Pynqrypt

A FPGA-accelerated encryption library for PYNQ

Roberto Alessandro Bertolini

FPGA101 - Politecnico di Milano

January 9, 2023

The hardware

PYNQ

The hardware

PYNQ

PYNQ is an open-source project which provides a Python-based development environment for Xilinx Zynq SoCs.

The hardware

PYNQ

PYNQ is an open-source project which provides a Python-based development environment for Xilinx Zynq SoCs.

Pros

The hardware

PYNQ

PYNQ is an open-source project which provides a Python-based development environment for Xilinx Zynq SoCs.

Pros

- Easy to use

The hardware

PYNQ

PYNQ is an open-source project which provides a Python-based development environment for Xilinx Zynq SoCs.

Pros

- Easy to use
- Portable

The hardware

PYNQ

PYNQ is an open-source project which provides a Python-based development environment for Xilinx Zynq SoCs.

Pros

- Easy to use
- Portable
- Fast

Encryption algorithms

AES

Encryption algorithms

AES

AES is a symmetric-key algorithm for the encryption of electronic data. It is widely used in both industry and government to protect sensitive data.

Encryption algorithms

AES

AES is a symmetric-key algorithm for the encryption of electronic data. It is widely used in both industry and government to protect sensitive data.

AES-CTR

Encryption algorithms

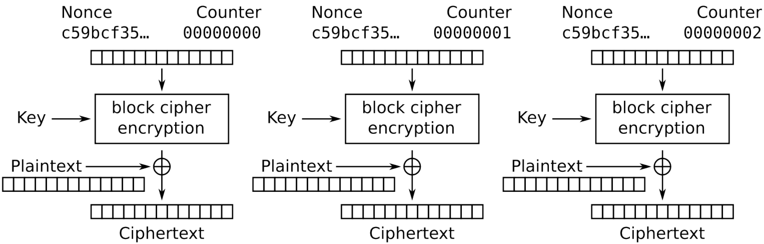
AES

AES is a symmetric-key algorithm for the encryption of electronic data. It is widely used in both industry and government to protect sensitive data.

AES-CTR

AES-CTR is a mode of operation for the AES block cipher. It is a highly-parallelizable and efficient encryption algorithm, well suited for hardware acceleration.

AES-CTR



Counter (CTR) mode encryption

Performance Considerations

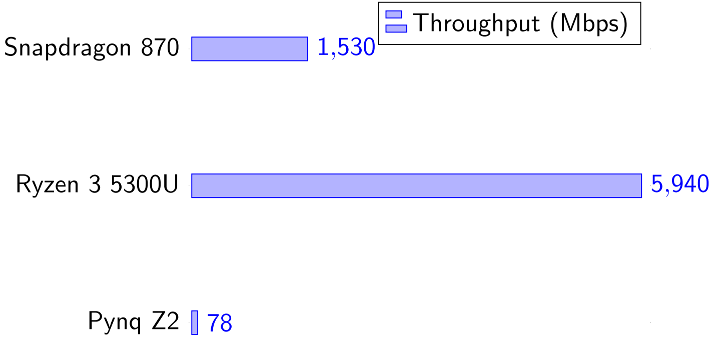
Security usually comes at the cost of performance.

Performance Considerations

Security usually comes at the cost of performance. High performance systems have no trouble satisfying these requirements, but the same cannot be said for low-power embedded systems.

Performance Considerations

Security usually comes at the cost of performance. High performance systems have no trouble satisfying these requirements, but the same cannot be said for low-power embedded systems.



What is Pynqrypt

Pynqrypt is a Python library for data encryption with the AES-CTR algorithm.

What is Pynqrypt

Pynqrypt is a Python library for data encryption with the AES-CTR algorithm.

- Works on every platform supported by PYNQ (with the correct bitstream)

What is Pynqrypt

Pynqrypt is a Python library for data encryption with the AES-CTR algorithm.

