Differential Fault Intensity Analysis

N. F. Ghalaty, B. Yuce, M. Taha, P. Schaumont

ECE Department
Virginia Tech

FDTC 2014

This research was supported in part by NSF Grant 1441710

Outline

1. **DFIA vs DFA?**
2. **Explaining Biased Faults**
3. **An Attack Based on Fault Bias**
4. **Experiments**
   - **Fault Bias Exists**
   - **DFIA Demonstration**
5. **Related Work and Conclusions**

Differential Fault Analysis (DFA)

Cryptographic Algorithm ➡ **Fault Model** { *Random Byte*, *Random Bit*, *Chosen Bit* } ➡ **DFA**

C, C', C'', .. → K

Implementations and Actual Faults

Cryptographic Algorithm ➡ **Fault Model**
- *Random Byte*
- *Random Bit*
- *Chosen Bit*

➡ **DFA**: C, C’, C’’, .. → K

Implementation / **Fault Injection**

Cryptographic Architecture ➡ **Fault**
- *Fault Bias*
- *1-bit, 2-bit, ..*

Differential Fault Intensity Analysis (DFIA)

Cryptographic Algorithm ➡ **Fault Model**

Random Byte
Random Bit
Chosen Bit

➡ **DFA**
C, C’, C’’, .. → K

Implementation

Fault Injection

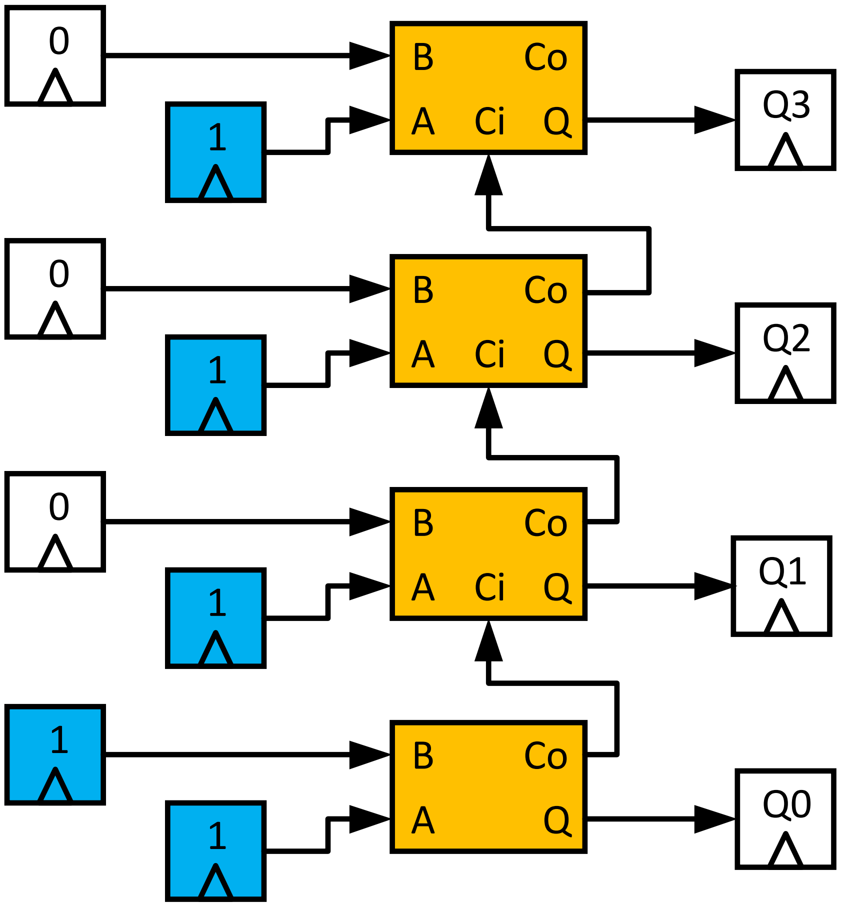
Variable Fault Intensity

Cryptographic Architecture ➡ **Fault**

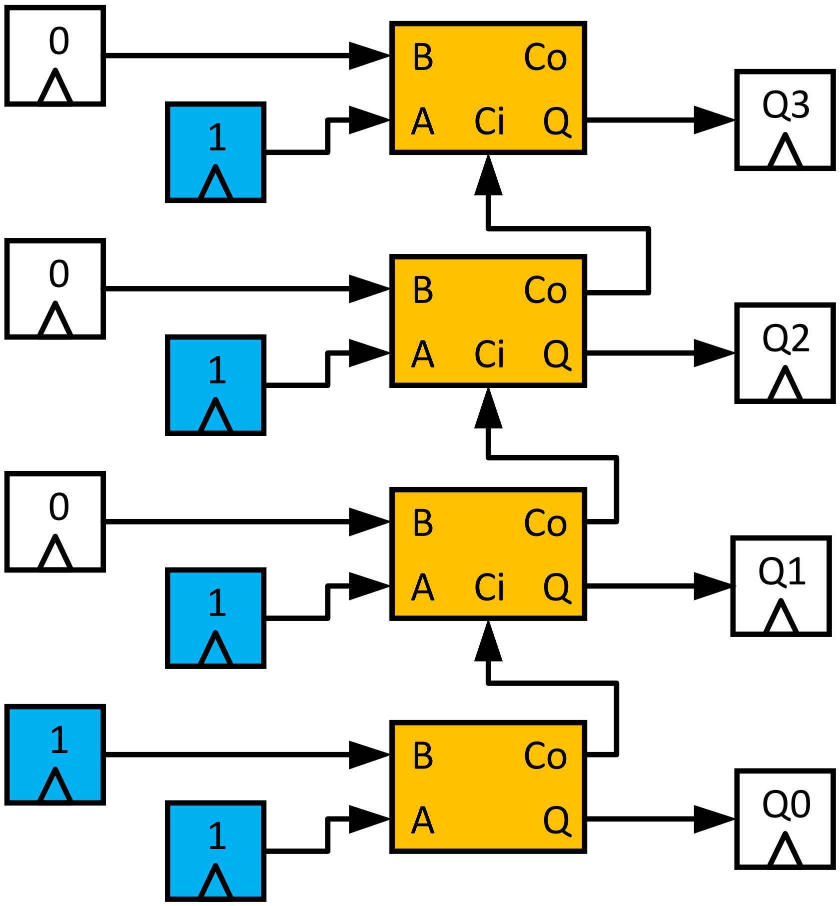
Fault Bias
1-bit, 2-bit, ..

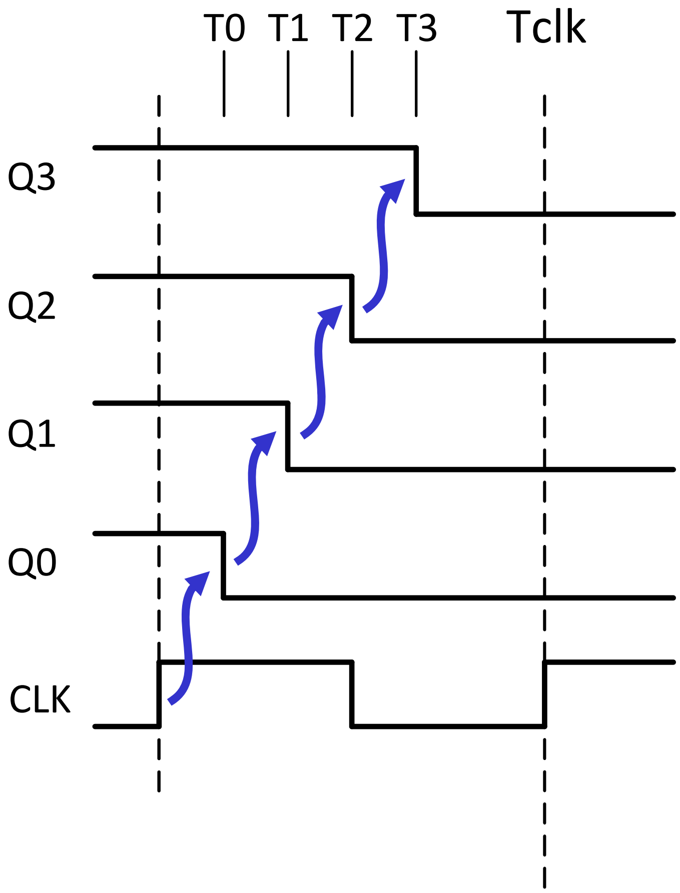
➡ **DFIA**
C, C_1’, C_2’, .. → K

Where do Biased Faults come from?

