SoC Security
FPGA Bitstream Encryption Basics

Nikolaus Grogger

3 November 2021

Outline

- Introduction
- Bitstream Encryption
- Bitstream Authentication
- Bitstream Structure
- Conclusion

Outline

- Introduction
- Bitstream Encryption
- Bitstream Authentication
- Bitstream Structure
- Conclusion

- No Vulnerabilities/Attacks/...

Outline

- Introduction
- Bitstream Encryption
- Bitstream Authentication
- Bitstream Structure
- Conclusion

- No Vulnerabilities/Attacks/...
- Details specific to Xilinx 7 Series FPGAs (Intel similar)

Introduction

Introduction

What we now about FPGAs so far:

- Large global market
- FPGAs are becoming increasingly popular
- Easy to configure

Introduction

What we now about FPGAs so far:

- Large global market
- FPGAs are becoming increasingly popular
- Easy to *configure*

Introduction

What we now about FPGAs so far:

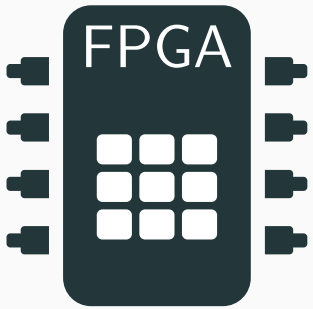
- Large global market
- FPGAs are becoming increasingly popular
- Easy to *configure*
  - Using bitstreams
  - Stored in external memory
  - In plaintext

Motivation

Why do we need bitstream encryption?

Inside our FPGA we store valuable secrets:

- Details of design
- Proprietary algorithms
- Implementation specifics



Motivation

Why do we need bitstream encryption?

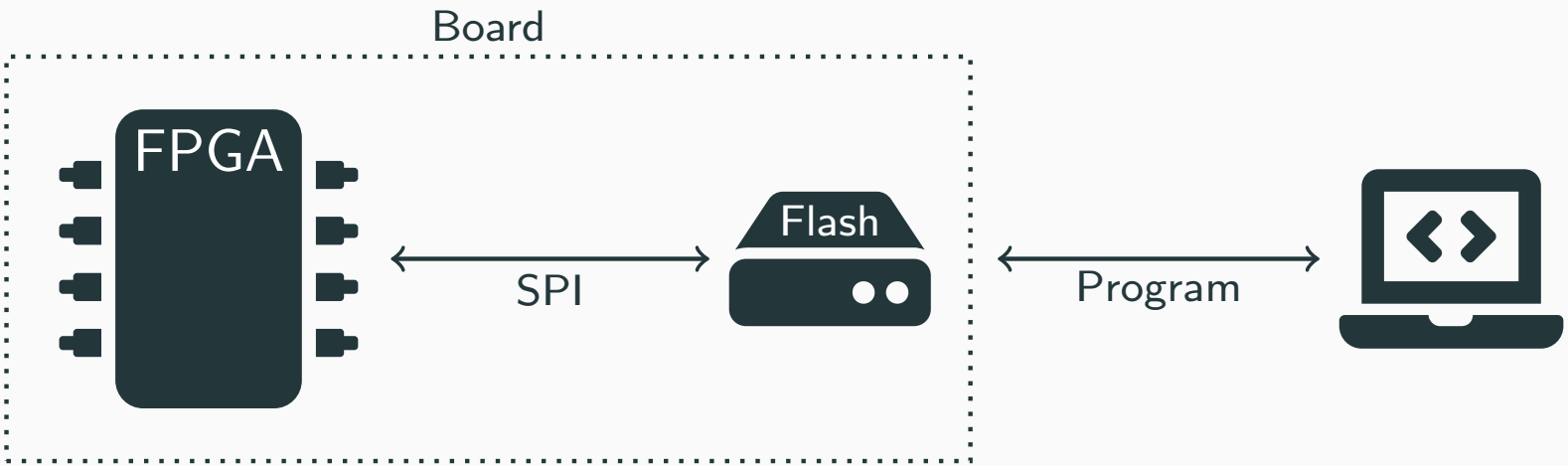
Inside our FPGA we store valuable secrets:

- Details of design
- Proprietary algorithms
- Implementation specifics

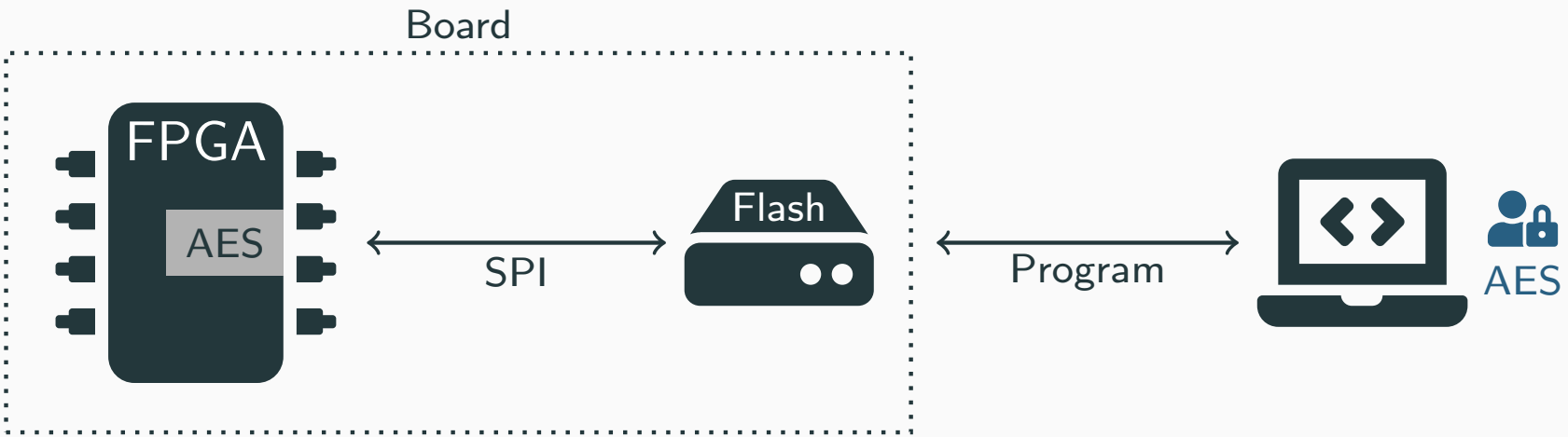
We want to secure our bitstream to protect our IP

Bitstream Encryption

Overview

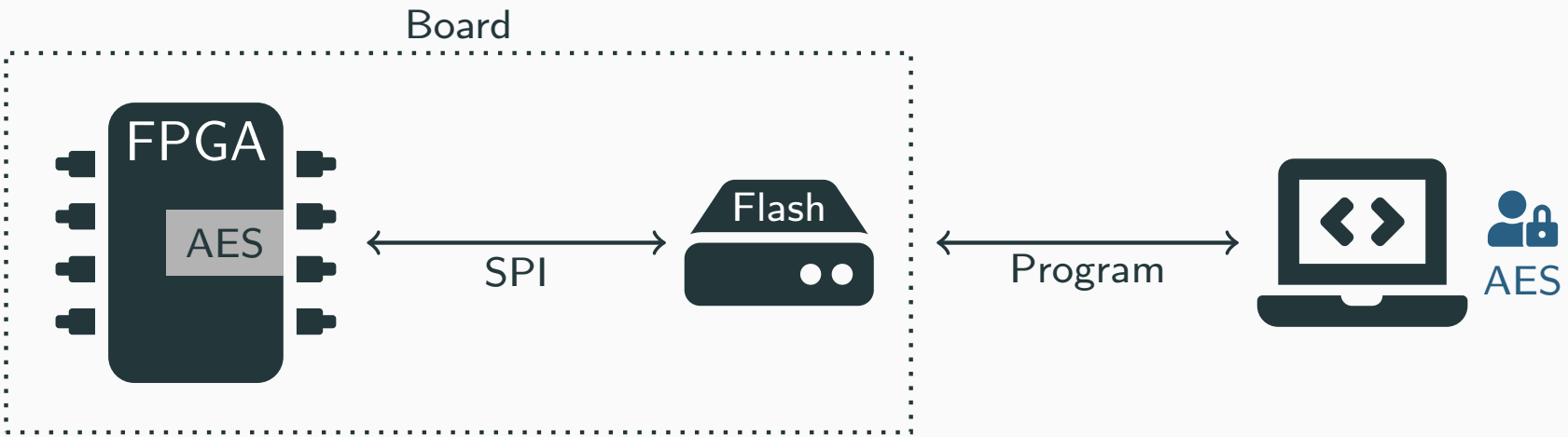


Overview



- Encrypt bitstream when creating
- Add decryption logic to FPGA

Overview



- Encrypt bitstream when creating
- Add decryption logic to FPGA
  - Where does the key come from?
  - Can we use that logic for other things?