- Works on every platform supported by PYNQ (with the correct bitstream)
- Compatible with other AES-CTR implementations

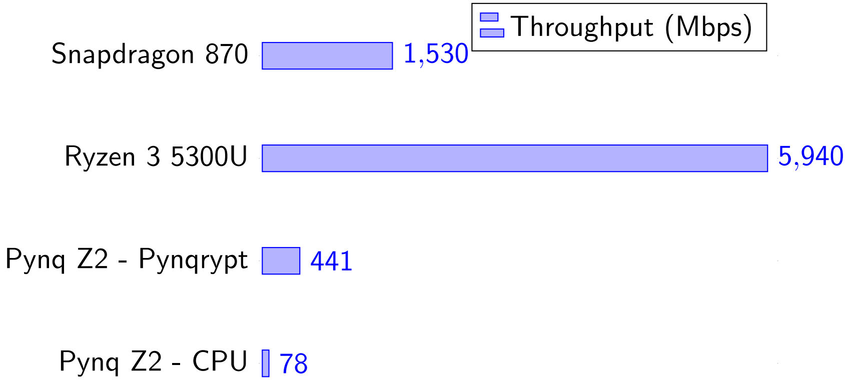
What is Pynqrypt

Pynqrypt is a Python library for data encryption with the AES-CTR algorithm.

- Works on every platform supported by PYNQ (with the correct bitstream)
- Compatible with other AES-CTR implementations
- Fast

Performance comparison

Performance comparison



Usage

Usage

```
from pynqrypt import Pynqrypt
import numpy as np
```

Usage

```
from pynqrypt import Pynqrypt
import numpy as np
```

```
pynqrypt = Pynqrypt(file='./bistream.xsa', post_ap=
True)
```

Usage

```python
from pynqrypt import Pynqrypt
import numpy as np
```

```python
pynqrypt = Pynqrypt(file='./bistream.xsa', post_ap=
True)
```

```python
data = np.frombuffer(..., np.uint8)
key = ...
nonce = ...

pynqrypt.set_key(key)
pynqrypt.set_nonce(nonce)
pynqrypt.set_length(len(data))
```

Usage

Usage

```
input_buffer = pynqrypt.get_input_array()
output_buffer = pynqrypt.get_output_array()

input_buffer[:] = data[:]

pynqrypt.prepare()
pynqrypt.run_blocking()
```

Usage

```
input_buffer = pynqrypt.get_input_array()
output_buffer = pynqrypt.get_output_array()

input_buffer[:] = data[:]

pynqrypt.prepare()
pynqrypt.run_blocking()
```

```
output_buffer.invalidate()

... = bytes(output_buffer)

pynqrypt.cleanup()
```

USBCrypt: let's see it in action!

Issues encountered

Issues encountered

- Issue: Vitis HLS doesn’t work
  Solution: install Ubuntu 22.04 LTS

Issues encountered

- Issue: Vitis HLS doesn't work
  Solution: install Ubuntu 22.04 LTS
- Issue: Vitis HLS doesn't work
  Solution: install `libncurses5-dev`

Issues encountered

- Issue: Vitis HLS doesn't work
  Solution: install Ubuntu 22.04 LTS
- Issue: Vitis HLS doesn't work
  Solution: install `libncurses5-dev`
- Issue: Vitis HLS doesn't work
  Solution: install g++ and other buildtools

Issues encountered

- Issue: Vitis HLS doesn't work
  Solution: install Ubuntu 22.04 LTS
- Issue: Vitis HLS doesn't work
  Solution: install `libncurses5-dev`
- Issue: Vitis HLS doesn't work
  Solution: install g++ and other buildtools
- Issue: Vitis HLS doesn't work
  Solution: always do a clean build of the project

Issues encountered

- Issue: Vitis HLS doesn't work
  Solution: install Ubuntu 22.04 LTS
- Issue: Vitis HLS doesn't work
  Solution: install `libncurses5-dev`
- Issue: Vitis HLS doesn't work
  Solution: install g++ and other buildtools
- Issue: Vitis HLS doesn't work
  Solution: always do a clean build of the project
- Issue: my IP doesn't work
  Solution: wire all the ports

Issues encountered

- Issue: Vitis HLS doesn't work
  Solution: install Ubuntu 22.04 LTS
- Issue: Vitis HLS doesn't work
  Solution: install `libncurses5-dev`
- Issue: Vitis HLS doesn't work
  Solution: install g++ and other buildtools
- Issue: Vitis HLS doesn't work
  Solution: always do a clean build of the project
- Issue: my IP doesn't work
  Solution: wire all the ports
  Maybe rewatch the lesson?

What did I learn?