MAX PLANCK INSTITUTE
FOR SECURITY AND
PRIVACY

STARBLEED
A FULL BREAK OF THE BITSTREAM ENCRYPTION OF XILINX 7-SERIES FPGAS

Maik Ender, Amir Moradi, and Christof Paar

↘ *Ruhr University Bochum & MPI for Privacy and Security*

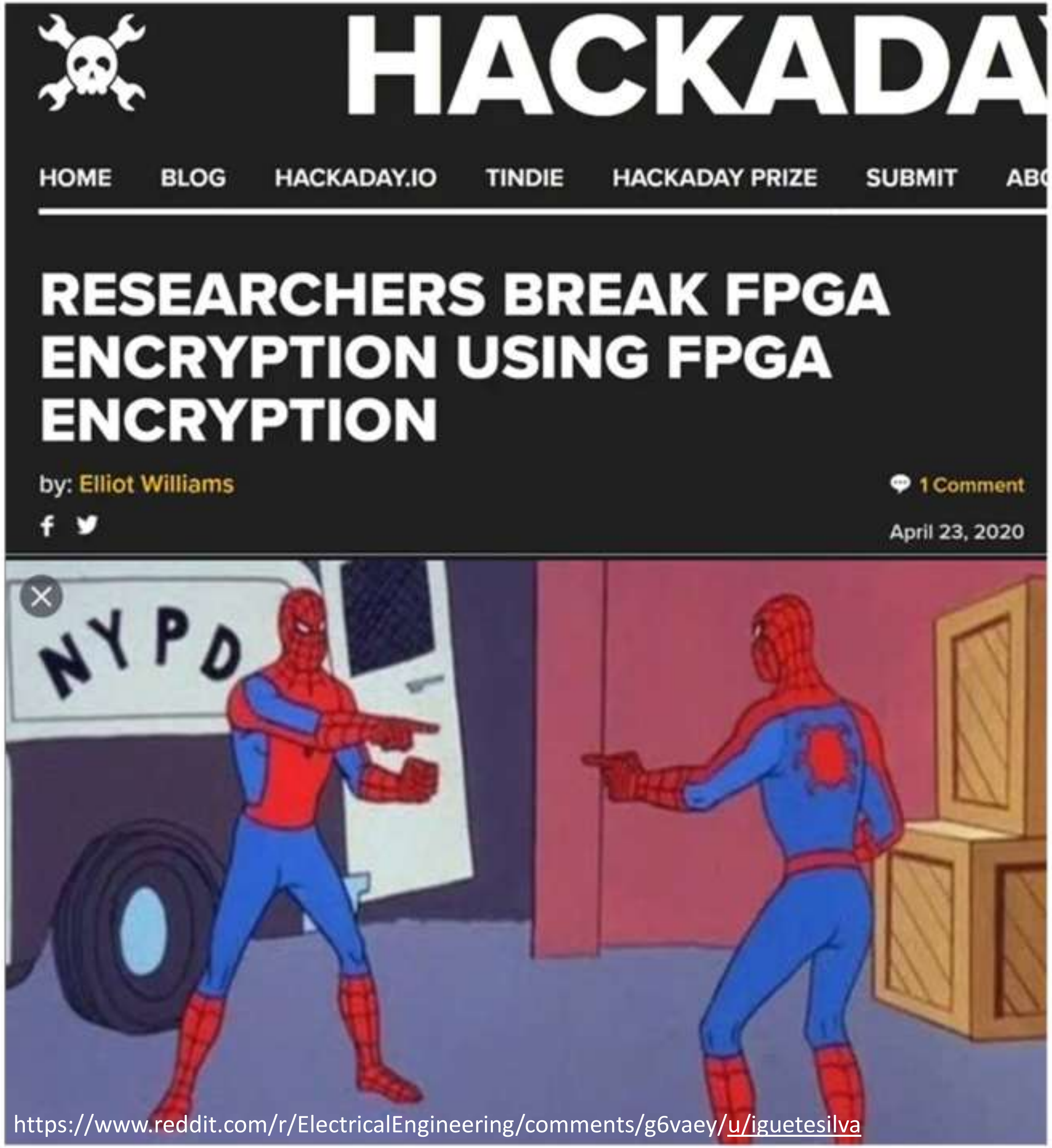
USENIX Security, August 14, 2020

STARBLEED
A FULL BREAK OF THE BITS
OF XILINX 7-SERIES FPGAS

Maik Ender, Amir Moradi, and C

↘ *Ruhr University Bochum & MPI for Privacy and Secu*

USENIX Security, August 14, 20



HACKADA

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT ABO

RESEARCHERS BREAK FPGA ENCRYPTION USING FPGA ENCRYPTION

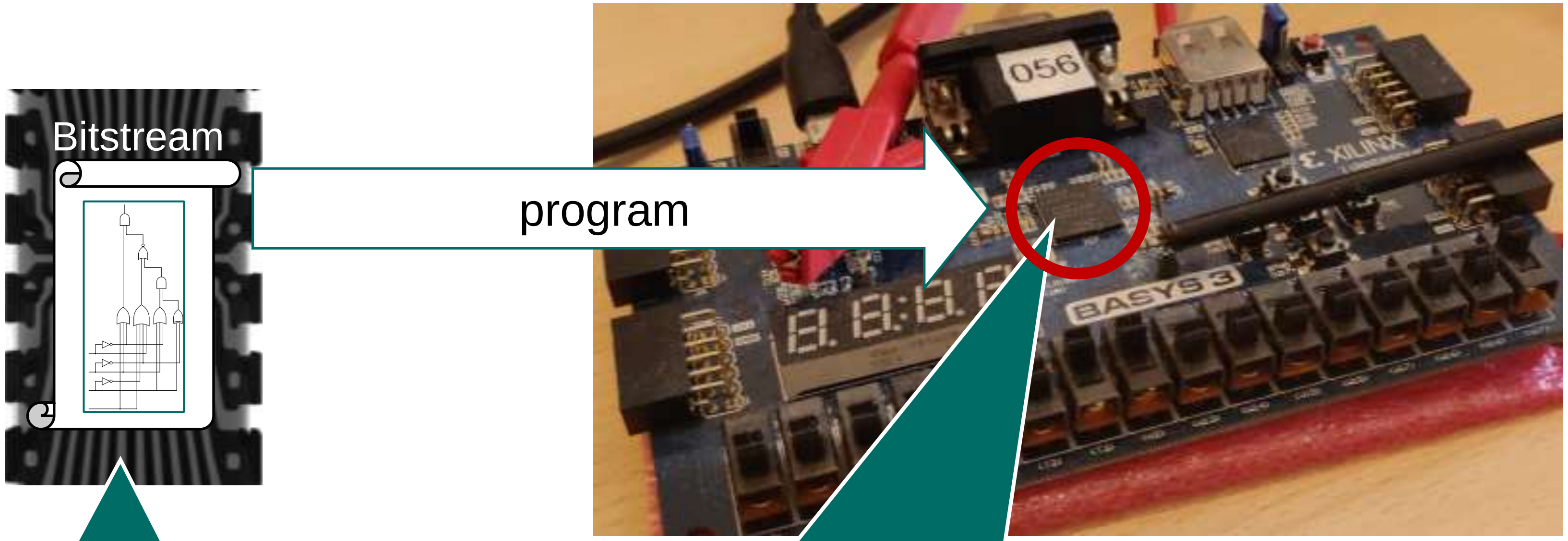
by: Elliot Williams

