# Bitstream Encryption Vulnerabilities

Kevin Pretterhofer

November 10, 2021

# Outline

- Introduction
- Excursus: eFuse vs. BBRAM
- Brief discussion on three different attacks
- Other mentionable attacks

# The Attacks

- Brief discussion about:

| Year | Attack | Technique |
|---|---|---|
| 2011 | Key Extraction | Differential Power Analysis |
| 2017 | Plaintext Extraction | Optical Contactless Probing |
| 2020 | Plaintext Extraction | CBC-Malleability |

- Other mentionable attacks:

| Year | Attack | Technique |
|---|---|---|
| 2012 | Plaintext Extraction | DPA / Pipeline Emission Analysis |
| 2018 | Key Extraction | Thermal Laser Stimulation |
| 2016 | Key Extraction | DPA on the EM side channel |

# This Presentation

- What it is about:
  - An overview of (recent) bitstream encryption vulnerabilities
  - A brief explanation of those vulnerabilities
- What it is **not** about:
  - An in-depth and detailed description of those vulnerabilities
  - Detailed mitigation strategies for those vulnerabilities

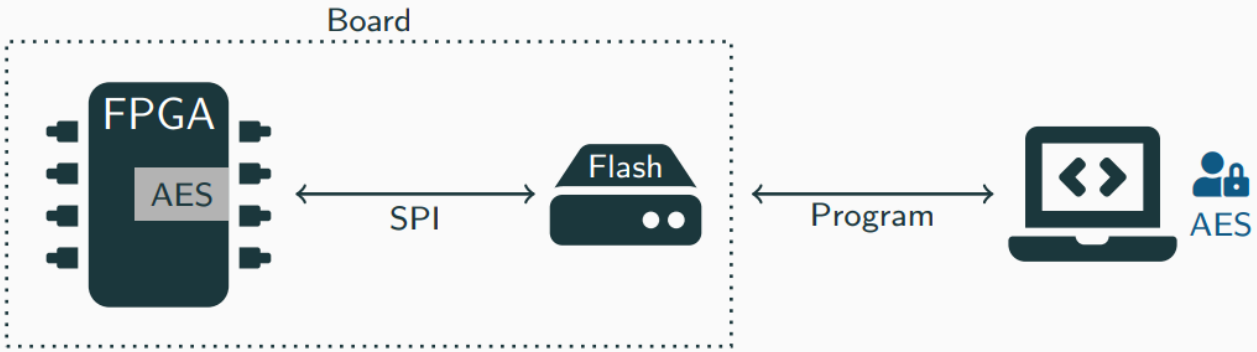
# Introduction

# Bitstream Encryption (Recap)

- FPGAs gain importance
- Already used
  - in military devices
  - for signal processing
  - several customer products
- IP needs to be secured
  - Prevent stealing/cloning
  - Prevent tampering
- Therefore: Bitstream Encryption

# Bitstream Encryption (Recap) cont.

- Bitstream encrypted on developer side
- Stored on Flash Memory
- Decryption happens on board before configuration
- Key for decryption stored in BBRAM or eFuse



# Excursus: eFuse vs BBRAM

# Overview

- eFuse
  - One-Time programmable
  - Values "burned in"
  - No readback path
  - No battery needed
- BBRAM
  - Re-programmable
  - Passive/Active clearing
  - Tamper resistant
  - No readback path
  - Battery backed

# Which is more secure?

- According to Xilinx: BBRAM is more secure [2]
  - If keys are revealed: BBRAM can be reprogrammed
  - If tampering detected: BBRAM can be zeroized
  - eFuse probably "easy" to reverse engineer (large footprints)
- Since both are non-volatile:
  - They can be targeted when power is off

