KEMT

TECHNICAL UNIVERSITY OF KOSICE

FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS

21/1/2015

AES Implementation on 8-bit Silabs Microcontrollers

Ioannis Liolis

Supervisor: Doc. Ing. Miloš Drutarovský, CSc.

KEMT FEI TU OF KOSICE

Diploma thesis assignment

Thesis preparation instructions:

Implement encrypted communication channel between embedded Silabs microcontroller and PC computer. Use Advanced Encryption Standard (AES) block cipher algorithm as a basic building block of your solution. Propose and use a suitable block cipher mode for continuous transfer of large volume of data. As development platform use Keil development tools for 8051 microcontrollers and hardware debug tools form Silabs company. Develop a simple hardware module for demonstration of implemented functionality. The implemented test module should support a connection to the PC computer via microcontroller UART interface. Create an application which will demonstrate encrypted communication. Analyze throughput of developed implementation and microcontroller resource utilization.

Language of the thesis: English

Thesis submission deadline: 30.04.2015

Assigned on 31.10.2014

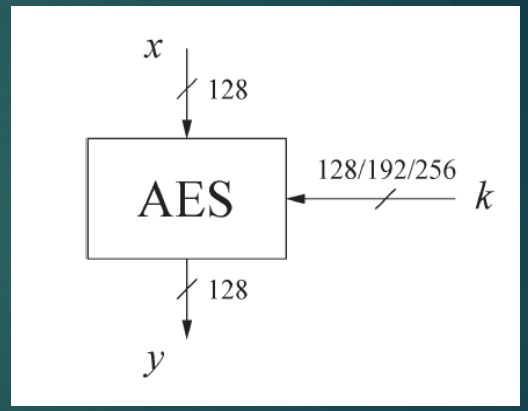
Contents

- First idea of the project
- AES encryption
- Implementation of project
- Block diagram
- Schematic
- Photo of the MCU
- Functionality test
- MCU development tools
- Future steps

AES encryption

- AES is the most widely used symmetric-key algorithm today. Symmetric-key means that the same key is used for both encrypting and decrypting the data.

- Three main features are:
  - Block cipher with 128-bit block size
  - Three supported key lengths: 128, 192 and 256 bit
  - Efficiency in software and hardware



- Due to its long keys, brute force attack is no possible (yet).

AES encryption

Internal structure of AES:

- Byte Substitution layer

  (consists of 16 S-Boxes)

- Diffusion layer

  (provides diffusion over all input state bits and consists of two sublayers:

  - ShiftRows Sublayer
  - MixColumn Sublayer)

- Key schedule

  (generates sub-keys for the next level. Subkeys are derived recursively from the original 128/192/256-bit input key)

- Key Addition layer

  (Output: $C \oplus ki$)

First idea

Huge and growing need of safe telecommunications.

Lots of people who do not respect privacy of telecommunications, as well as very big and aggressive competition in companies, which leads into hacking of personal data especially messages.

A relatively low cost and small size, easy to carry on device, that could apply encryption (and decryption) at both sides, sounds very promising.

Implementation of project

Main devices and elements:

- Microcontroller Silabs 8-bit C8051 F342

  (stores the AES algorithm, key, and applies encryption or decryption)

- Chip MAX 3232

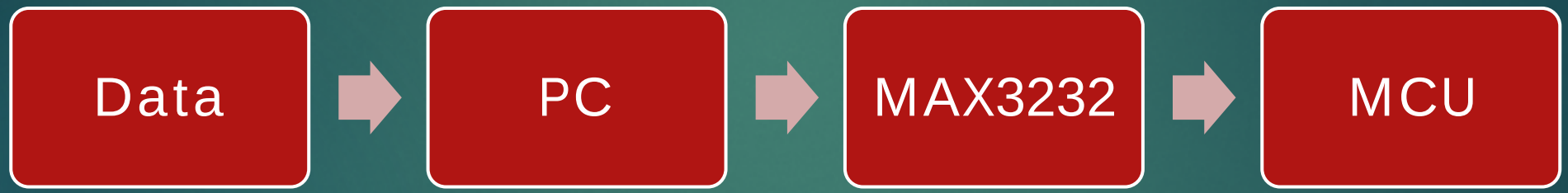
  (rearranges voltage to the appropriate levels, in order to communicate with PC directly through Rx and Tx ports of the microcontroller)

