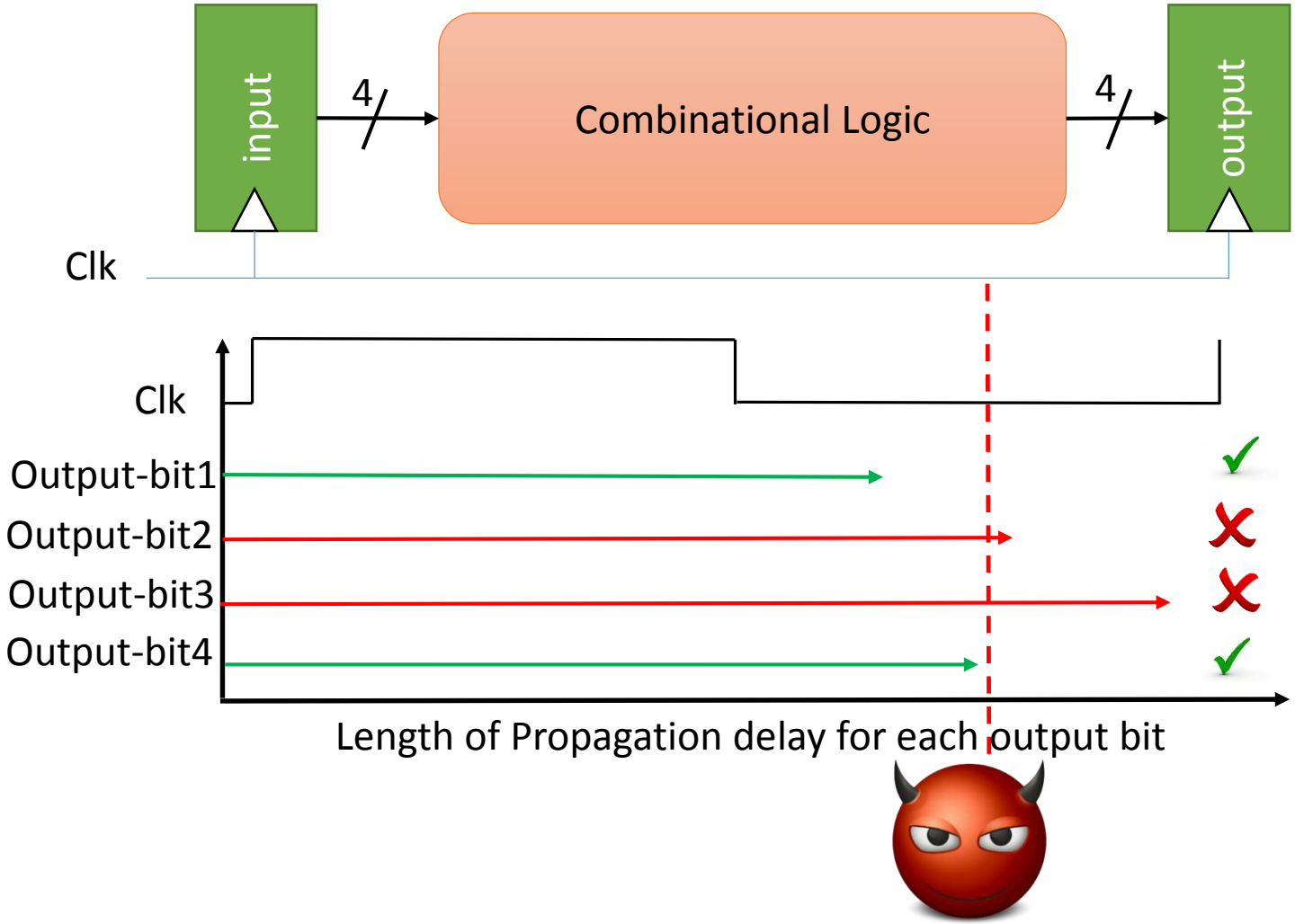
A Fault Mechanism (cont.)

- Setup Time Violation:



A Fault Mechanism (cont.)