1 Comment

April 23, 2020

https://www.reddit.com/r/ElectricalEngineering/comments/g6vaey/u/iguetesilva

FIELD PROGRAMMABLE GATE ARRAYS



Bitstream contains FPGA‘s design

Stored on external memory

Field **Programmable** Gate Array (FPGA)

Special IC
Reprogrammable logic

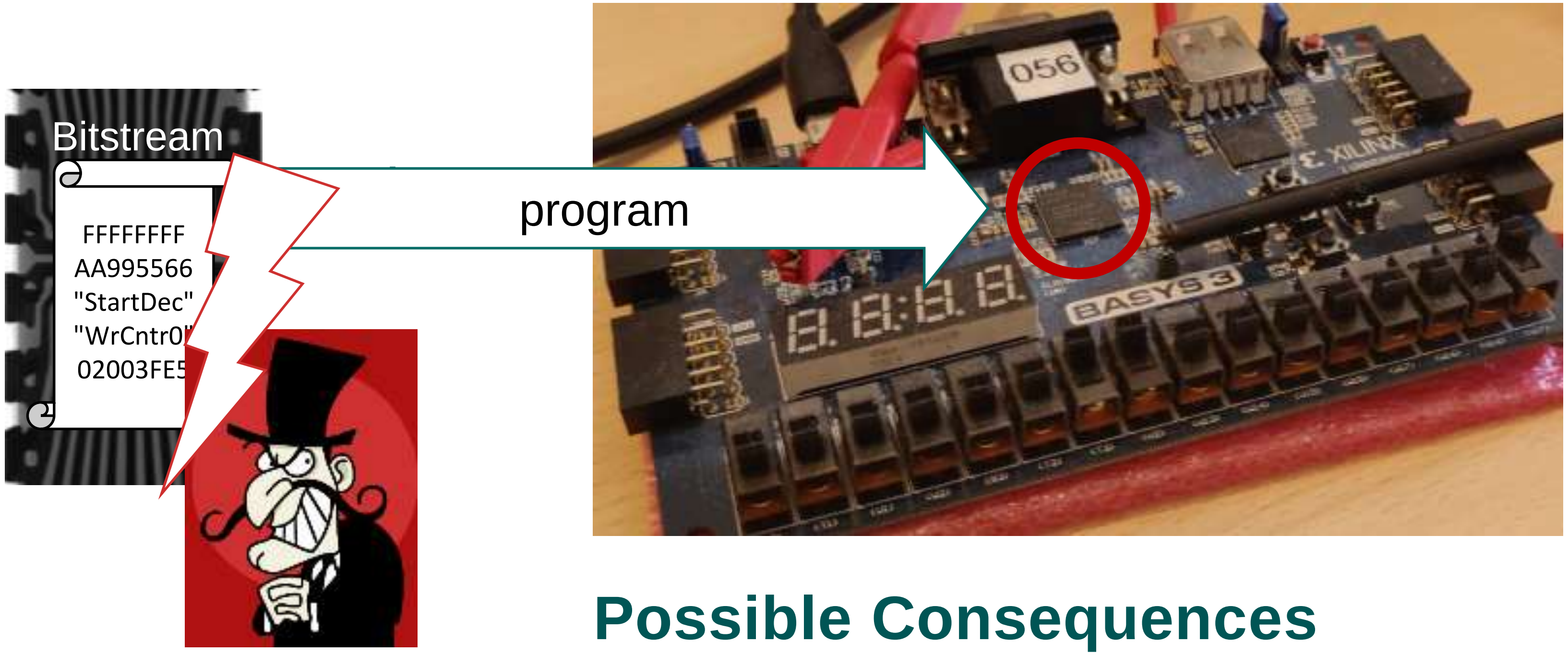
Photo by Thomas Jensen on Unsplash

Photo by American Public Power Association on Unsplash

Photo by Patrick Tomasso on Unsplash

Photo by Chuanchai Pundej on Unsplash

BITSTREAM SECURITY



```
FFFFFFFF
AA995566
"StartDec"
"WrCntr0
02003FE5
```

Possible Consequences

- IP theft & design cloning
- Reverse engineering
- Design manipulation
- Hardware Trojans