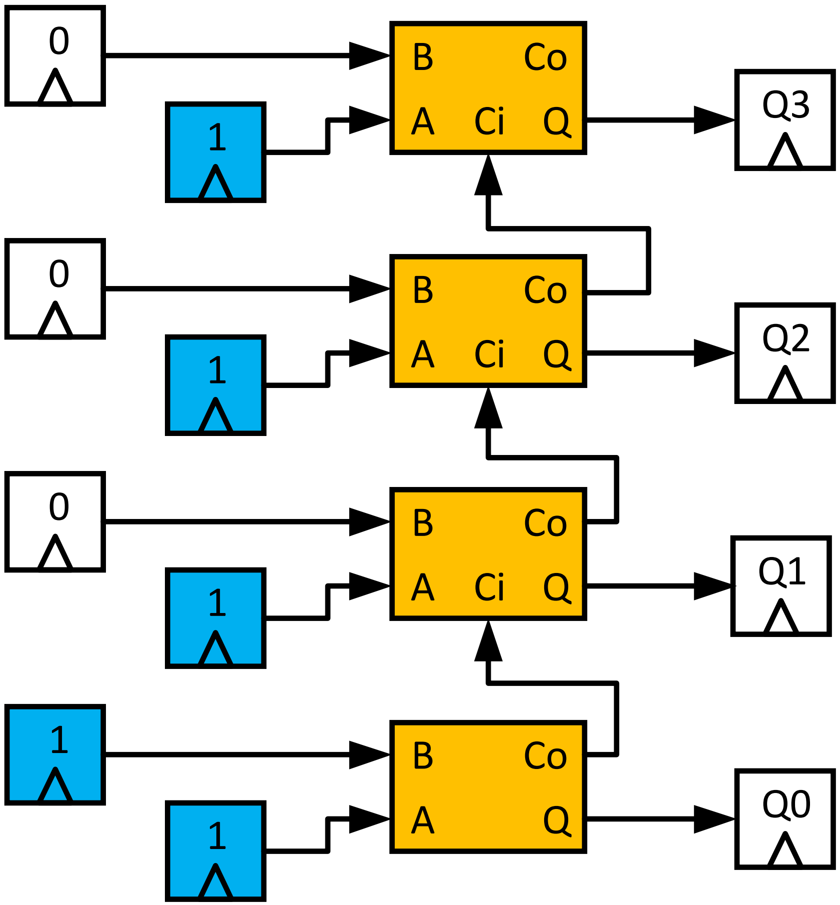


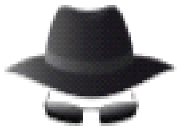
Where do Biased Faults come from?



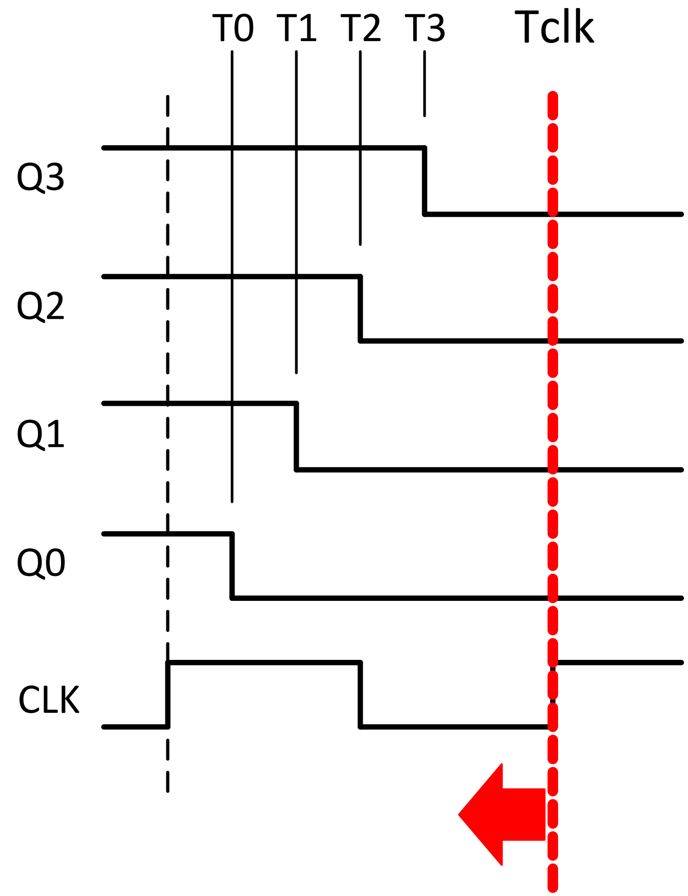


Where do Biased Faults come from?