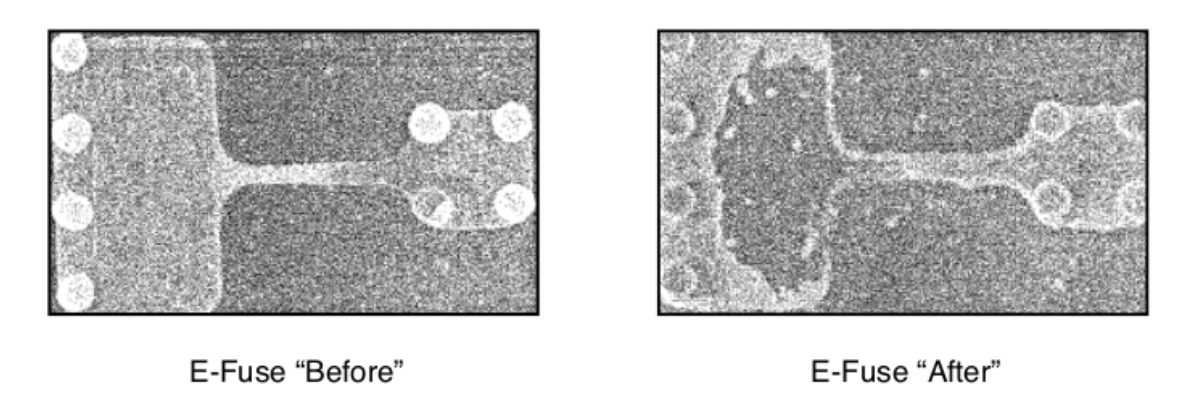



**Figure 1:** eFuse key storage: before and after being programmed

# Power Analysis Attacks

# Overview: Moradi et al. in 2011 [5]

- Virtex-II Pro XC2VP7 FPGA (Xilinx)
- Triple-DES Bitstream Encryption
- Reverse Engineering + Differential Power Analysis + Profiling approach
- Key extracted in 2 - 3 minutes

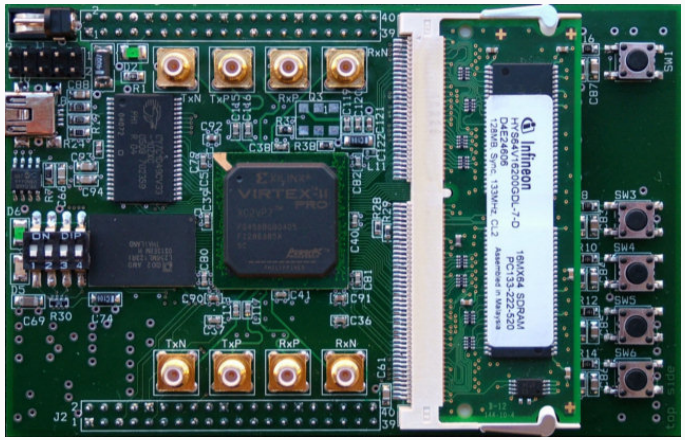


**Figure 2:** XC2VP7

# Concepts: Triple-DES

- Three consecutive DES ciphers
- Two or three 56-bit keys
- 48 Rounds
- Deprecated by NIST in 2018

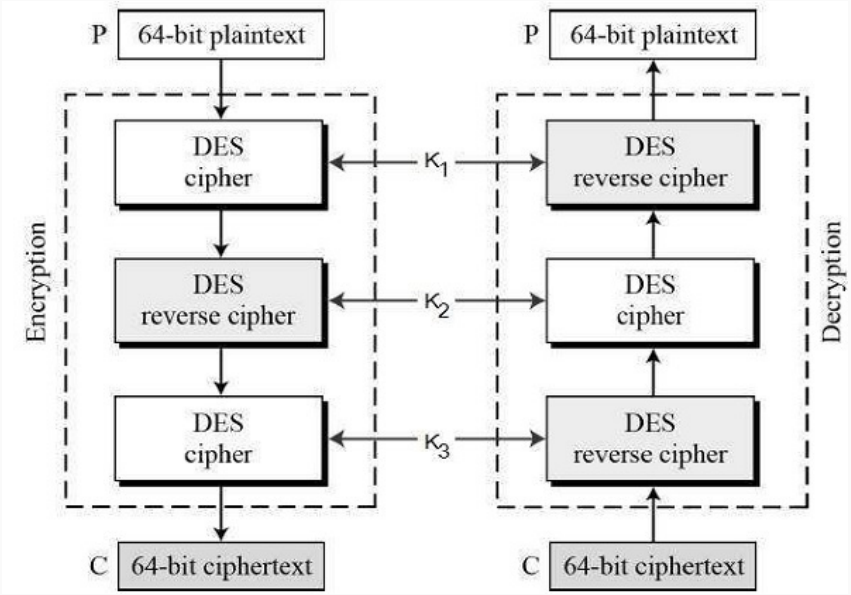



**Figure 3:** Triple-DES

# Concepts: Differential Power Analysis

- Exploit power consumption
- Attack a specific operation of the algorithm (e.g. SBOX)
- Query en/decryption for different inputs
  - and measure power consumption
- Enumerate possible sub-keys
  - and calculate the targeted operation for every input
- Derive a power consumption model
  - typically hamming weight / hamming distance
- Find correlations
  - Pearson Correlation Coefficient

# Approach

1. Reverse Engineering of the Bitstream
    - Basically comparing encrypted and plain bitstreams
2. Customizing the Measurement Setup
    - Microcontroller comprising JTAG protocol
    - Oscillator
    - ...
3. Timing and Power Profile Analysis
    - Gain information about underlying HW
    - Derive a power model
4. Extracting the Keys