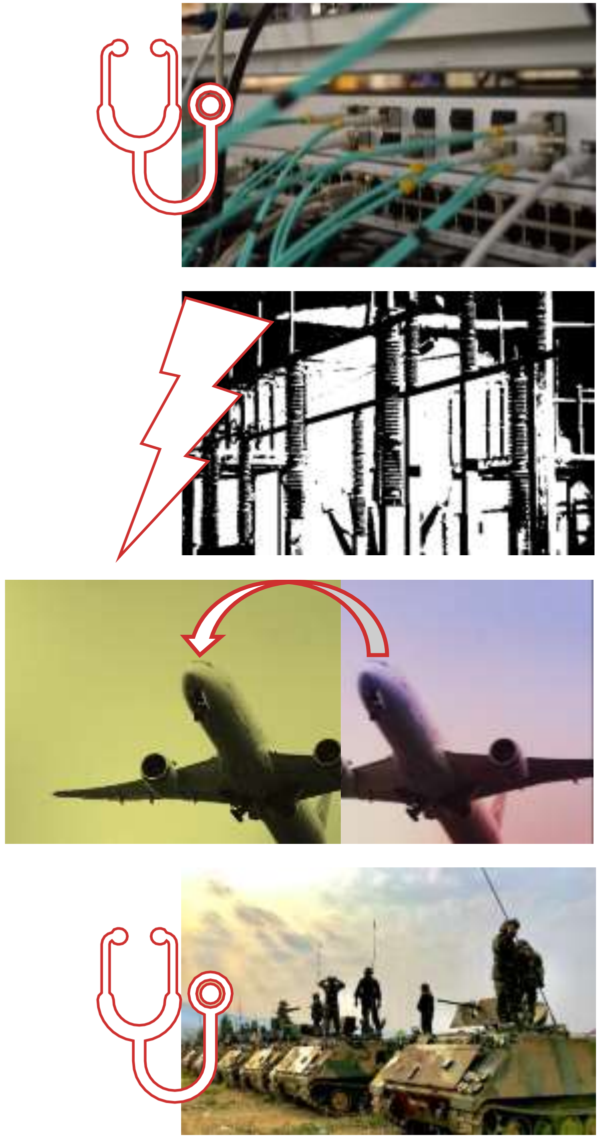


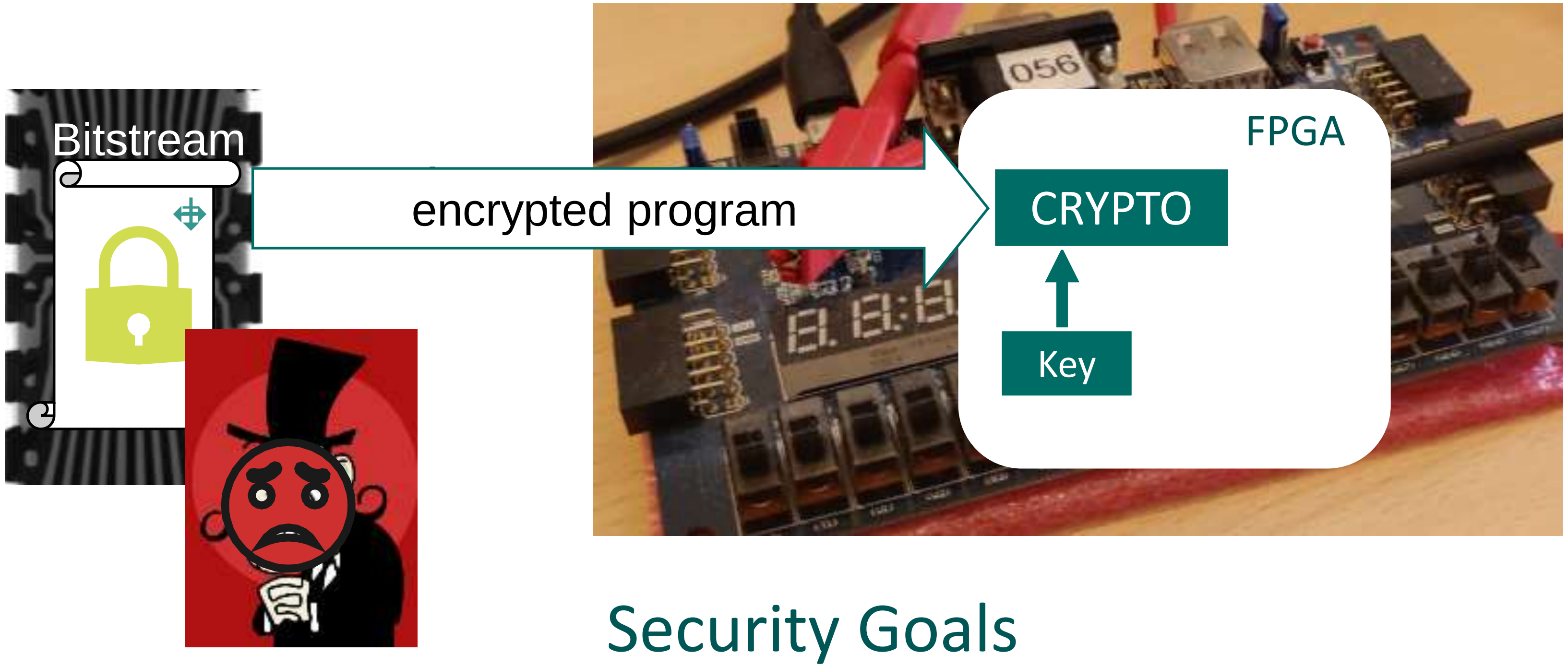
Photo by Thomas Jensen on Unsplash

Photo by American Public Power Association on Unsplash

Photo by Patrick Tomasso on Unsplash

Photo by Chuanchai Pundej on Unsplash

BITSTREAM ENCRYPTION



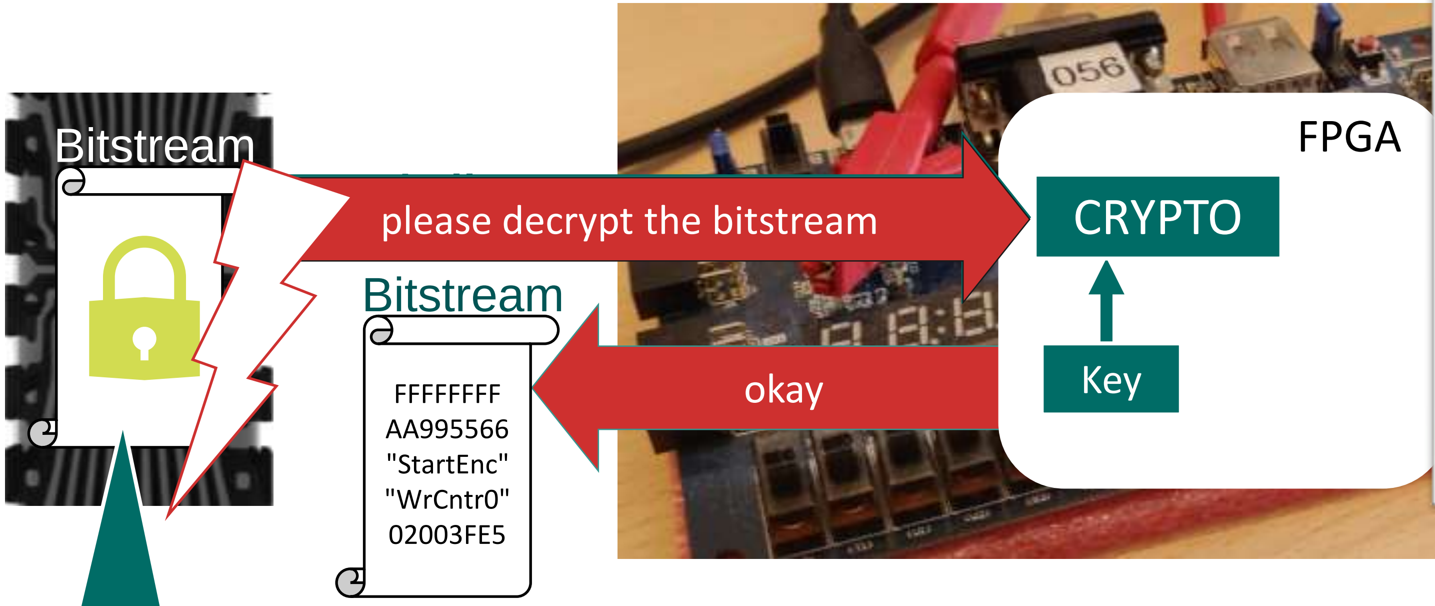
Security Goals

AES-256

- **Confidentiality:** bitstream is encrypted
- **Authenticity:** FPGA loads only designs from integrator
- **Integrity:** Bitstream is not changed

