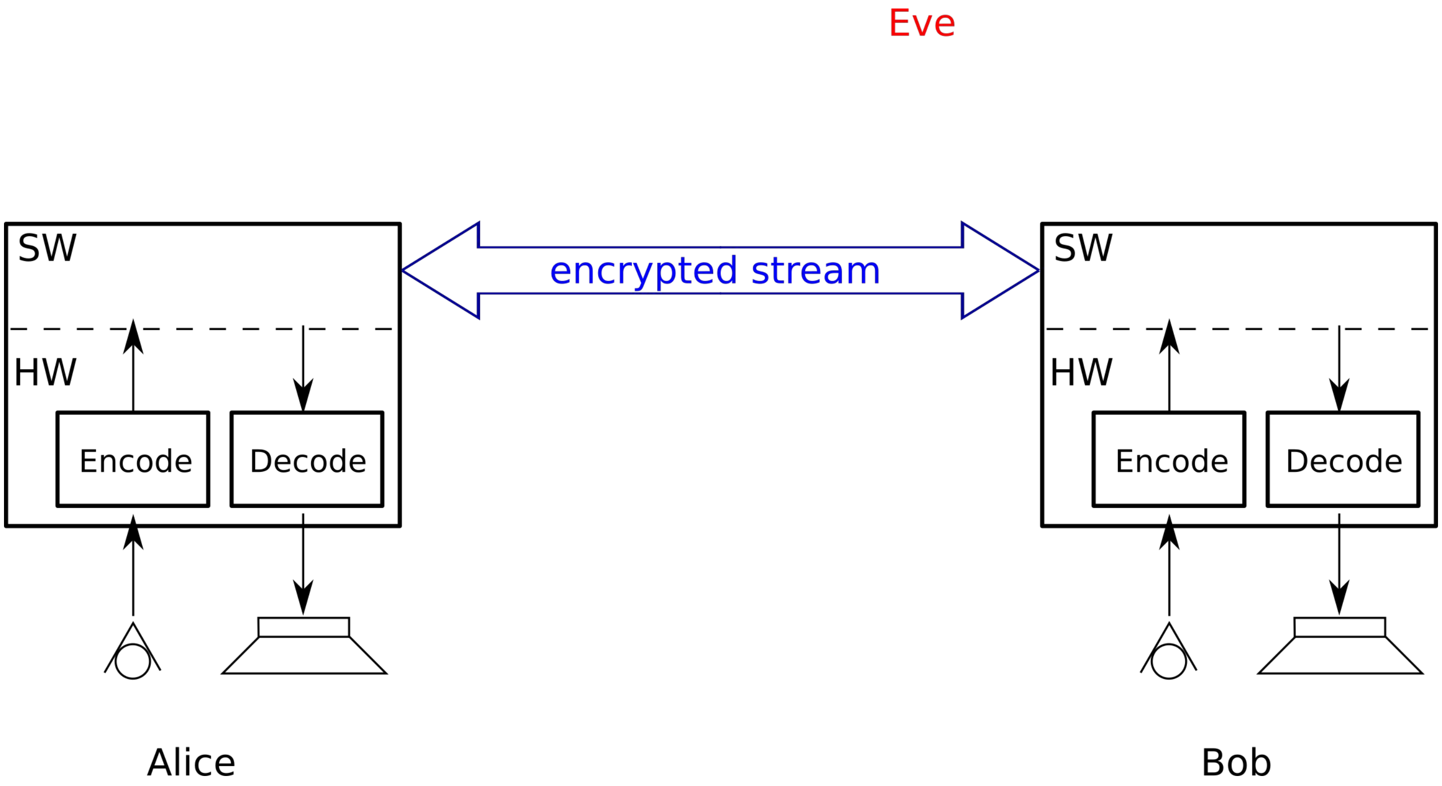
Secure On Chat

SoC Architectures and Modelling
WS 2015

Aguarón, Hartinger, Hummel, Manninger, Pöschl, Primas, Schaffenrath, Zajc

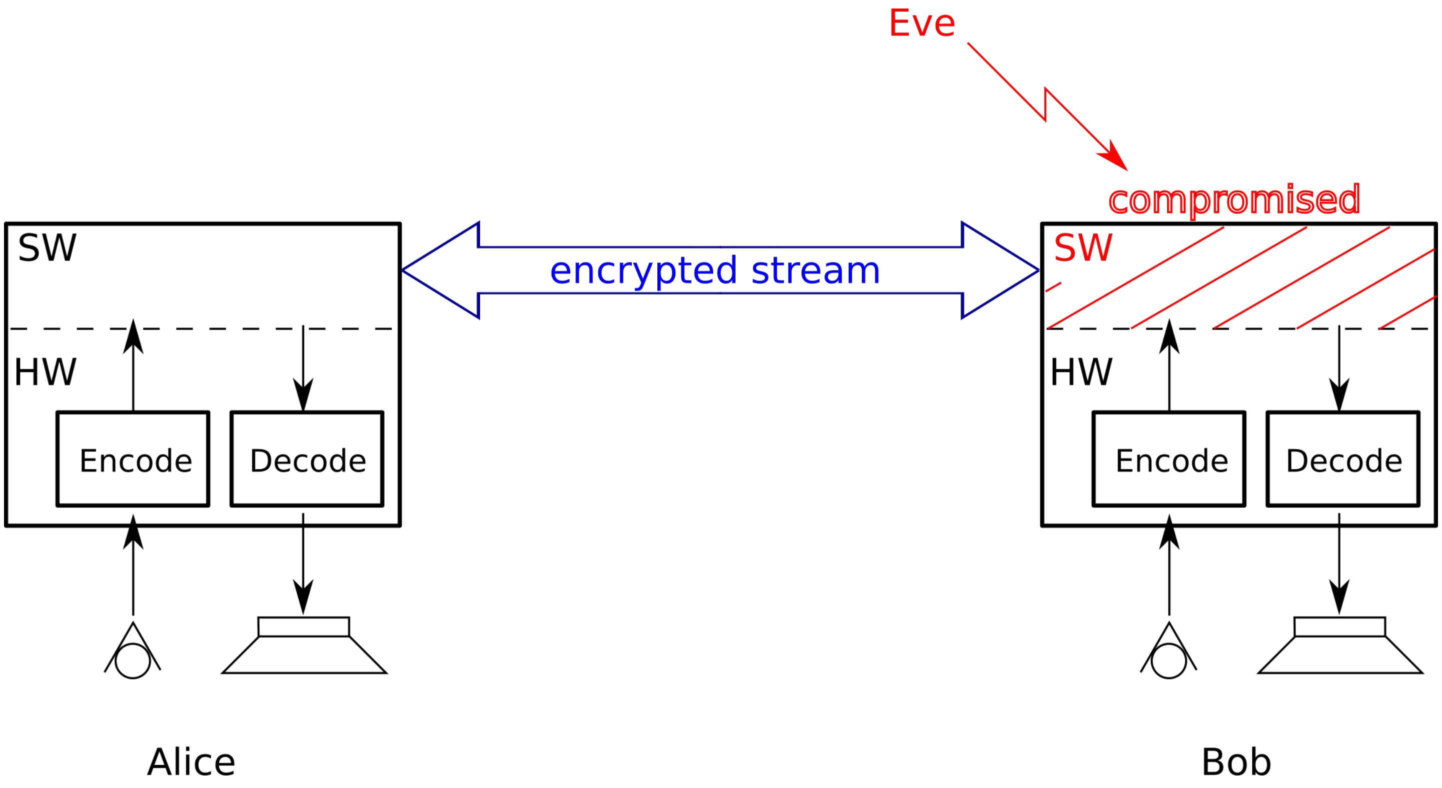
What is it about?

