KU LEUVEN

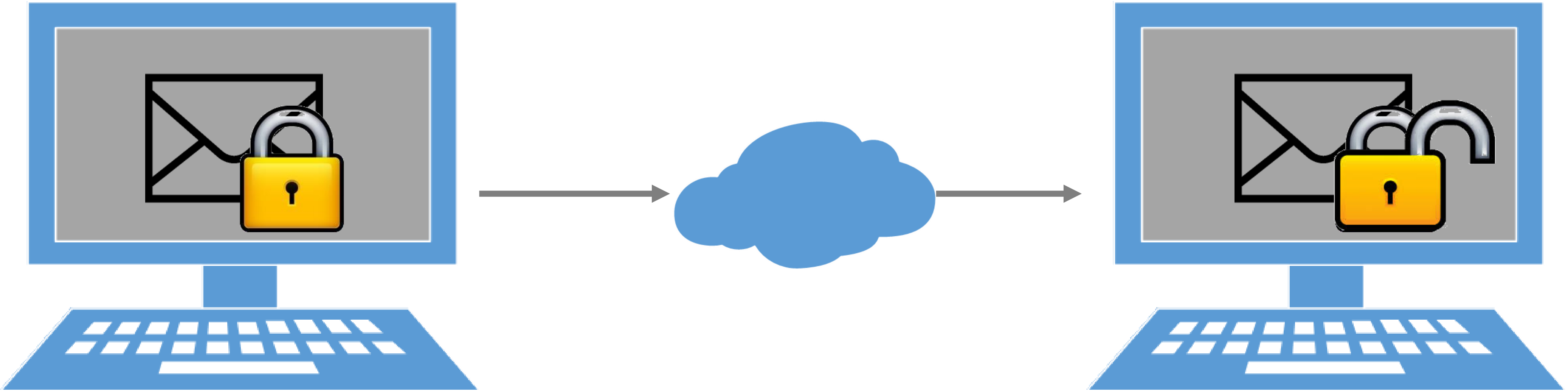

# Hardware Acceleration of a Software-based VPN

Furkan Turan
Ruan de Clercq, Pieter Maene, Oscar Reparaz
Ingrid Verbauwhede

KU Leuven - COSIC

# VPN Introduction

VPN (Virtual Private Network) encrypts the communication between two parties.

