



# 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 Security

**USENIX Security, August 14, 2020**



# HACKADAY

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT ABOUT

## RESEARCHERS BREAK FPGA ENCRYPTION USING FPGA ENCRYPTION

by: **Elliot Williams**

1 Comment

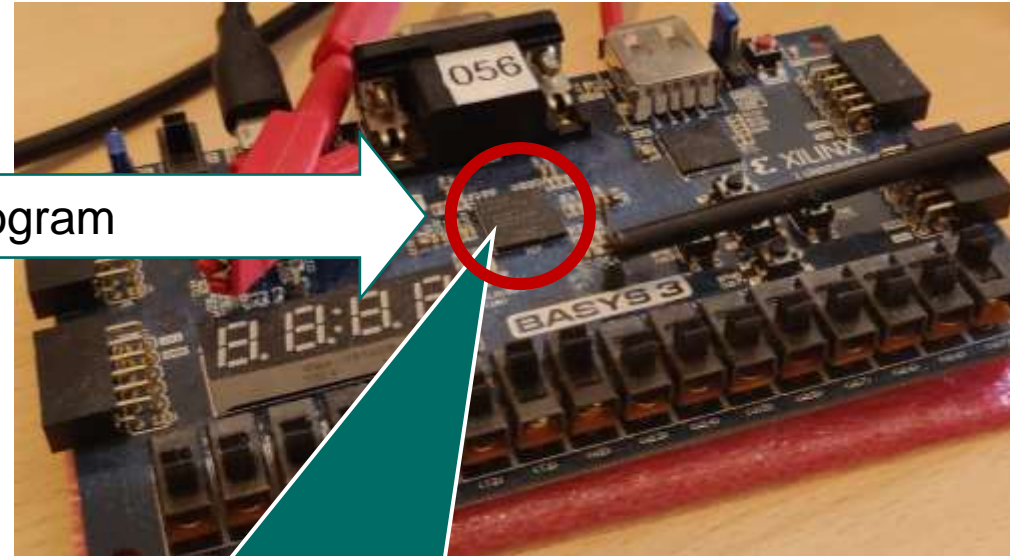
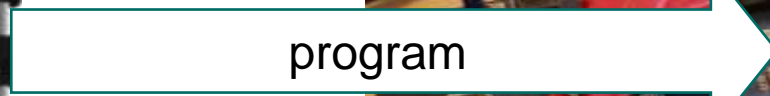
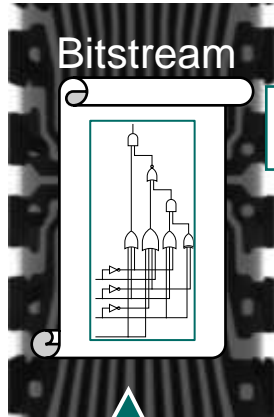


