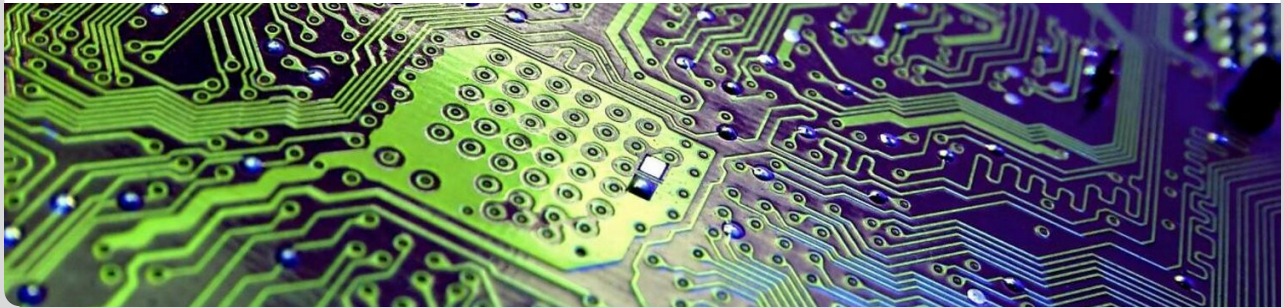
Karlsruhe Institute of Technology

Secure sharing of FPGAs in the Cloud: New Challenges at the Technology Level

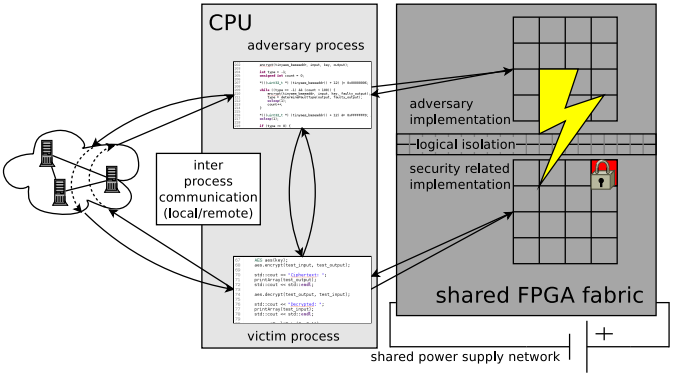
Fall School on Nano-Electronics for Secure Systems 2021

Jonas Krautter, Dennis R. E. Gnad, Mehdi B. Tahoori | 10.11.2021

ITEC – CHAIR OF DEPENDABLE NANO COMPUTING (CDNC)

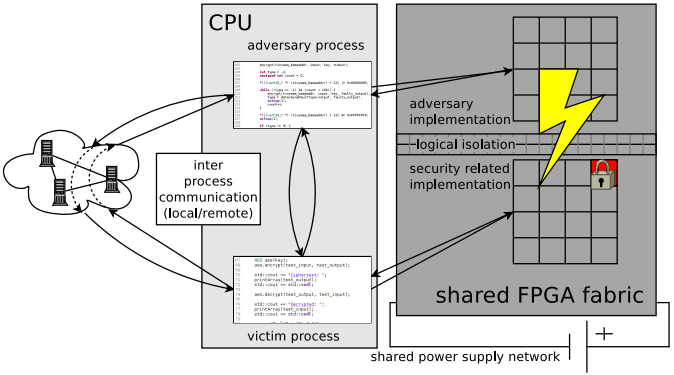


Threat Model



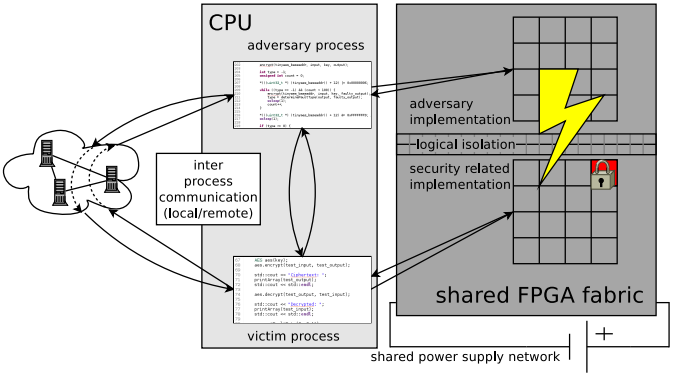
- Attacker and victim design **logically isolated**