# Approach cont.

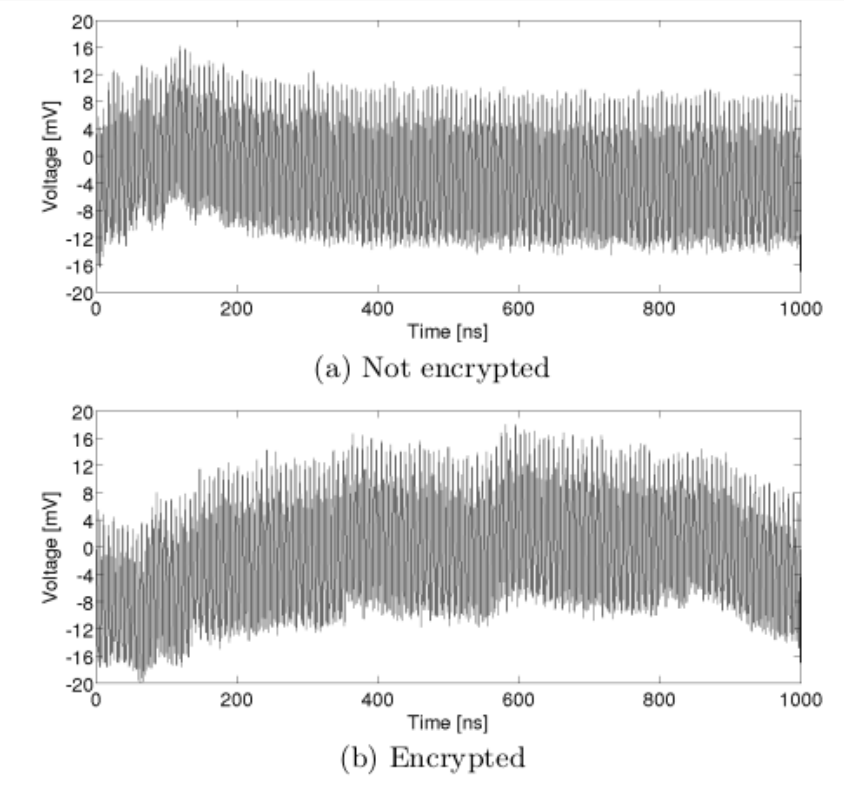



**Figure 4:** Raw measurements of power consumption during decryption

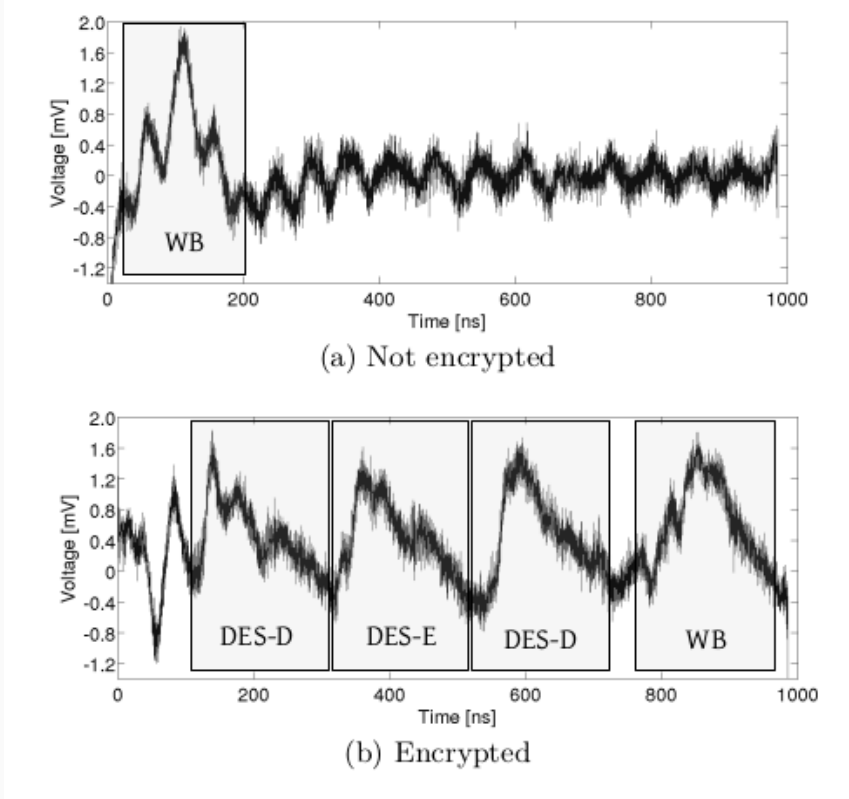



**Figure 5:** Filtered measurements of power consumption during decryption

# Optical Contactless Probing

# Overview: Tajik et al. in 2017 [7]

- XC7K70T Kintex 7 FPGA (Xilinx)
- AES Bitstream Encryption (semi-important for that attack)
- Electro-Optical Probing / Electro-Optical Frequency Mapping
- Raw plaintext acquisition 43 minutes
- Overall work about 10 days