Encryption

- Happens during creation of bitstream
- Specify key and options in XDC file
- For details see [5]

Encryption Example

Add to XDC file:

```
set_property BITSTREAM.ENCRYPTION.ENCRYPT
↪  YES [current_design]
set_property BITSTREAM.ENCRYPTION.ENCRYPTKEYSELECT
↪  BBRAM [current_design]
#set_property BITSTREAM.ENCRYPTION.ENCRYPTKEYSELECT
↪  eFUSE [current_design]
set_property BITSTREAM.ENCRYPTION.KEY0
↪  256'h46AC...3E7A [current_design]
```

- Other options: `HKEY`, `KEYFILE`, and `STARTCBC`

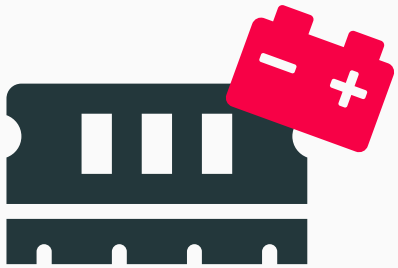
➔ Generates NKY file which can be loaded into FPGA

Decryption logic

- AES-256 in CBC mode
  - Supply key and IV when writing bitstream
- Decryption logic can not be used for anything else
- Key storage
  - BBRAM
  - eFUSE

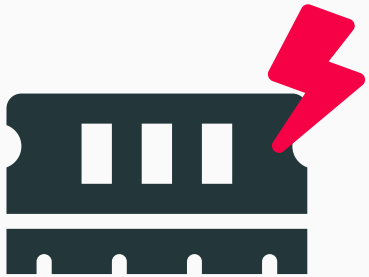
Key storage: BBRAM

- Battery-backed RAM
- Volatile storage
- ⊕ Reprogrammable
- ⊖ Needs external battery



Key storage: eFUSE

- Non-volatile
- One-time programmable
- ⊕ No battery required
- ⊖ Key can not be cleared/changed/removed
- ⊖ “Less secure than BBRAM” (?)



Bitstream Authentication

Bitstream Authentication

Not only confidentiality

- Make sure no one changed bitstream
- Comes together with encryption
- Key not stored on-chip

