Tutorial: Implementing Cryptography on Microcontrollers

Matthias J. Kannwischer and Bo-Yin Yang
Academia Sinica, Taipei, Taiwan
matthias@kannwischer.eu

08 June 2023, Summer School on real-world crypto and privacy, Vodice, Croatia

Speakers

Bo-Yin Yang

Matthias J. Kannwischer

Agenda

- 9:00 - 9:05 Intro
- 9:05 - 9:45 Modular Multiplication and Reduction
- 9:45 - 10:30 Polynomial Arithmetic I
- **10:30 - 11:00 Coffee break**
- 11:00 - 11:45 Polynomial Arithmetic II
- 11:45 - 12:30 Cortex-M4
- **12:30 - 14:00 Lunch break**
- 14:00 - 15:30 Hands-on: Implement Chacha20, Dilithium NTT, Kyber NTT
- **15:30 - 16:00 Coffee break**
- 16:00 - 17:30 Hands-on continued

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at
  `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at
  `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at
  `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Material

- Slides are available at `https://kannwischer.eu/croatia2023`
  - We will fix mistakes after the tutorial; get the most recent version from there
- Assignment is available at
  `https://github.com/mkannwischer/m4-tutorial-croatia2023`
  - Tests can be emulated using qemu. Benchmarks need to be performed on actual hardware.
  - We brought 26 STM32F407 discovery board for use during the tutorial.
    $\Longrightarrow$ Return after the tutorial.
  - Tested on Linux and MacOS (Windows: Probably want to run a Linux VM)
  - Solutions: Sent us an e-mail after you have tried solving it yourselves.

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?

Some questions

- Who has written C code before?
- Who has written assembly before?
- Who has written Arm assembly before?
- Who has implemented Chacha20 or AES (in any language)?
- Who has implemented (parts of) Kyber or Dilithium (in any language)?
- Who has implemented NTT or FFTs before?