- Provide a secure channel for communication
- Without trusting the SW



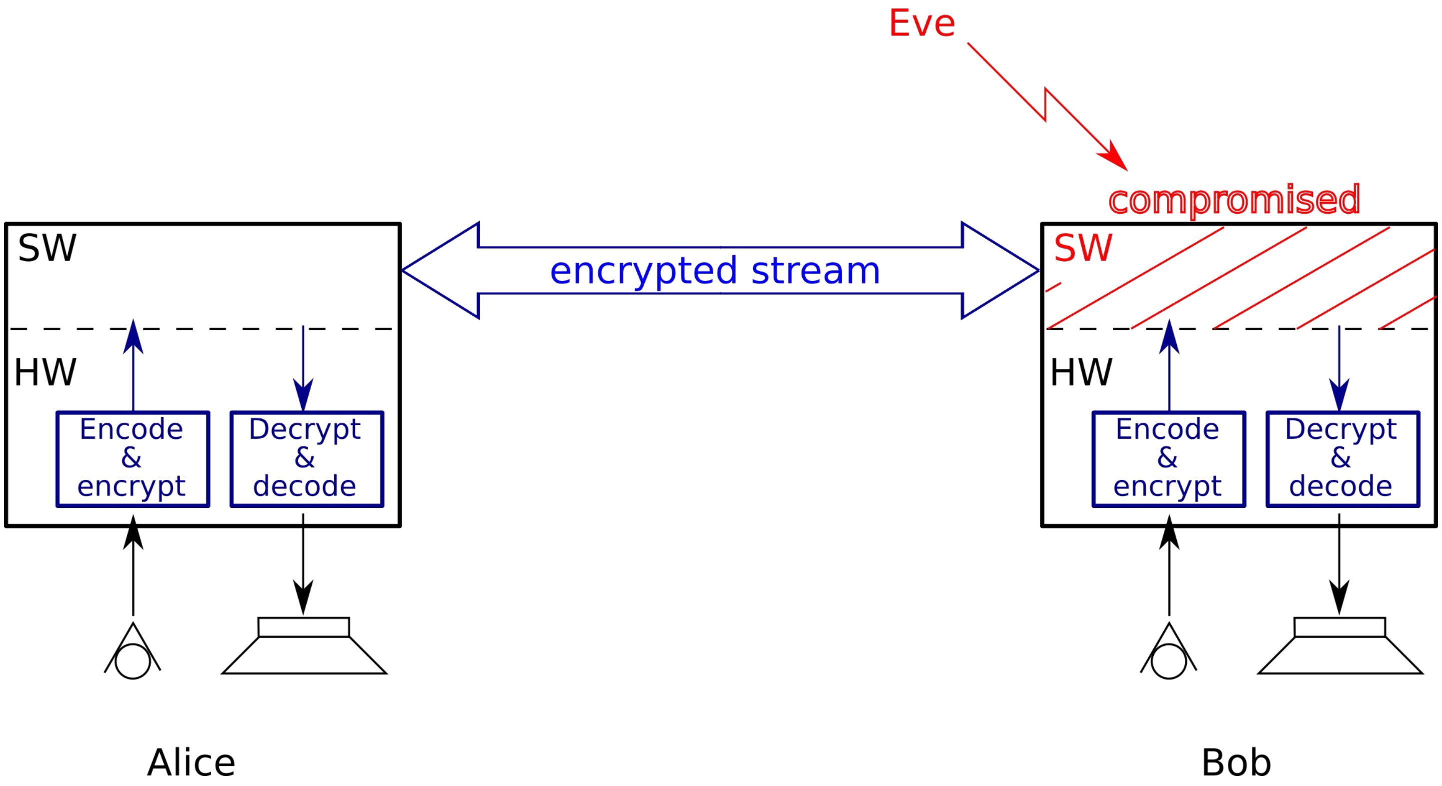
What is it about?

- Provide a secure channel for communication
- Without trusting the SW



What is it about?

- Provide a secure channel for communication
- Without trusting the SW



What is it about?