Threat Model



- Attacker and victim design **logically isolated**
- Shared FPGA fabric ⇒ **Shared Power Supply Network**

Threat Model



- Attacker and victim design **logically isolated**
- Shared FPGA fabric ⇒ **Shared Power Supply Network**
- ⇒ **Fault attacks** from one design to the other

Related work

Related work

- FPGAs can be crashed with a large amount of Ring Oscillators (ROs)[1]

[1] Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams", FPL 2017

Related work

- FPGAs can be crashed with a large amount of Ring Oscillators (ROs)[1]
- Precise fault attack to recover secret AES keys[2]

[1] Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams", FPL 2017

[2] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

Related work

- FPGAs can be crashed with a large amount of Ring Oscillators (ROs)[1]
- Precise fault attack to recover secret AES keys[2]
- ROs easy to detect (combinational loop)
  $\Rightarrow$ Use other primitives for the attack[3]

[1] Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams", FPL 2017

[2] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

[3] Sugawara et al., "Oscillator without a combinatorial loop and its threat to FPGA in data centre", Electronics Letters 2019

Related work

- FPGAs can be crashed with a large amount of Ring Oscillators (ROs)[1]
- Precise fault attack to recover secret AES keys[2]
- ROs easy to detect (combinational loop)
  $\Rightarrow$ Use other primitives for the attack[3]
- BRAM collisions[4] or AES modules[5] can induce faults in simple logic

[1] Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams", FPL 2017

[2] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

[3] Sugawara et al., "Oscillator without a combinatorial loop and its threat to FPGA in data centre", Electronics Letters 2019

[4] Alam et al., "RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions", FDTC 2019

[5] Provelengios et al., "Power Wasting Circuits for Cloud FPGA Attacks", FPL 2020

Related work

- FPGAs can be crashed with a large amount of Ring Oscillators (ROs)[1]
- Precise fault attack to recover secret AES keys[2]
- ROs easy to detect (combinational loop)
  $\Rightarrow$ Use other primitives for the attack[3]
- BRAM collisions[4] or AES modules[5] can induce faults in simple logic
- Seemingly benign logic can be used to precisely inject faults into AES[6]

[1] Gnad et al., "Voltage drop-based fault attacks on FPGAs using valid bitstreams", FPL 2017

[2] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

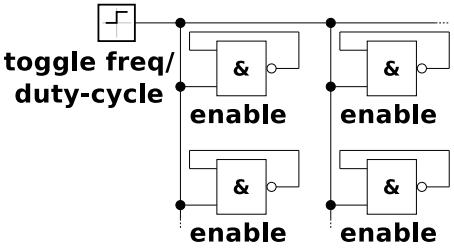
[3] Sugawara et al., "Oscillator without a combinatorial loop and its threat to FPGA in data centre", Electronics Letters 2019

[4] Alam et al., "RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions", FDTC 2019

[5] Provelengios et al., "Power Wasting Circuits for Cloud FPGA Attacks", FPL 2020

[6] Krautter et al., "Remote and Stealthy Fault Attacks on Virtualized FPGAs", DATE 2021

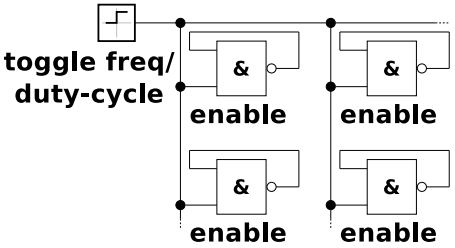
Voltage Virus Logic



- Ring Oscillators (ROs) cause high power consumption[1]

[1] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

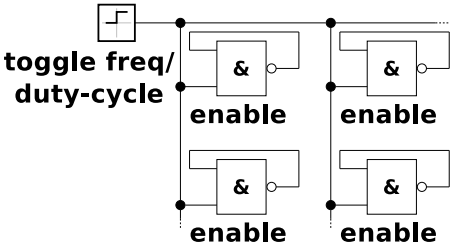
Voltage Virus Logic



- Ring Oscillators (ROs) cause high power consumption[1]
- Gate switching ⇒ Current variation ⇒ Voltage fluctuations