HMAC

ATTACK IN A NUTSHELL



Manipulate the encrypted bitstream

RESEARCHERS BREAK FPGA ENCRYPTION USING FPGA ENCRYPTION

by: Elliot Williams

1 Comment

April 23, 2020

Security Goals

- **Confidentiality:** bitstream is encrypted
- **Authenticity:** FPGA loads only designs from integrator
- **Integrity:** Bitstream is not changed

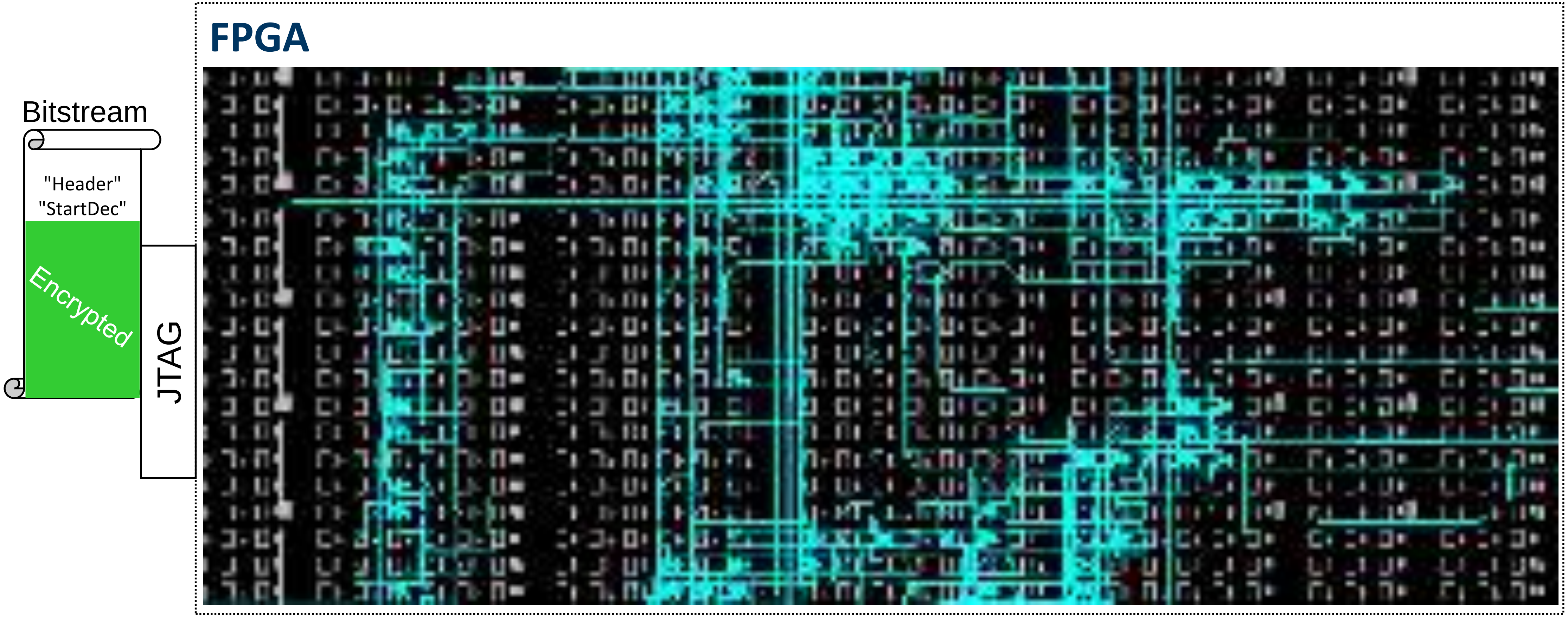
Starbleed Attack I: Break Confidentiality

Starbleed Attack II: Break Authenticity

1

HOW TO PROGRAM AN FPGA?

CONFIGURATION ENGINE



Bitstream

"Header"

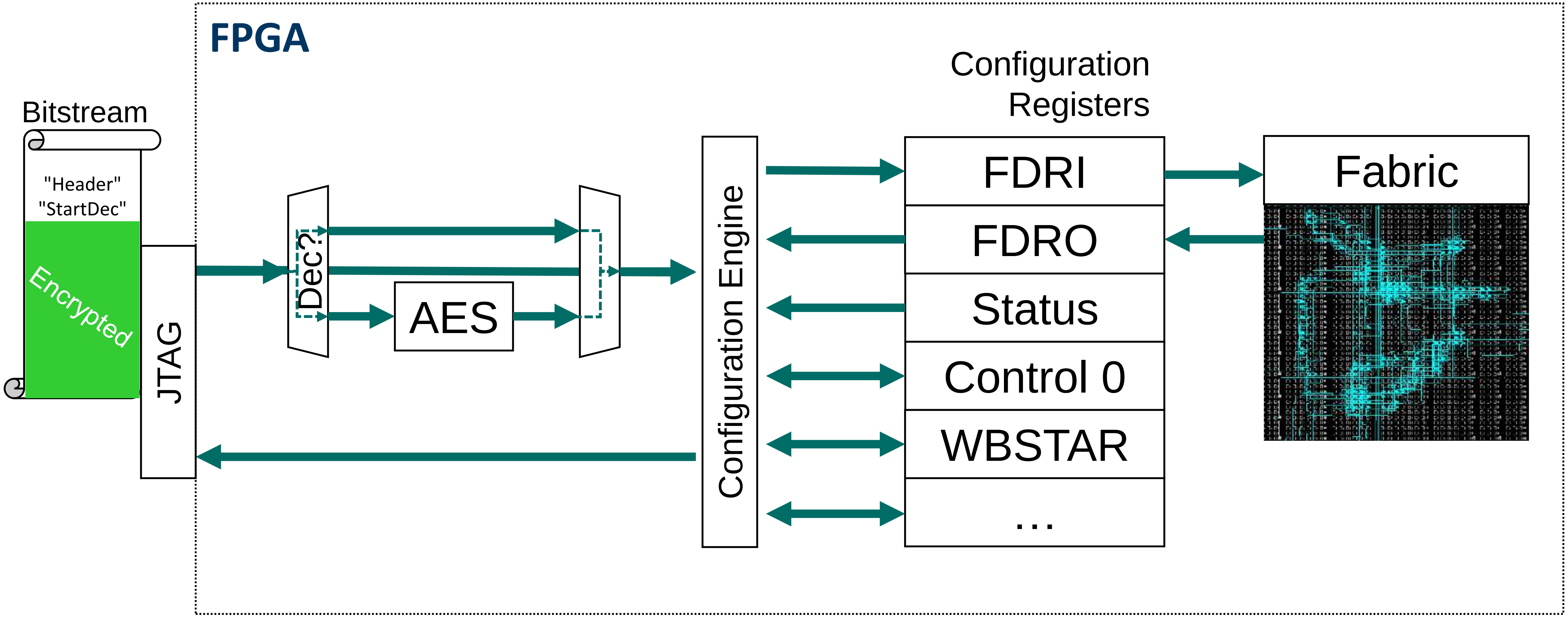
"StartDec"