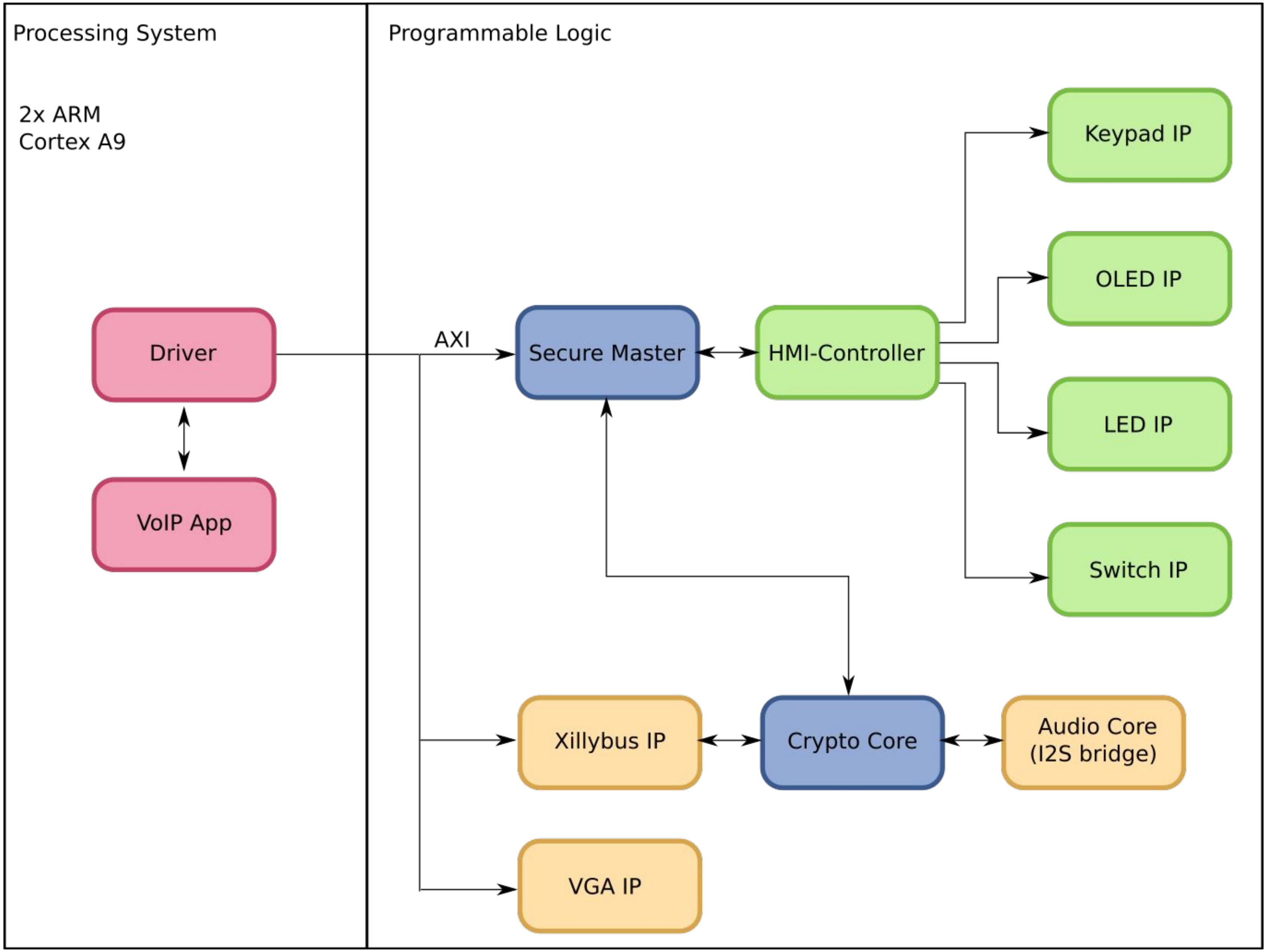
End-to-end encryption in hardware

- Operating system has no access to
  - Unencrypted data stream (secure mode)
  - Unencrypted keys
  - Secure display
  - Status LED

Design Decisions

- Key exchange
  - Meet up in person
  - Generation of random keys from seeds
  - Display of key on secure screen -> OLED
  - Enter key via keypad (not readable by OS)
- OS only gets encrypted keys
  - Encrypt with device key
- Switch to “Secure Mode” via dedicated HW switch
  - Mode indicated by LED

System overview



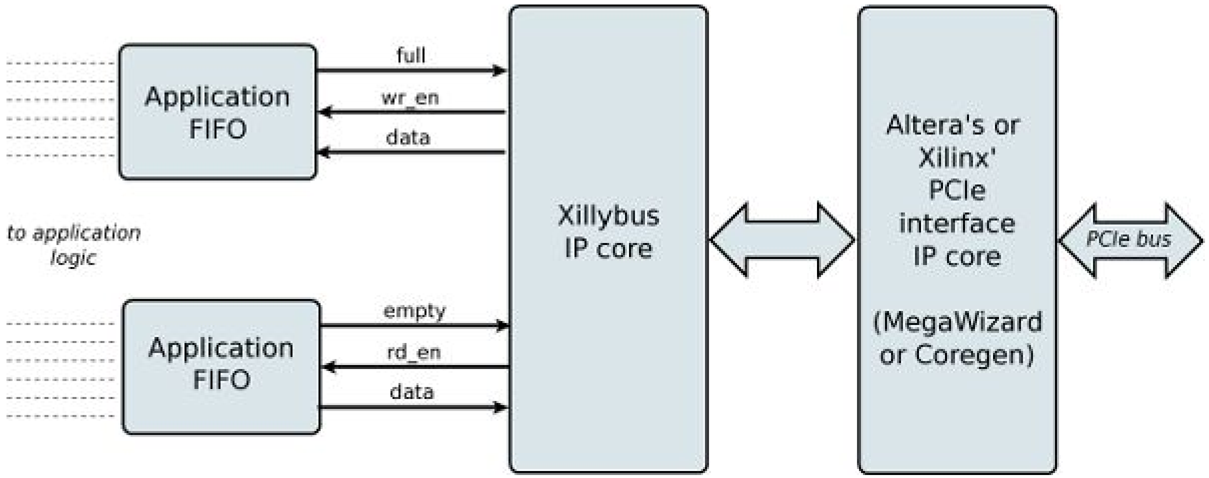
Chosen Development Platform

ZedBoard provides

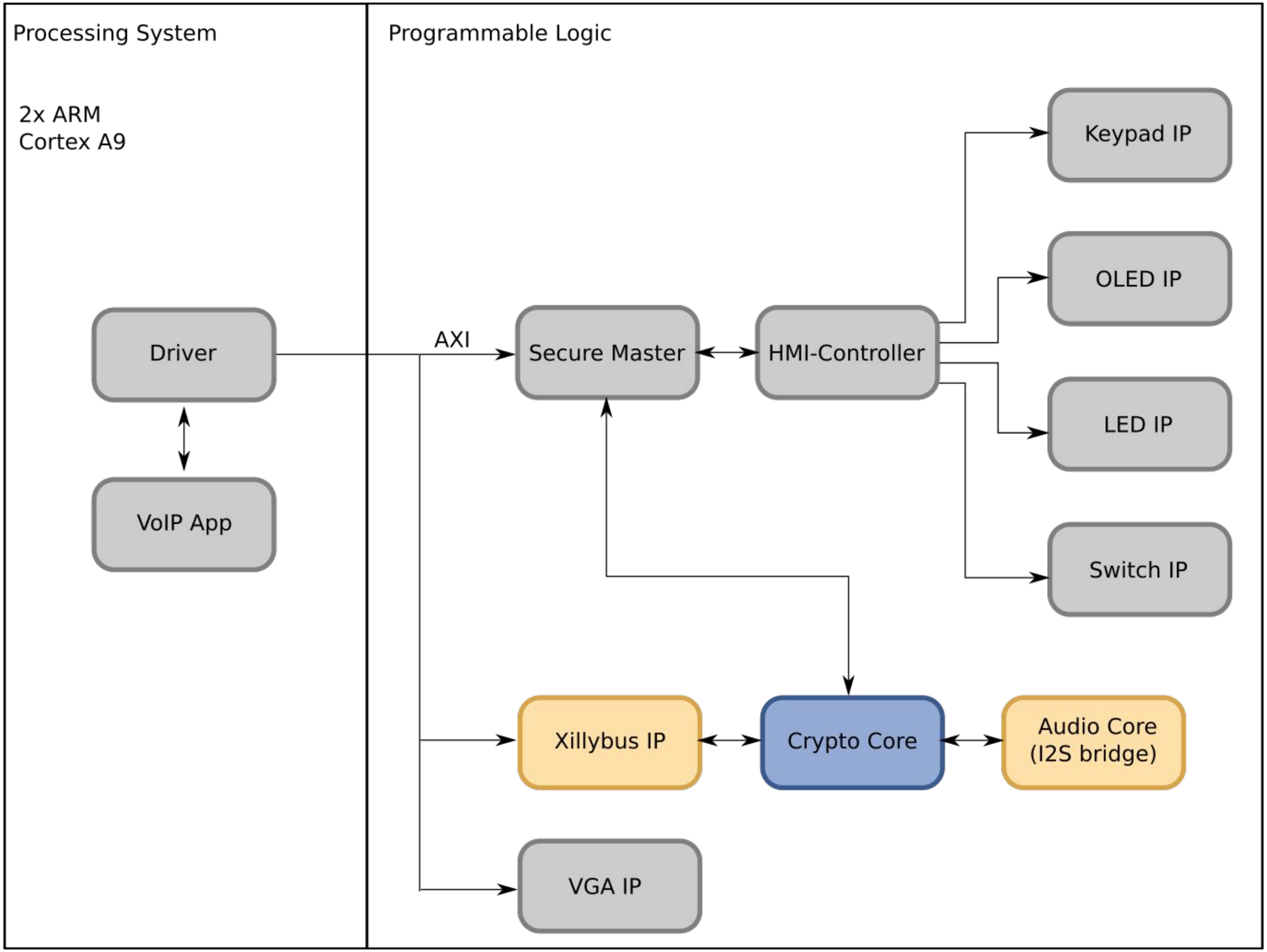
- Zynq®-7000 All Programmable SoC
- Integrated CPU (2xARM Cortex A9)
- On-board OLED
- Audio I/O via FPGA
- Ethernet
- GPIO and buttons/switches