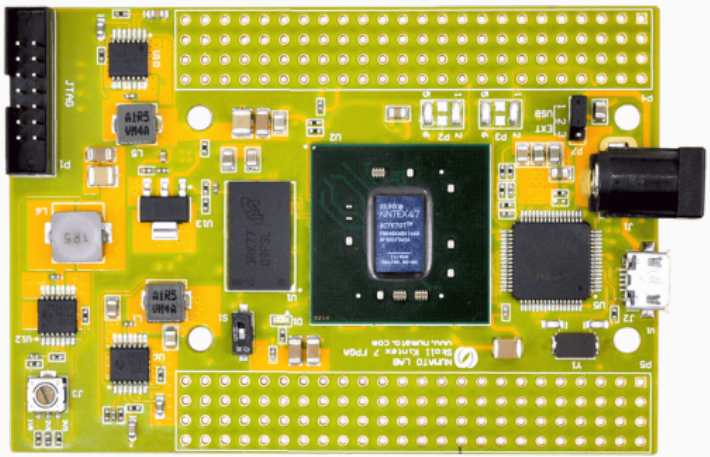


**Figure 6:** Skoll Kintex 7 FPGA (with XC7K70T)

# Concepts: EOP / EOFM

- Electro-Optical Probing
  - Probe electrical signals
  - Measure density of reflected light
- Electro-Optical Frequency Mapping
  - Create activity map of active circuits
  - Reflected light fed into spectrum analyzer

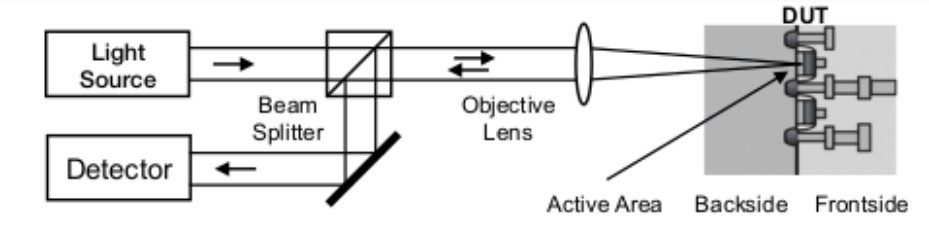



**Figure 7:** Simplified illustration of optical probing

# Approach

1. Localize general configuration logic area
    - Light reflection (find irregular patterns)
    - EOFM with CCLK frequency
2. Localize AES decryption core
    - EOFM with CCLK frequency
    - If NOT in encrypted bitstream mode: disabled
3. Determine bus width
    - Induce patterns and perform EOFM
4. Localize gates, carrying the plaintext data
    - Induce patterns and perform EOFM
    - Enumerate nodes accordingly
5. Extract the data from those gates
    - EOP on individual bus lines