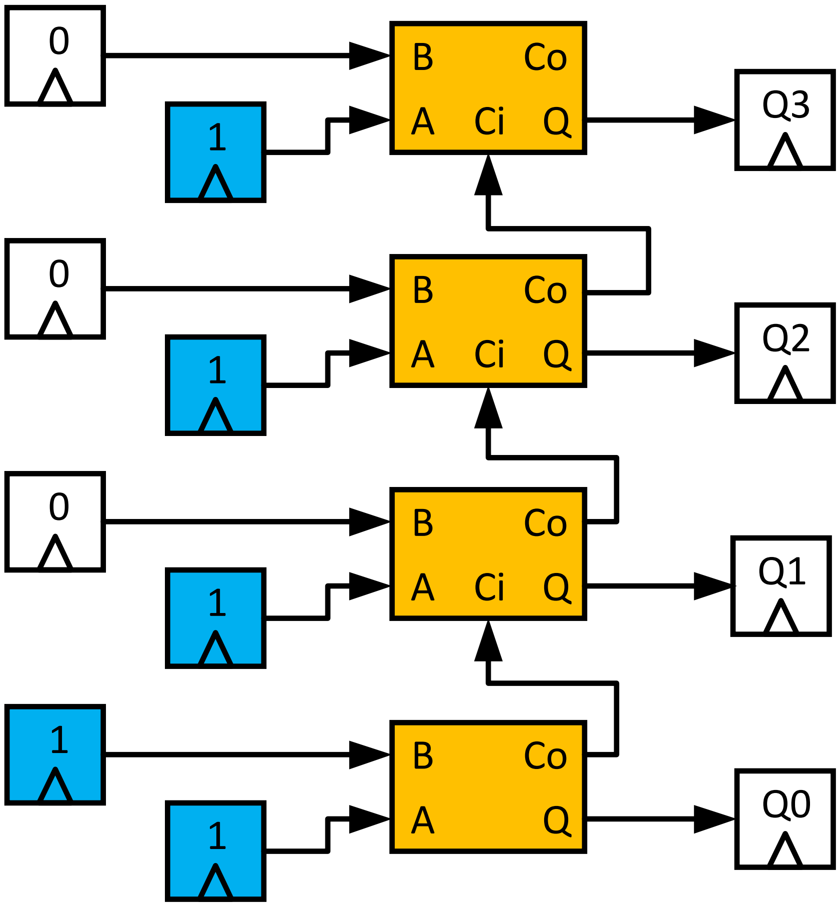


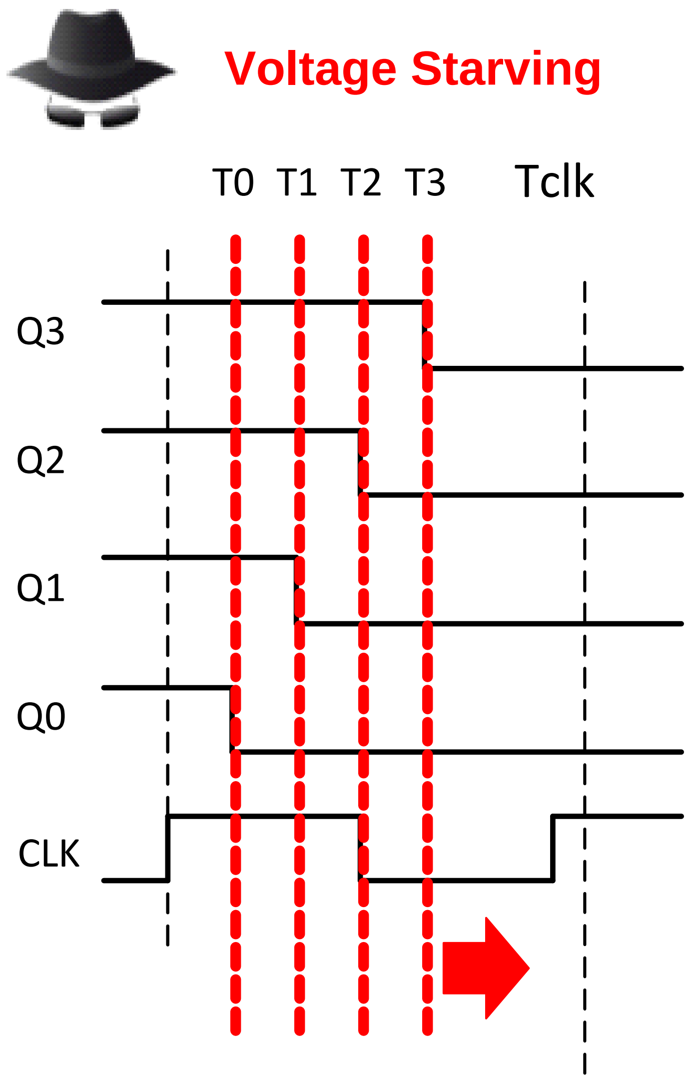
Clock Glitching



$P_{fault}(Q3) > P_{fault}(Q2) > P_{fault}(Q1) > P_{fault}(Q0)$

Where do Biased Faults come from?



