High-Performance Computing Group
Dr. Tobias Kenter
Paderborn Center for Parallel Computing

Enigma Code Breaking with SUS

Bachelor Thesis

At a glance

- Reseach how the Enigma code works
- Implement an encoder/decoder on FPGA
- Research old code breaking techniques
- Implement an enigma code breaker on FPGA

At PC2 we currently develop a new language and compiler, named “SUS”, that aims to help in the design and development of high-frequency FPGA accelerators. It does this by explicitly encoding pipelining information in the type of each wire, and using it both to automatically balance pipelines, as well as participating in type inference of submodule parameters.

We wish to see what the capabilities and limitations of the SUS language thus far are. In this thesis you will use SUS to develop an FPGA implementation for the famous WW2-era Enigma Encryption Machine. Once a working encoder/decoder is finished, you can try your hand at building a second accelerator to break the code, and see how our current FPGA technology stacks up against that of the past.

Further reading:
https://github.com/pc2/sus-compiler
https://www.youtube.com/watch?v=G2_Q9FoD-oQ

Contact:
Lennart Van Hirtum, Phone: 05251/60-4542 E-Mail: lennartv@mail.uni-paderborn.de