# Approach cont.

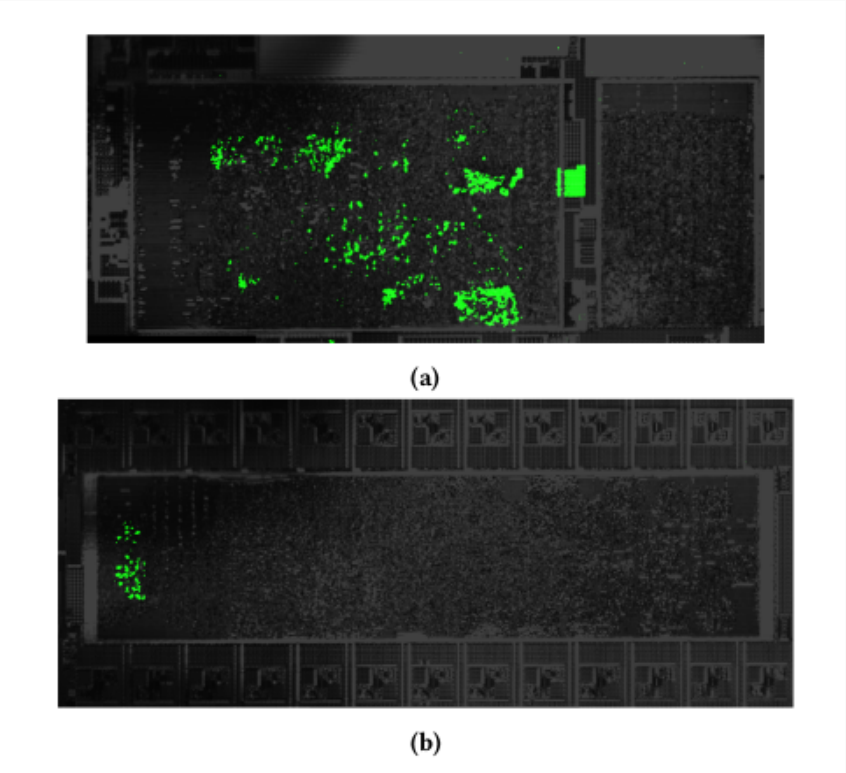



**Figure 8:** Activity map (32-bit word frequency, unencrypted), (a) Main logic area, (b) AES logic area

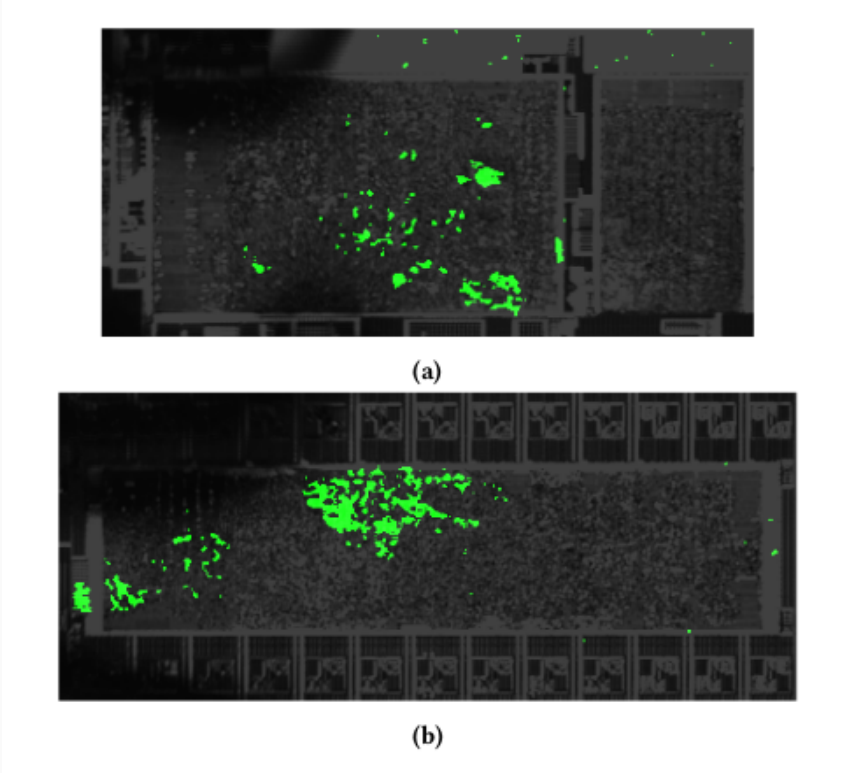



**Figure 9:** Activity map (plaintext data frequency, encrypted), (a) Main logic area, (b) AES logic area

# Approach cont.

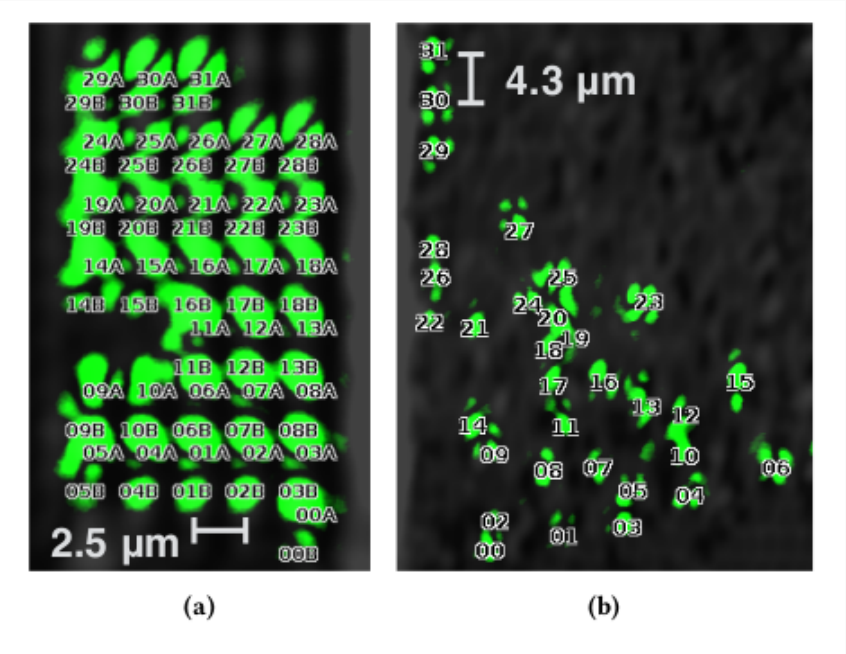



**Figure 10:** Mapping of plaintext bus bit locations, (a) AES output port, (b) alternative locations

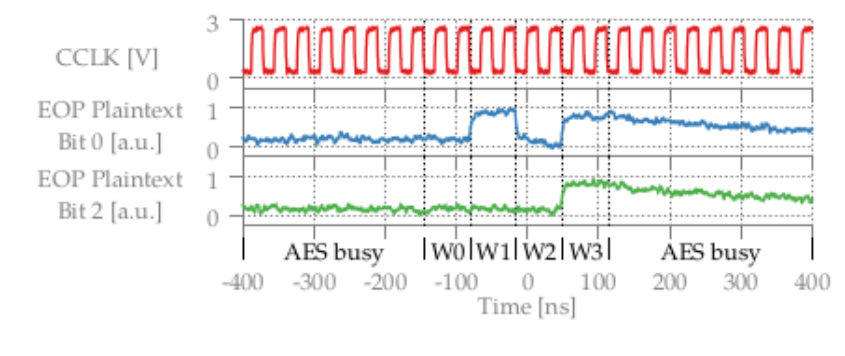



**Figure 11:** Optically extracted plaintext data for two bus lines. Bit0: 0101, Bit2: 0001

# Low Cost Full Break

# Overview: Ender et al. in 2020 [1]

- Xilinx 7-Series
- AES Bitstream Encryption
- CBC Malleability
- 3 to 4 hours to have decrypted bitstream