- JTAG adapter

  (programing of microcontroller)

Block Diagram

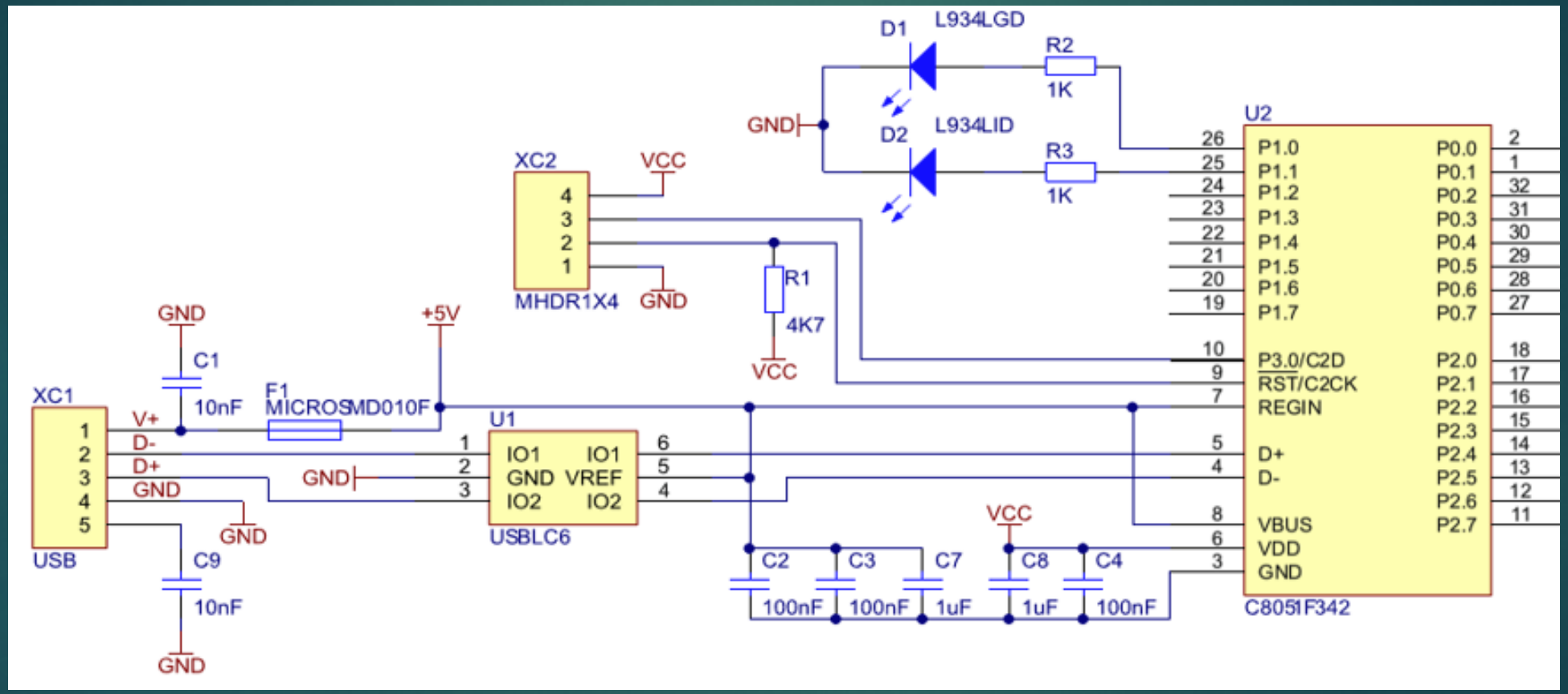
of the whole hardware



*Each block communicates with its next or previous