Encrypted

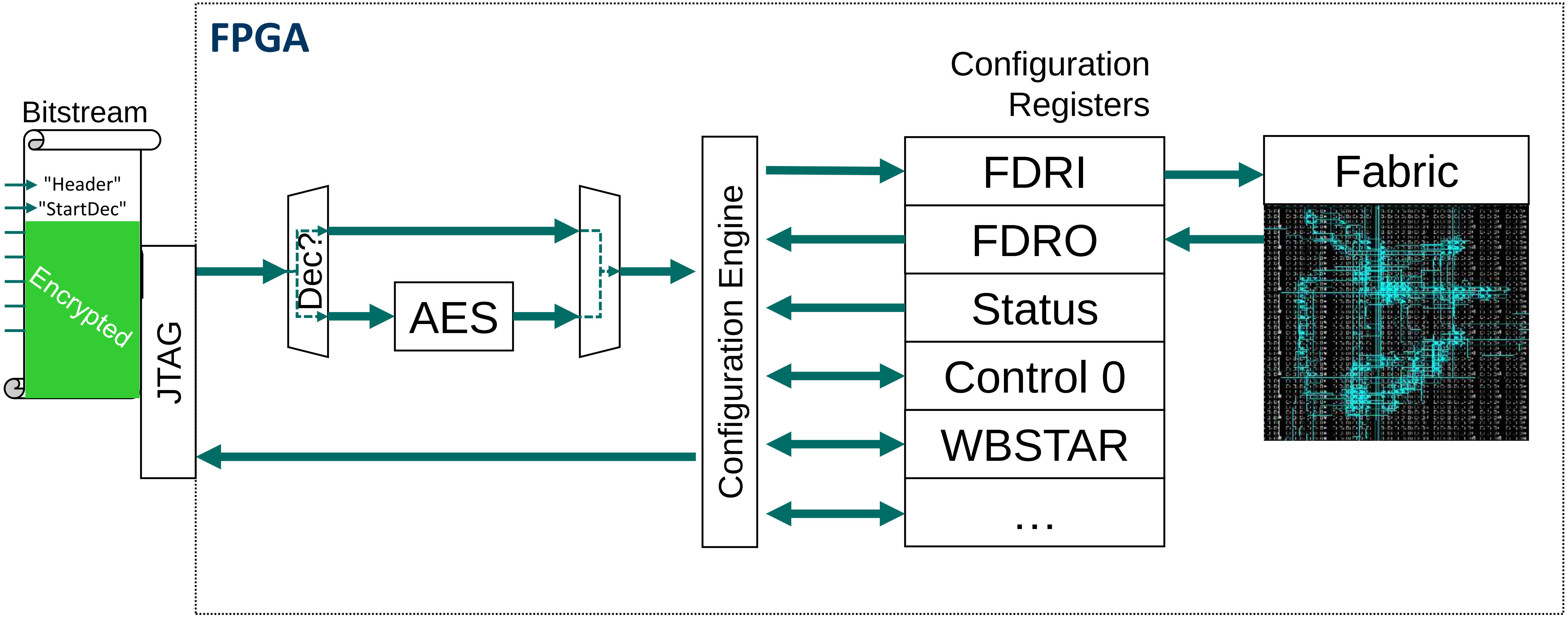
JTAG

FPGA

CONFIGURATION ENGINE



BITSTREAM PROGRAM

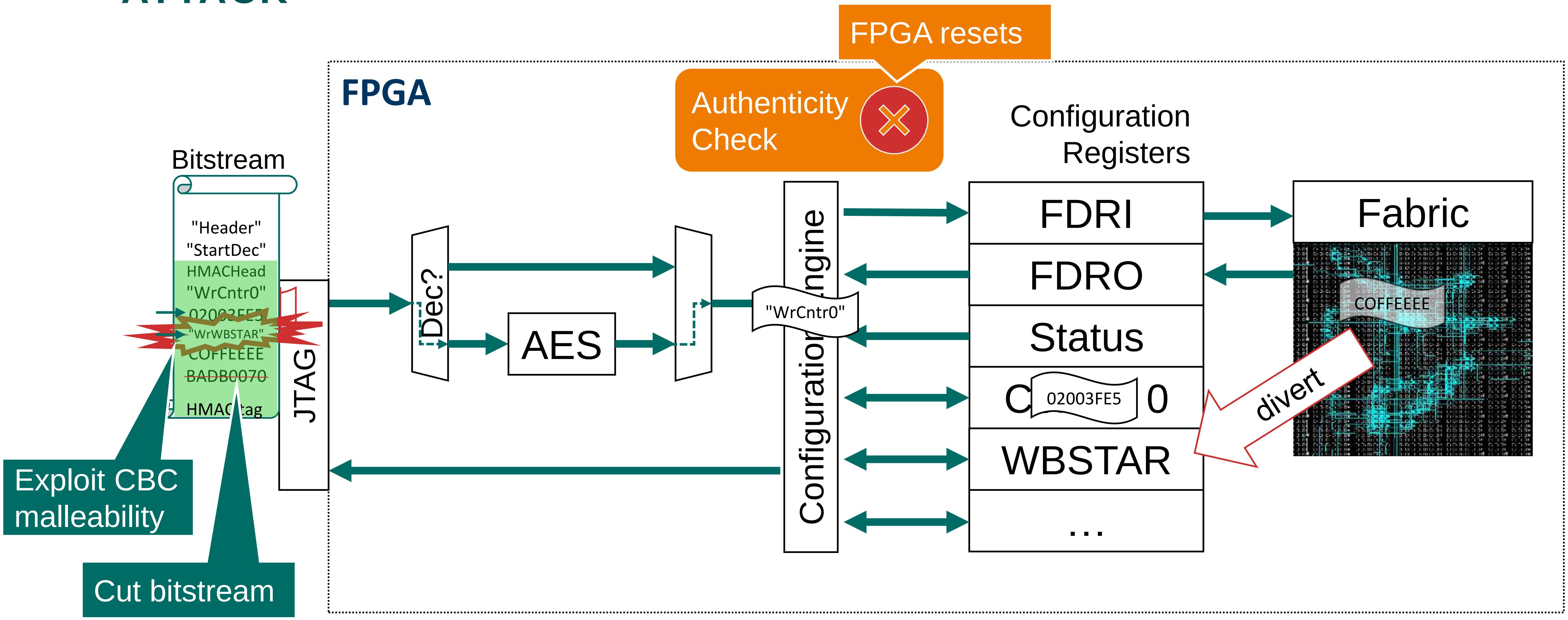


2

ATTACK I

BREAKING CONFIDENTIALITY

ATTACK



FPGA resets