- Setup Time Violation:

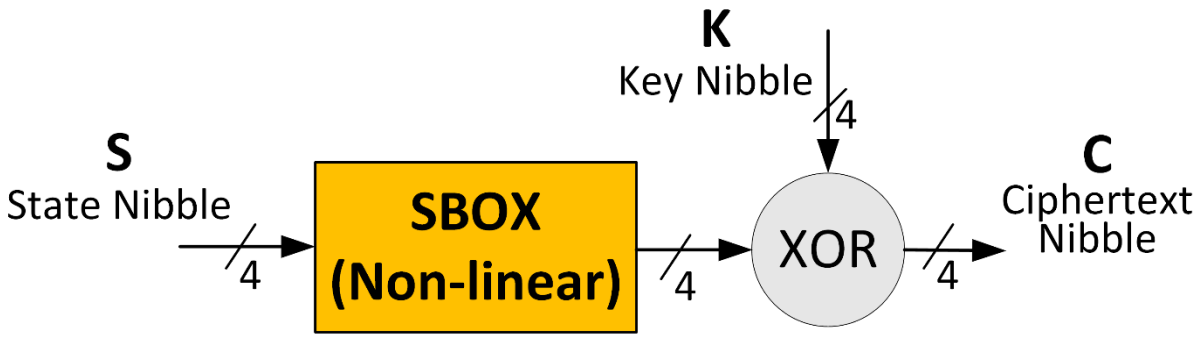


Outline

1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
   - Differential Fault Intensity Analysis (DFIA)
   - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

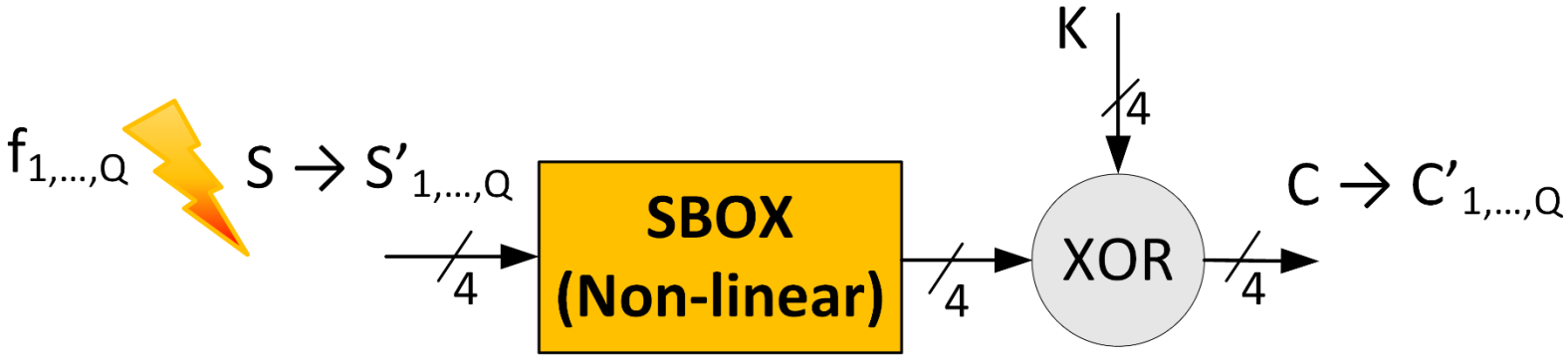
Differential Fault Intensity Analysis

- Differential Fault Intensity Analysis (DFIA):
  - Combines fault injection and DPA principles
  - Induces biased faults by varying the fault intensity
  - Applies a hypothesis test with biased faults
  - Uses biased faults as the source of leakage