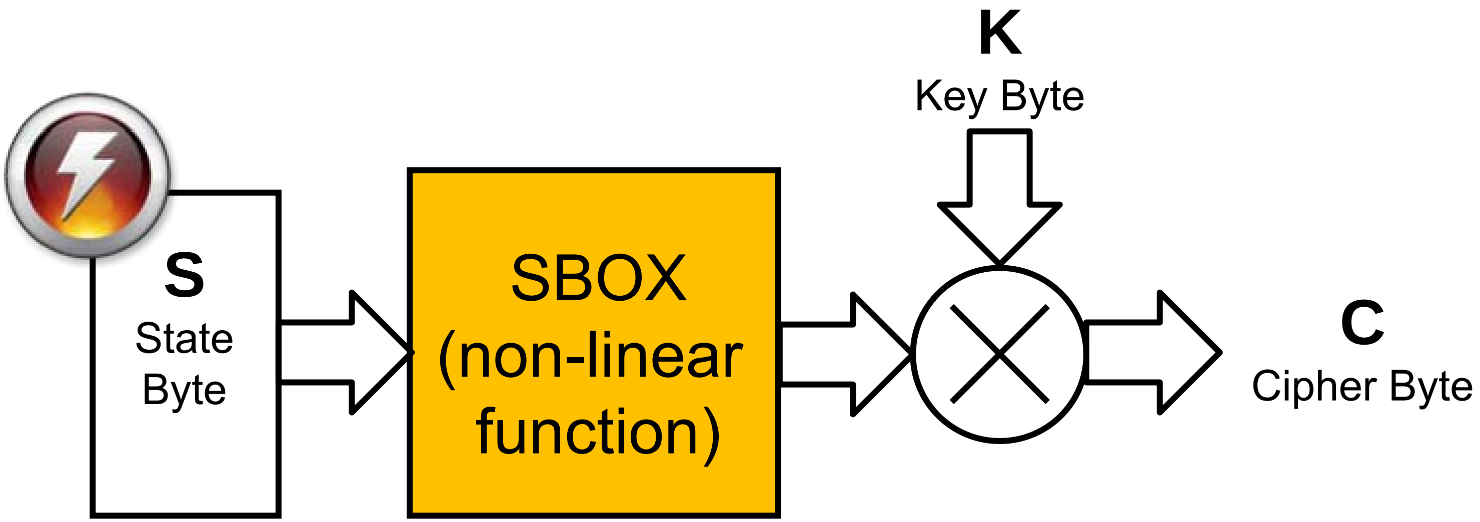


$P_{fault}(Q3) > P_{fault}(Q2) > P_{fault}(Q1) > P_{fault}(Q0)$

Biased Faults

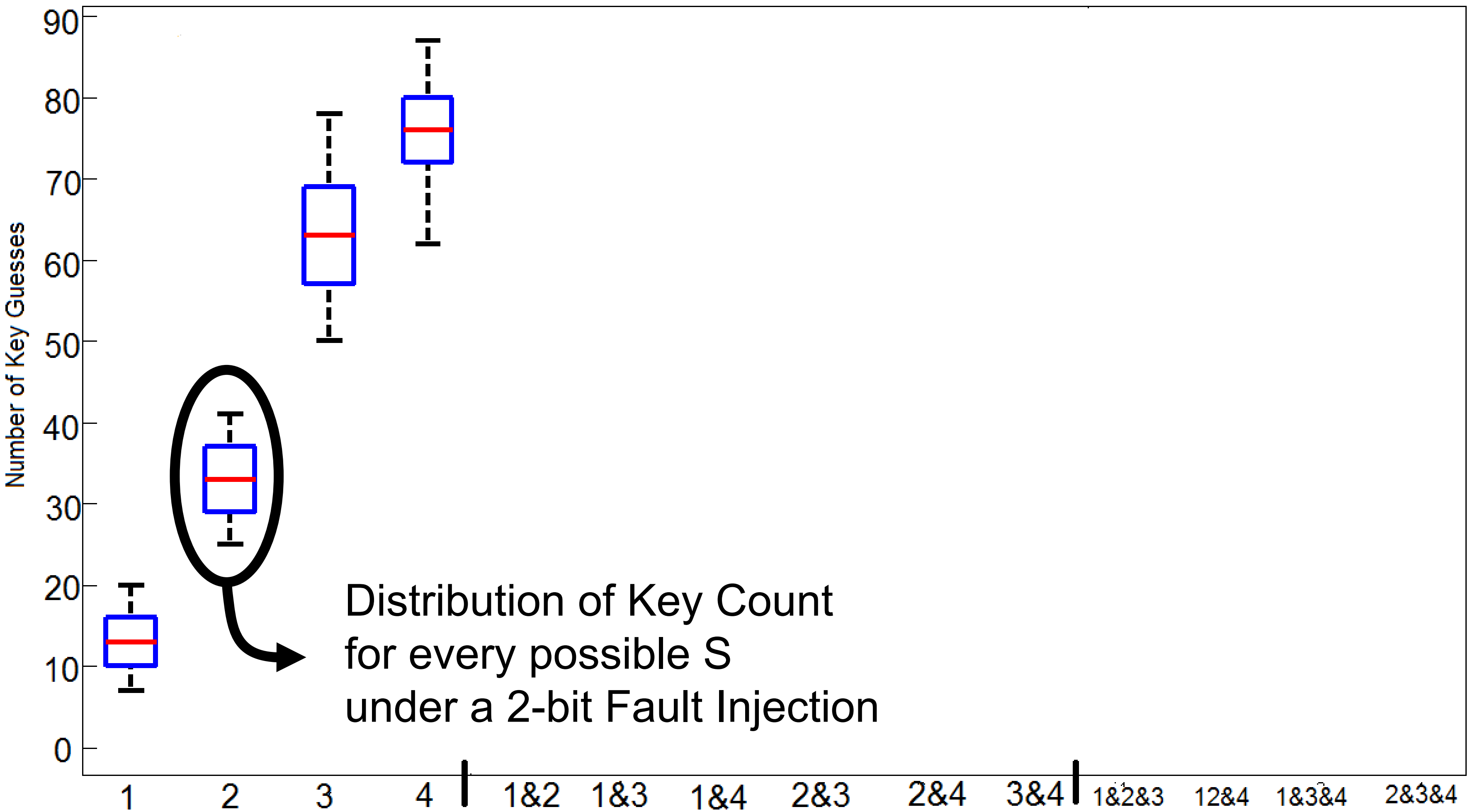
- **Non-uniform propagation time results in non-uniform fault response.**
- **Varying Fault Intensity [Li 2010] will trigger non-uniform faults. We call this Fault Bias.**
- **Fault Bias is the basis of DFIA.**

Using Biased Faults for Cryptanalysis

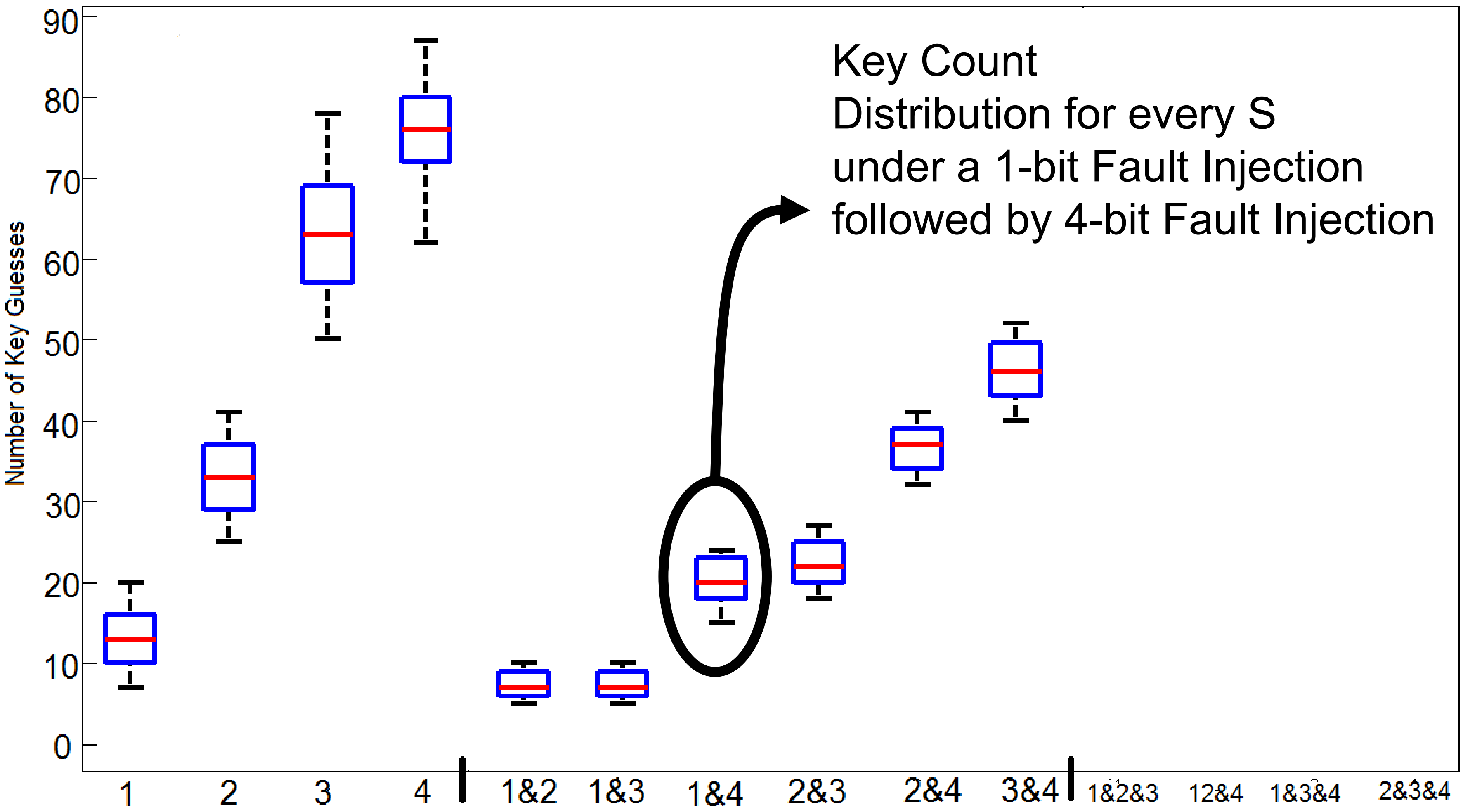


Given: C, C’ for a given fault bias B (1-bit, 2-bit, ...)
Find: number of keys that result in a solution for
C’ = SBOX(S’) xor K, C = SBOX(S) xor K
for all S, S’ where HD(S, S’) <= B