Xillybus provides

- Ubuntu Linux
  - Display driver
  - Audio driver
- Hardware cores
  - Xillybus VGA core
  - I2S bridge



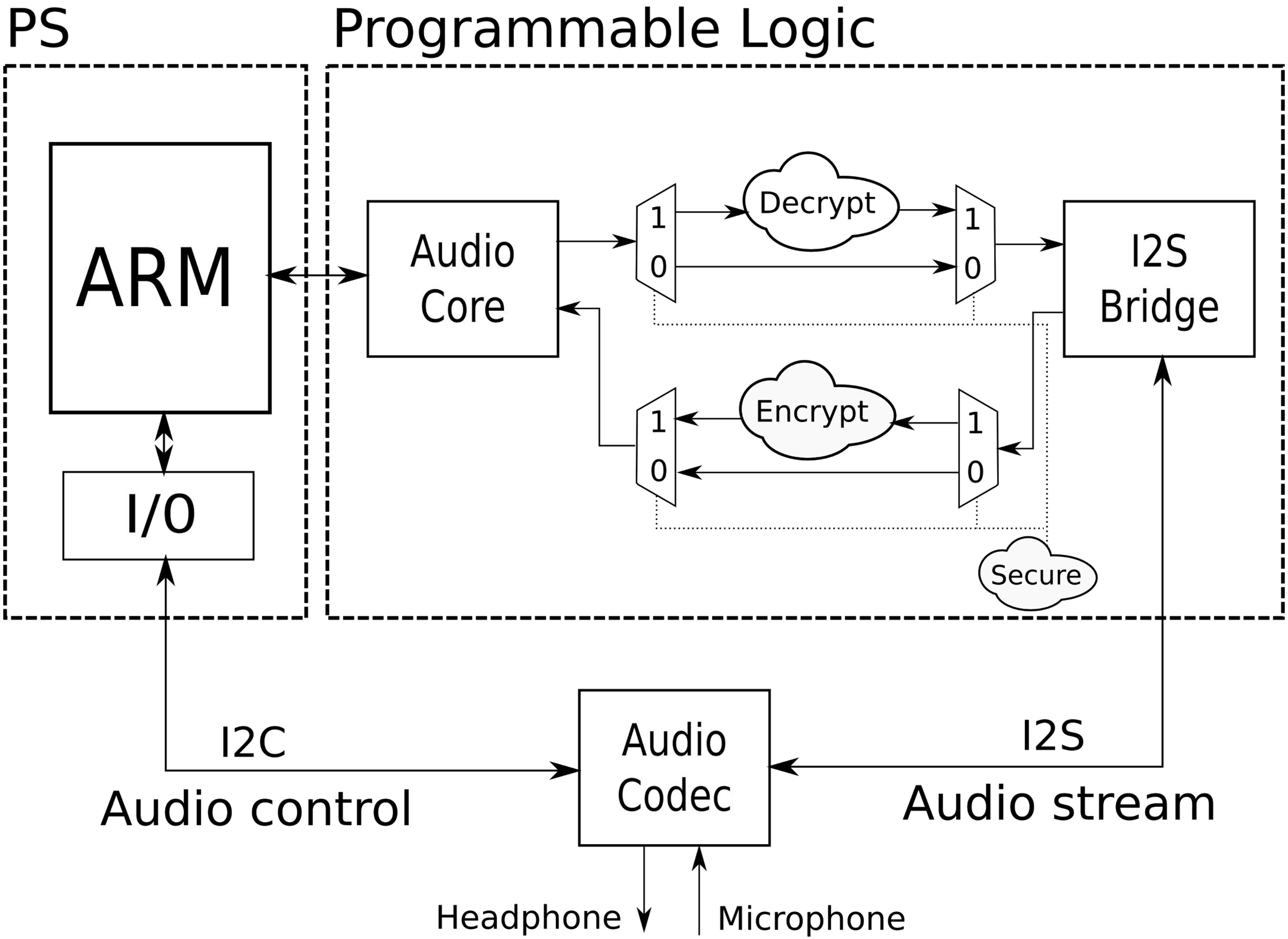
Audio


Processing System
2x ARM
Cortex A9
Driver
VoIP App
Programmable Logic
AXI
Secure Master
HMI-Controller
Keypad IP
OLED IP
LED IP
Switch IP
Xillybus IP
Crypto Core
Audio Core
(I2S bridge)
VGA IP