April 23, 2020



<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

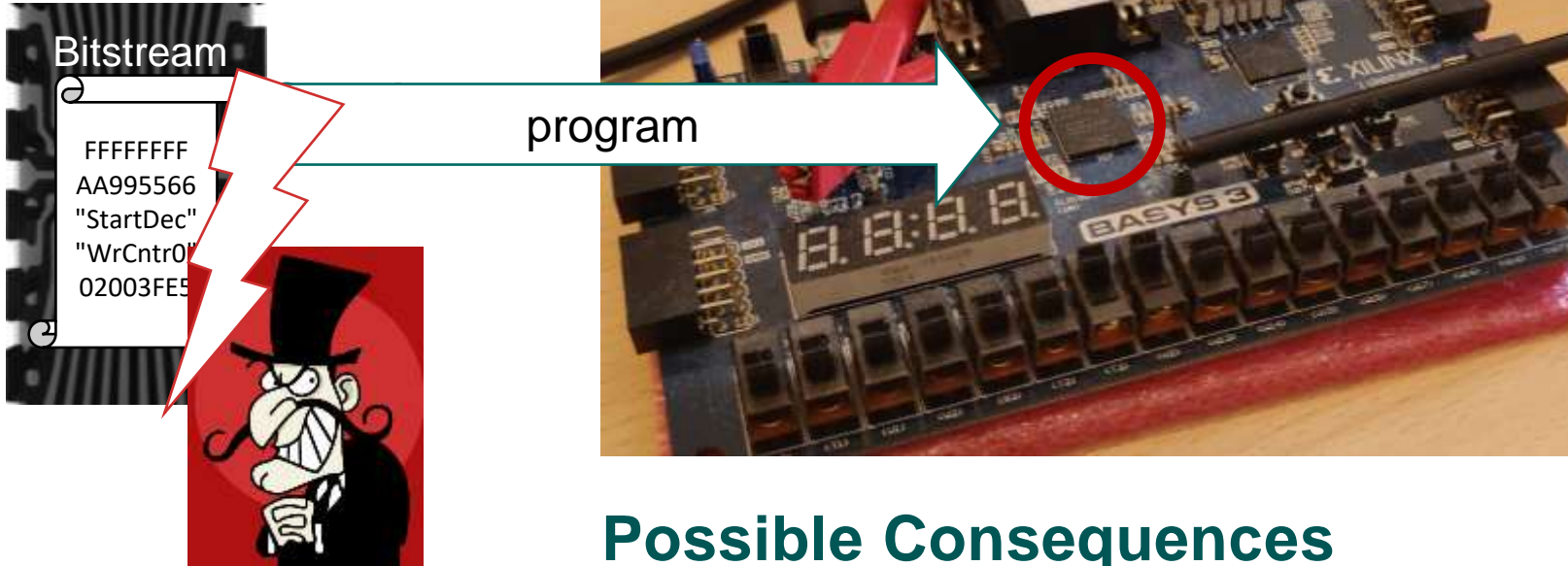


Photo by Patrick Tomasso on Unsplash



Photo by Chuanchai Pundel on Unsplash

# BITSTREAM SECURITY



## Possible Consequences

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



Photo by Thomas Jensen on Unsplash

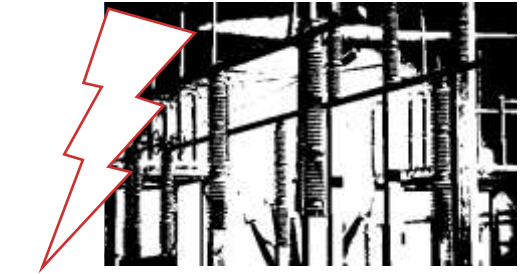


Photo by American Public Power Association on Unsplash

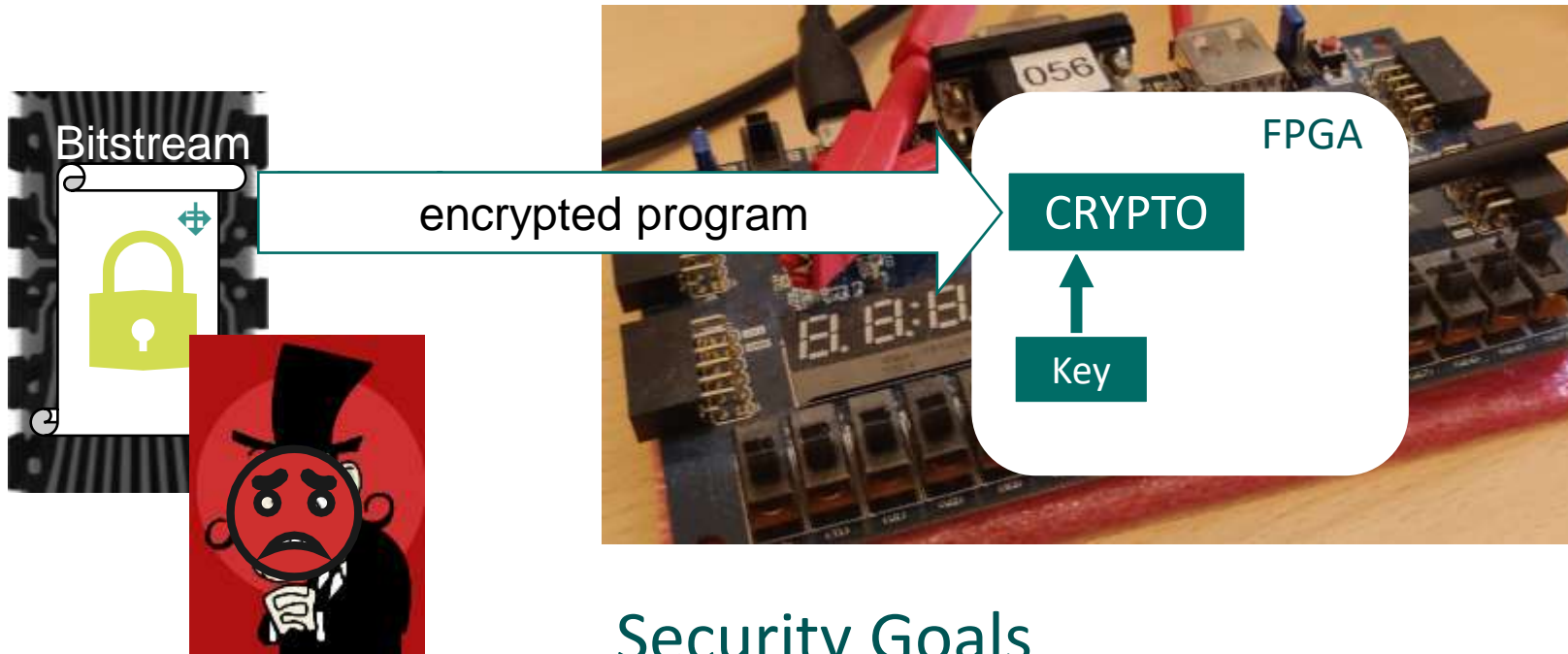


Photo by Patrick Tomasso on Unsplash



Photo by Chuanchai Pundel on Unsplash

