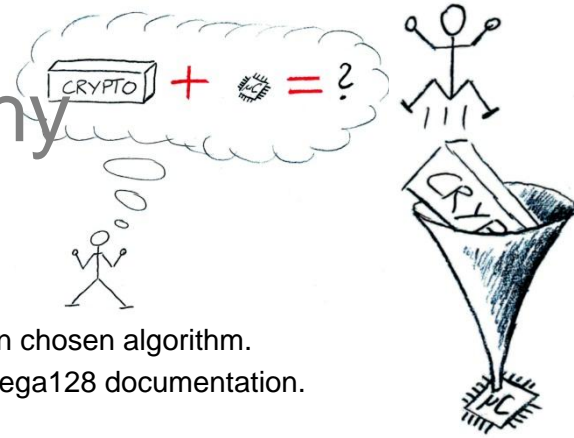


# VLSI: Implement Cryptography for ATmega128 processor



## Motivation

During our latest research project, we implemented a full cycle accurate model of an ATmega128 processor in VHDL! Therefore we can modify and improve the processor for cryptography on a fundamental level. Our goal is to improve its performance regarding cryptography.

## Project description

- Goals
  - Improve the performance
- Possible algorithms:
  - AES, Grøstl, Elliptic Curve Cryptography
- Tasks
  - Understand the algorithm
    - Read about efficient ways to implement the algorithm
    - Read about already existing instruction set extension
  - Implement algorithm
    - First, implement the cryptographic primitive in C
    - Second, optimize the source code, using Assembler
    - Third, change the internals of the processor: Extend the instruction set of the processor in order to improve the AES implementation (area, speed, security)
  - WRITE A CONFERENCE PAPER!  
(if the work is successful)

## Literature

- Depends on chosen algorithm.
- Atmel ATmega128 documentation.

## Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

## Project schedule

- Start Immediately
- Month 1 Reading, design flow
- Month 2 Development of crypto module
- Month 3 Final deliverables

## Master Project

Studies:  INF  SEW  TEL

## Prerequisites

- Basics in C

## Gained know-how

- Cryptographic algorithm
- Microprocessor design
- Instruction set extension
- Hardware design flow

## Advisor / contact

[Erich.Wenger@iaik.tugraz.at](mailto:Erich.Wenger@iaik.tugraz.at)