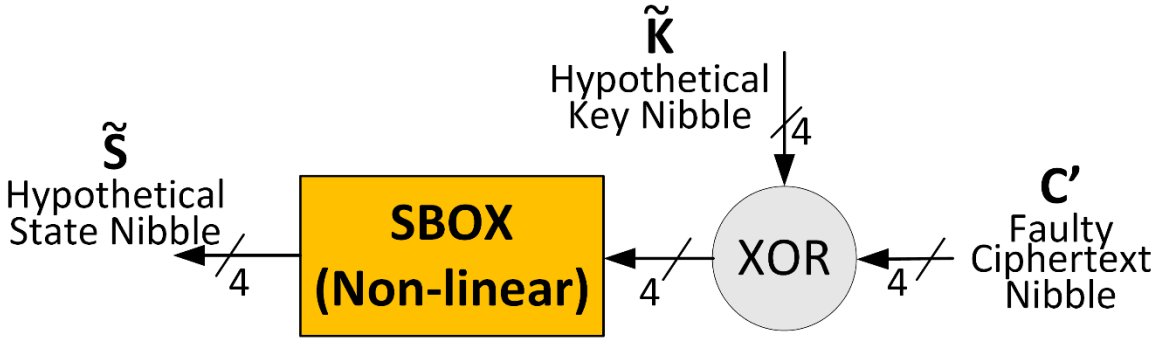
DFIA – Biased Fault Injection

- Step 1: Biased Fault Injection
  - Apply Q different fault intensities ($f_{1,\ldots,Q}$)
  - Induce biased faults ($S'_{1,\ldots,Q}$)
  - Collect faulty ciphertexts ($C'_{1,\ldots,Q}$)



DFIA – Hypothesis Test

- Step 2: Hypothesis Test with Biased Faults



Given: C' and a KNOWN fault bias f

Find: Most likely key nibble $\tilde{K}$

For all $\tilde{K}$, find $\tilde{S} = SBOX^{-1}(C' \oplus \tilde{K})$

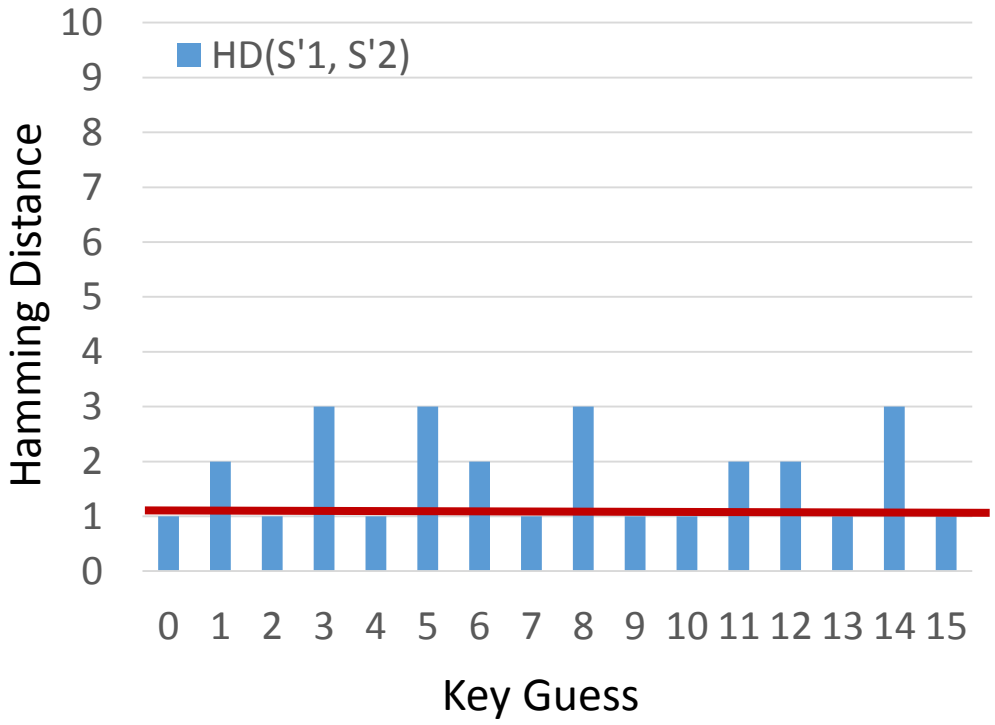
Accumulate $\rho_{\tilde{K}} = \sum HD(\tilde{S})$