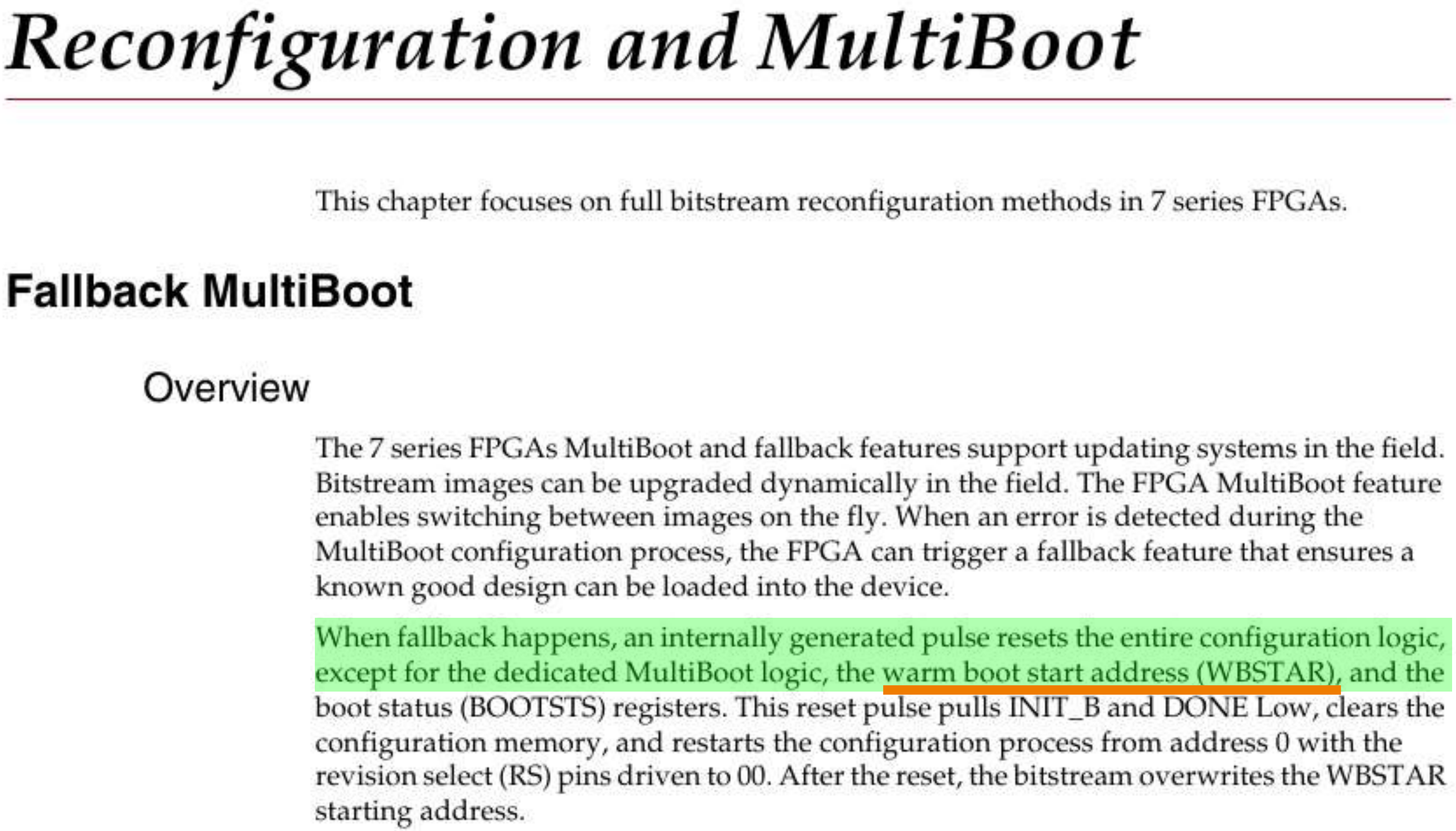
Authenticity Check

Exploit CBC malleability

Cut bitstream

divert

MULTIBOOT – DOCUMENTATION



Reconfiguration and MultiBoot

This chapter focuses on full bitstream reconfiguration methods in 7 series FPGAs.