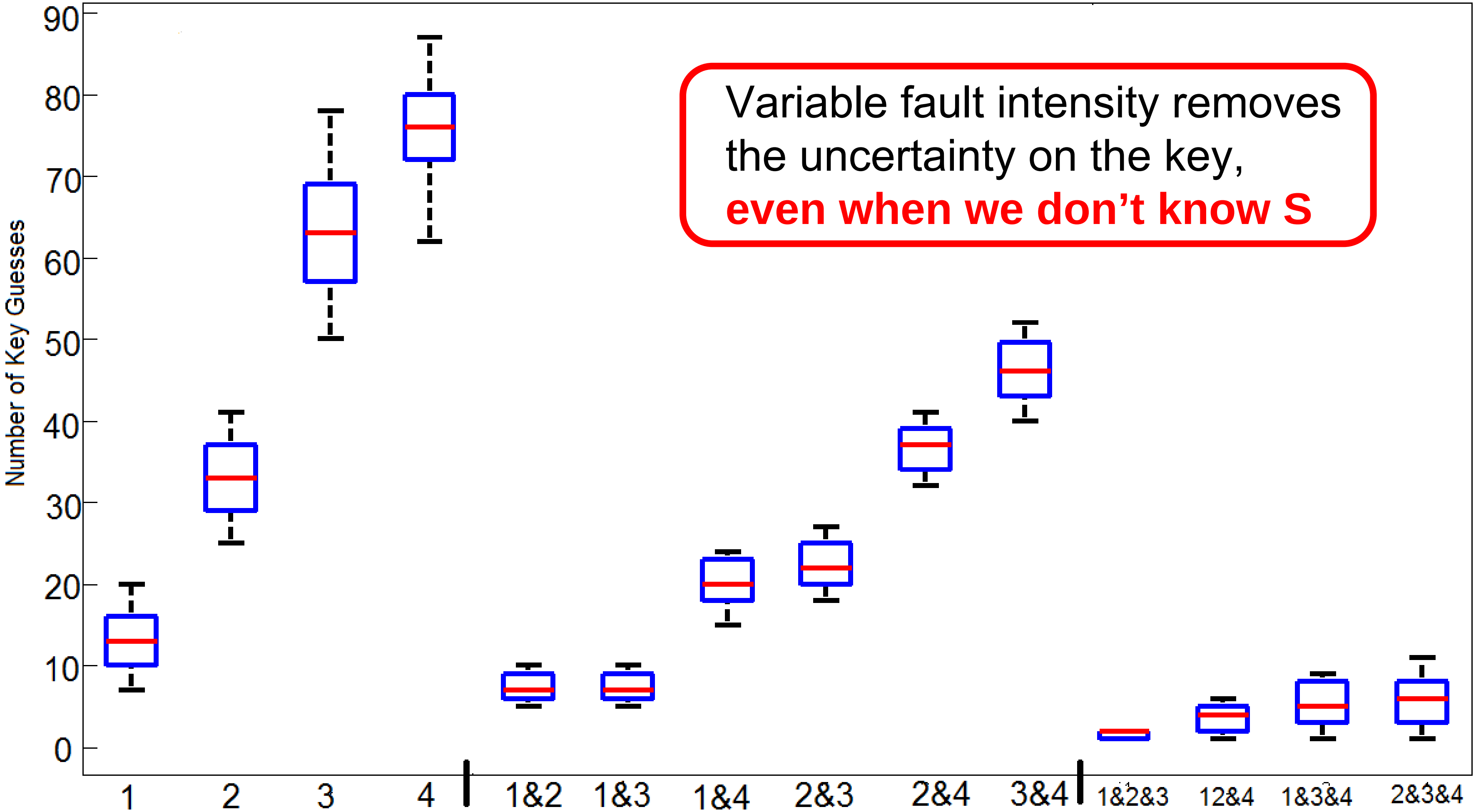
Key uncertainty for **single** biased fault



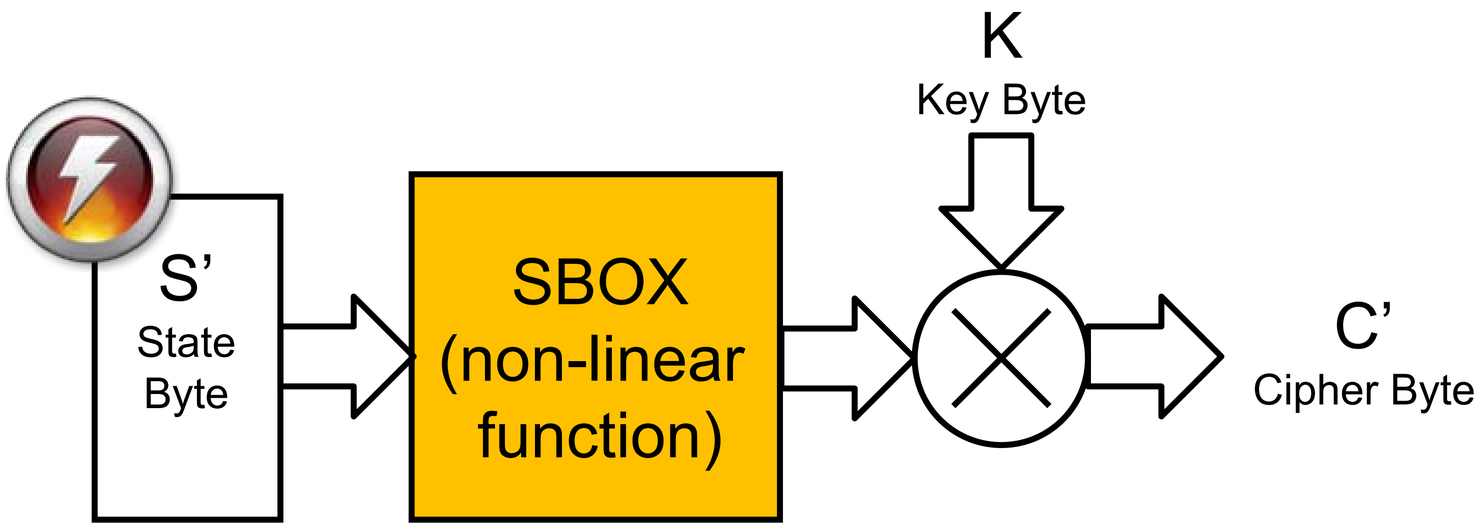
Key uncertainty for **dual** biased fault



Key uncertainty for **triple** biased fault



Hypothesis Test with Biased Faults



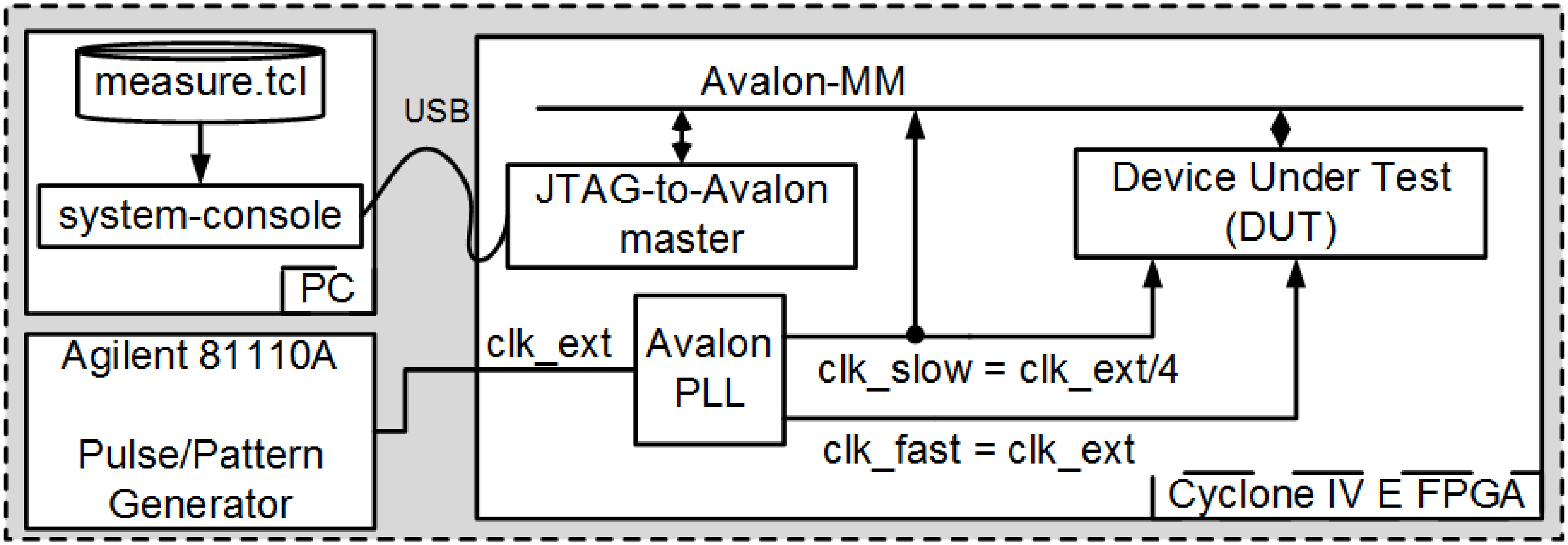
Given: C, C' for a known fault bias B
Find: most likely key byte K