[1] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

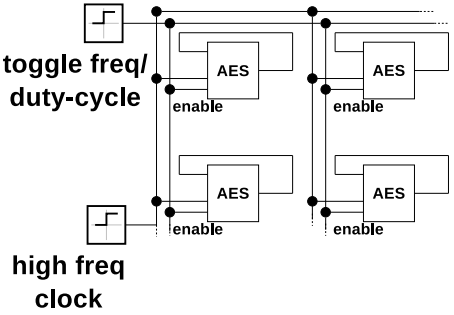
Voltage Virus Logic



- Ring Oscillators (ROs) cause high power consumption[1]
- Gate switching ⇒ Current variation ⇒ Voltage fluctuations
- RO grid additionally toggled in a very specific way

[1] Krautter et al., "FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, suitable for DFA on AES", CHES 2018

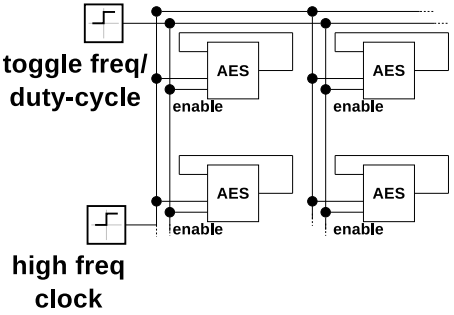
Voltage Virus Logic



- ROs can be detected ⇒ Use instances of non-malicious logic[1]

[1] Krautter et al., "Remote and Stealthy Fault Attacks on Virtualized FPGAs", DATE 2021

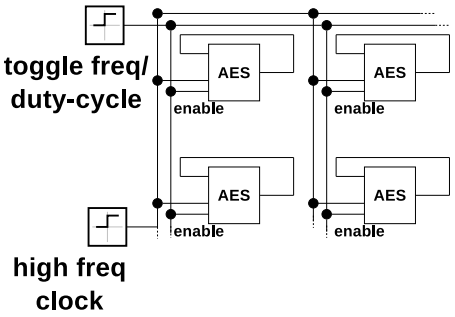
Voltage Virus Logic



- ROs can be detected ⇒ Use instances of non-malicious logic[1]
- Sequential logic driven by a high speed clock

[1] Krautter et al., "Remote and Stealthy Fault Attacks on Virtualized FPGAs", DATE 2021

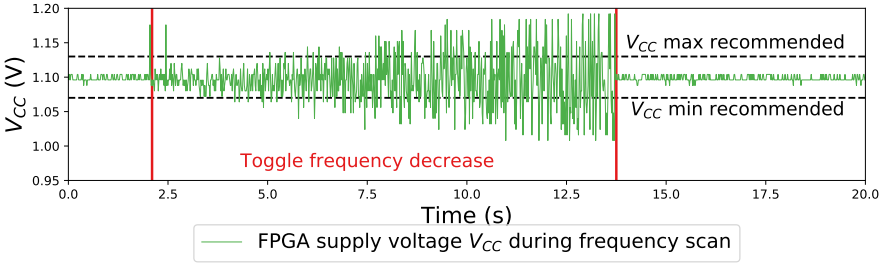
Voltage Virus Logic



- ROs can be detected ⇒ Use instances of non-malicious logic[1]
- Sequential logic driven by a high speed clock
- Again: Common enable signal for synchronized toggling

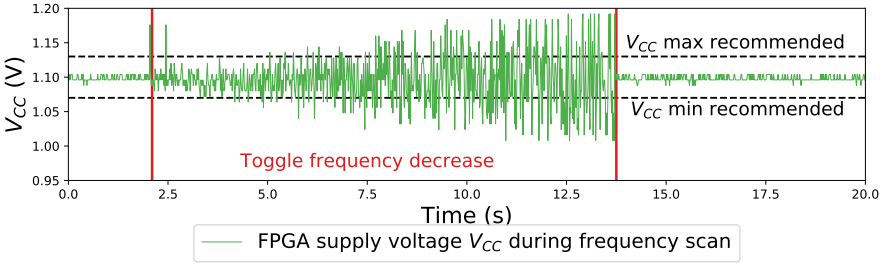
[1] Krautter et al., "Remote and Stealthy Fault Attacks on Virtualized FPGAs", DATE 2021