Select K = argmin ρ

DFIA – Hypothesis Test Example

- Step 2: Example for PRESENT

$f_{1,\ldots,4}$ → $S'_{1,\ldots,4}$
where $HD(S'_i, S'_{i+1}) = 1$

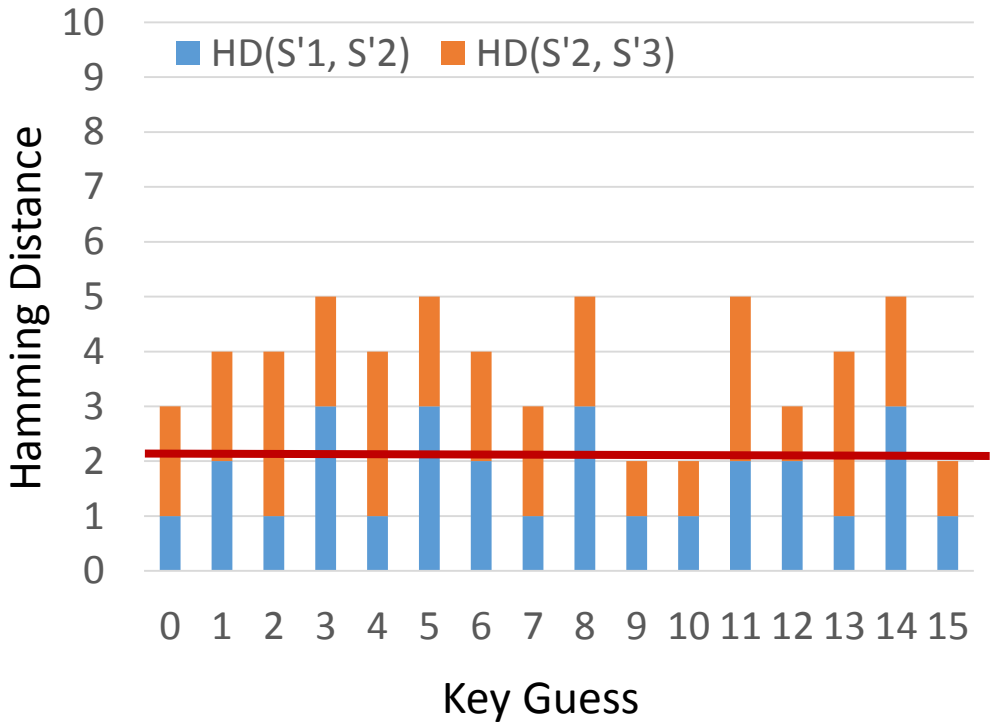


Possible Key Values:
{0,2,4,7,9,10,13,15}

DFIA – Hypothesis Test Example (cont.)

- Step 2: Example for PRESENT

$f_{1,\ldots,4}$ → $S'_{1,\ldots,4}$
where $HD(S'_i, S'_{i+1}) = 1$

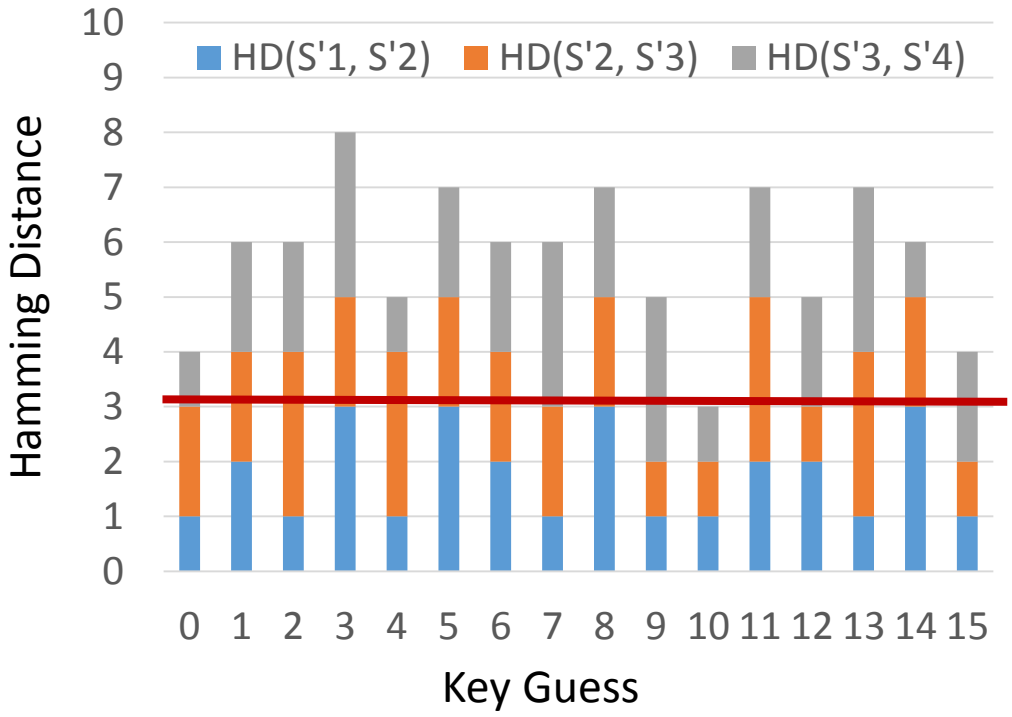


Possible Key Values:
{9,10,15}

DFIA – Hypothesis Test Example (cont.)