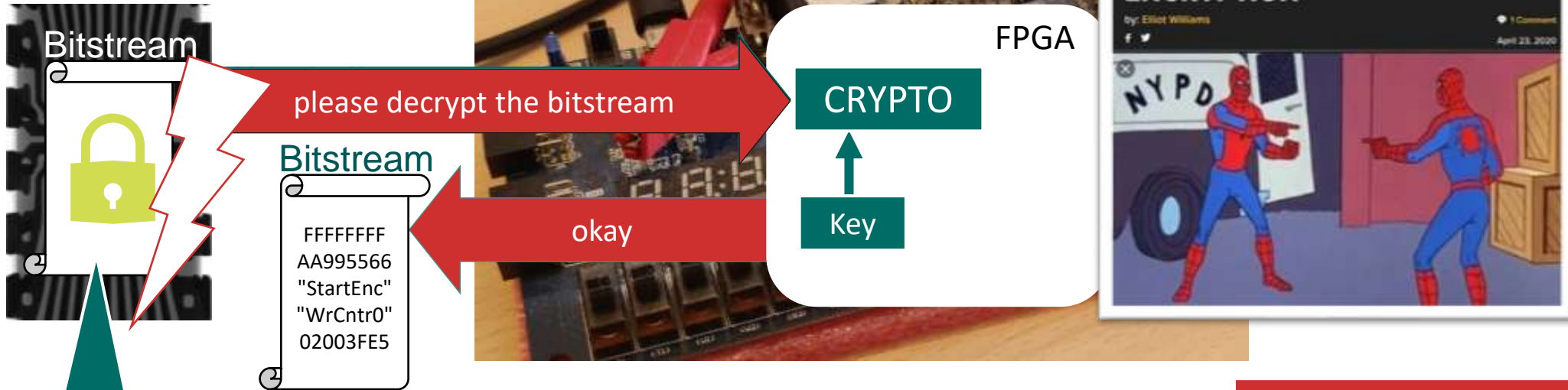
# BITSTREAM ENCRYPTION



## Security Goals

- AES-256
  - **Confidentiality:** bitstream is encrypted
- HMAC
  - **Authenticity:** FPGA loads only designs from integrator
  - **Integrity:** Bitstream is not changed

# ATTACK IN A NUTSHELL



Manipulate the encrypted bitstream

## Security Goals

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

Starbleed Attack I:  
Break Confidentiality

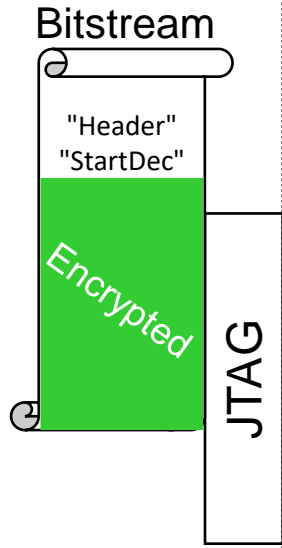
Starbleed Attack II:  
Break Authenticity