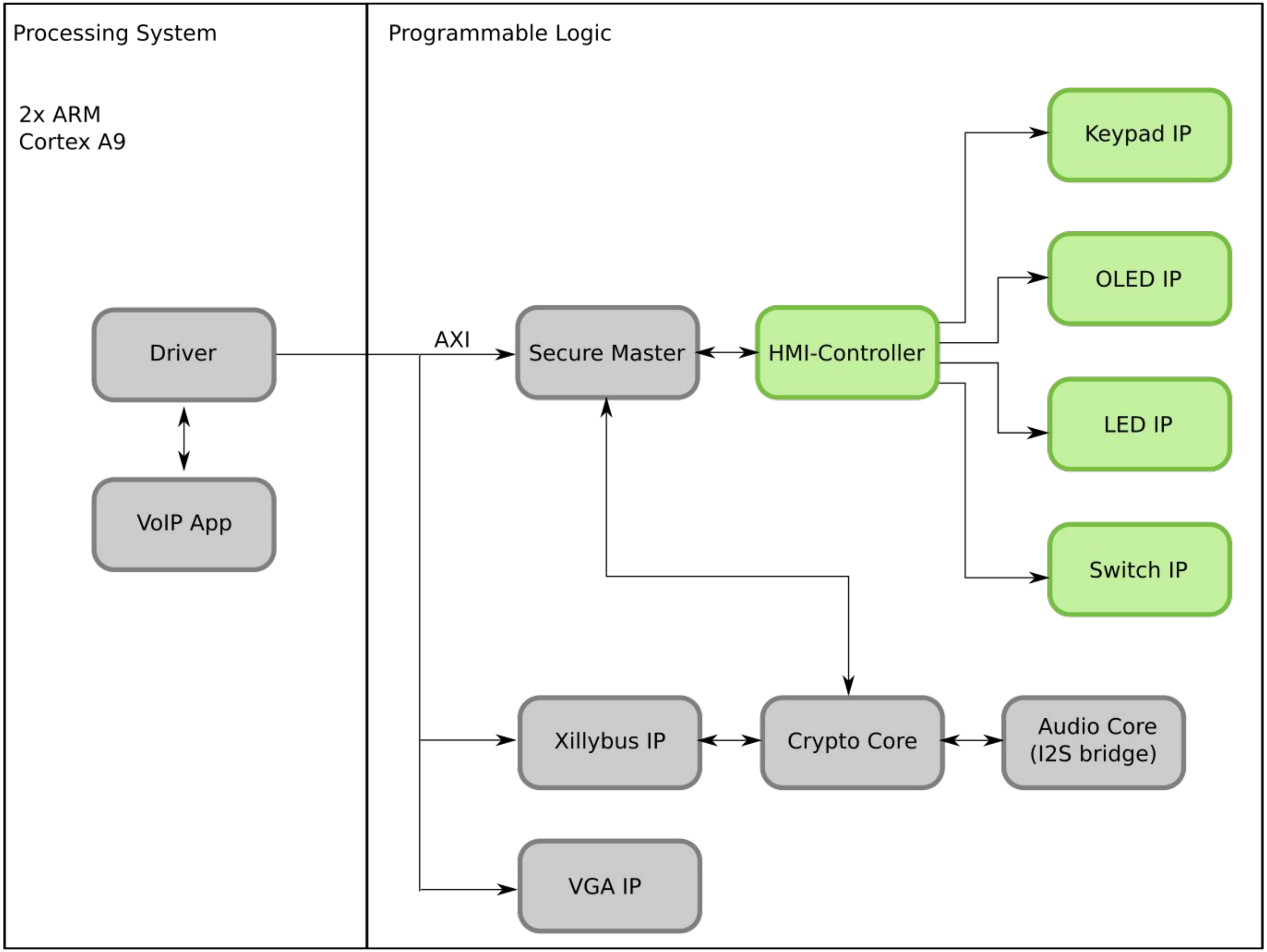
Audio

- Base audio design from Xillybus
- Adaptations according to our needs
  - En-/decrypt datastream
  - Drivers
  - Mute other applications

Audio

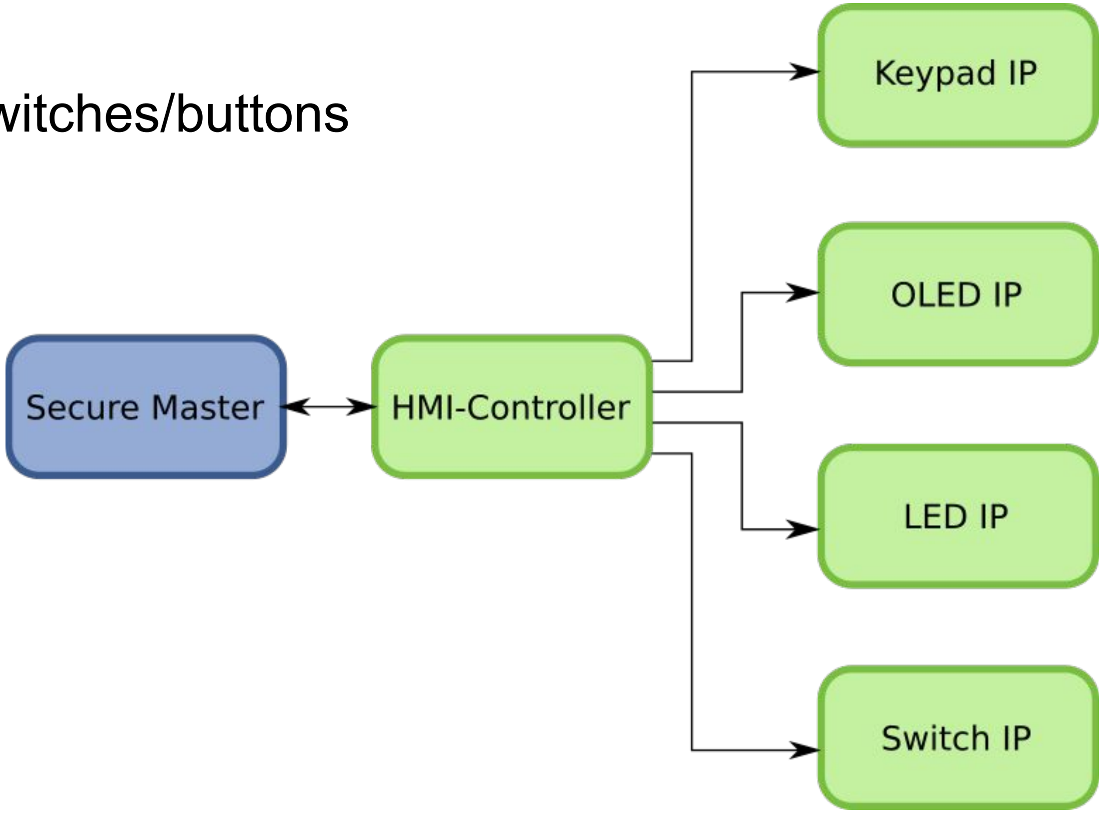

PS
Programmable Logic
ARM
I/O
Audio Core
1
0
Decrypt
1
0
I2S Bridge
1
0
Encrypt
1
0
Secure
I2C
Audio control
Audio Codec
I2S
Audio stream
Headphone
Microphone

HMI


Processing System
2x ARM
Cortex A9
Driver
VoIP App
Programmable Logic
AXI
Secure Master
HMI-Controller
Keypad IP
OLED IP
LED IP
Switch IP
Xillybus IP
Crypto Core
Audio Core
(I2S bridge)
VGA IP

HMI overview

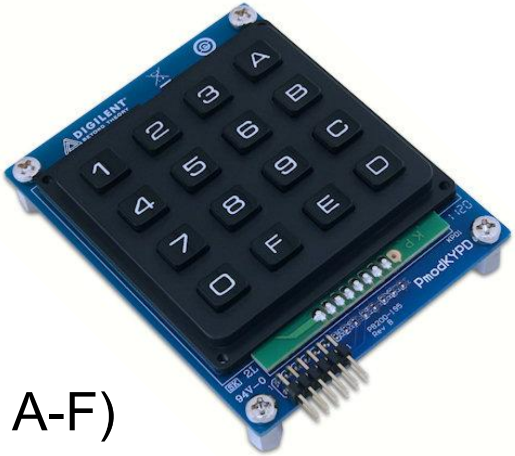
- Controller handles the IO operations and requests from the crypto unit
  - Messages for OLED
  - Input from keypad/switches/buttons
  - LED toggling



HMI keypad

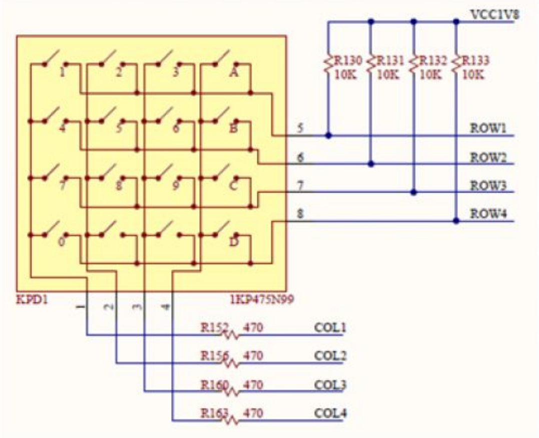
General

- Keypad used for entering key and seed value
- 16 buttons
- Keys numbered in a hexadecimal fashion (0-9 and A-F)