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

Accumulate $\rho_{\tilde{K}} = \Sigma(HD(S', S))$

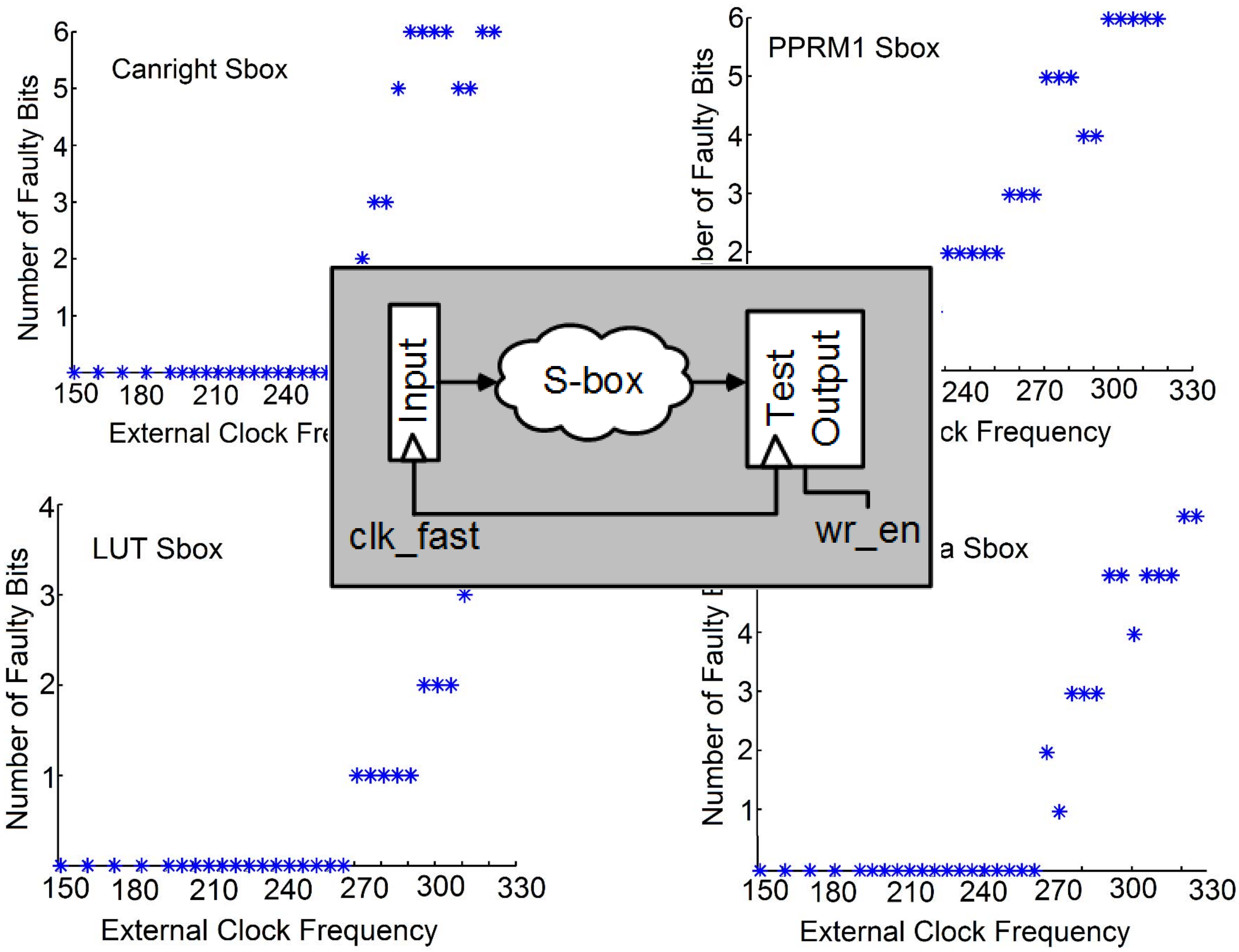
Select K = argmin ρ

Experimental Setup

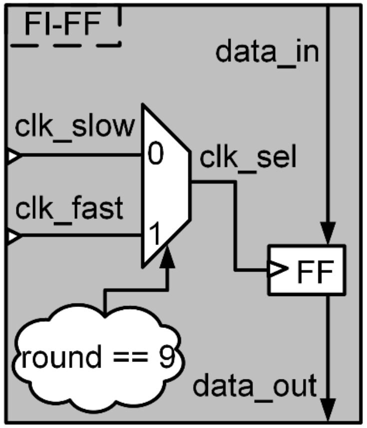


- **FPGA: Altera Cyclone IV (DE2-115)**
- **Agilent 81110A Pulse/Pattern Generator**

