

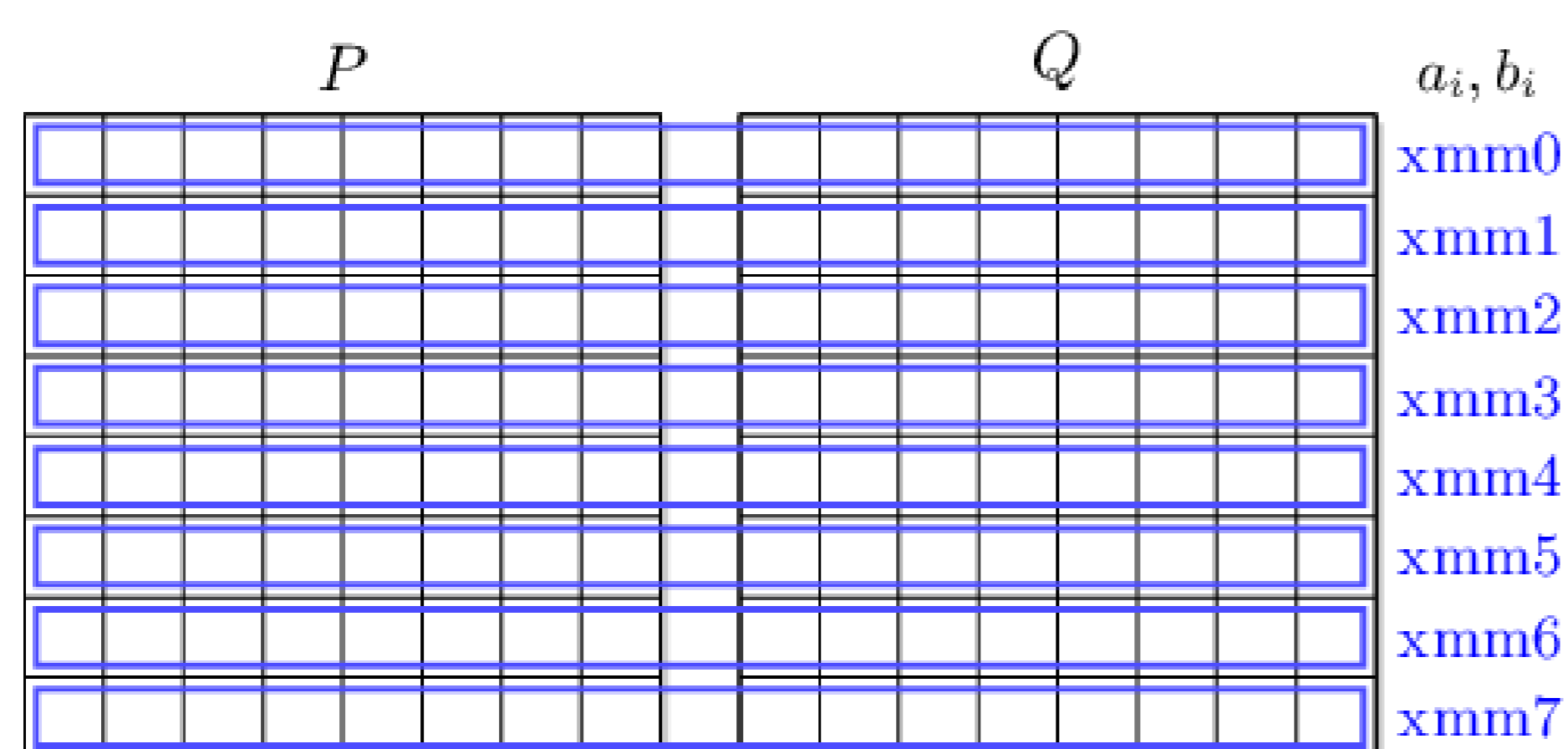
## Motivation

Grøstl is a candidate algorithm for the new SHA-3 standard and similar to AES. New Intel processors with AVX extension provide 256-bit vector instructions. Using these instructions, 16 or 32 columns of Grøstl can be computed in parallel. Moreover, using the vperm implementation of Mike Hamburg, also the S-boxes can be computed in parallel without AES instruction.

Previous vector implementations of Grøstl should be improved by optimizing the S-box computation and using more parallelism of AVX instructions in the MixBytes computation.

## Goals and Tasks

- ▶ Acquire the necessary background on Intel AVX instructions, Grøstl and the vperm implementation
- ▶ Replace critical parts of the given Grøstl assembly using new methods
- ▶ Analyze and optimize the implementation



$$\begin{aligned}
 t_i &= a_i \oplus a_{i+1} & y_i &= t_i \oplus t_{i+2} \oplus a_{i+6} \\
 x_i &= t_i \oplus t_{i+3} & b_i &= 2 \cdot (2 \cdot x_{i+3} \oplus y_{i+7}) \oplus y_{i+4}
 \end{aligned}$$

Figure 1: Schematic view of a vector implementation of Grøstl.

## Literature

- ▶ P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen.  
Grøstl – a SHA-3 candidate.  
Submission to NIST, 2008.  
Available online: <http://groestl.info>.
- ▶ M. Hamburg.  
Accelerating AES with Vector Permute Instructions.  
In *CHES*, volume 5747 of *LNCS*, pages 18–32.  
Springer, 2009.

## Deliverables

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

## Project Schedule

- ▶ Start Immediately
- ▶ Month 1 Reading literature
- ▶ Month 2 Implementing
- ▶ Month 3 Final deliverables

## Master Project

Studies:  INF  SW  TEL  TM

## Prerequisites

- ▶ C programming

## Advisor / Contact

[martin.schlaeffer@iaik.tugraz.at](mailto:martin.schlaeffer@iaik.tugraz.at)