Interface of keypad core

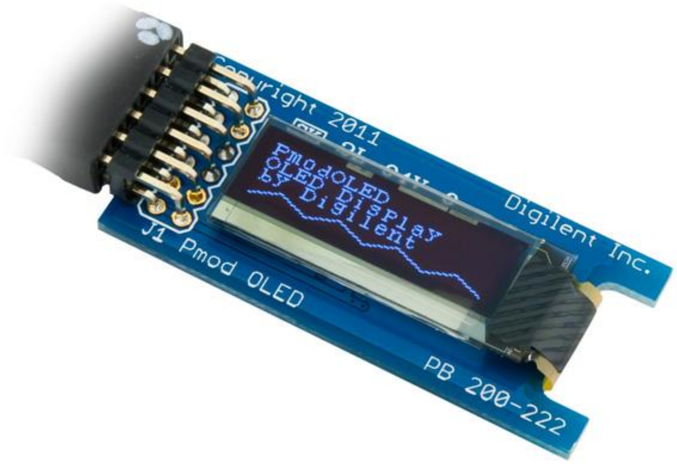
- Buffer for pressed button
- Handshake signals for HMI controller



HMI OLED

General

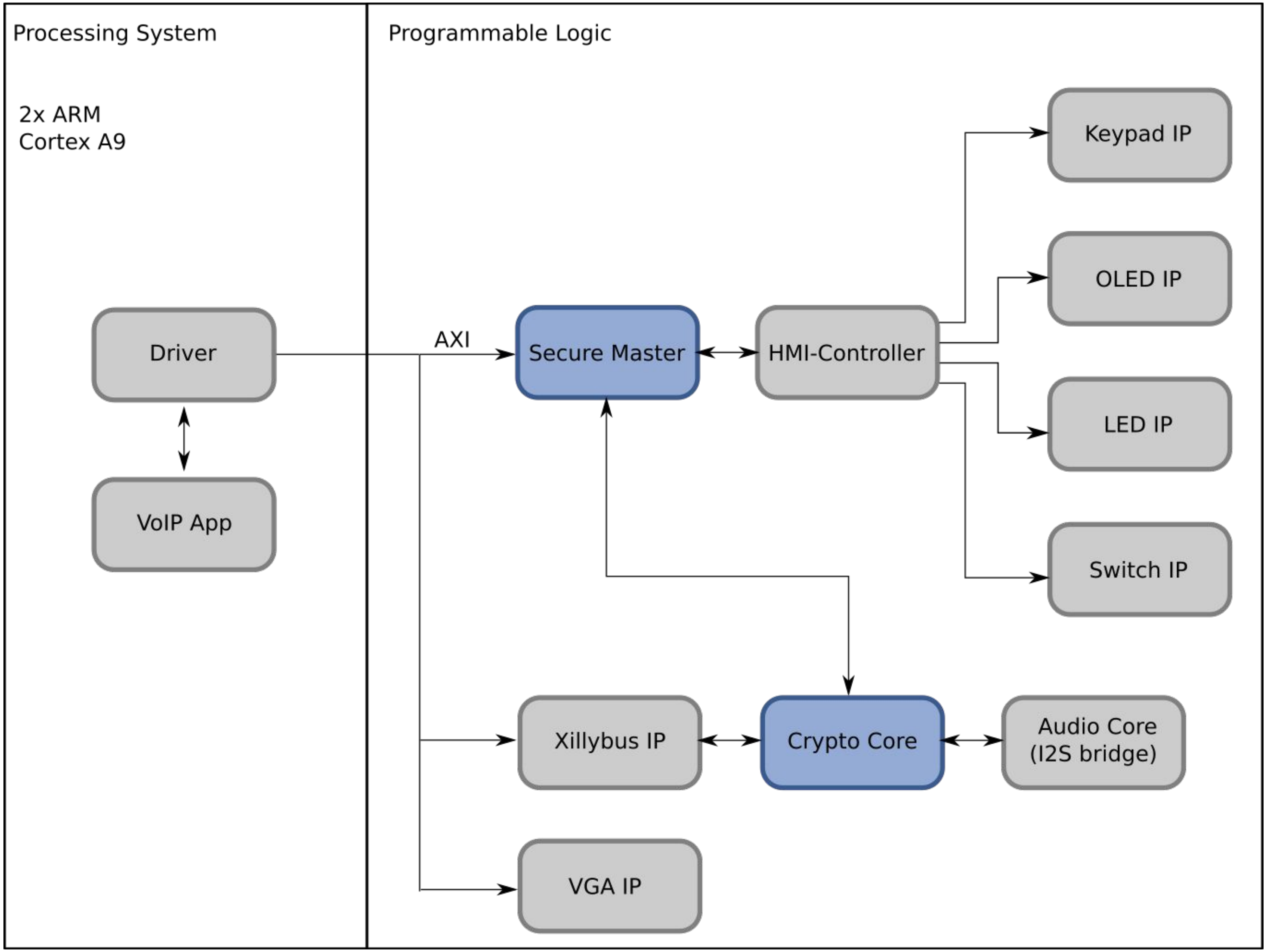
- The display is used to display secret information
- Standard SPI interface (CLK max. 10 MHz)
- 128x32 pixel (equivalent to 4 rows with 16 characters)
- Internal display buffer



Interface of display core

- Handshake to HMI controller
- Input character
- Position signals for row and column selection

Crypto Unit


Processing System
Programmable Logic
2x ARM
Cortex A9
Driver
VoIP App
AXI
Secure Master
HMI-Controller
Keypad IP
OLED IP
LED IP
Switch IP
Xillybus IP
Crypto Core
Audio Core
(I2S bridge)
VGA IP

Crypto Unit

Base AES design from opencores.org

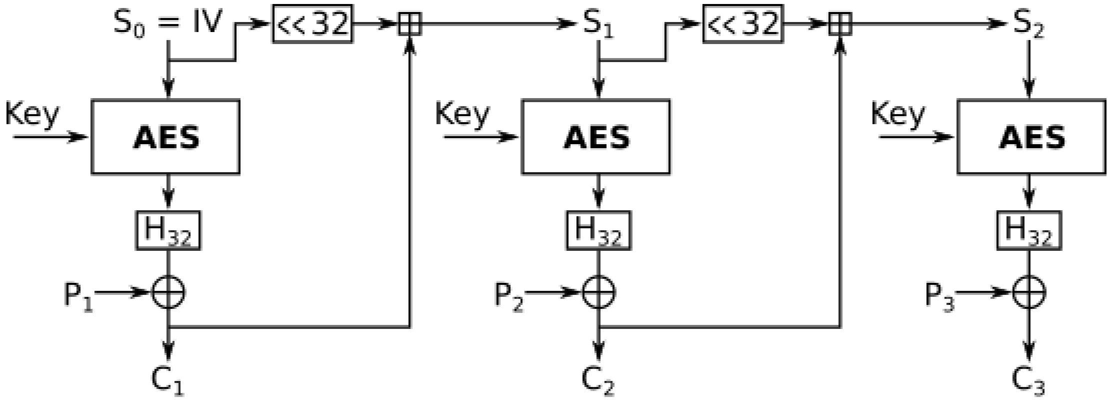
- ECB mode of operation
- Avalon interface
- 128-bit key size (alternatively 192 or 256 bit)