block via secured channel

Schematic

of the MCU block



Schematic

of the MAX3232 circuit

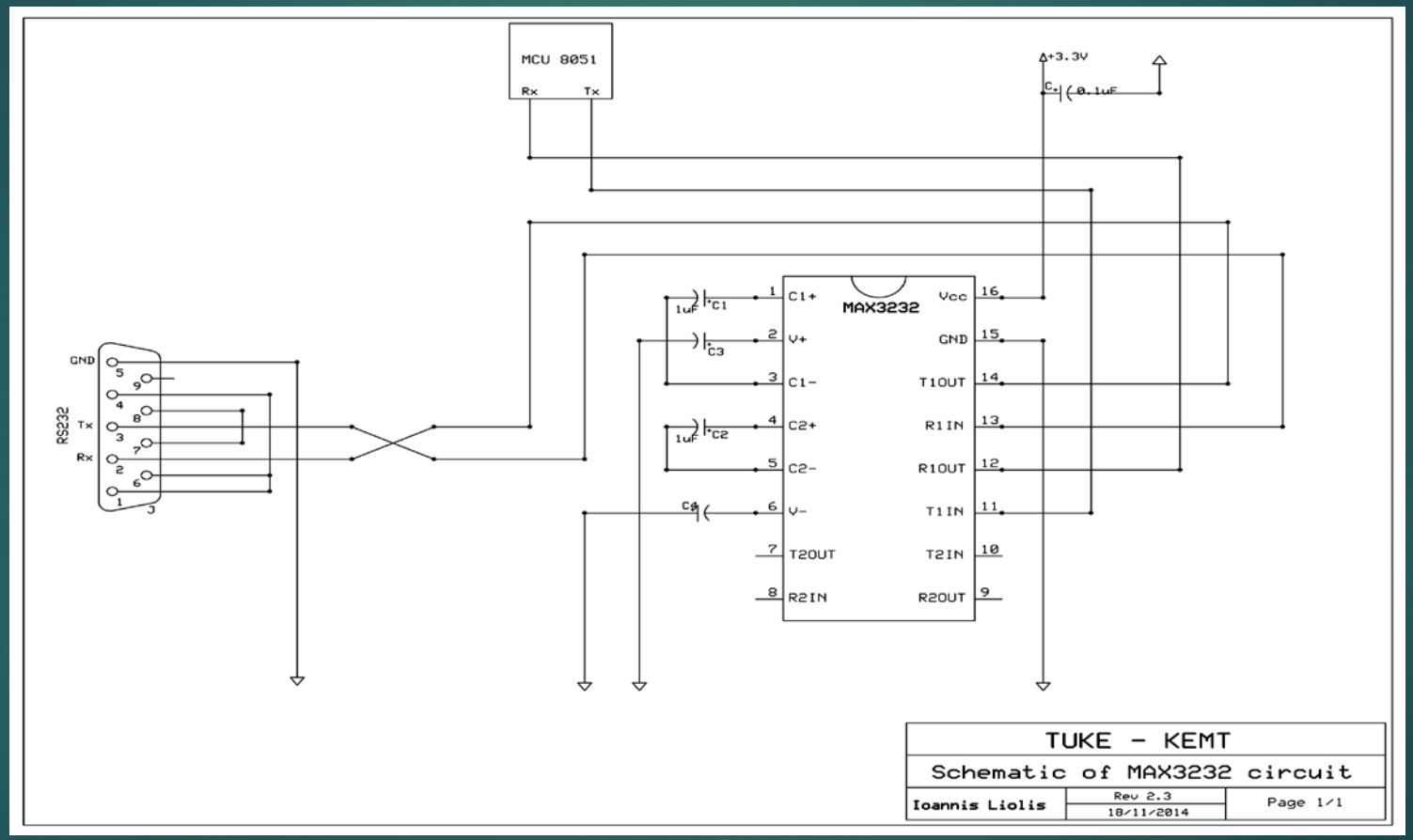
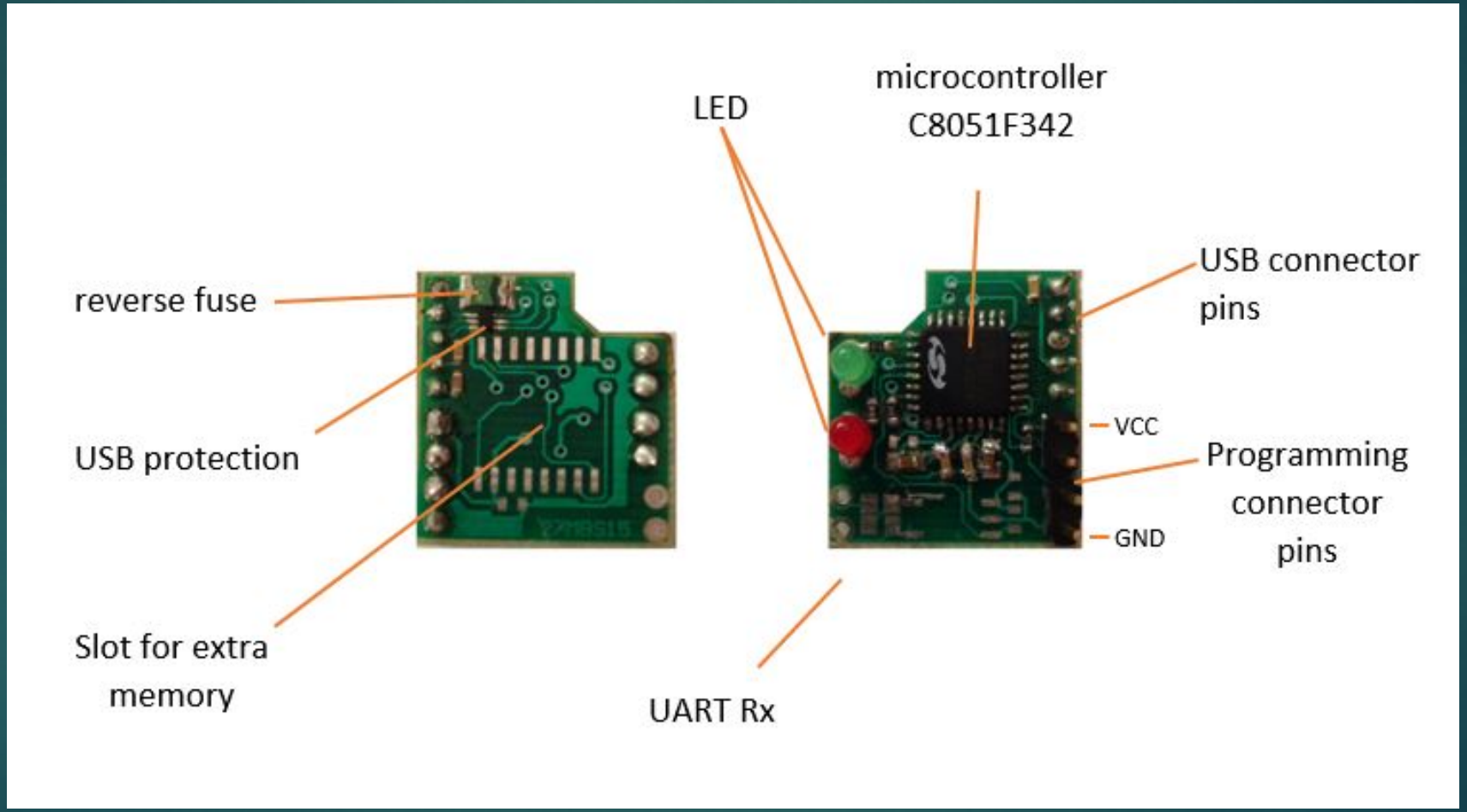


