Minerva: Automated Hardware Optimization Tool
Farnoud Farahmand, Ahmed Ferozpur, William Diehl and Kris Gaj
Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia 22030, USA

INTRODUCTION

- Static timing analysis provided by CAD tools lets us determine the maximum clock frequency of the digital system.
- Finding the actual maximum clock frequency is difficult, especially in Xilinx Vivado, due to the multitude of tool options, and a complex dependence between the requested clock frequency and the actual clock frequency achieved by the tool.
- In this research, we introduce an automated hardware optimization tool that determines the close-to-optimal settings of tools, using static timing analysis and a heuristic algorithm developed by the authors.
- We evaluate RTL designs of 29 Round 2 CAESAR candidates and the current standard, AES-GCM, in terms of throughput and TPA ratio. Compared to a binary search for maximum frequency, our results demonstrate up to 25% improvement in terms of throughput, and up to 38% improvement in terms of TPA ratio.

VIVADO EVALUATION: Dependence of the WNS on the Requested Clock Frequency

1. WNS: Worst Negative Slack
2. Req Freq: Requested Clock Frequency
3. High-speed implementation of AES-GCM:

![AES-GCM Graph](image1)

Reference Frequency = 246 MHz
Maximum Frequency = 270 MHz

![Graph showing WNS vs. Req Freq for AES-GCM](image2)

4. High-speed implementation of Scream:

![Scream Graph](image3)

Reference Frequency = 188 MHz
Maximum Frequency = 175 MHz

![Graph showing WNS vs. Req Freq for Scream](image4)

5. High-speed implementation of ICEPOLE:

![ICEPOLE Graph](image5)

Reference Frequency = 396 MHz
Maximum Frequency = 389 MHz

![Graph showing WNS vs. Req Freq for ICEPOLE](image6)

ENVIRONMENT: Graphical Representation of Minerva Frequency Search Algorithm

![Algorithm Graph](image7)

- Runs in parallel
- Starting point
- Maximum Freq.
- Runs in parallel
- Maximum Freq.

RESULTS: Minerva vs. Binary Search

- Ratios of Minerva TP / Binary Search TP for three modes of Minerva frequency search, and 30 authenticated ciphers. Notation: TP - Throughput

![Graph showing Ratios of Minerva TP / Binary Search TP](image8)

- Ratios of Minerva TPA / Binary Search TPA for three modes of Minerva frequency search, and 30 authenticated ciphers. Notation: TPA - Throughput/Area ratio

![Graph showing Ratios of Minerva TPA / Binary Search TPA](image9)

RESULTS: Run Time

- Run time comparison of Minerva TP, Minerva TPA and binary search for 29 Round 2 CAESAR candidates and AES-GCM

![Graph showing Run Time Comparison](image10)

- Run time comparison of Minerva Fast and binary search for 29 Round 2 CAESAR candidates and AES-GCM

![Graph showing Run Time Comparison](image11)

CONCLUSIONS

- Minerva searches for the best requested clock frequency and the best set of tool options, leading to the highest clock frequency, or the highest frequency to area ratio.
- It can apply an arbitrary number of preselected tool option sets and combine them with a frequency search in order to achieve the best results.
- The results for 30 authenticated ciphers indicate that we can achieve up to 38% improvement in terms of the TPA ratio in comparison to a simpler binary search.
- The average run time for the Minerva_TP and Minerva_TPA modes is over 6 and 9 times longer than binary search, respectively. However, Minerva_Fast has an execution time equal to binary search, and produces acceptable results.

Minerva source code and user’s manual are available for free at: https://crypto.gmu.edu/athena/index.php?id=Minerva

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1314540.