Voltage Virus Logic



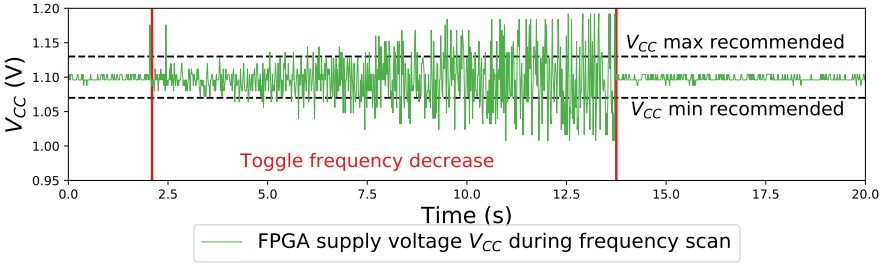
- Toggle signal controls the timing and intensity of the voltage drop

Voltage Virus Logic



- Toggle signal controls the timing and intensity of the voltage drop
- Both frequency and duty-cycle have an impact

Voltage Virus Logic



- Toggle signal controls the timing and intensity of the voltage drop
- Both frequency and duty-cycle have an impact
- $\Rightarrow$ **Calibration** of fault injection parameters required

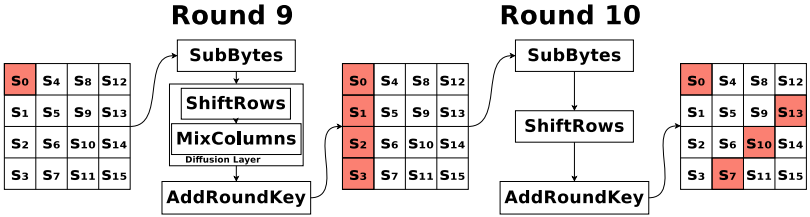
Fault Attack on AES

- Differential Fault Analysis on AES[3]
- Differential $\Rightarrow$ **Pairs** (c, c') of correct and incorrect ciphertexts

[3] Piret et al., "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad", CHES 2003

Fault Attack on AES

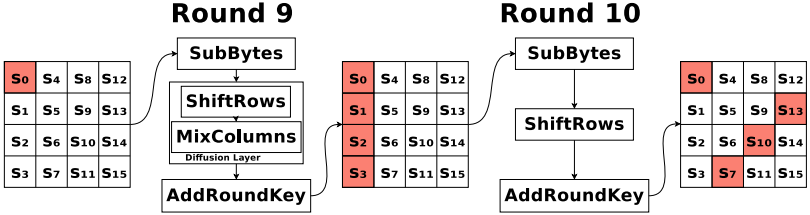
- Differential Fault Analysis on AES[3]
- Differential $\Rightarrow$ **Pairs** (c, c') of correct and incorrect ciphertexts
- Fault injection: Single byte before 9th encryption round



[3] Piret et al., "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad", CHES 2003

Fault Attack on AES

- Differential Fault Analysis on AES[3]
- Differential $\Rightarrow$ **Pairs** (c, c') of correct and incorrect ciphertexts
- Fault injection: Single byte before 9th encryption round

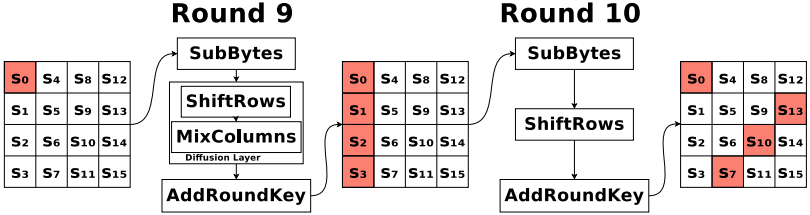


- $\Rightarrow$ Fault model allows us to **verify** successful injection

[3] Piret et al., "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad", CHES 2003

Fault Attack on AES

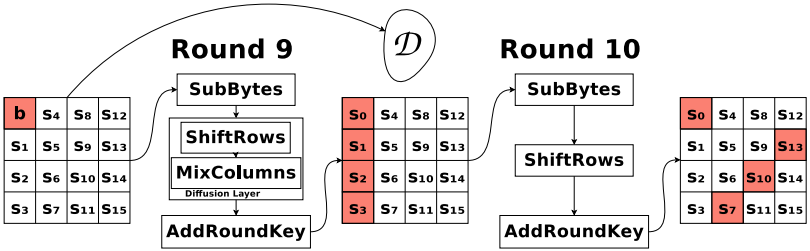
- Differential Fault Analysis on AES[3]
- Differential $\Rightarrow$ **Pairs** (c, c') of correct and incorrect ciphertexts
- Fault injection: Single byte before 9th encryption round



- $\Rightarrow$ Fault model allows us to **verify** successful injection
- How do we get the secret key?