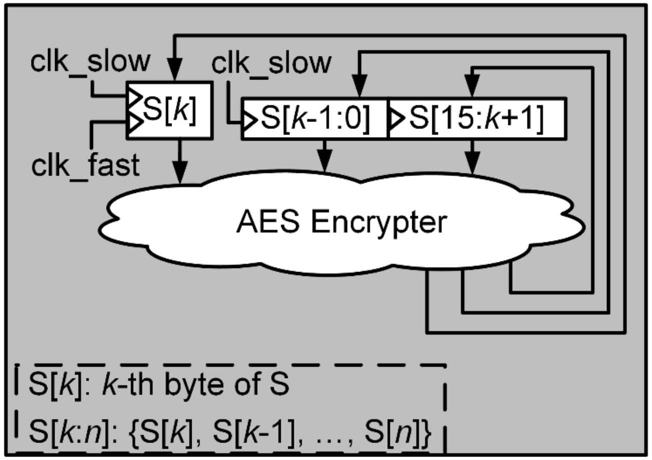
Biased Fault Behavior for Sbox



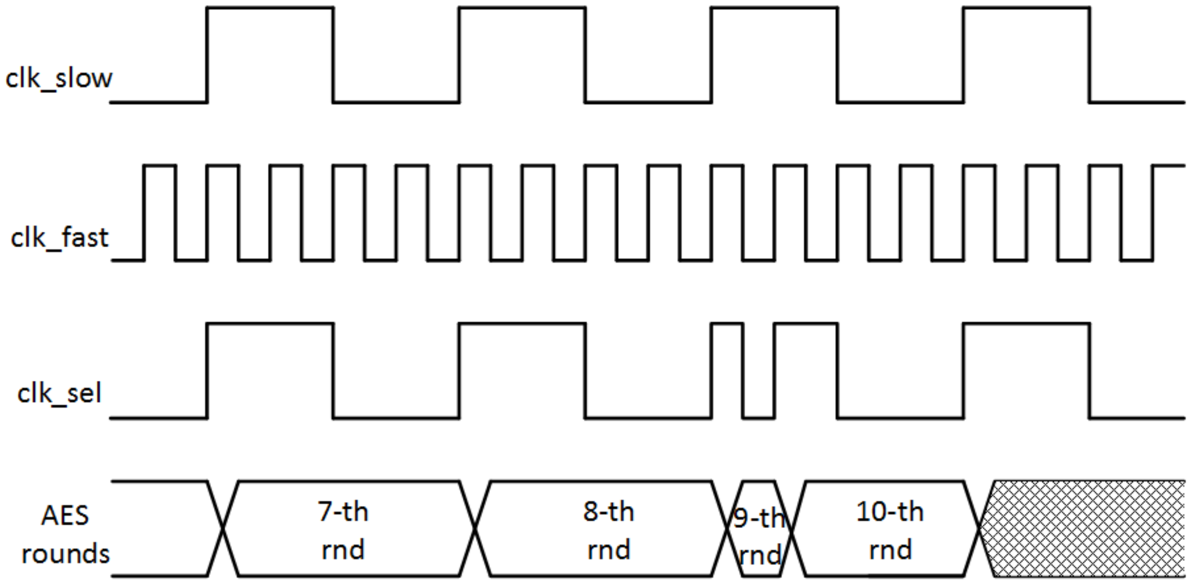
Experimental Setup for AES



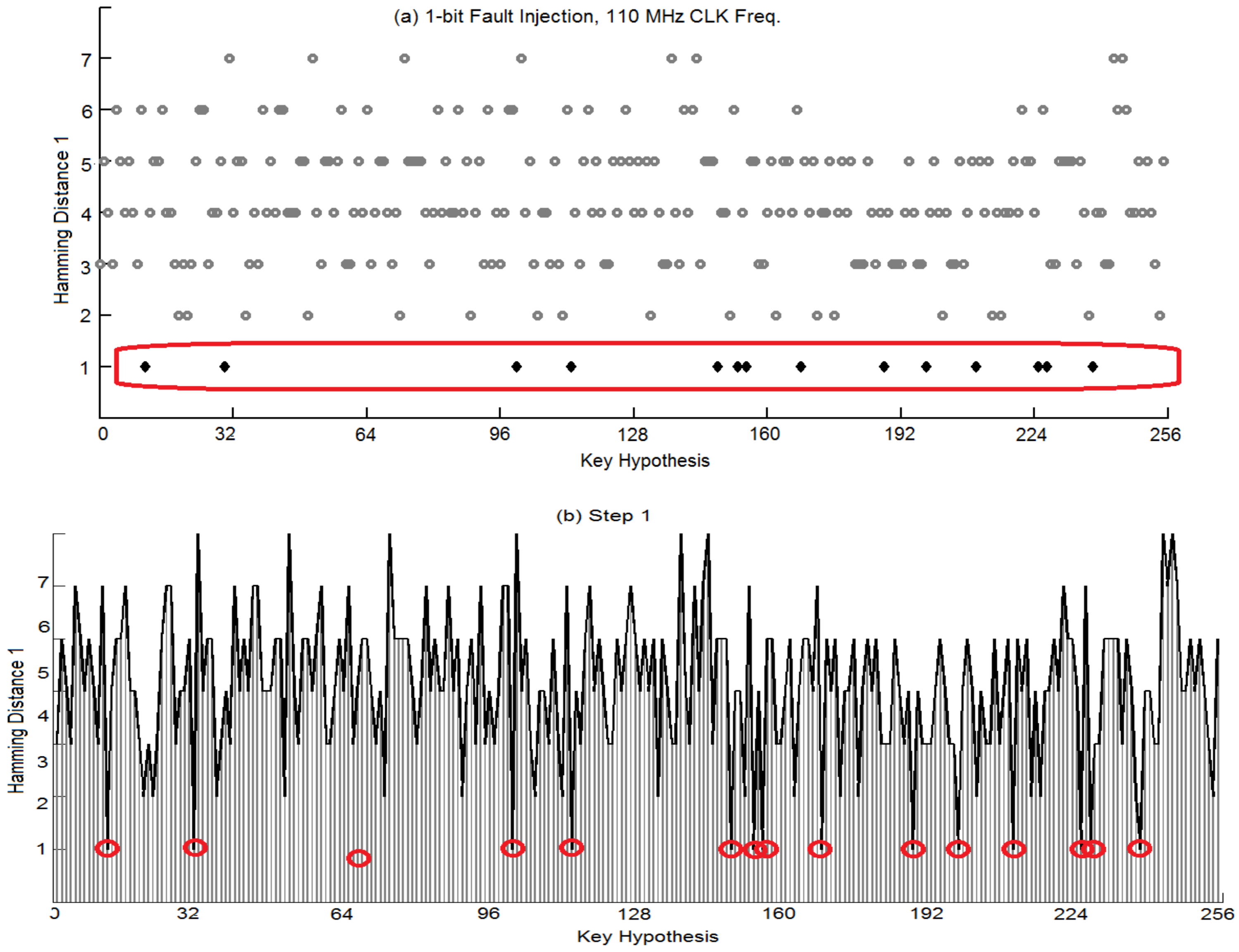
(a)



(b)

