Differential Fault Intensity Analysis

N. F. Ghalaty, B. Yuce, M. Taha, P. Schaumont
ECE Department
Virginia Tech
FDYC 2014

This research was supported in part by NSF Grant 1441710
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 $\rightarrow$ Fault Model $\rightarrow$ DFA

Fault Model:
- Random Byte
- Random Bit
- Chosen Bit

$C, C', C'', .. \rightarrow K$
Implementations and Actual Faults

Cryptographic Algorithm \rightarrow \text{Fault Model} \begin{cases} \text{Random Byte} \\ \text{Random Bit} \\ \text{Chosen Bit} \end{cases} \rightarrow \text{DFA} \\
C, C', C'', \ldots \rightarrow K

Implementation \rightarrow \text{Fault Injection}

Cryptographic Architecture \rightarrow \text{Fault} \begin{cases} \text{Fault Bias} \\ 1\text{-bit}, 2\text{-bit}, \ldots \end{cases}
Differential Fault Intensity Analysis (DFIA)

Cryptographic Algorithm → Fault Model

\[
\text{Random Byte} \quad \text{Random Bit} \quad \text{Chosen Bit}
\]

Implementation → Fault Injection

\[
\text{Fault Bias} \quad 1\text{-bit, 2\text{-bit,}..}
\]

Cryptographic Architecture → Fault

\[
\text{DFIA} \quad C, C', C'', .. \rightarrow K
\]

\[
\text{DFA} \quad C, C', C'', .. \rightarrow K
\]

Variable Fault Intensity
Where do Biased Faults come from?
Where do Biased Faults come from?
Where do Biased Faults come from?

Clock Glitching

\[ P_{\text{fault}}(Q3) > P_{\text{fault}}(Q2) > P_{\text{fault}}(Q1) > P_{\text{fault}}(Q0) \]
Where do Biased Faults come from?

Voltage Starving

\[ P_{\text{fault}}(Q3) > P_{\text{fault}}(Q2) > P_{\text{fault}}(Q1) > P_{\text{fault}}(Q0) \]
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.
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

Distribution of Key Count for every possible $S$ under a 2-bit Fault Injection
Key uncertainty for **dual** biased fault

Key Count Distribution for every S under a 1-bit Fault Injection followed by 4-bit Fault Injection
Key uncertainty for **triple** biased fault

Variable fault intensity removes the uncertainty on the key, even when we don’t know S.
Given: C, C’ for a known fault bias B
Find: most likely key byte K

For all \( \tilde{K} \), find \( S' = SBOX^{-1}(C' \ xor \ \tilde{K}) \)
Accumulate \( \rho_{\tilde{K}} = \sum (HD(S', S)) \)
Select \( K = \text{argmin} \rho \)
• FPGA: Altera Cyclone IV (DE2-115)
• Agilent 81110A Pulse/Pattern Generator
Biased Fault Behavior for Sbox

[Diagram showing scatter plots for Canright Sbox and LUT Sbox with number of faulty bits against external clock frequency.]
Experimental Setup for AES

(a) FI-FF

(b) AES Encrypter

- clk_slow
- clk_fast
- clk_sel
- data_in
- data_out
- round == 9
- S[k]: k-th byte of S
- S[k:n]: {S[k], S[k-1], ..., S[n]}
DFIA on AES

(a) 1-bit Fault Injection, 110 MHz CLK Freq.

(b) Step 1
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)
• 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