Fachhochschule Nordwestschweiz
Hochschule für Technik

Quantensichere Verschlüsselung und Authentifizierung mit FPGA

Bachelor-Thesis von **Alice** und **Bob**

Studiengang **Elektro- und Informationstechnik**


AES
IDEA
SECURE ?
Rijndael
RIPEMD-160
SHA-2

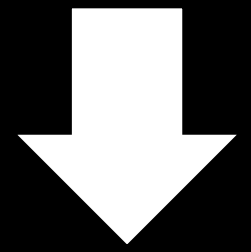
Kryptographie

System

Kryptographie

Symmetric Key Encryption

Dan Boneh, Mark Zhandry



Boneh-Zhandry-Symmetric „BZS“

Literatur: D. Boneh und M. Zhandry, „Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World“, in Proc. of Crypto, Ser. LNCS, Bd. 8043, 2013, S. 361–379.

Eigenschaften

Blockschiffre

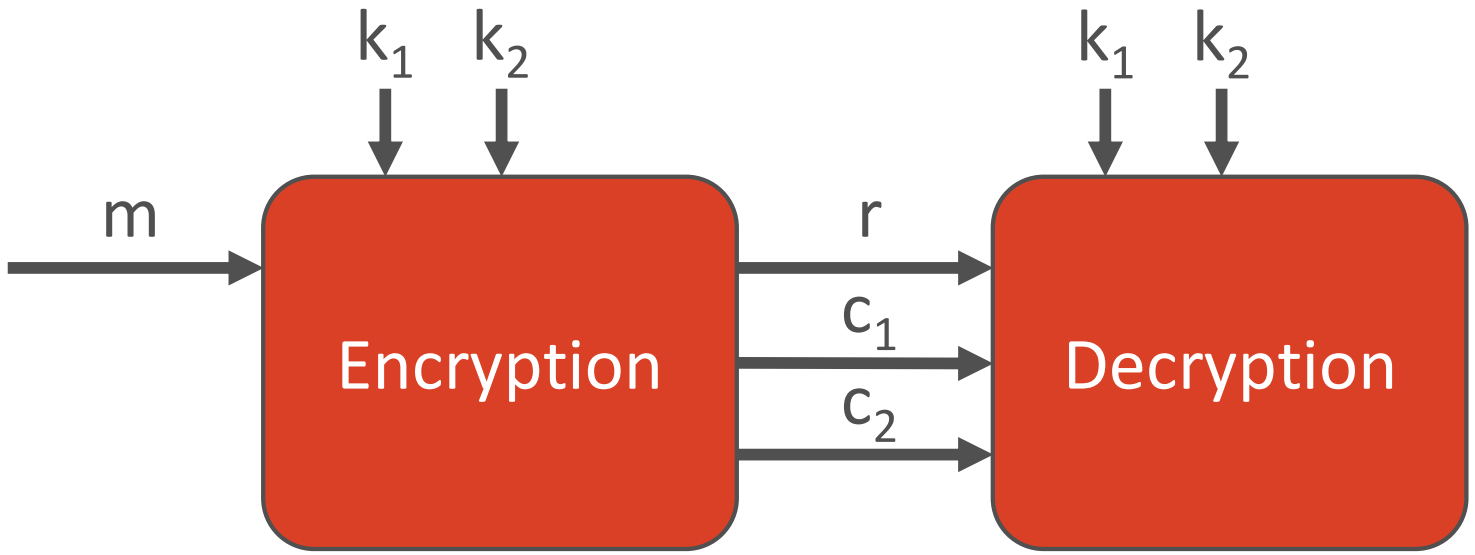
Vertraulichkeit (confidentiality)

Authentizität (authenticity)

Integrität (integrity)

encrypt-then-MAC

quantum chosen ciphertext secure



BZS

$\mathsf{Enc}((k_1, k_2), m) : r \xleftarrow{R} \{0,1\}^\lambda$

Verschlüsselung

$c_1 \leftarrow F(k_1, r) \oplus m,\ c_2 \leftarrow G(k_2, (r, m))$

$output\ (r, c_1, c_2)$

$\mathsf{Dec}((k_1, k_2), (r, c_1, c_2)) : m \leftarrow c_1 \oplus F(k_1, r),\ c_2' \leftarrow G(k_2, (r, m))$

Entschlüsselung

$if\ c_2' \neq c_2,\ output\ \perp$

$otherwise,\ output\ m$

BZS

Quantis QRNG Chip

- ID-Quantique
- wahre Zufallszahlen
- 4.2 x 5 x 1.1 mm
- 1.5 Mbps (SPI Interface)
- 2.8 V