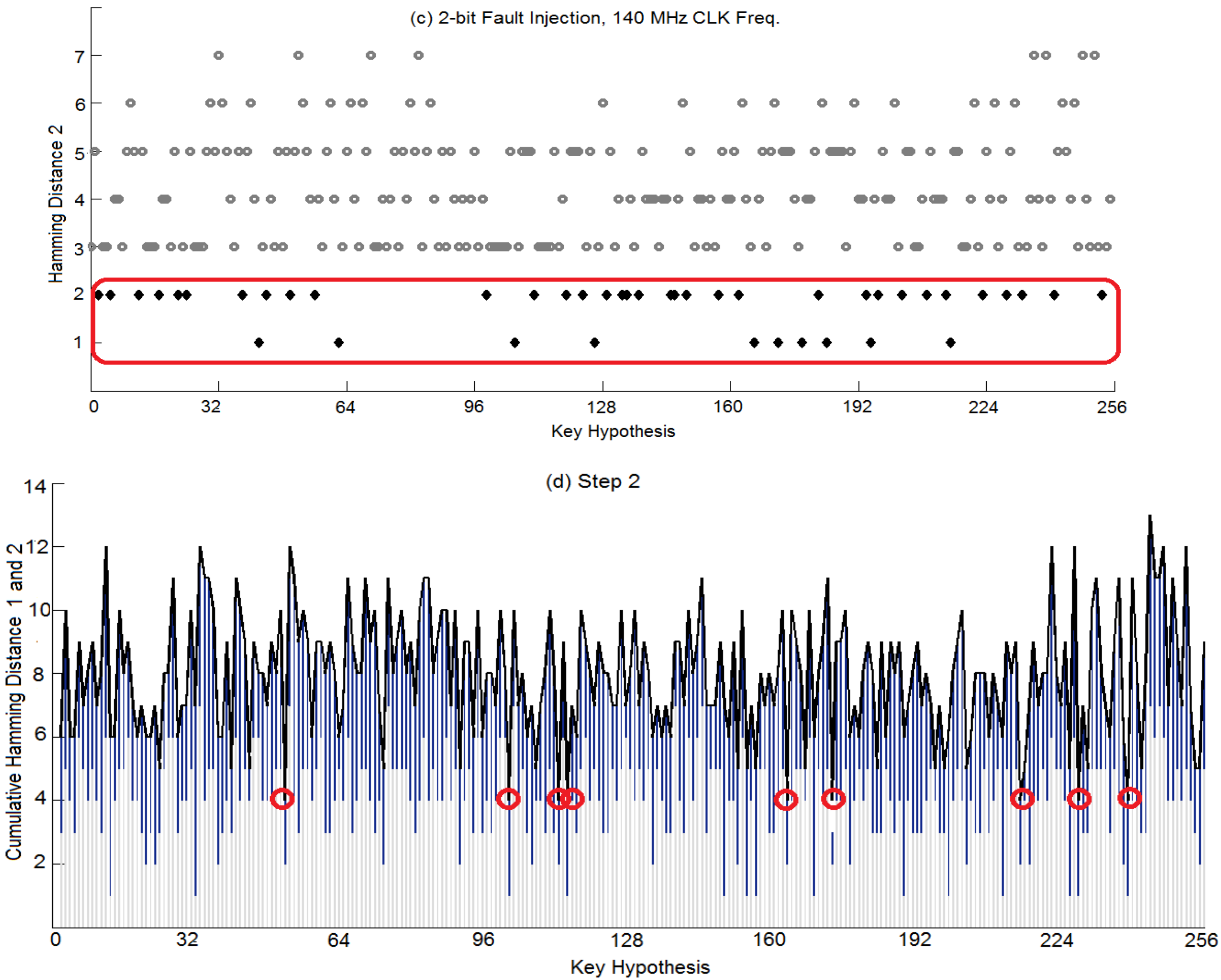


DFIA on AES

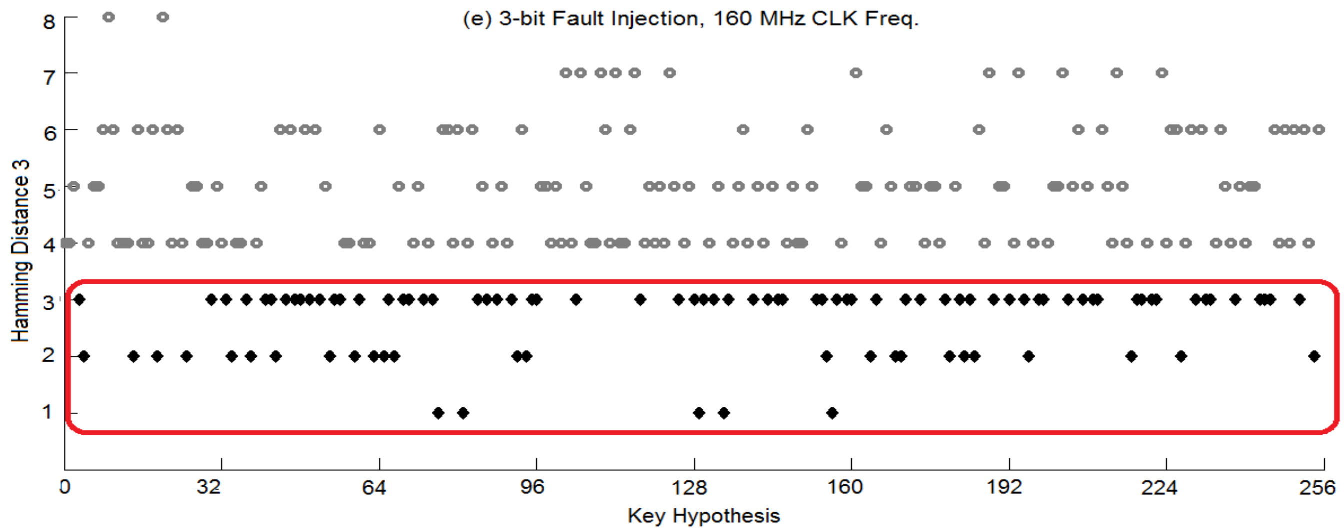


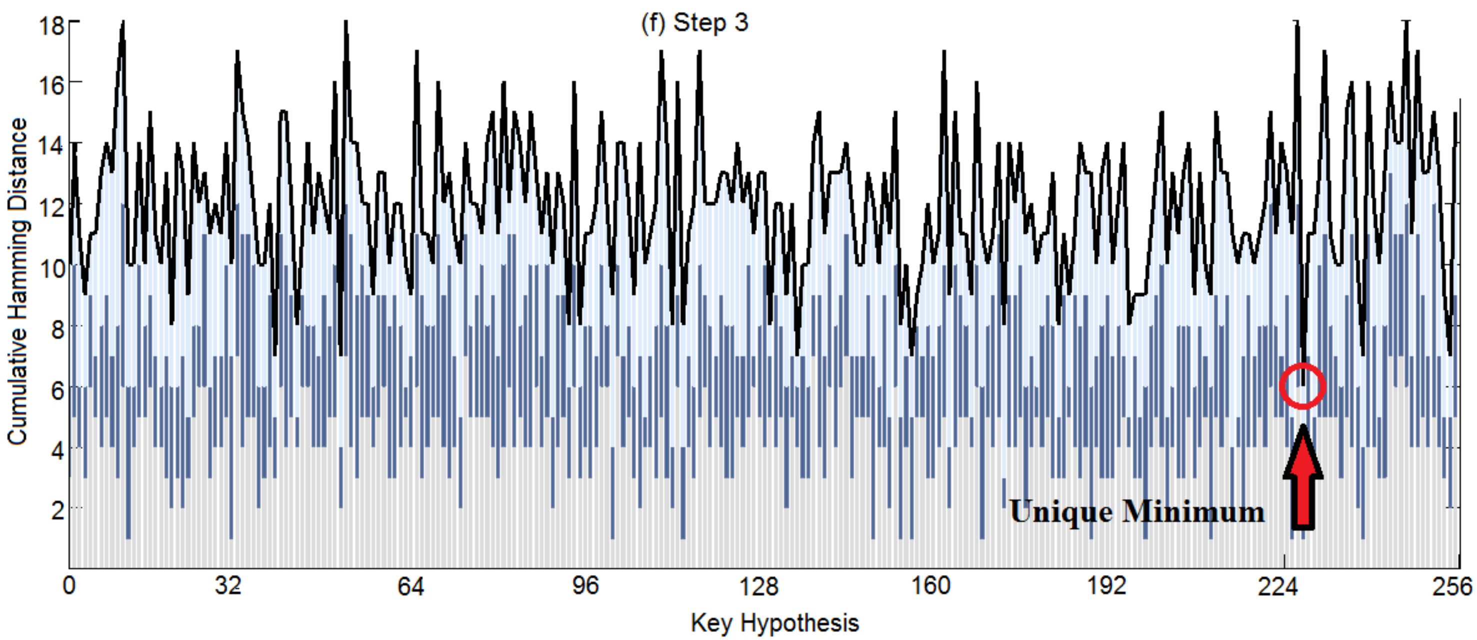
(a) 1-bit Fault Injection, 110 MHz CLK Freq.
Hamming Distance 1
1
2
3
4
5
6
7
0
32
64
96
128
160
192
224
256
Key Hypothesis
(b) Step 1
Hamming Distance 1
1
2
3
4
5
6
7
0
32
64
96
128
160
192
224
256
Key Hypothesis

DFIA Steps on AES



DFIA Steps on AES





DFIA Results on AES

- **AES DFIA when injecting a single-byte fault in round 9**
  - **4.6 fault injections to retrieve 1 key byte (90 exp)**
  - **68 fault injections to retrieve all key bytes (3 exp)**
- **AES DFIA when injecting multiple single-byte faults in round 9**
  - **Fault analysis at 24 clock frequencies between 100MHz and 330 MHz**
  - **7 fault injections to retrieve AES key (1 exp)**

Related Work

- **DFIA is similar to DPA, uses fault bias as a source of side-channel leakage**
- **Unlike FSA [Li], DFIA does not require data dependency on fault sensitivity. It uses fault bias and associated differential effects.**
- **Several recent attacks [Fuhr FDTC 13, deSantis LightSec 14] use bias on the faulty state.**
  - **DFIA does not require bias in the faulty state.**
  - **DFIA is experimentally demonstrated.**

Conclusions

- **DFIA requires slightly more faults than some other round-9 fault attacks**
- **On the other hand, DFIA only uses a loose fault injection requirement, and assumes only the presence of fault bias**

- **Future efforts:**
  - **Apply DFIA to other Algorithms**
  - **Apply DFIA to Software Platforms**
  - **DFIA Countermeasures**