# HOW TO PROGRAM AN FPGA?

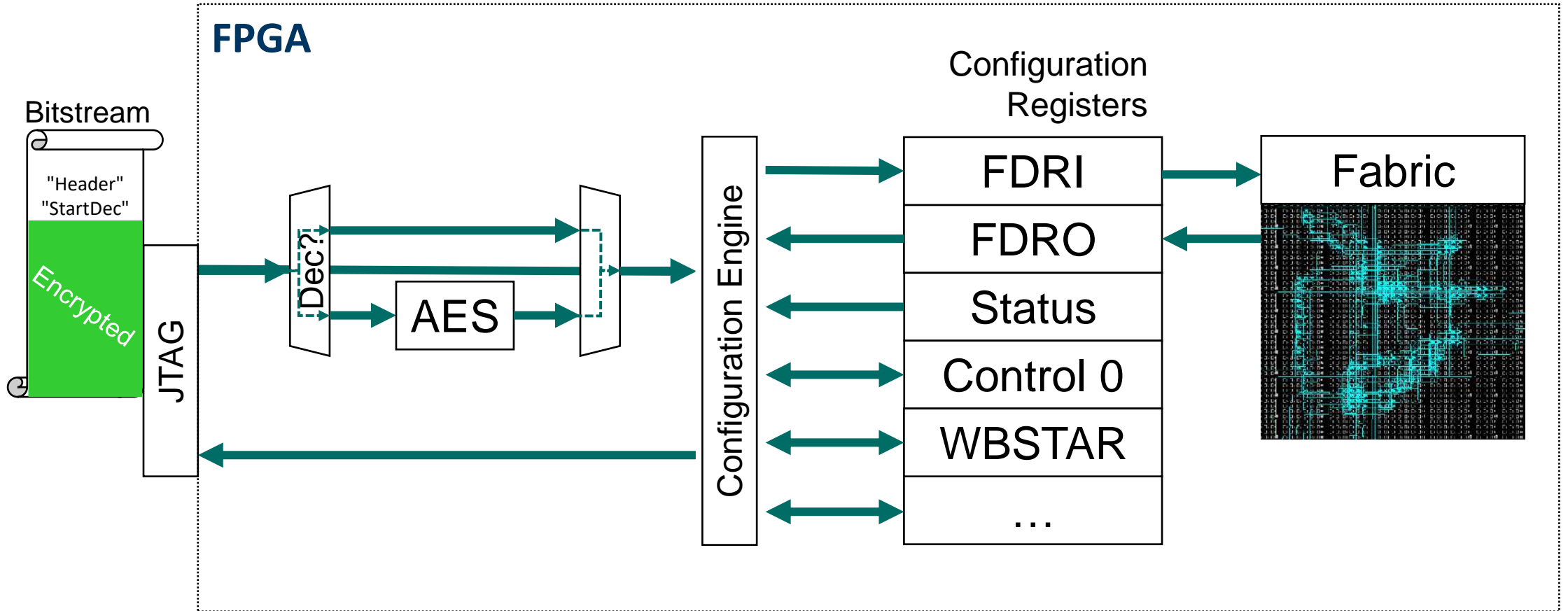
# CONFIGURATION ENGINE

## FPGA

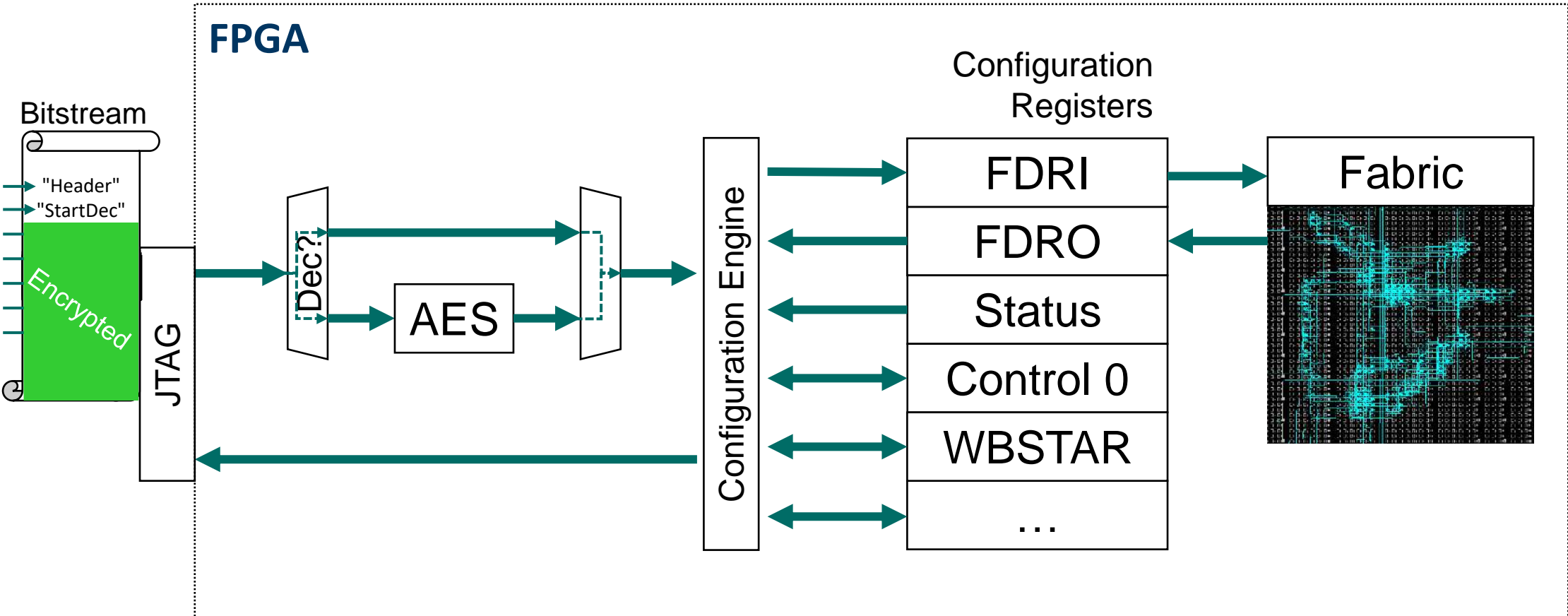




# CONFIGURATION ENGINE