Adaptations according to our needs

- Stream cipher mode
- Interface adaptations

32-bit synchronized stream cipher

- CFB mode of operation
  - 32-bit block size
  - One shift register per direction

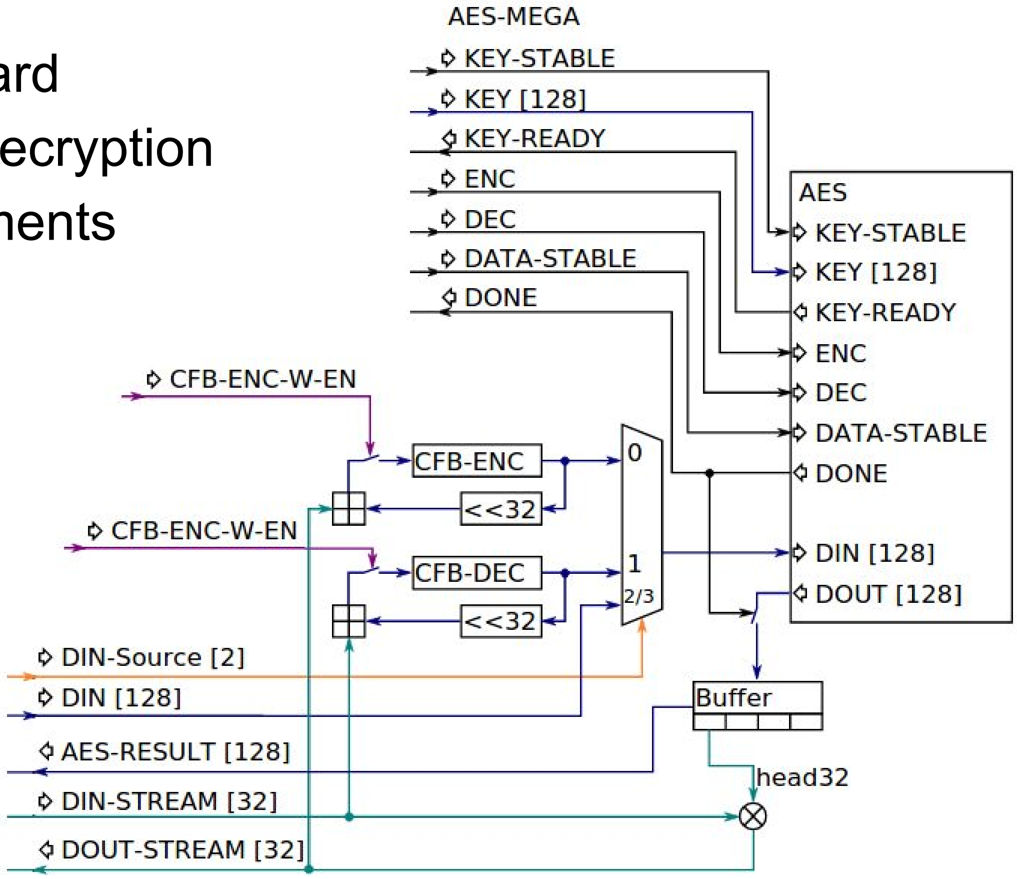


Cipher Feedback (CFB) mode encryption

Crypto Unit

Usage in our implementation

- One AES core per board
- Time scheduled enc/decryption
- Dynamic key replacements

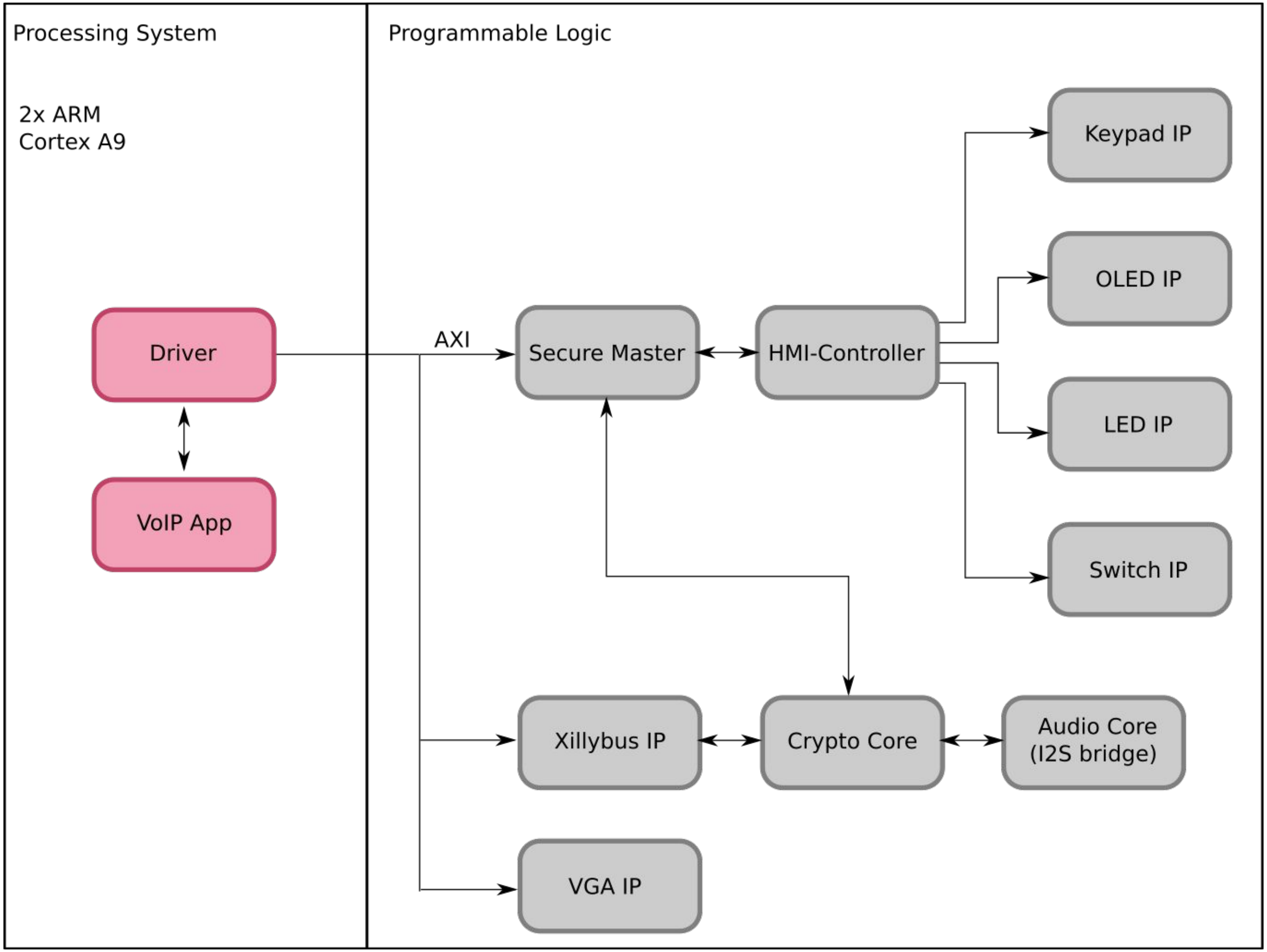


Crypto Unit

Controller

- Switch between modes of operation
  - Block cipher mode
  - Stream cipher
  - Key generator
- Handle keys
  - Load key into crypto core
  - AES core generates round keys
- Handle data
  - Handle FIFOs for stream data
  - Data from/to HMI (new key or seed)
  - Data from/to OS (encrypted key)