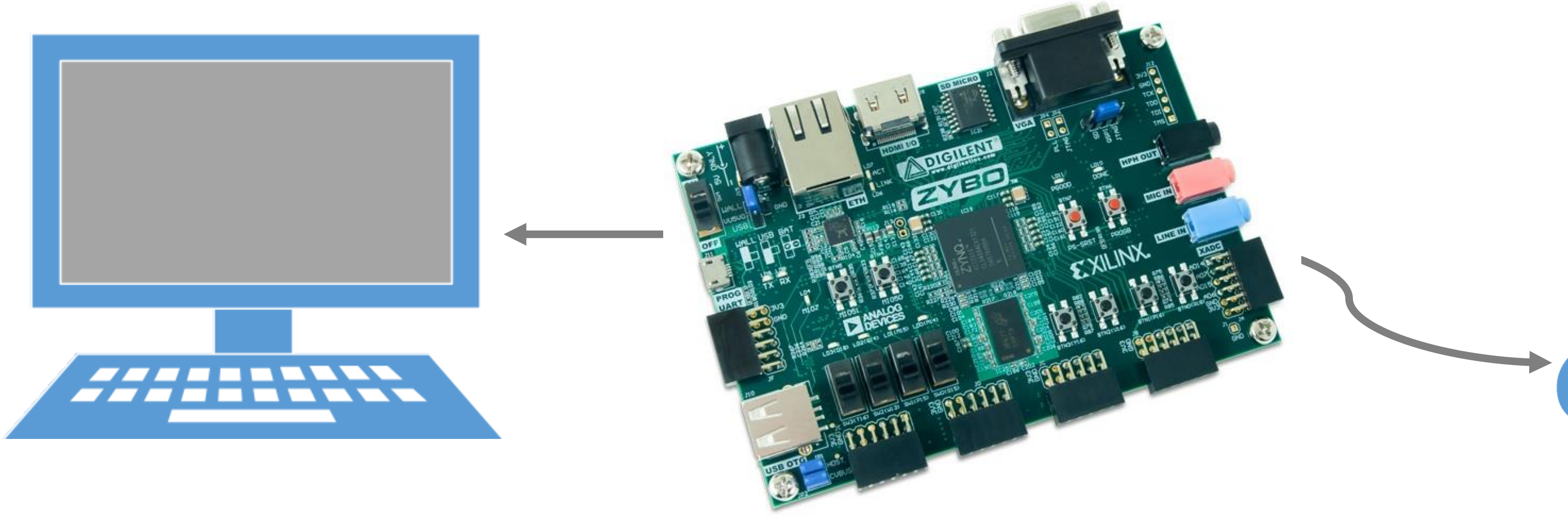


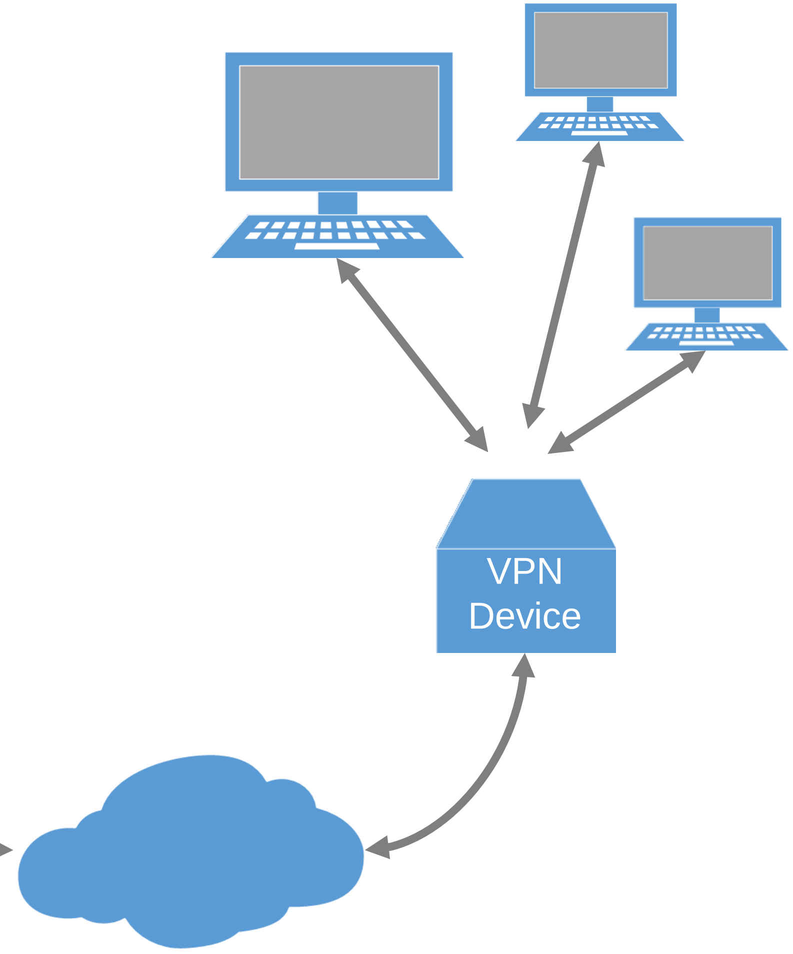
# VPN Device Introduction

Goal: Start with a VPN application,

Convert it into a 2 port VPN device,

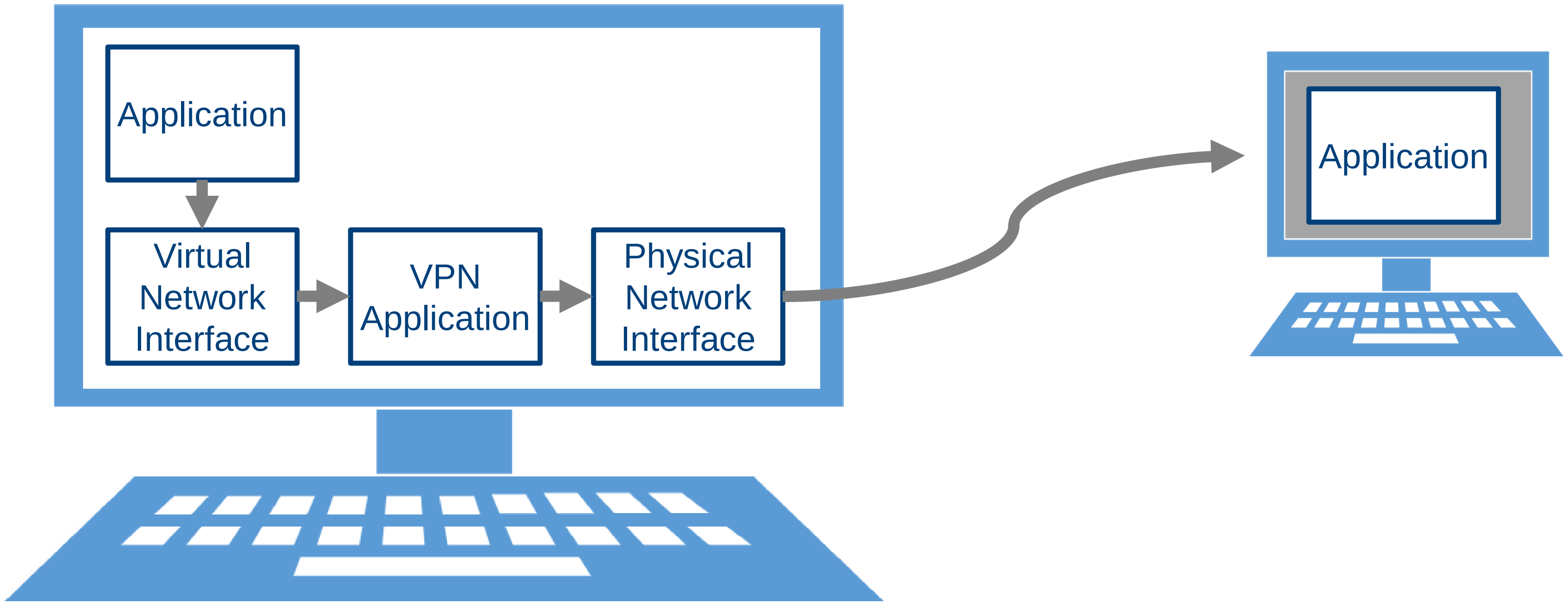
Accelerate it with a cryptographic coprocessor.



# Software-based VPN

How a software-based VPN application works:

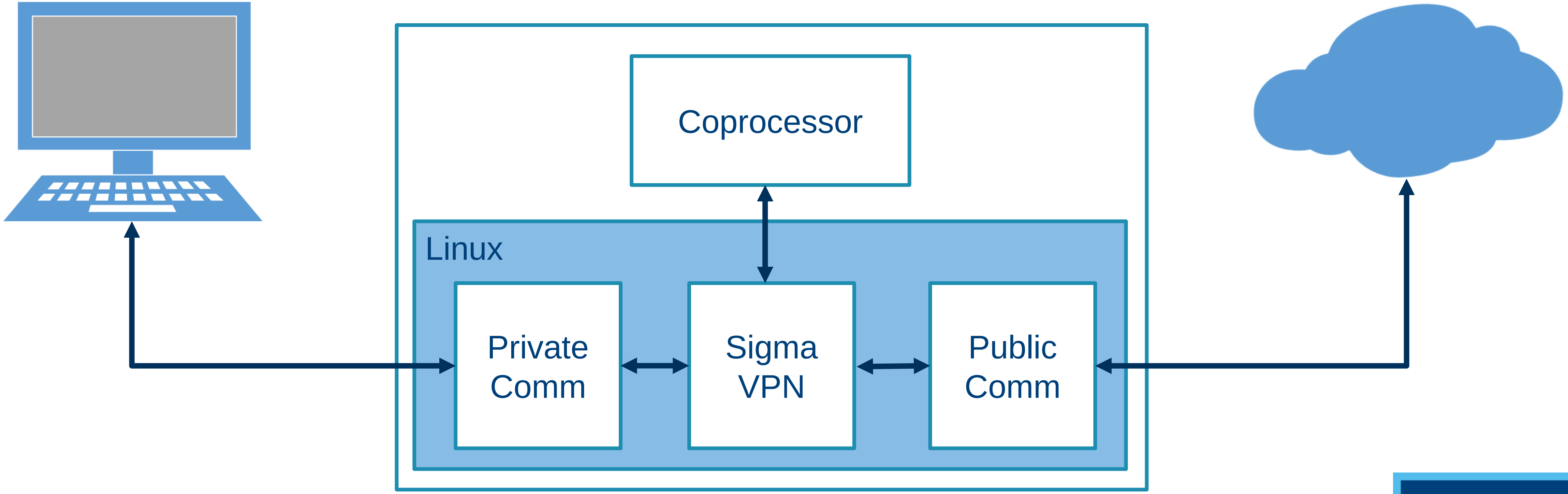



**SigmaVPN:** Light-weight, secure and modular software-based VPN

# 2 Port VPN Device with Hardware Accelerator

The new Private Comm. module uses a Physical Network Interface.

It is capable of even capturing broadcast messages.



# NaCl's CryptoBox

**Alice**

$K_S \leftarrow \text{ECDH}(K_{SEC,A}, K_{PUB,B})$

$K_D \leftarrow \text{HSalsa20}(K_S, N_1)$

$S \leftarrow \text{Salsa20}(K_{D,} N_2 \,||\, \text{CTR})$

$CT \leftarrow S \oplus MSG$

$MAC_A \leftarrow \text{Poly1305}(CT, S)$

$CT, MAC_A, N_{1,2}$

**Bob**

$K_S \leftarrow \text{ECDH}(K_{SEC,B}, K_{PUB,A})$

$K_D \leftarrow \text{HSalsa20}(K_S, N_1)$

$S \leftarrow \text{Salsa20}(K_{D,} N_2 \,||\, \text{CTR})$

$MAC_B \leftarrow \text{Poly1305}(CT, S)$

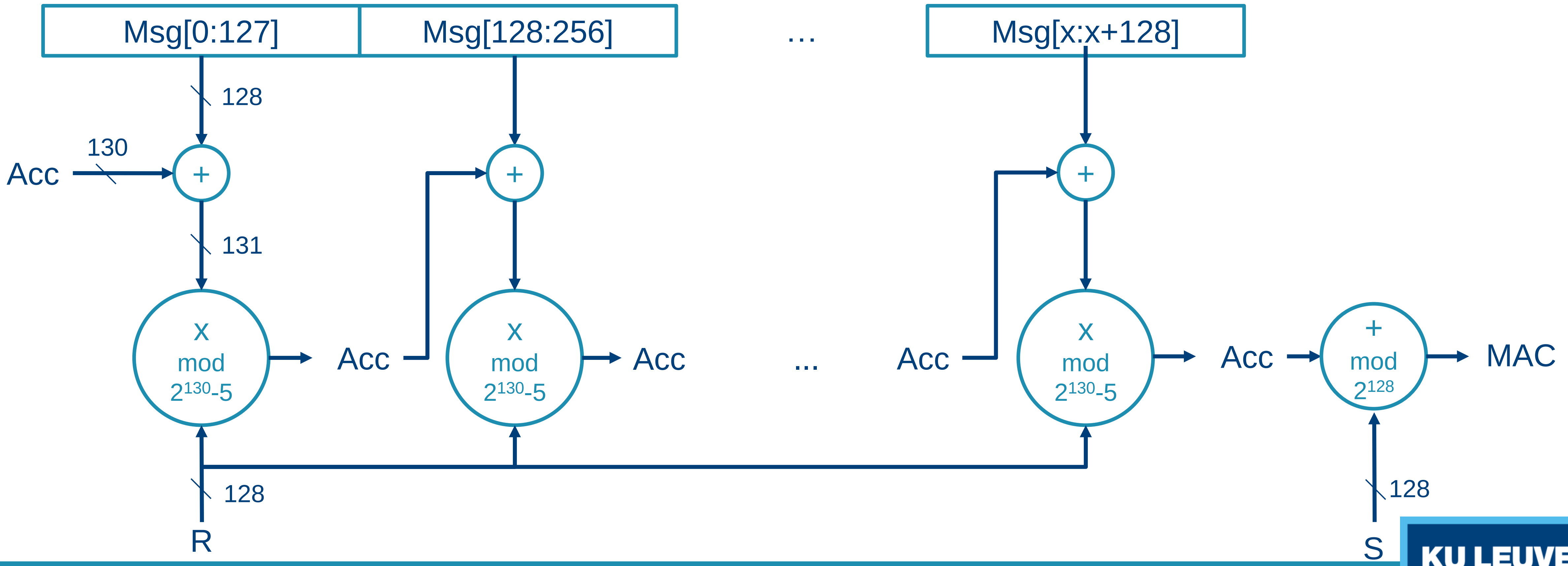
$\text{Compare}(MAC_A, MAC_B)$

$MSG \leftarrow S \oplus CT$

# One-time Authenticator: Poly1305

An update operation for each 128-bit blocks of the message

The operation implements a modular multiplication in radix ($2^{130}$-5)