# BITSTREAM PROGRAM

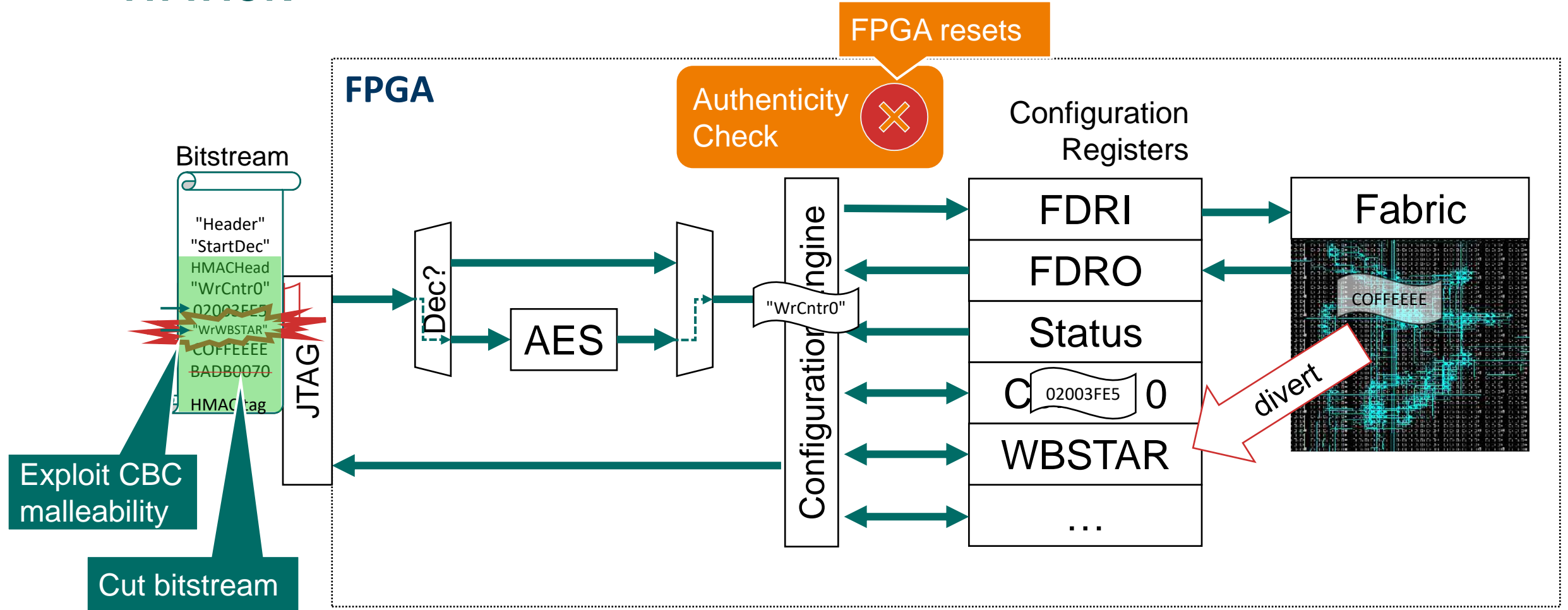




**ATTACK I**

*BREAKING CONFIDENTIALITY*

# ATTACK



# MULTIBOOT – DOCUMENTATION

## *Reconfiguration and MultiBoot*

---