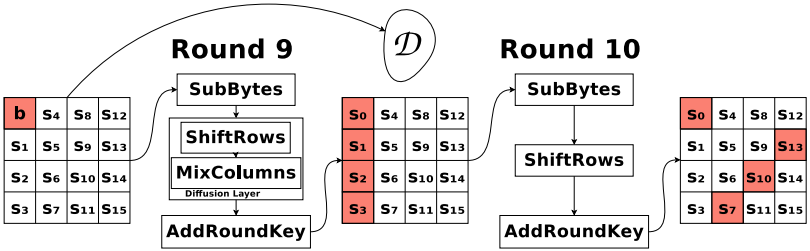
[3] Piret et al., "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad", CHES 2003

Fault Attack on AES



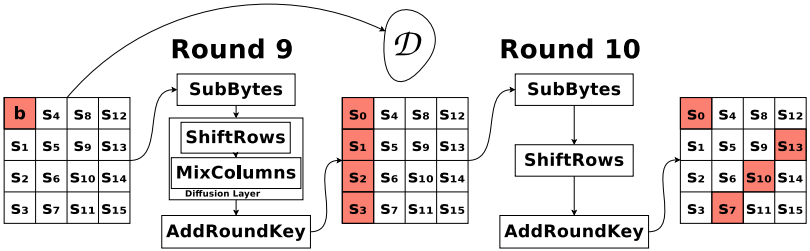
- Consider a single faulty byte $b' \neq b$ before the 9th round

Fault Attack on AES



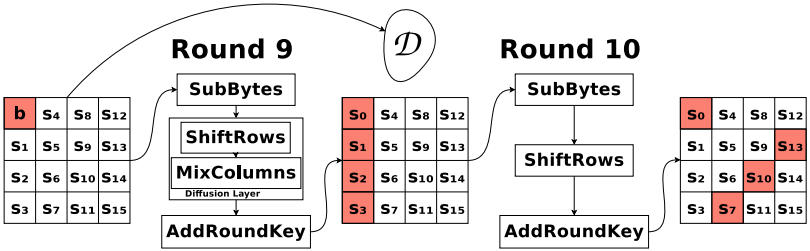
- Consider a single faulty byte $b' \neq b$ before the 9th round
- $\Rightarrow$ There are 255 possible **differences** between b and b'

Fault Attack on AES



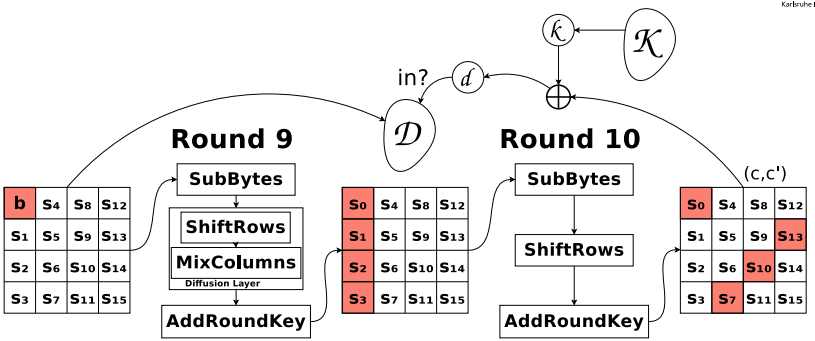
- Consider a single faulty byte $b' \neq b$ before the 9th round
- $\Rightarrow$ There are 255 possible **differences** between b and b'
- $\Rightarrow$ There are 255 possible differences in the AES state **after** round 9