- Step 2: Example for PRESENT

$f_{1,\ldots,4}$ → $S'_{1,\ldots,4}$
where $HD(S'_i, S'_{i+1}) = 1$



Possible Key Values:
{10}

DFIA – Results

- Nibble-serial and Round-serial Implementations:
  - Verilog RTL codes
  - Gate-level netlists for an Altera Cyclone IV FPGA

- Biased Fault Injection:
  - Clock Glitches
  - Gate-level (post-place-and-route) simulation

DFIA – Results (cont.)

- PRESENT (and LED):
  - Step size (resolution): 100ps

	# of Fault Intensity Levels(Q)		# of Glitched Clock Cycles	
	Nibble-Serial	Round-Serial	Nibble-Serial	Round-Serial
PRESENT-80	10	12	10×16=160	12×1=12
PRESENT-128	16	18	16×16=256	18×1=18

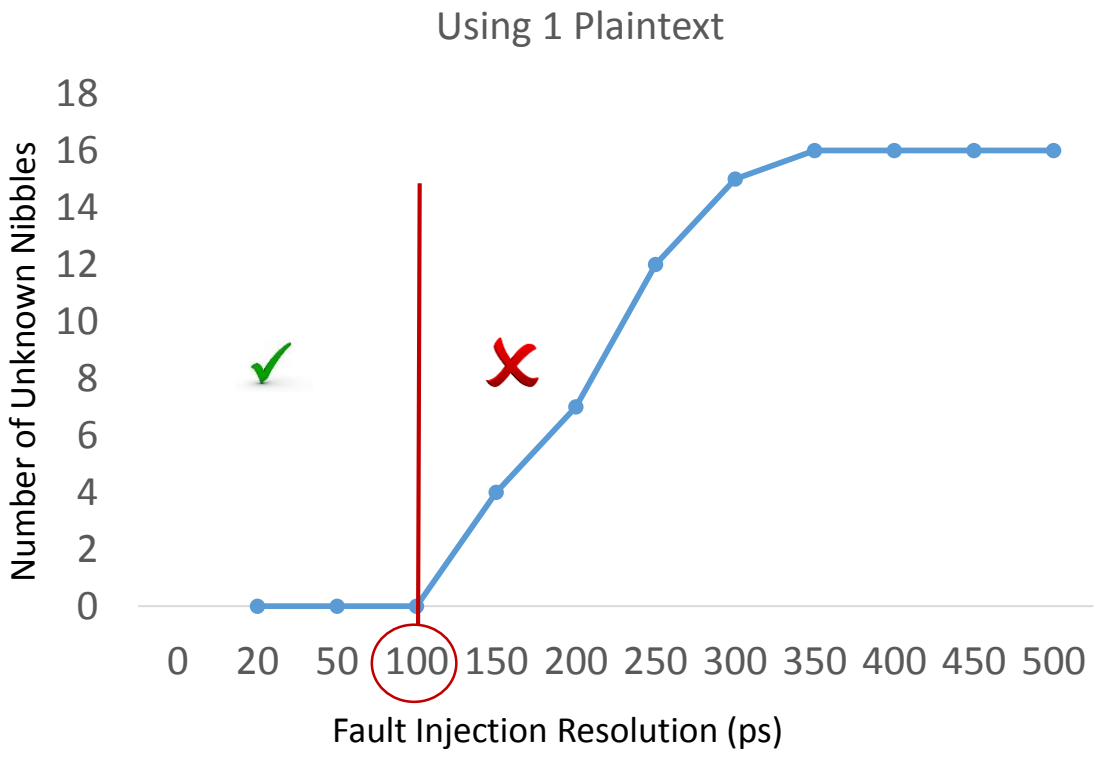
DFIA is FEASIBLE on PRESENT (and LED)