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

### Fallback MultiBoot

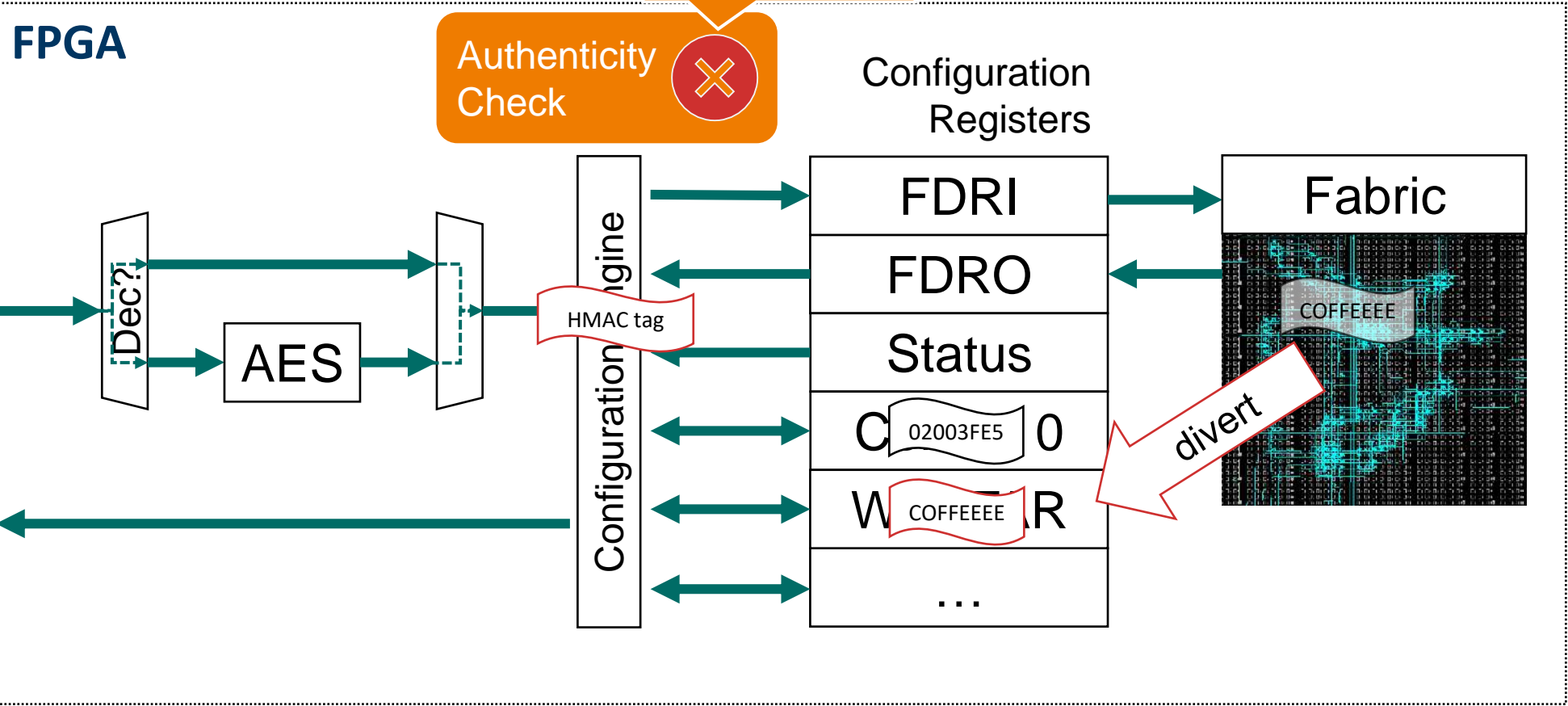
#### Overview

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