**Figure 12:** Module with XC7K160T

# Concepts: CBC Malleability

- Inducing a delta propagates to plaintext
- $c_i \oplus \Delta \rightarrow p_{i+1} \oplus \Delta$

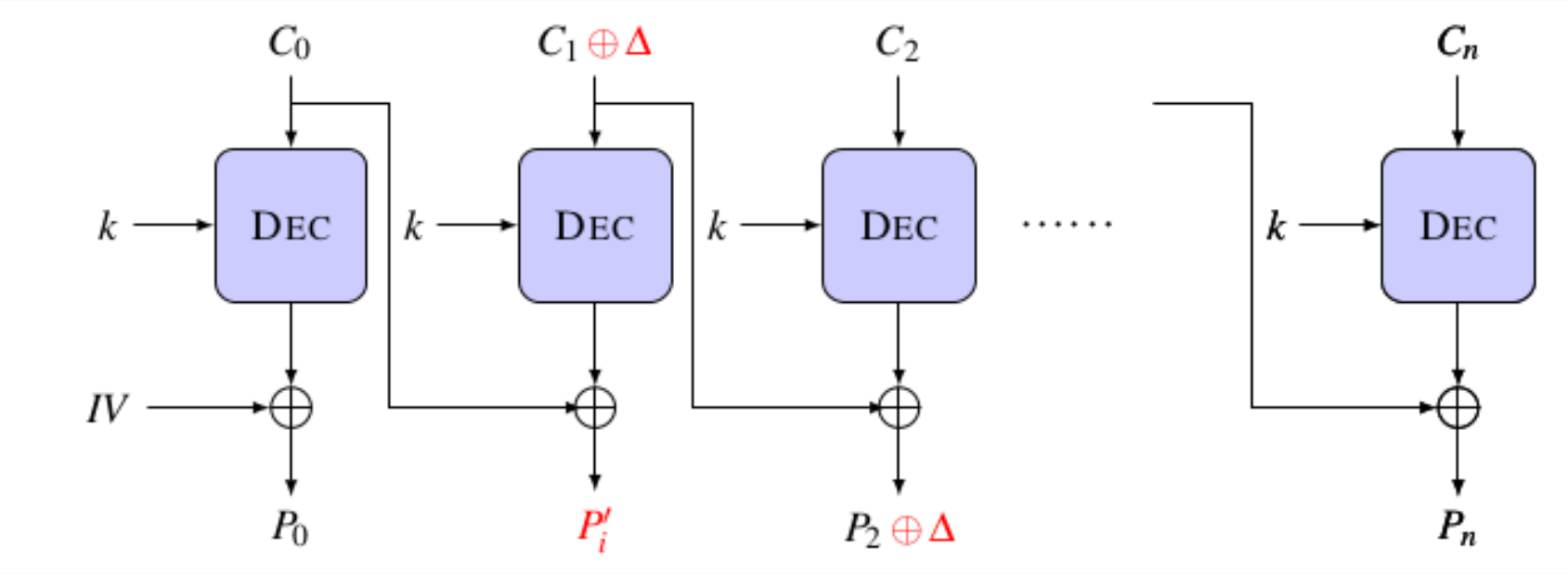



**Figure 13:** CBC Malleability

# Concepts: MultiBoot / Fallback Routine

- If a remote-update fails: fall back
- Load working bitstream from specific address
- Stored in WBSTAR register