Outline

1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
    - Differential Fault Intensity Analysis (DFIA)
    - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

Fault Injection Resolution - Problem

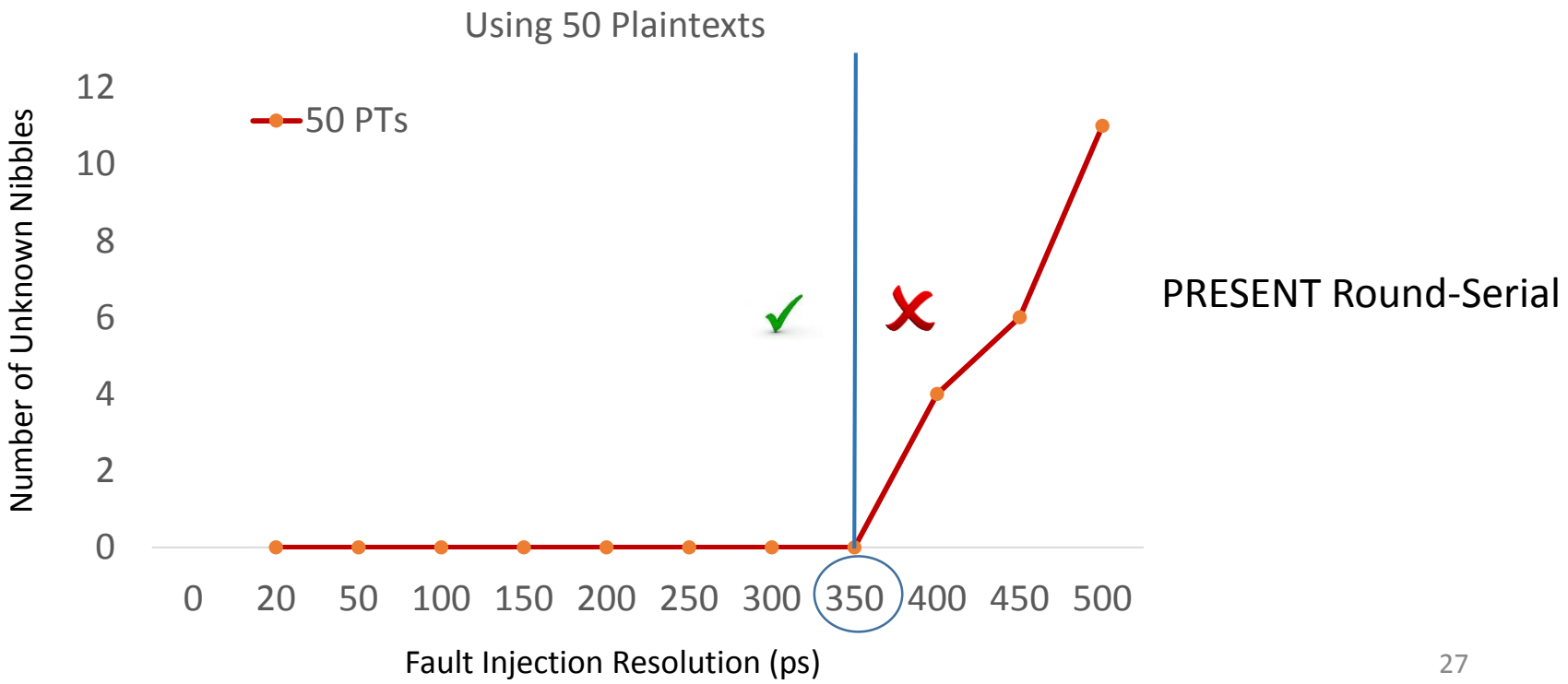
- Does DFIA work with low-resolution fault injection equipment?
  - Resolution: Minimum fault intensity step size
  - Some nibbles of the key cannot be fully retrieved if we use 1 plaintext.