Quelle: https://marketing.idquantique.com/acton/attachment/11868/f-025e/1/-/-/-/-/Quantis%20QRNG%20Chip_Brochure.pdf

$$\mathsf{Enc}((k_1, k_2), m) : r \xleftarrow{R} \{0,1\}^\lambda$$

AES-256

$$c_1 \leftarrow F(k_1, r) \oplus m, \quad c_2 \leftarrow G(k_2, (r, m))$$

$$output\ (r, c_1, c_2)$$

HMAC-SHA-256

$$\mathsf{Dec}((k_1, k_2), (r, c_1, c_2)) : m \leftarrow c_1 \oplus F(k_1, r),\ c_2' \leftarrow G(k_2, (r, m))$$

$$if\ c_2 \neq c_2',\ output\ \perp$$

$$otherwise,\ output\ m$$

BZS

$$\mathsf{Enc}((k_1, k_2), m) : r \xleftarrow{R} \{0,1\}^\lambda$$

AES-256

$$c_1 \leftarrow F(k_1, r) \oplus m \qquad c_2 \leftarrow G(k_2, (r, m))$$

$$output\ (r, c_1, c_2)$$

HMAC-SHA-256

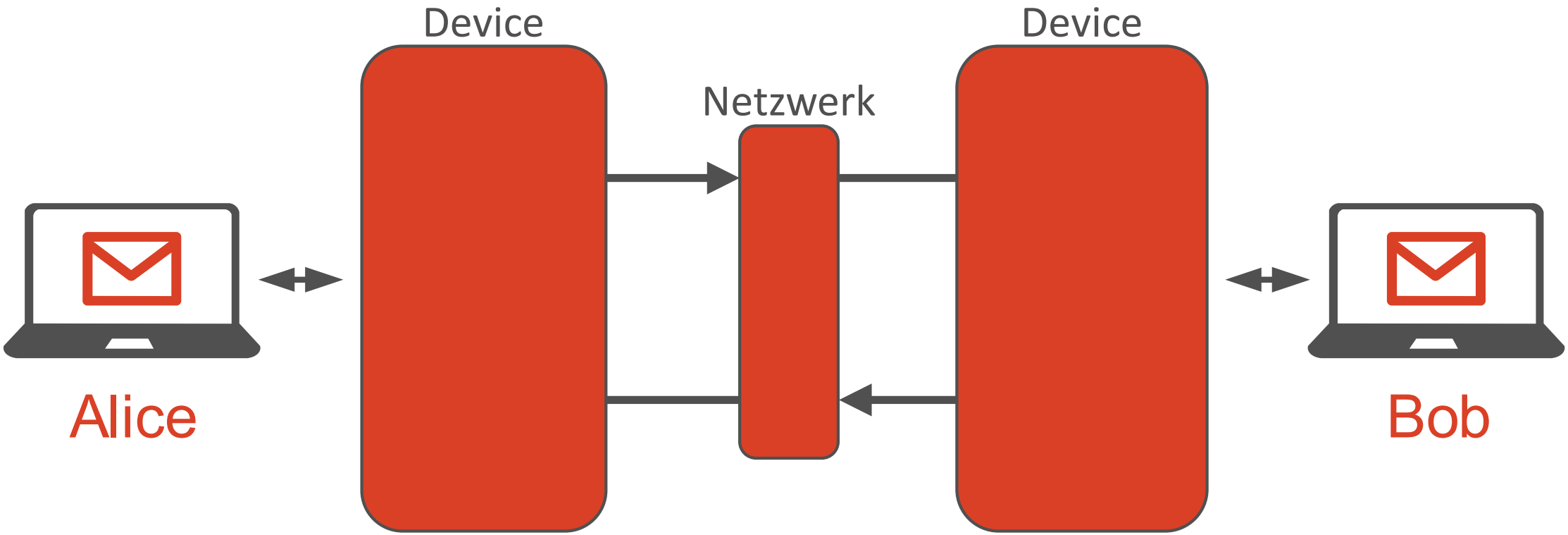
$$\mathsf{Dec}((k_1, k_2), (r, c_1, c_2)) : m \leftarrow c_1 \oplus F(k_1, r) \qquad c_2' \leftarrow G(k_2, (r, m))$$

$$if\ c_2 \neq c_2',\ output\ \perp$$

$$otherwise,\ output\ m$$

BZS

System



Systemübersicht

Anforderungen

Device:

- Integration BZS
- Übertragungsprotokolle
- klein, low-power

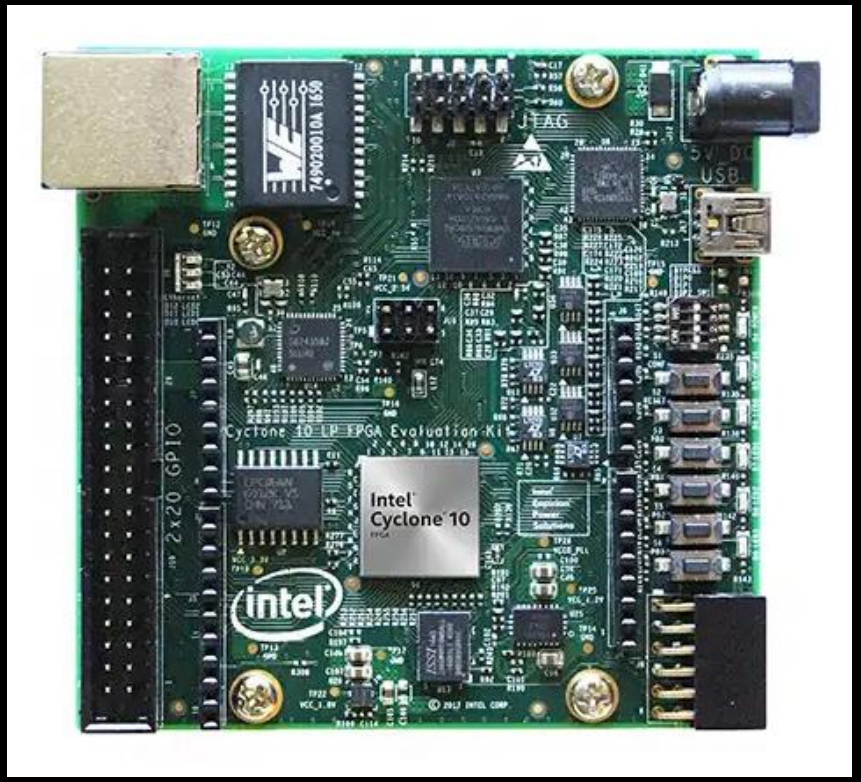
Netzwerk:

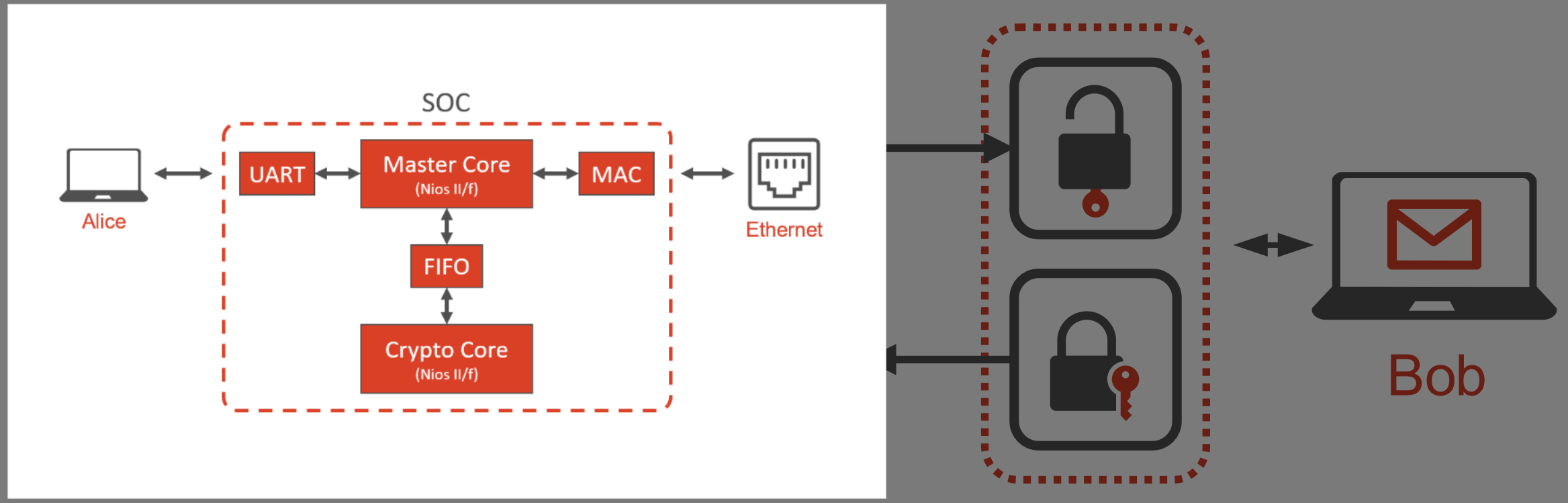
- verbreitet
- Internet
- Ethernet

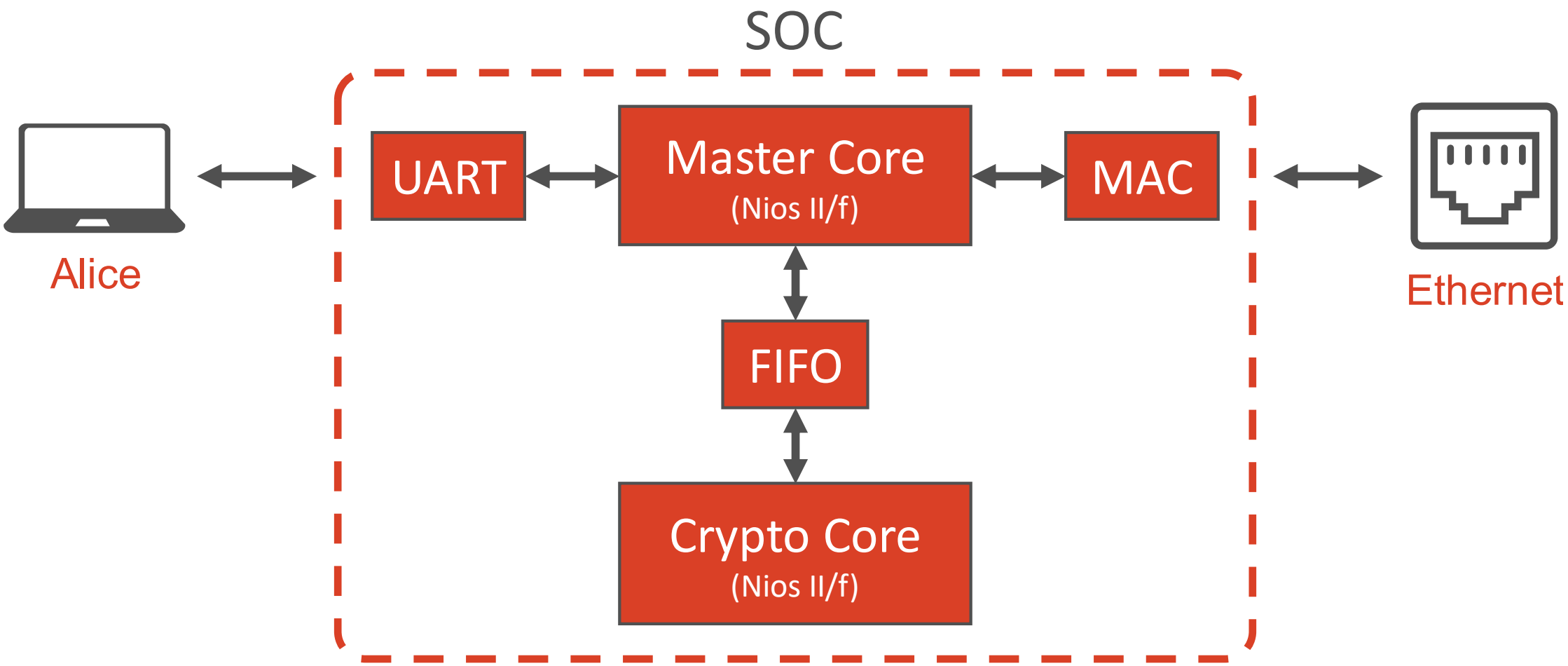
Device: FPGA
Intel Cyclone 10 LP Evaluation Board

- 2017
- 25k Logic Elements
- 14x14mm
- Ethernet, PHY

System On Chip




SOC
Alice
UART
Master Core
(Nios II/f)
MAC
FIFO
Crypto Core
(Nios II/f)
Ethernet
Bob


SOC
Alice
UART
Master Core
(Nios II/f)
MAC
FIFO
Crypto Core
(Nios II/f)
Ethernet

Software

eine pro Core

objektorientiertes C++

kein fremder Code

Resultate

Quantensichere Verschlüsselung von Alice zu Bob

20k Logic Elements (80%)

800 Byte/s

Es ist möglich, auf einem
kleinen FPGA mit klassichen Algorithmen
Daten quantensicher zu übermittlen.

?