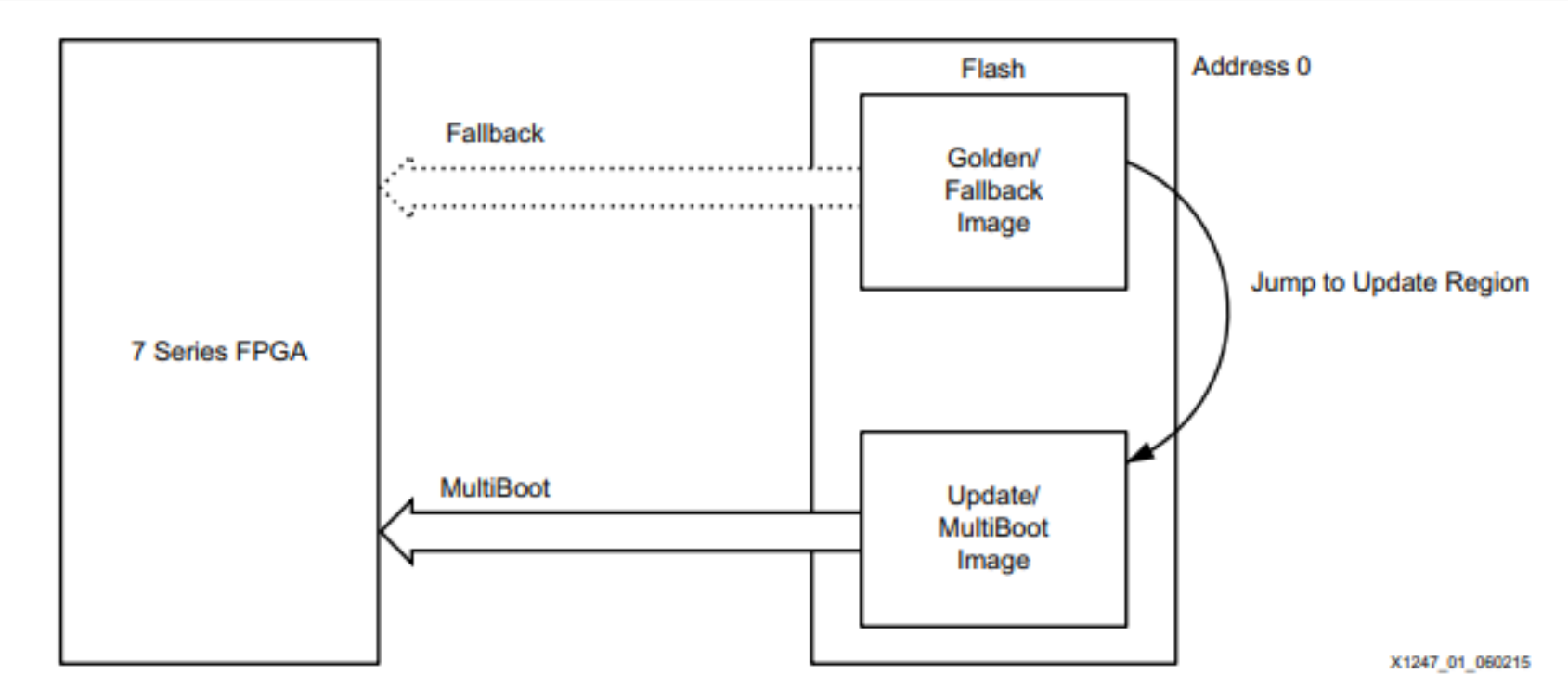



**Figure 14:** MultiBoot / Fallback Flow

# Approach

1. Create malicious bitstream
    - Utilizing CBC-Malleability
2. Create readout bitstream
3. Configure FPGA with malicious bitstream
4. Let the FPGA reset
    - Due to wrong HMAC
5. Read out the WBSTAR register (readout bitstream)
6. Reset FPGA manually