# Poly1305's Implementation

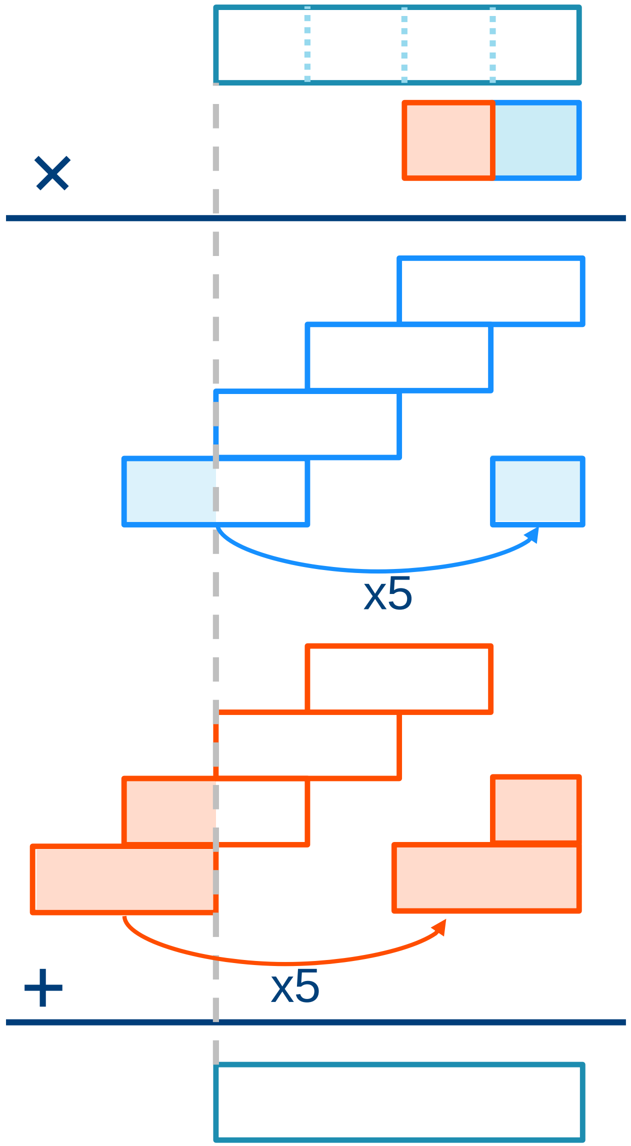
Implemented using a school-book multiplication:

- Big multiplication is divided into smaller blocks
- Followed by propagation of the results

Each small block multiplication is handled in single-cycle multipliers of Zynq's DSP48 Slices

To boost the performance:

- Parallel execution of smaller-block multiplications
- Parallel propagating the results