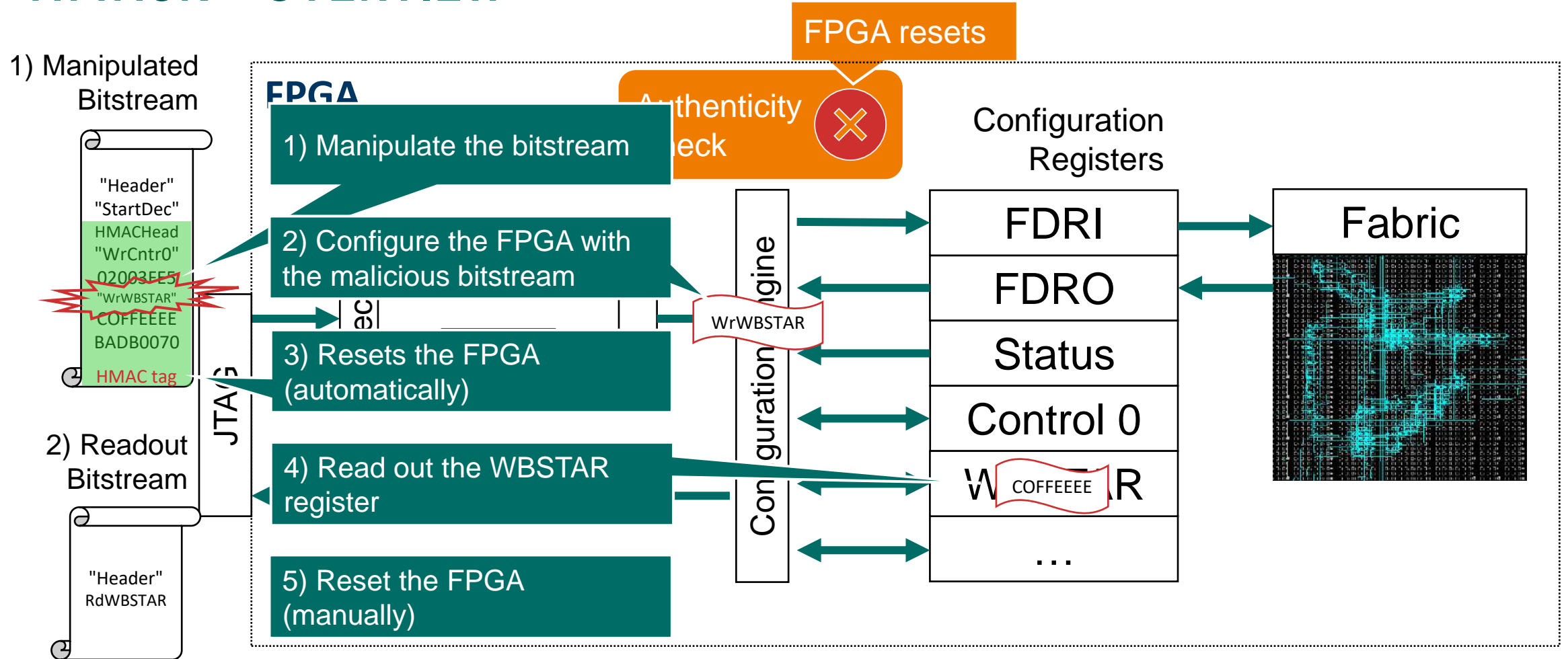


Exploit CBC malleability

Cut bitstream

divert

# ATTACK – OVERVIEW



→ Leaks one bitstream word (32 bits)