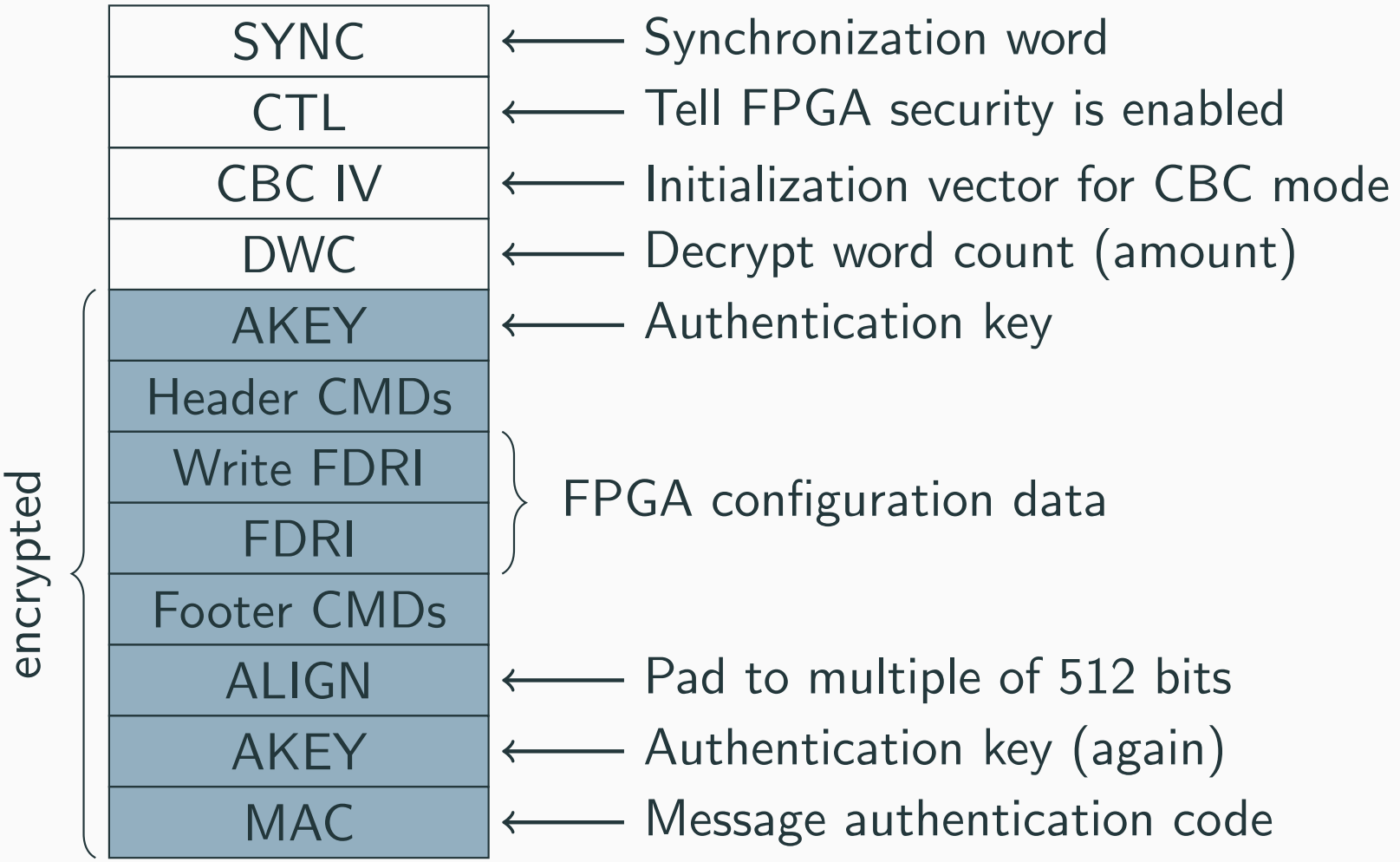
Bitstream Authentication Details

Providing integrity and authenticity

- HMAC using SHA-256
- Separate key from AES (XDC)
- Key wrapped in encrypted bitstream
- MAC contained in encrypted bitstream

Bitstream Structure

Bitstream Structure

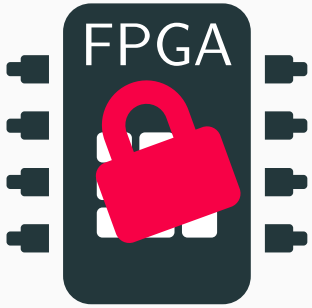


Conclusion

Conclusion

FPGAs contain valuable secrets

- Protect IP in FPGA
- Encrypt bitstream using AES
- Authenticate bitstream



SoC Security
FPGA Bitstream Encryption Basics

Nikolaus Grogger

3 November 2021

References i

[1] Intel. AN 556: Using the Design Security Features in Intel FPGAs (Version 2021.05.21). https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an556.pdf. (Visited on 2021-10-29).

[2] Stephen M. Trimberger and Jason J. Moore. FPGA Security: Motivations, Features, and Applications. In: Proceedings of the IEEE 102.8 (2014), pp. 1248–1265. DOI: 10.1109/JPROC.2014.2331672.

[3] Xilinx. 7 Series FPGAs Configuration User Guide (UG470 v1.13.1). https://www.xilinx.com/support/documentation/user_guides/ug470_7Series_Config.pdf. (Visited on 2021-10-29).

[4] Xilinx. Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs (XAPP1084 v1.4). https://www.xilinx.com/support/documentation/application_notes/xapp1084_tamp_resist_dsgns.pdf. (Visited on 2021-10-29).

References ii

[5] Xilinx. Using Encryption to Secure a 7 Series FPGA Bitstream (XAPP1239 v1.2). https://www.xilinx.com/support/documentation/application_notes/xapp1239-fpga-bitstream-encryption.pdf. (Visited on 2021-10-29).