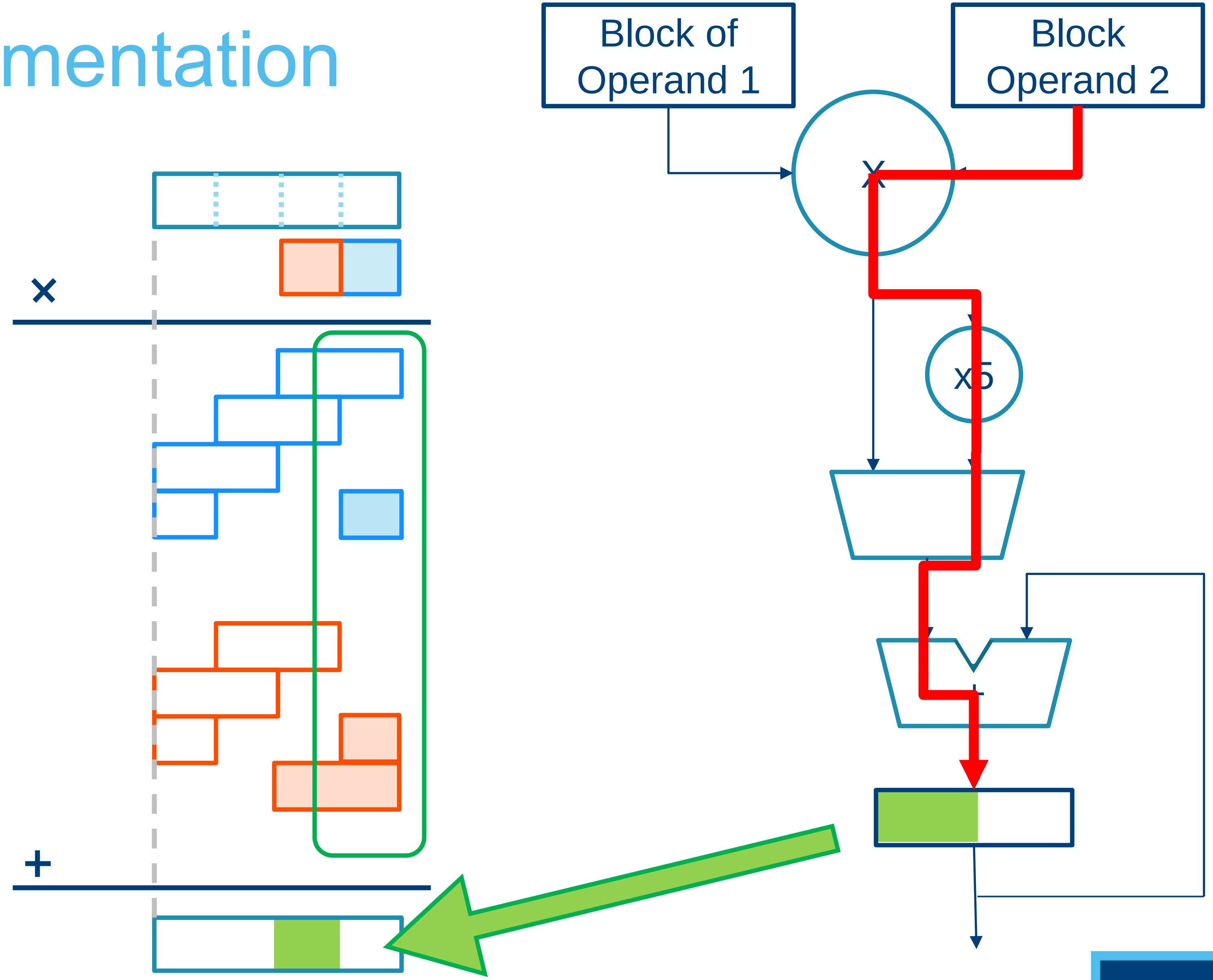

KU LEUVEN

# Poly1305's Implementation

A datapath for each column to handle smaller block multiplications.

Result of a column is propagated to the next.

The multipliers set the critical path.