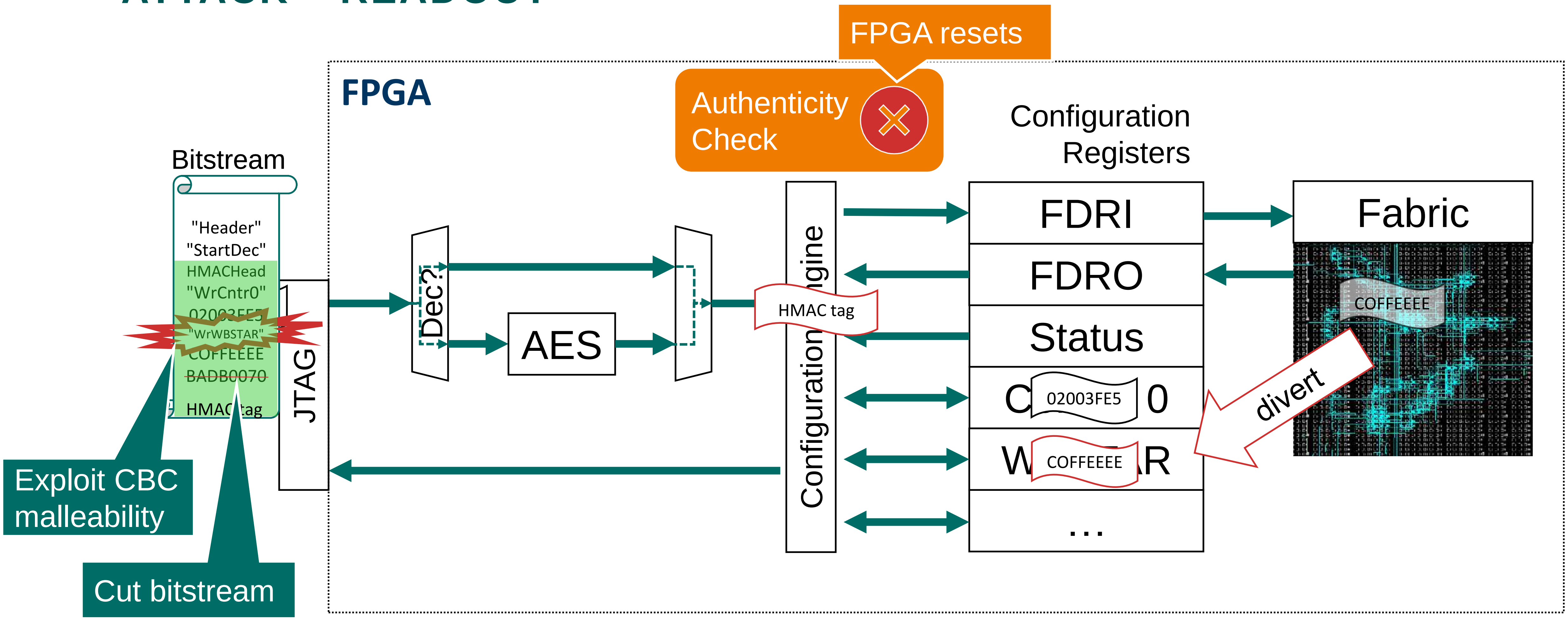
Fallback MultiBoot

Overview

The 7 series FPGAs MultiBoot and fallback features support updating systems in the field. Bitstream images can be upgraded dynamically in the field. The FPGA MultiBoot feature enables switching between images on the fly. When an error is detected during the MultiBoot configuration process, the FPGA can trigger a fallback feature that ensures a known good design can be loaded into the device.

When fallback happens, an internally generated pulse resets the entire configuration logic, except for the dedicated MultiBoot logic, the warm boot start address (WBSTAR), and the boot status (BOOTSTS) registers. This reset pulse pulls INIT_B and DONE Low, clears the configuration memory, and restarts the configuration process from address 0 with the revision select (RS) pins driven to 00. After the reset, the bitstream overwrites the WBSTAR starting address.

ATTACK – READOUT



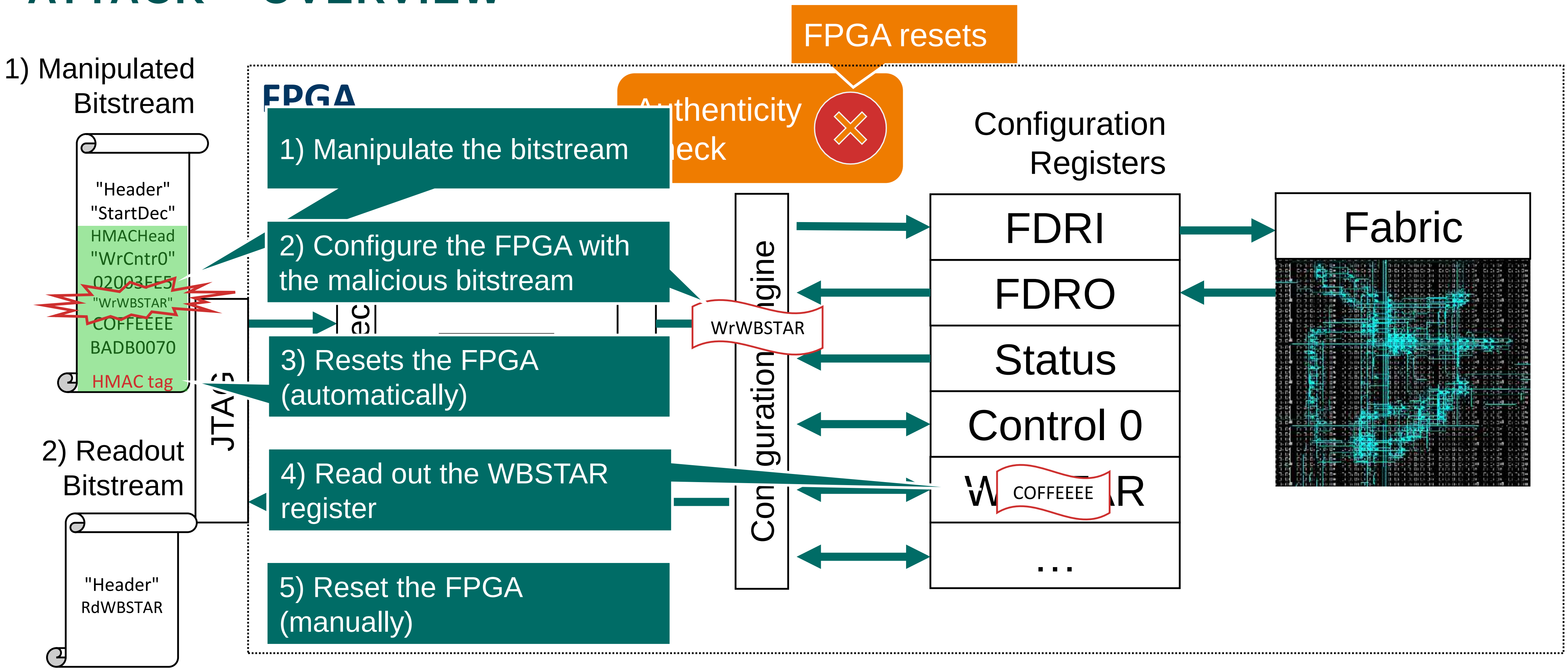
FPGA resets

Authenticity Check

Exploit CBC malleability

Cut bitstream

ATTACK – OVERVIEW



1) Manipulate the bitstream

2) Configure the FPGA with the malicious bitstream

3) Resets the FPGA (automatically)