Fault Attack on AES



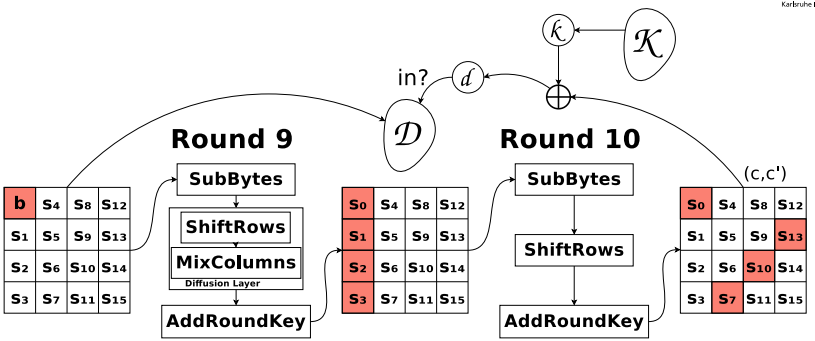
- Consider a single faulty byte $b' \neq b$ before the 9th round
- $\Rightarrow$ There are 255 possible **differences** between b and b'
- $\Rightarrow$ There are 255 possible differences in the AES state **after** round 9
- Compute these differences into a set $\mathcal{D}$

Fault Attack on AES



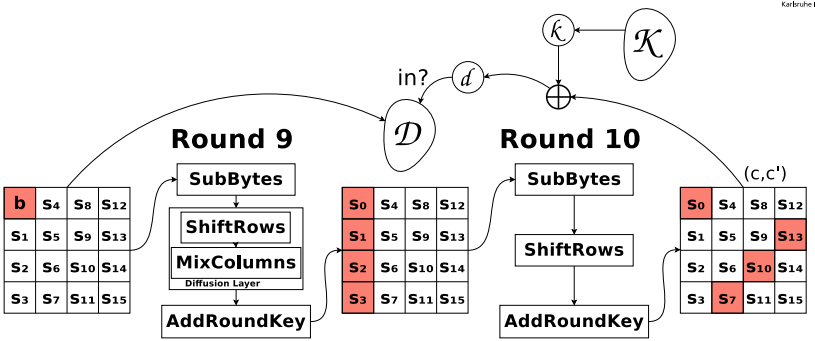
- We have 2^{32} possible candidates for four bytes of the last round key
  $\Rightarrow$ Set of key candidates $\mathcal{K}$

Fault Attack on AES



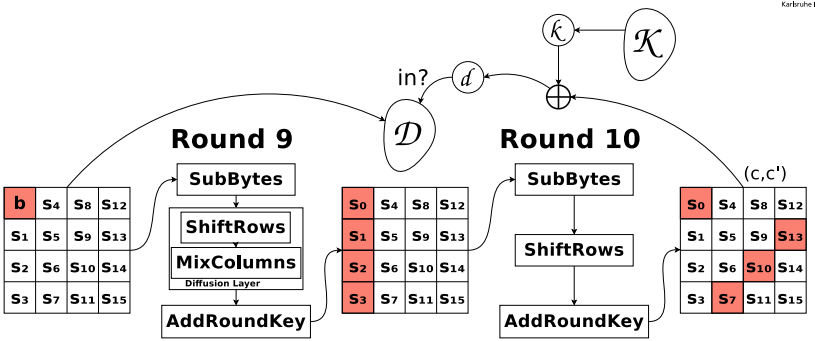
- We have 2^{32} possible candidates for four bytes of the last round key
  $\Rightarrow$ Set of key candidates $\mathcal{K}$
- Now consider a pair (c, c') of correct and fault ciphertexts

Fault Attack on AES



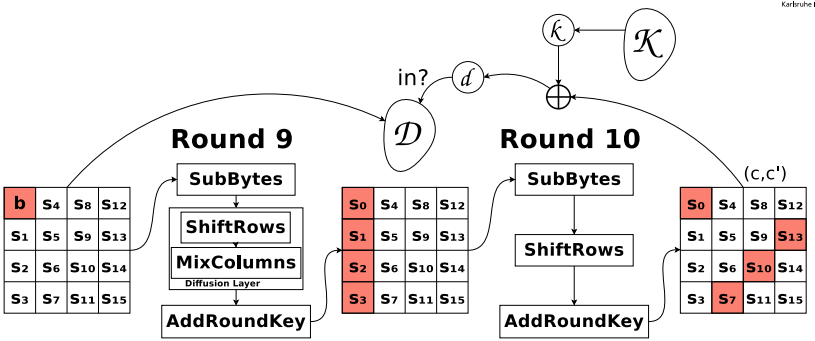
- We have 2^{32} possible candidates for four bytes of the last round key $\Rightarrow$ Set of key candidates $\mathcal{K}$
- Now consider a pair (c, c') of correct and fault ciphertexts
- Compute difference d before the last round using a candidate $k \in \mathcal{K}$