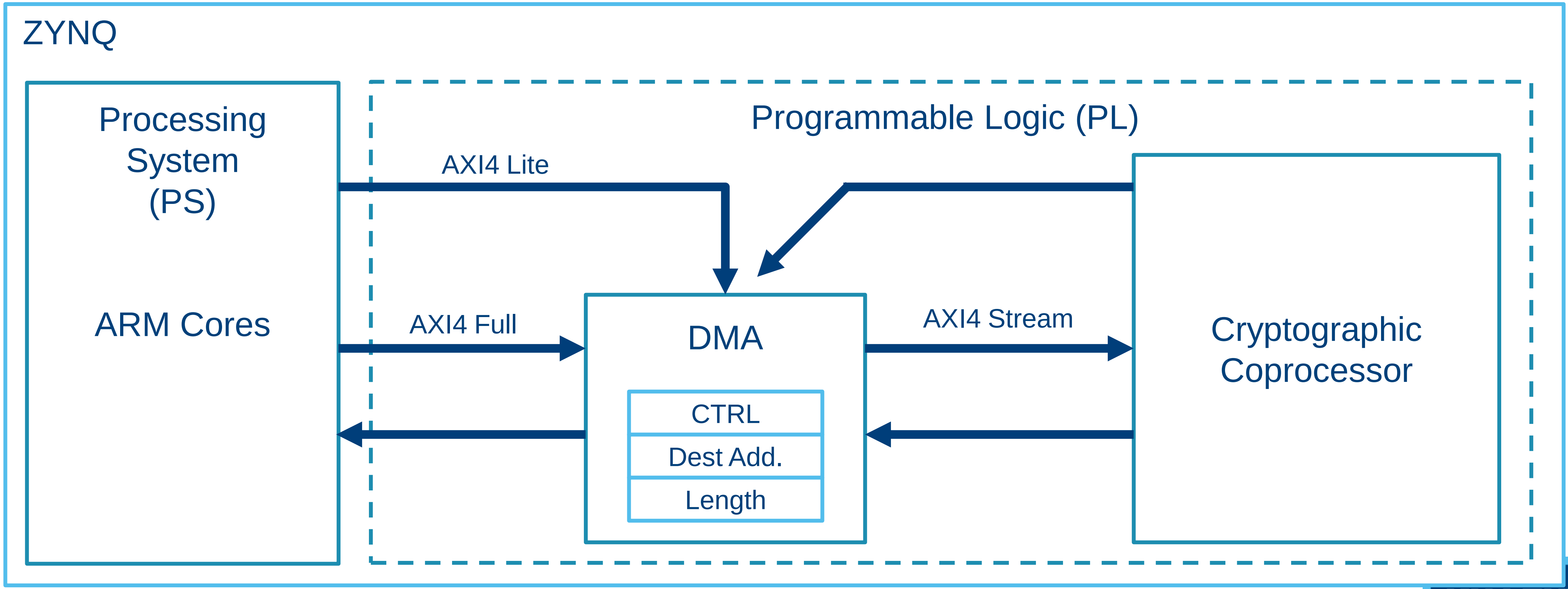





KU LEUVEN

# Hardware Implementation

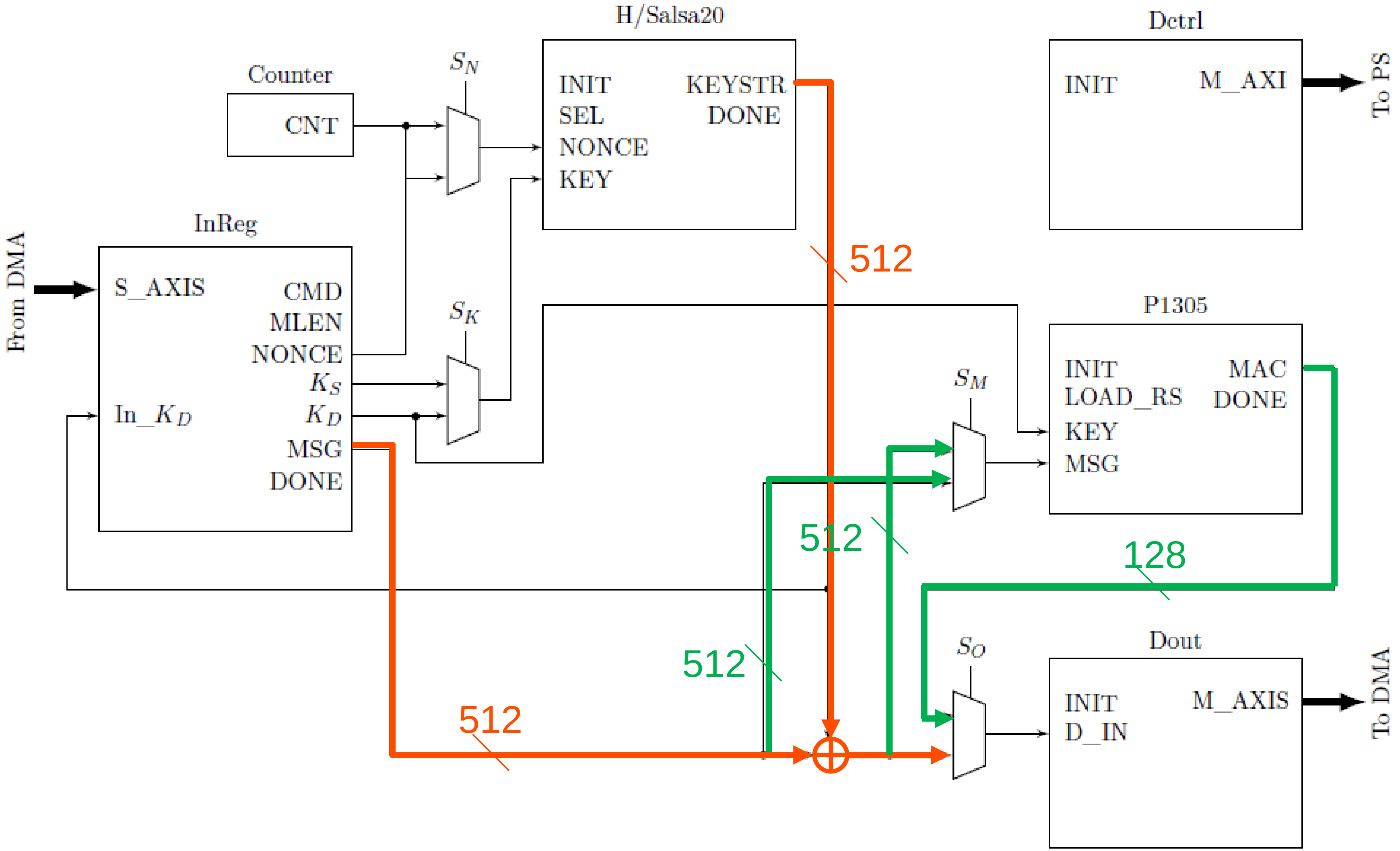
- Processing System runs Linux - SigmaVPN.
- DMA transfers data between co-processor and RAM.





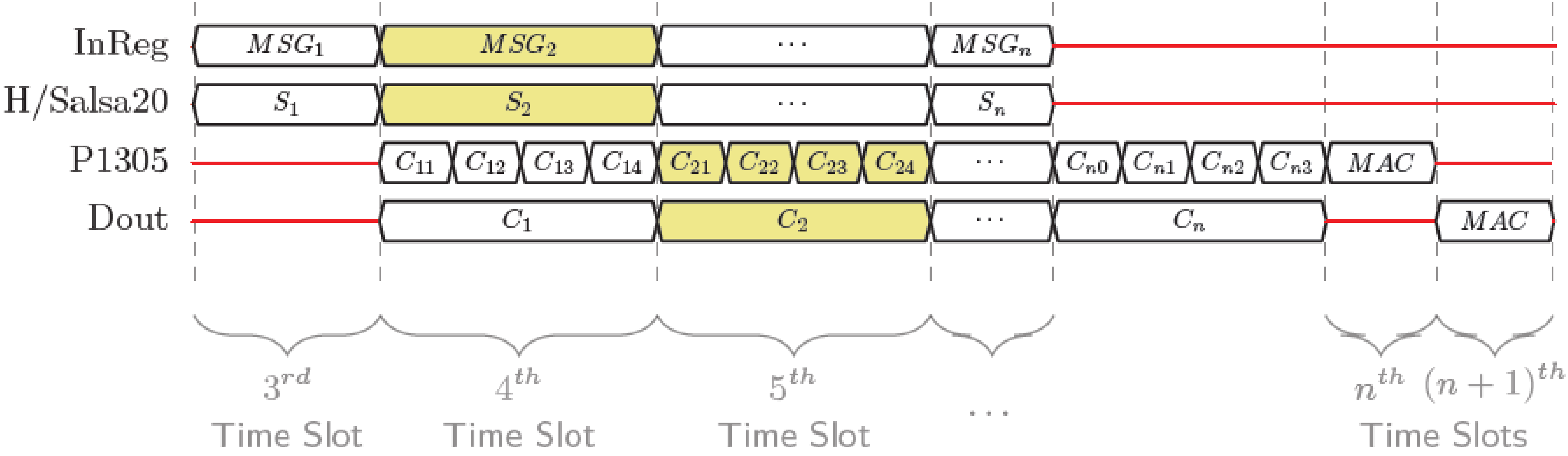

KU LEUVEN

# Coprocessor's Datapath



# Scheduling

- Operation is divided into *time slots*
- A time slot is the time to process a 512-bit message block
- Each hardware module is active in each time slot



# Hardware Utilization

**Single Instance of Processing Blocks**

- Resource Utilization: 53.67%
- Max Clock Freq: 92.85 MHz
- Process 512-bit block in a time slot

**Duplicated Processing Blocks**

- Resource Utilization: 97.25%
- Max Clock Freq: 81.25 MHz
- Process 1024-bit block in a time slot

ZYBO Board comes with Zynq Z-7010 SoC;

- The smallest Zynq device
- Has limited resources

# Communication btw. HW & SW

Configuring DMA for transferring buffers requires:

- Accessing physical addresses
- Coherent memory accesses

**Created a Linux kernel space module (Device File)**

Problem: Overhead of making context switches

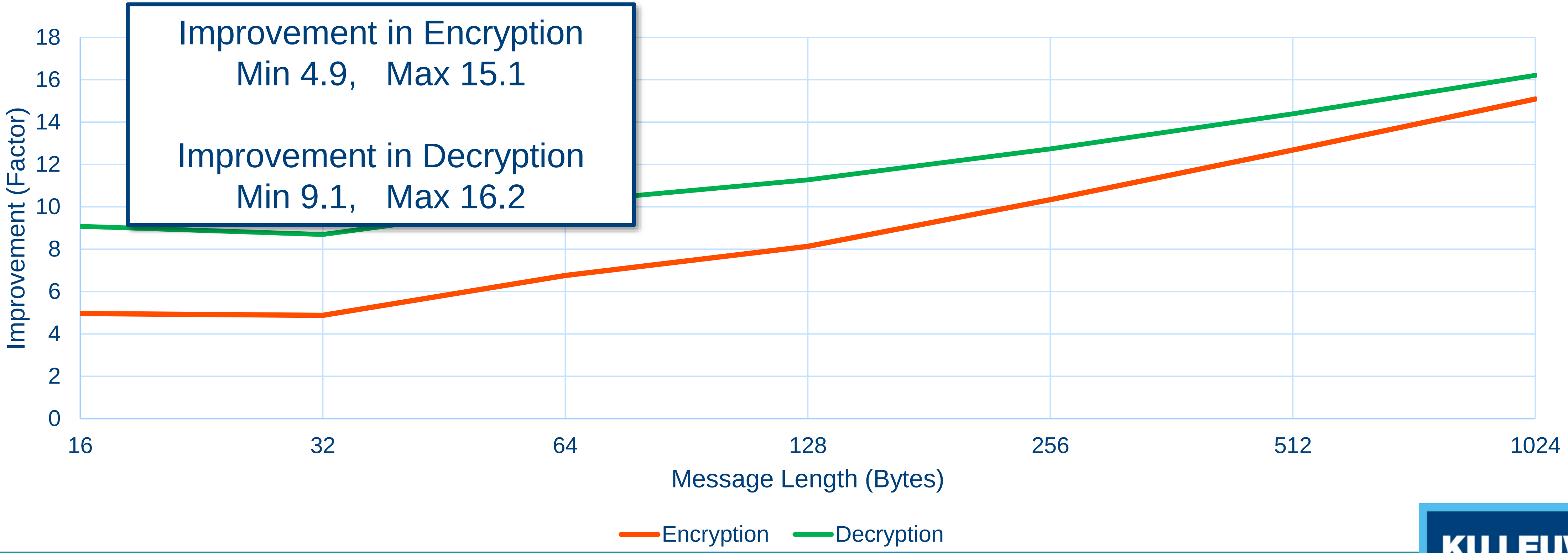
- Going do kernel space costs ~800 cycles.
- Transferring the frame btw. User and Kernel space costs ~740 cycles.



KU LEUVEN

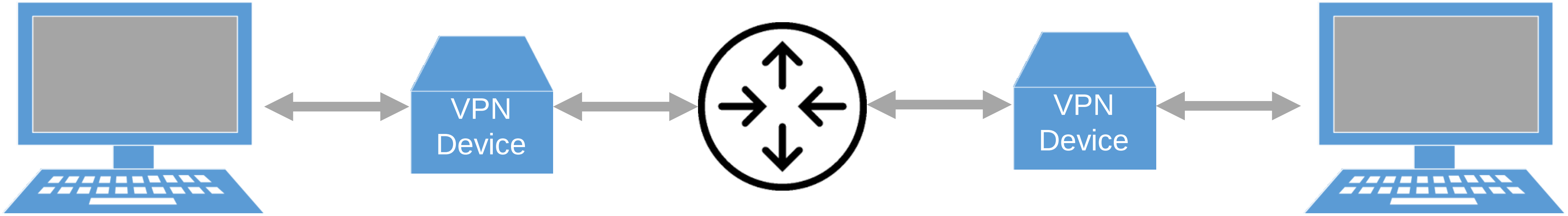
# Improvements to Cryptographic Operations

- Encrypted and decrypted many test vectors with both SW-only and SW+HW implementations.
- Compared results for accuracy and execution times.



# Improvements to VPN Bandwidth

Test Network Structure:




Bandwidth tests using

**Iperf** Network Bandwidth Measurement Tool

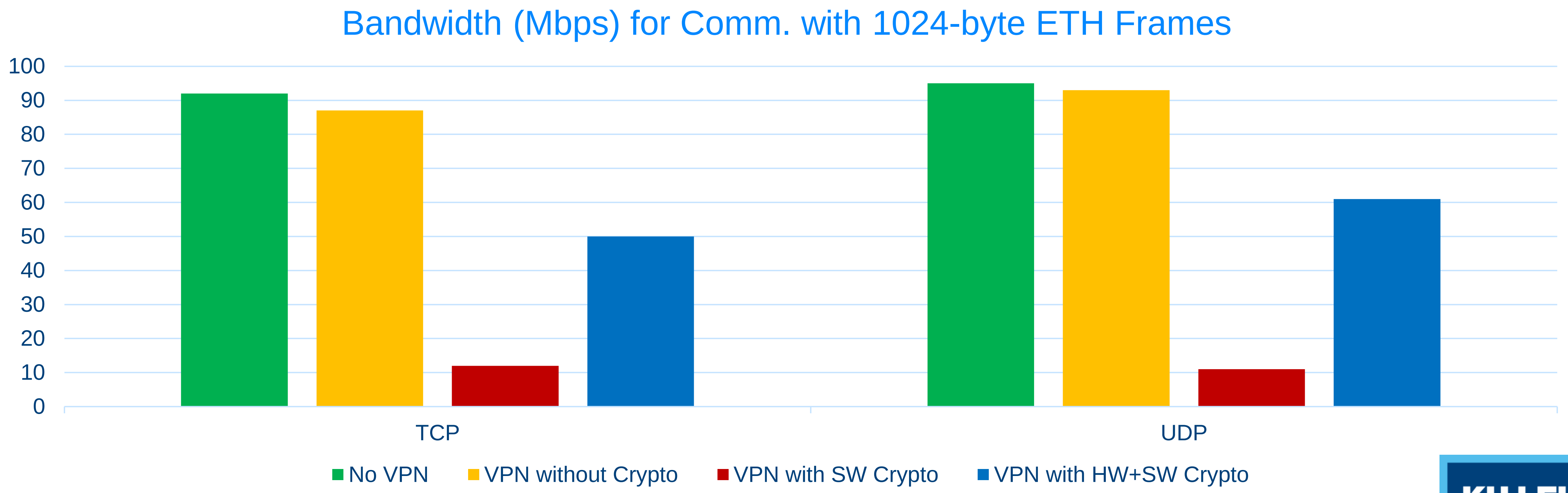
# Improvements to VPN Bandwidth

TCP bandwidth increase

- 2.9 times for 128-byte frames,
- 4.36 times for 1024-byte frames.

UDP bandwidth increase

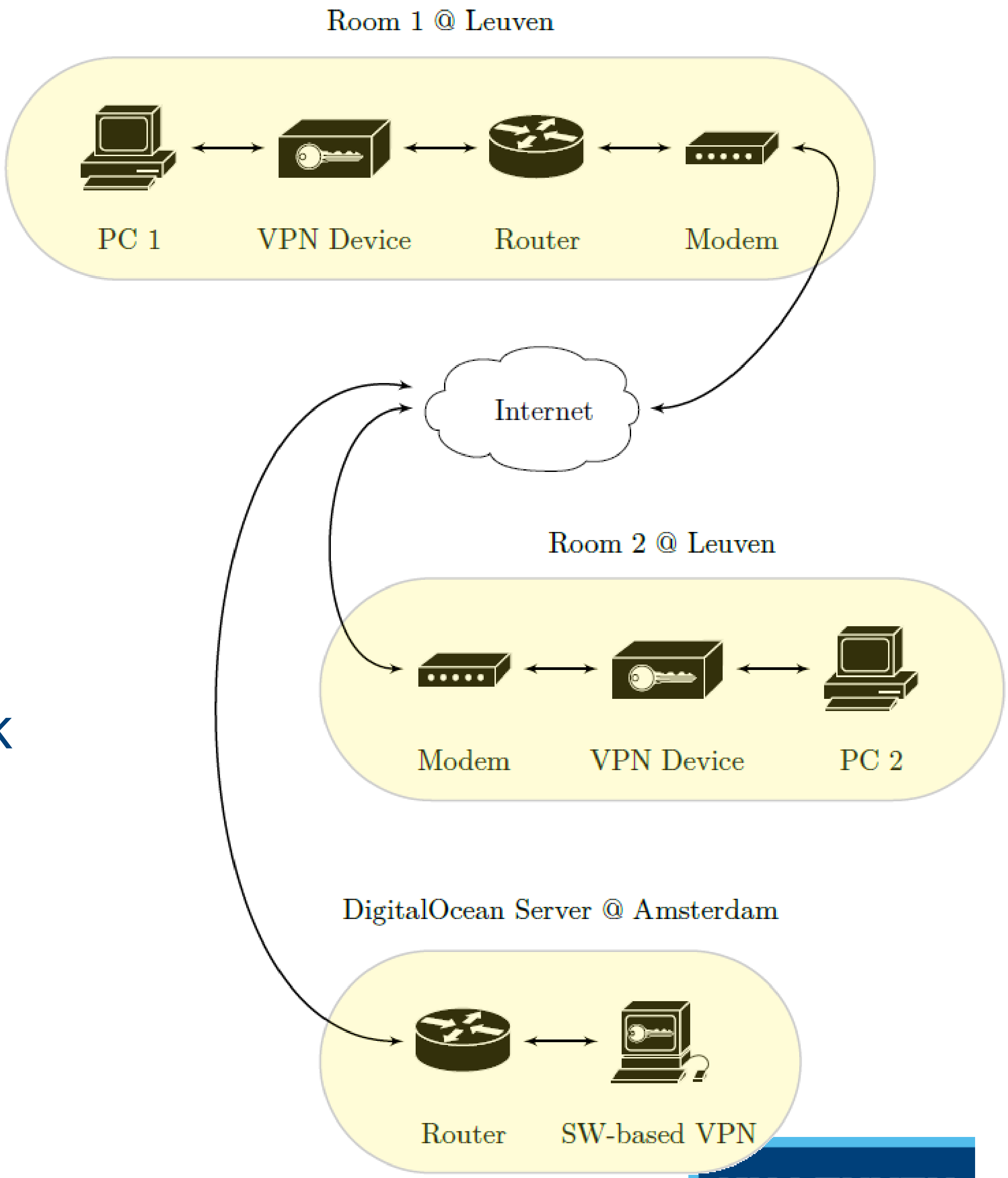
- 2 times for 128-byte frames,
- 5.36 times for 1024-byte frames.



# Functionality Test

- The designed VPN device is still capable of establishing a secure communication with original SigmaVPN application.

    - A VPN device on a low-cost dev-board, providing confidential communication between a whole home/business network and a remote server.






KU LEUVEN

# Conclusion

- A cryptographic hardware accelerator is offered for NaCl's CryptoBox specifically for SigmaVPN.
- Encrypting a 1024-byte message in 94% less time compared to SW-only implementation.
- Integrating our HW-SW codesign into SigmaVPN offers up to 6 times more communication bandwidth.
- Xilinx Open HW Design Contest Finalist: http://www.openhw.eu/2016-finalists.html
- It's available open source: https://github.com/furkanturan/Hardware-Accelerated-SigmaVPN


KU LEUVEN