# Approach cont.

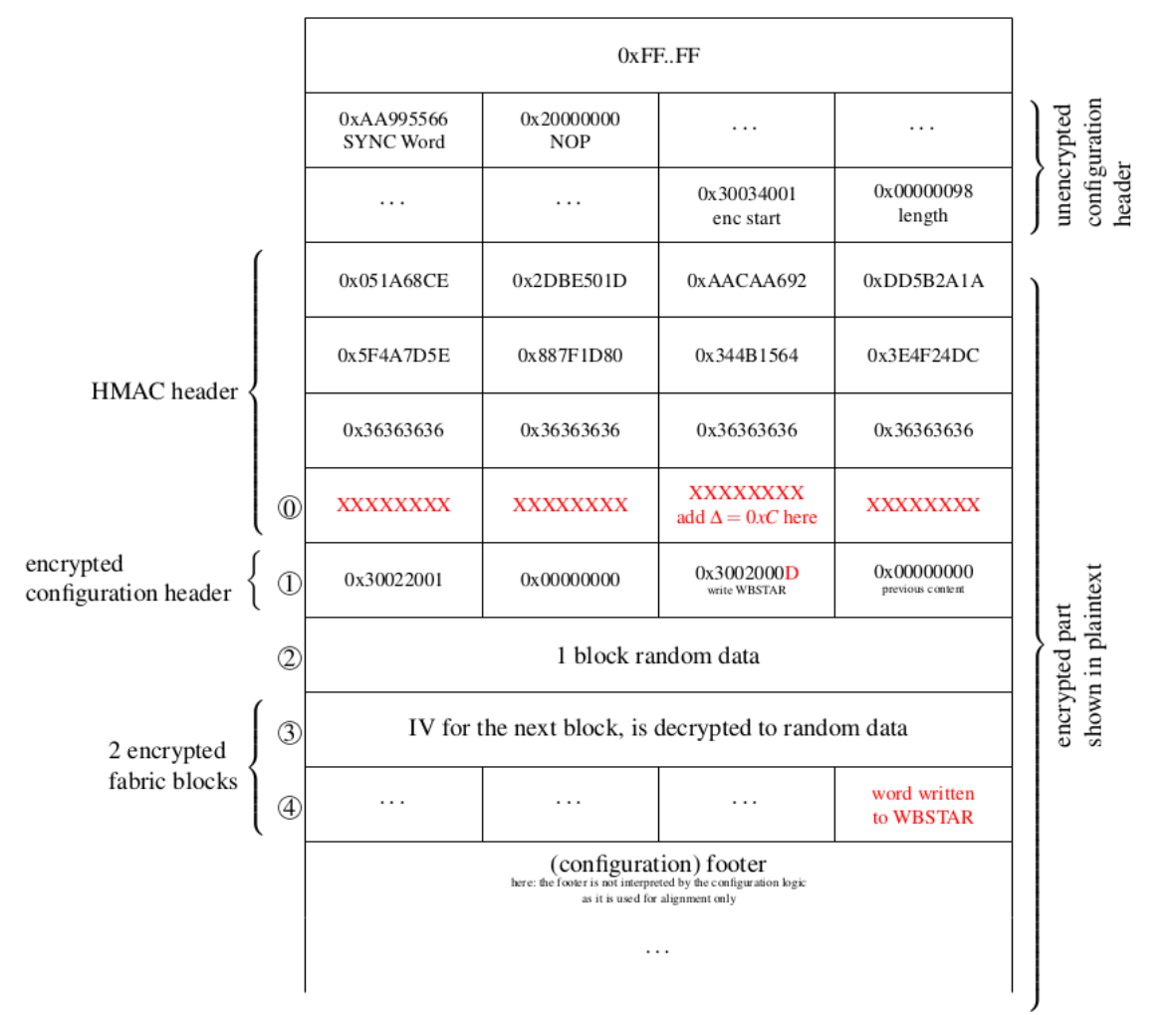



**Figure 15:** Example Malicious Bitstream

# Other mentionable Attacks

# Other Attacks

- Skorobogatov and Woods in 2012 [6]
  - Actel/Microsemi ProASIC3 chips
  - Power Analysis
  - DPA and PEA (Pipeline Emission Analysis)
  - Backdoor: Read out bitstream
- Lohrke et al. in 2018 [3]
  - Xilinx Ultrascale Series
  - Optical Attack
  - Thermal Laser Stimulation
  - Revealed key from BBRAM

# Other Attacks cont.

- Moradi and Schneider in 2016 [4]
  - Xilinx 5, 6 and 7 series
  - Power Analysis
  - Similar to DPA but with EM sidechannel
  - Revealed key

# Bitstream Encryption Vulnerabilities

Kevin Pretterhofer

November 10, 2021

# References i


[1] Maik Ender, Amir Moradi, and Christof Paar. The Unpatchable Silicon: A Full Break of the Bitstream Encryption of Xilinx 7-Series FPGAs. In: 29th USENIX Security Symposium, USENIX Security 2020, August 12-14, 2020. Ed. by Srdjan Capkun and Franziska Roesner. USENIX Association, 2020, pp. 1803–1819. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/ender.

[2] Austin Lesea. IP security in FPGAs, WP261. Tech. rep. Xilinx, 2007.

[3] Heiko Lohrke et al. Key Extraction Using Thermal Laser Stimulation A Case Study on Xilinx Ultrascale FPGAs. In: IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018.3 (2018), pp. 573–595. DOI: 10.13154/tches.v2018.i3.573-595. URL: https://doi.org/10.13154/tches.v2018.i3.573-595.

# References ii

[4] Amir Moradi and Tobias Schneider. Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series. In: Constructive Side-Channel Analysis and Secure Design - 7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers. Ed. by François-Xavier Standaert and Elisabeth Oswald. Vol. 9689. Lecture Notes in Computer Science. Springer, 2016, pp. 71–87. DOI: 10.1007/978-3-319-43283-0_5. URL: https://doi.org/10.1007/978-3-319-43283-0%5C_5.

[5] Amir Moradi et al. On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011. Ed. by Yan Chen, George Danezis, and Vitaly Shmatikov. ACM, 2011, pp. 111–124. DOI: 10.1145/2046707.2046722. URL: https://doi.org/10.1145/2046707.2046722.

# References iii


[6] Sergei Skorobogatov and Christopher Woods. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip. In: Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings. Ed. by Emmanuel Prouff and Patrick Schaumont. Vol. 7428. Lecture Notes in Computer Science. Springer, 2012, pp. 23–40. DOI: 10.1007/978-3-642-33027-8_2. URL: https://doi.org/10.1007/978-3-642-33027-8%5C_2.

[7] Shahin Tajik et al. On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 1661–1674. DOI: 10.1145/3133956.3134039. URL: https://doi.org/10.1145/3133956.3134039.