Application / OS layer

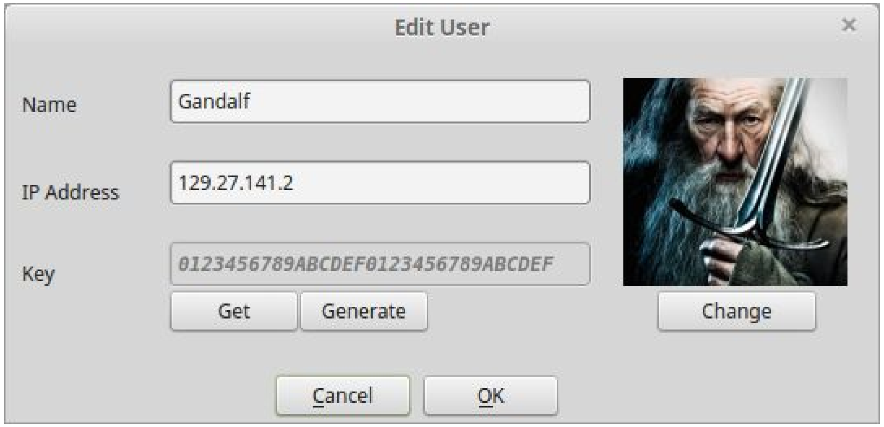


Application / OS layer

Xillinux OS based on Ubuntu LTS 12.04

Custom Application:

- add / change / delete users
- store users in file
- request key from hardware
- do / accept / reject / stop call

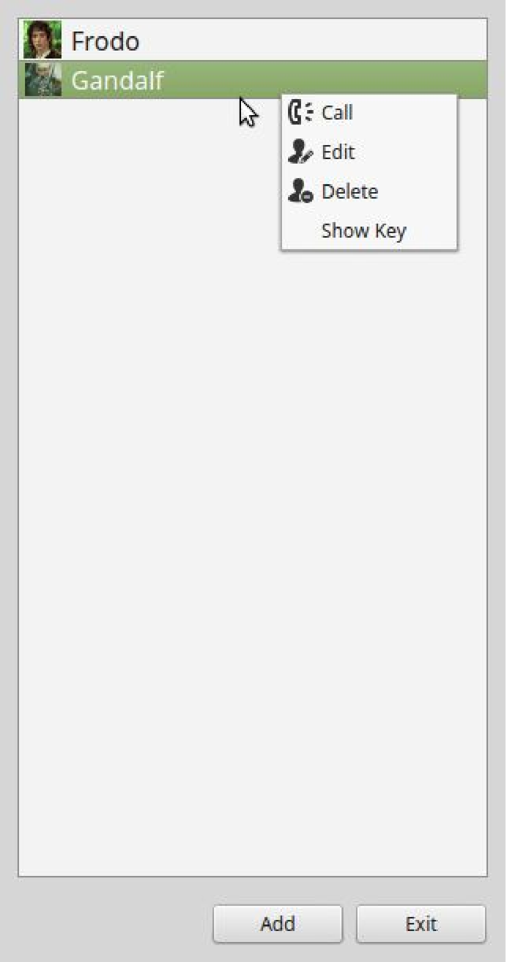


Edit User

Name: Gandalf

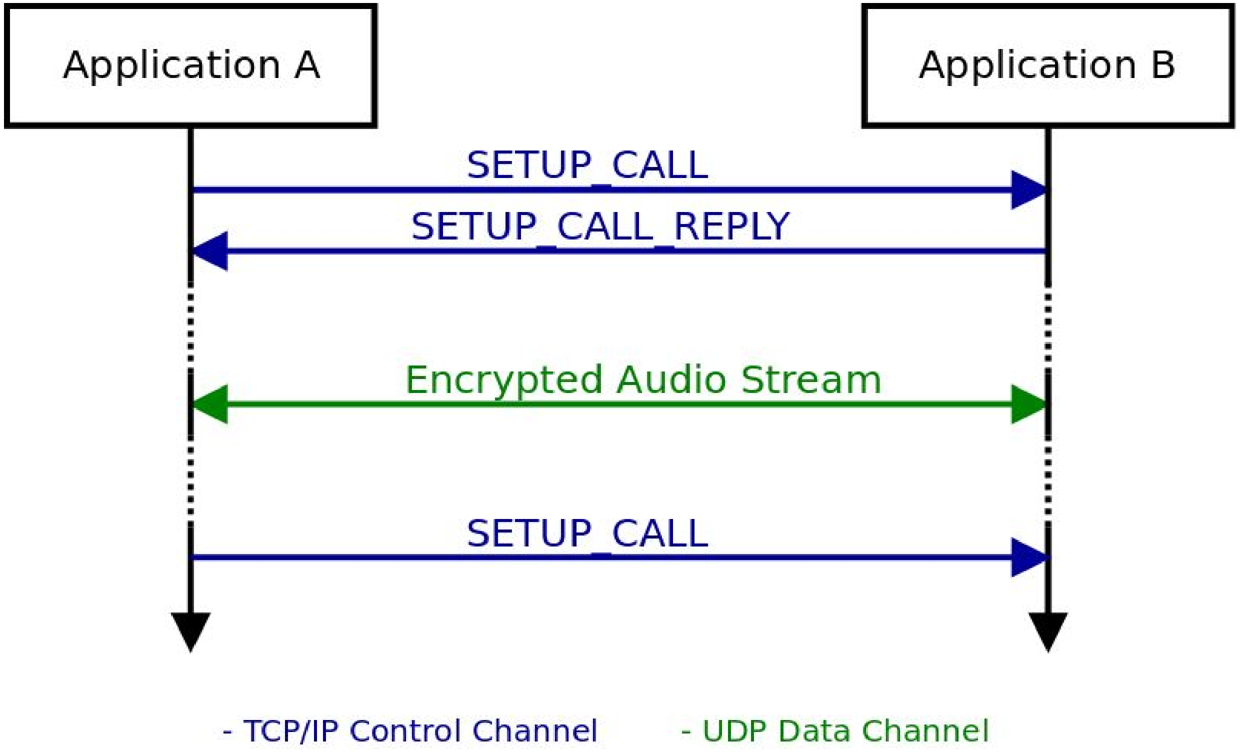
IP Address: 129.27.141.2

Key: 0123456789ABCDEF0123456789ABCDEF



Application / OS layer

Communication between two applications



Outlook

Integration in one device

- Mobile phone with secure keypad

Keyexchange

- Via a secure wireless connection (bluetooth, NFC, ...)
- Public key infrastructure

Additional features

- Conference calls
  - Session keys
- Stream compression
  - In HW on unencrypted stream

LIVE DEMO