4) Read out the WBSTAR register

5) Reset the FPGA (manually)

→Leaks one bitstream word (32 bits)

3

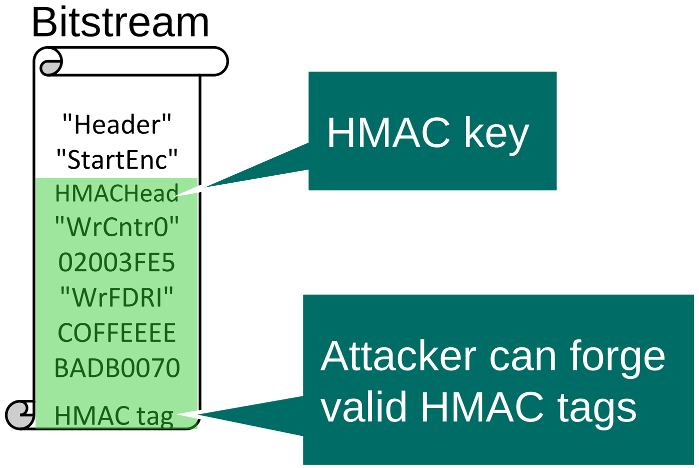
ATTACK II

BREAKING AUTHENTICITY

ATTACK II: BREAKING AUTHENTICITY

- HMAC key can be decrypted by attack I

  →Forge new valid HMAC tags



Bitstream

"Header"
"StartEnc"
HMACHead
"WrCntr0"
02003FE5
"WrFDRI"
COFFEEEE
BADB0070
HMAC tag

HMAC key

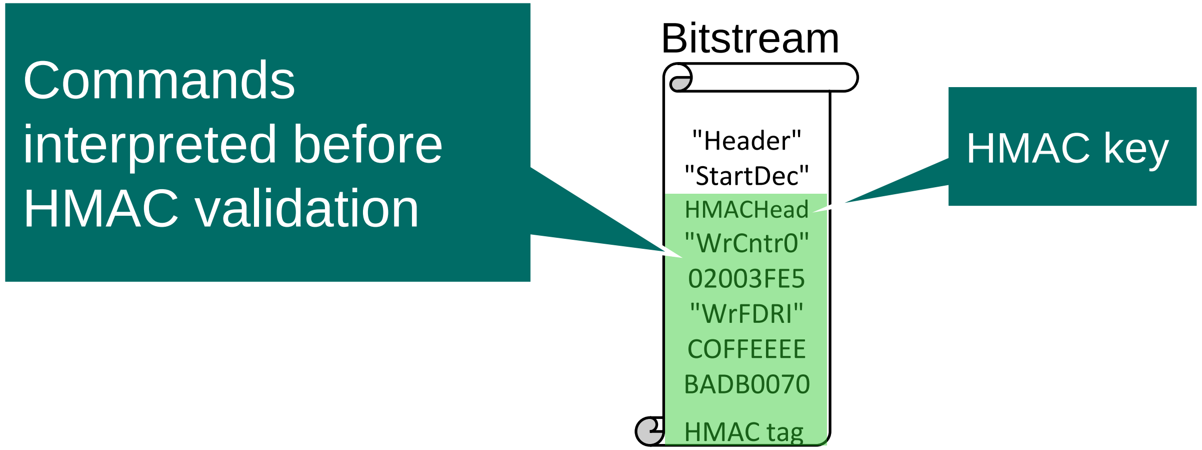
Attacker can forge valid HMAC tags

4

WHAT WENT WRONG?

WHAT WENT WRONG?

1. **“Use before validate“ (Attack I)**
2. **Key dependency (Attack II)**



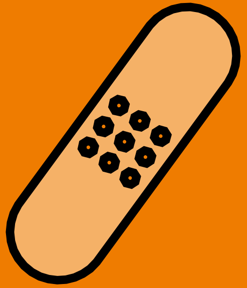
5

COUNTERMEASURES AND DEFENSE TECHNIQUES

COUNTERMEASURES & DEFENSE TECHNIQUES

Countermeasures Current 7-Series

Only raise-the-bare countermeasures exists

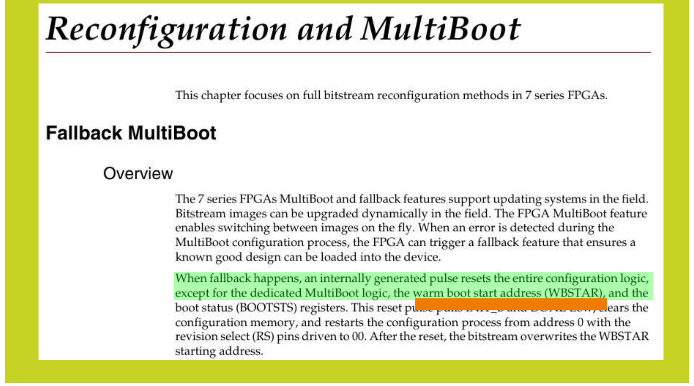


Countermeasures New FPGA Series

- Validate the bitstream before use
- Needs new silicon
- Available in new FPGA Series

General defense techniques

- Avoid ad-hoc security designs
- Model checking, information flow analysis
- Community analysis



Reconfiguration and MultiBoot

This chapter focuses on full bitstream reconfiguration methods in 7 series FPGAs.

Fallback MultiBoot

Overview

The 7 series FPGAs MultiBoot and fallback features support updating systems in the field. Bitstream images can be upgraded dynamically in the field. The FPGA MultiBoot feature enables switching between images on the fly. When an error is detected during the MultiBoot configuration process, the FPGA can trigger a fallback feature that ensures a known good design can be loaded into the device.

When fallback happens, an internally generated pulse resets the entire configuration logic, except for the dedicated MultiBoot logic, the warm boot start address (WBSTAR), and the boot status (BOOTSTS) registers. This reset pu[redacted]clears the configuration memory, and restarts the configuration process from address 0 with the revision select (RS) pins driven to 00. After the reset, the bitstream overwrites the WBSTAR starting address.

CONCLUSION

6

CONCLUSION

Full break of Xilinx 7-Series Bitstream Encryption

Any questions?

@MaikEnderEU

Amir Moradi

@ChristofPaar