PRESENT Round-Serial

Fault Injection Resolution - Solution

- DFIA still works with low-resolution fault injection equipment:
- Solution:
  - Repeat DFIA steps for different plaintexts $\{P_1, P_2, \ldots, P_m\}$ until finding a unique key



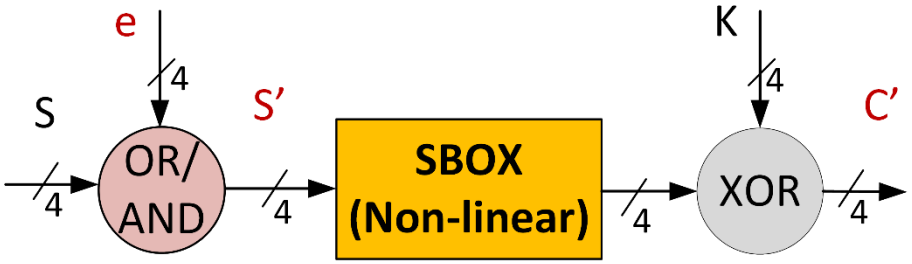
Outline

1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
    - Differential Fault Intensity Analysis (DFIA)
    - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

Related Work – Biased Fault Definitions

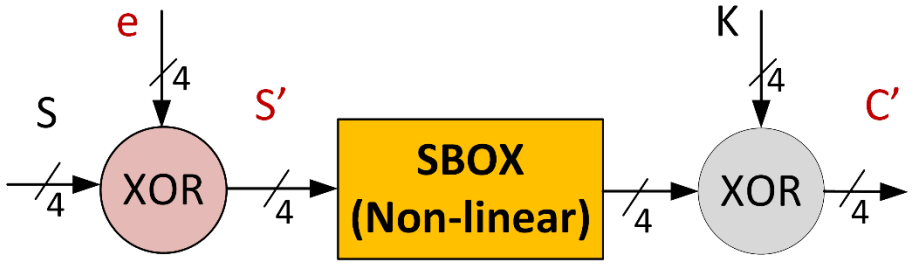
- Biased-Fault-Based Fault Analysis:
  - Non-Uniform Faulty Value Analysis (NUFVA):
    [Fuhr et al. FDTC'13, De Santis et al. LightSec'14, and Li et al. FPS'13]
  - Non-Uniform Error Value Analysis (NUEVA):
    [Lashermes et al. FDTC'12]

NUFVA



e: uniform
S': non-uniform (some values occur more than others)
C': non-uniform (some values occur more than others)

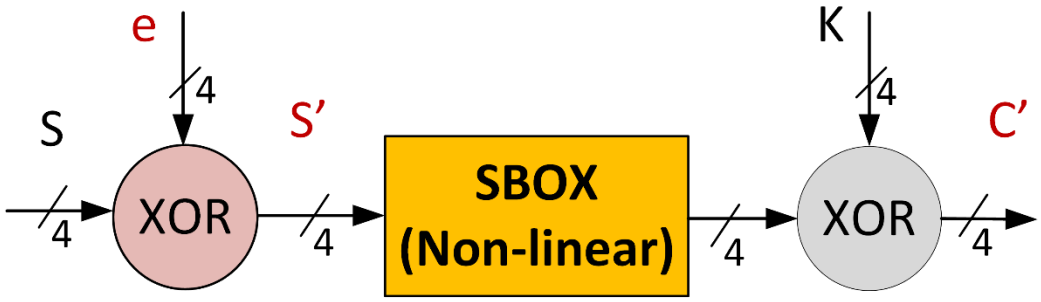
NUEVA



e: non-uniform (some values occur more than others)
S': non-uniform (some values occur more than others)
C': no assumption

Related Work – DFIA vs. NUFVA, NUEVA

- DFIA does not make any assumptions on the biased value of faulty states or ciphertexts.



e: non-uniform (successive values are close to each other)
S': non-uniform (successive values are close to each other)
C': no assumption

- DFIA provides a cheap and general methodology to control the induced faults.

Outline

1. Fault Attack Requirements
2. Biased Faults
3. Exploiting Biased Faults:
    - Differential Fault Intensity Analysis (DFIA)
    - Results for PRESENT
4. Fault Injection Resolution and DFIA
5. Related Work
6. Conclusion

Conclusion

- DFIA provides
  - a feasible (cheap, general) biased fault model
  - a DPA-like fault analysis methodology
- DFIA is feasible on LED and PRESENT.
- DFIA still works with lower-capability fault injection equipment.

Thank you!