From physical stresses to timing constraints violation

ZUSSA Loïc,
DUTERTRE Jean-Max,
CLEDIERE Jessy,
TRIA Assia
Research subject

• Characterization and analysis of common fault injection mechanism

Today’s subject

• Power glitches as a fault injection mechanism
  Analysis and practice
Agenda

- Timing constraints of synchronous digital IC
- Static stresses (global effect)
- Transient stresses
- Conclusion
Timing constraints

Upstream

Downstream

\[ T_{\text{clk}} + T_{\text{skew}} - \delta_{\text{su}} \]

Data arrival time:
\[ D_{\text{clk}\rightarrow Q} + D_{\text{pMax}} \]

Data required time:
\[ T_{\text{clk}} + T_{\text{skew}} - \delta_{\text{su}} \]

\[ T_{\text{clk}} > D_{\text{clk}\rightarrow Q} + D_{\text{pMax}} - T_{\text{skew}} + \delta_{\text{su}} \]
How to inject faults through timing constraints violation?

- Overclocking: (Frequency increase, i.e. period decrease)

\[ T_{clk} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su} \]

- Underpowering or overheating: (Propagation time increase)

\[ T_{clk} < D_{clk \rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su} \]
Target

- Platform: FPGA Spartan 3A
- Algorithm: AES 128 bit
  none-secure implementation
- Frequency: 100 MHz
- Power supply: 1.2V
Common fault injection means

- Clock stress (overclocking)
- Power stress (underpowering)
- Overheating

A common mechanism!

Experimental proof

- 10,000 input dataset
- Critical path faulted

⇒ Timing constraints violations.
Transient perturbations

- Clock glitch
- Power supply glitch

Questions

- Injection mechanism? Timing violation?
- Achievable resolution?
Clock glitch

• 35ps resolution
• Global effect
• Timing constraints violation (obvious)
• A tool for critical time measurement
• Used to build a template/reference library

To be compared.
Power glitch: Ideal
Power glitch: Ideal
Power glitch: capacitances

\[ V_{\text{core}} \ (V) \]

(a) expected  
(b) injected

\[ 10\text{ns} \]

\[ 80\text{ns} \]
Power glitch: impedance adaptation
Power glitch: capacitances
Transient perturbations

Spartan 3A
Power glitch: impedance adaptation
Power glitch
Power glitch

- Target a specific round but **also affect the neighboring rounds**
Power glitch

- Target a specific round but **also affect the neighboring rounds**

- Global offset must be added.
Power glitch

- When a specific round is targeted.
- Monobit fault during the targeted round 90% of the time.
Power glitch

- When a specific round is targeted.
- Monobit fault during the targeted round 80% of the time.
Power glitch

BUT 20% of the time the fault appear during a neighboring round.
Power glitch

• Analysis of injected faults:
  70% identical to clock glitch injection
  20% neighboring rounds
  10% the second most critical path of the round

• **Conclusion**: Clock and power glitch induced faults are due to timing constraints violation

• >90% single-bit fault
Power glitch

- Analysis of injected faults:
  70% identical to clock glitch injection
  20% neighboring rounds
  10% the second most critical path of the round

- Conclusion: Clock and power glitch induced faults are due to timing constraints violation

- >90% single-bit fault

A spatial effect component?
Linked to voltage transient propagation through the power supply grid
Most Critical Path (MCP)

D_{pMax} increasing \equiv T_{clk} decreasing

Clock glitch
FPGA + AES + Countermeasure

Fpga: spartan 3A

1.2 Volt

100 MHz

CM

AES

FSM

RS-232
1 : detection zone

2 : faulted zone (bit 64 / round 2)