Photo of the MCU



Functionality test

After soldering the hardware and double-checking all the connections with ohmmeter, we tested the appropriate functionality of our device by loading a simple program to the microcontroller, configuring first all the appropriate parameters according the datasheets of our microcontrollers manufacturer.

The testing program responded exactly as expected, so now we were convinced that everything was working properly.

Ready for our next step..!

MCU development tools

- Keil uVision

  (very well built program for programming and configuring microcontroller. Also used for simulating the code)

- Silabs JTAG adapter

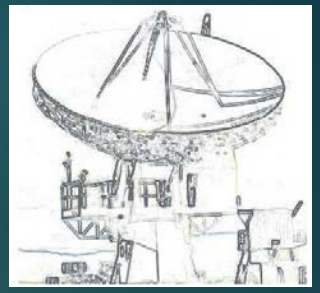
  (device which connects MCU programming pins to PC and allows uploading and debugging the code)

- C programming language

  (suitable for programming hardware)

Future steps

- Our goal is to master the microcontroller to perform strong encryption depending on our needs, being simultaneously a friendly to user device.
- Although wireless technology is more sensitive to attackers, our vision is to try to add a (somehow secured) wireless channel, additionally to the ordinary cable connection to PCs.



THANK YOU!!!
D’AKUJEM!!!