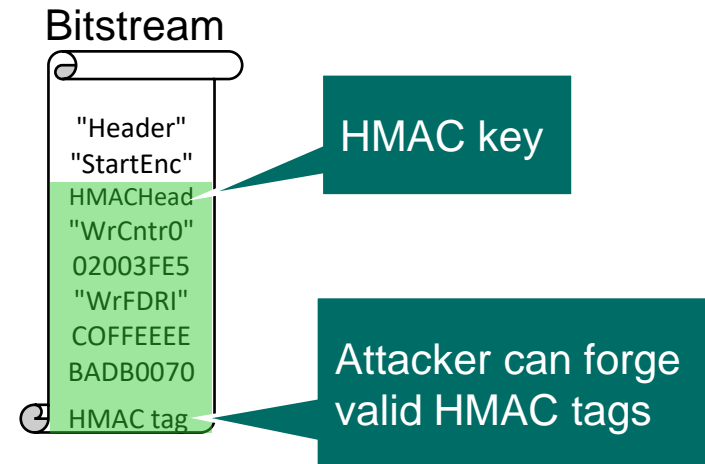
# ATTACK II

*BREAKING AUTHENTICITY*



# ATTACK II: BREAKING AUTHENTICITY

- HMAC key can be decrypted by attack I  
 → Forge new valid HMAC tags

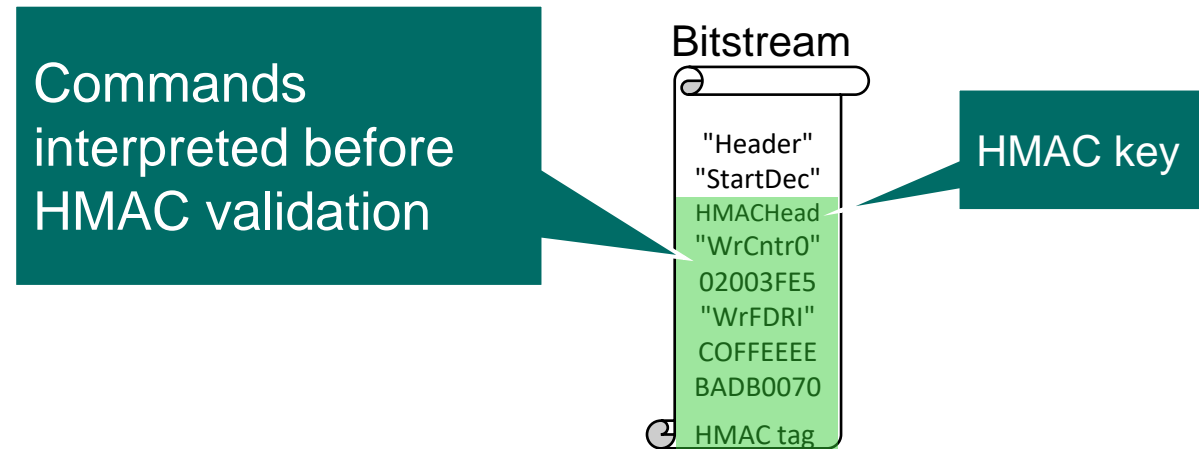




**WHAT WENT WRONG?**

# WHAT WENT WRONG?

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



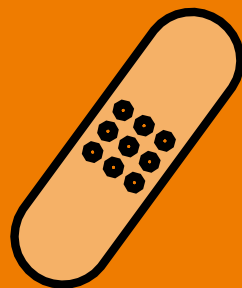


**COUNTERMEASURES  
AND  
DEFENSE TECHNIQUES**

# 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 pulse also 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



# CONCLUSION

**Full break of  
Xilinx 7-Series  
Bitstream  
Encryption**

**Any questions?**

**@MaikEnderEU  
Amir Moradi  
@ChristofPaar**

