

Motivation

Bit slicing is a software implementation technique which mimics hardware or GPU implementations. By replacing table lookups with simple logical operations, the full parallelism of 128-bit (SSE) or 256-bit (AVX) registers can be used. For cryptographic algorithms, this increases their speed and additionally prevents certain implementation attacks.

Grøstl is a candidate algorithm for the new SHA-3 standard and very similar to AES. Based on bit slice implementations of AES, an efficient bit slice implementation of Grøstl should be developed using the newest Intel/AMD SSE and AVX instructions.

Goals and Tasks

- ▶ Acquire the necessary background on bit slicing and SSE instructions
- ▶ Implement bit sliced Grøstl using a given bit sliced AES implementation
- ▶ Analyze and optimize implementation

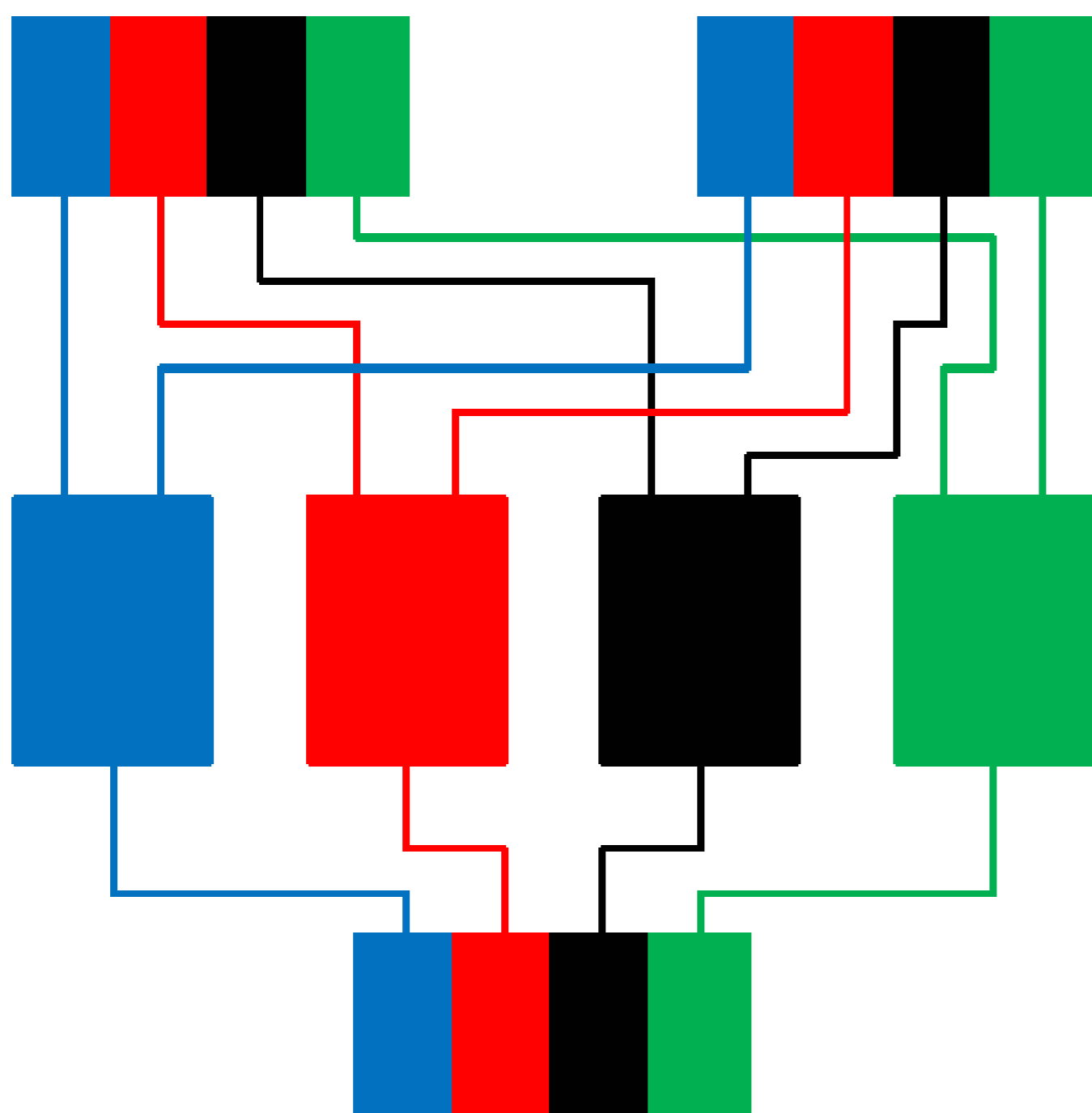


Figure 1: Schematic view of bit slicing.

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>.
- ▶ E. Käsper and P. Schwabe.
Faster and Timing-Attack Resistant AES-GCM.
In C. Clavier and K. Gaj, editors, *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 1–17.
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

Studies

INF SW TEL TM

Prerequisites

- ▶ C programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at