Fault Attack on AES



- We have 2^{32} possible candidates for four bytes of the last round key $\Rightarrow$ Set of key candidates $\mathcal{K}$
- Now consider a pair (c, c') of correct and fault ciphertexts
- Compute difference d before the last round using a candidate $k \in \mathcal{K}$
- If $d \notin \mathcal{D}$, remove k from $\mathcal{K}$

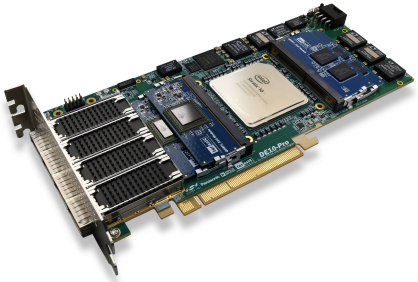
Fault Attack on AES

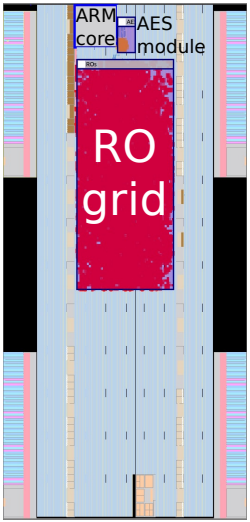


- We have 2^{32} possible candidates for four bytes of the last round key $\Rightarrow$ Set of key candidates $\mathcal{K}$
- Now consider a pair (c, c') of correct and fault ciphertexts
- Compute difference d before the last round using a candidate $k \in \mathcal{K}$
- If $d \notin \mathcal{D}$, remove k from $\mathcal{K}$
- Repeat with a fresh pair until one key candidate remains

Edge and Cloud Devices

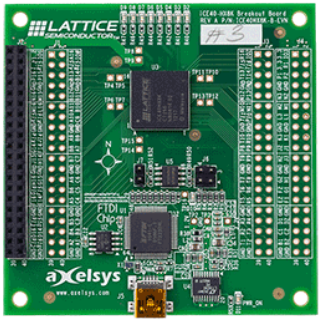
Terasic DE10-Pro – Intel Stratix 10 (2.8M LUTs):

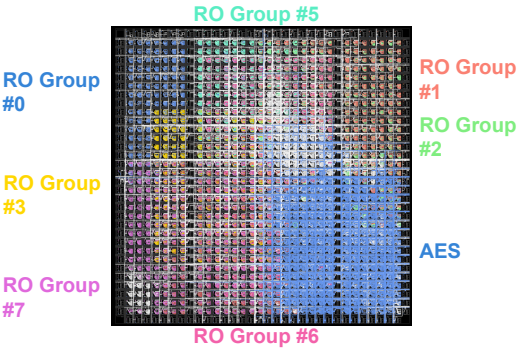




Edge and Cloud Devices

Lattice iCE40-HX8K Breakout Board (8K LUTs):





FPGA-based fault attacks on AES

FPGA-based fault attacks on AES

- We now use the voltage virus logic to inject faults into AES

FPGA-based fault attacks on AES

- We now use the voltage virus logic to inject faults into AES
- But: Only single byte faults before 9th round are usable!

FPGA-based fault attacks on AES

- We now use the voltage virus logic to inject faults into AES
- But: Only single byte faults before 9th round are usable!
- $\Rightarrow$ We need to adapt injection parameters to achieve precise injection

FPGA-based fault attacks on AES

- We now use the voltage virus logic to inject faults into AES
- But: Only single byte faults before 9th round are usable!
- $\Rightarrow$ We need to adapt injection parameters to achieve precise injection
- $\Rightarrow$ Live-Demo on Intel Stratix 10

Thank you for your attention!

Questions? Write us an email!

{jonas.krautter,dennis.gnad,mehdi.tahoori}@kit.edu