Minerva: Automated Hardware Optimization Tool

Farnoud Farahmand, Ahmed Ferozpuri, William Diehl and Kris Gaj
Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia 22030, USA

GEORGE MASON UNIVERSITY

CERG Cryptographic Engineering Research Group

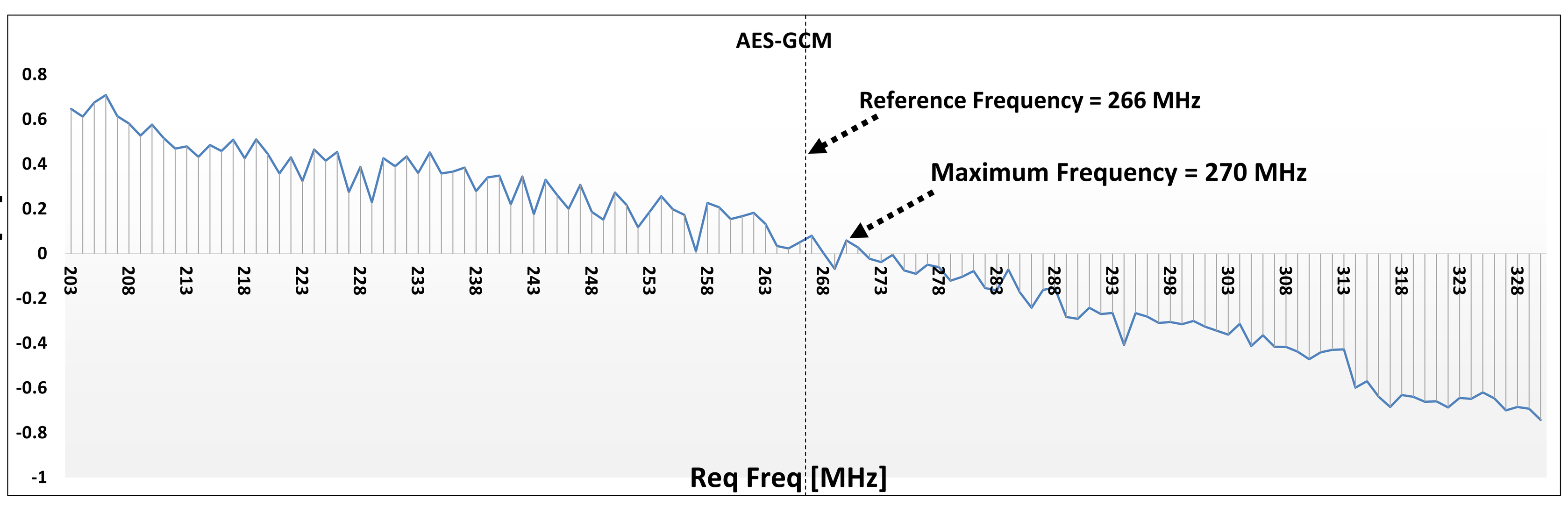
INTRODUCTION

- **Static timing analysis** provided by CAD toolsets let 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**.

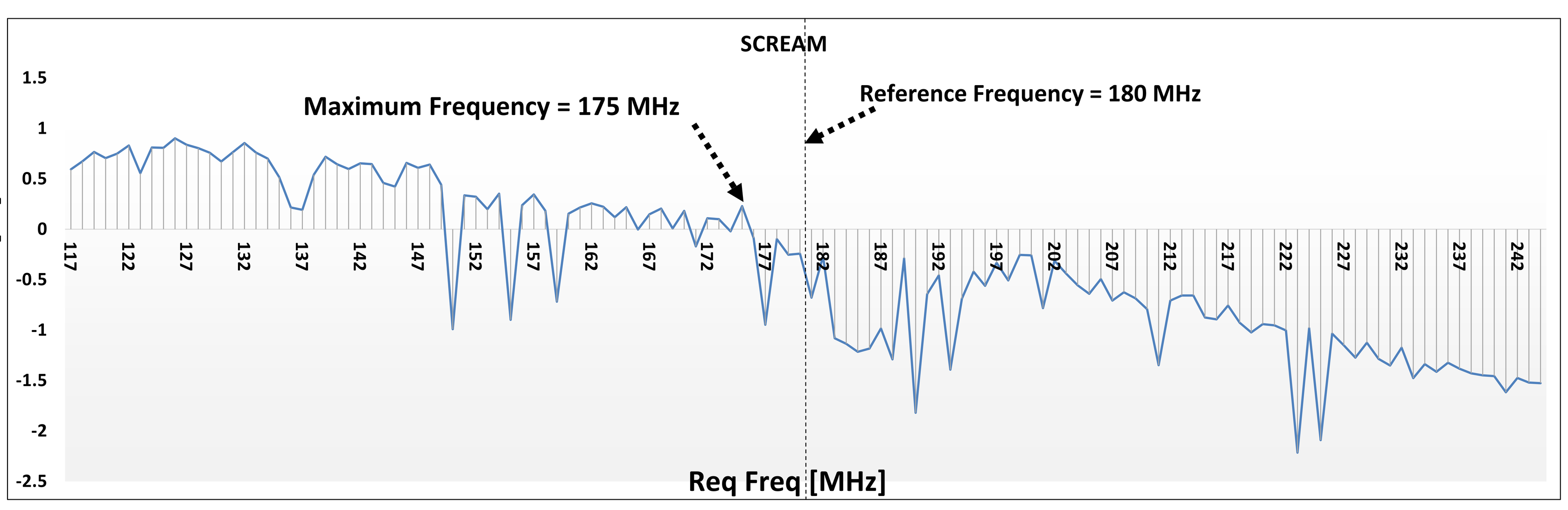
VIVADO EVALUATION: Dependence of the WNS on the Requested Clock Frequency

1. WNS: Worst Negative Slack.
2. Req Freq: Requested Clock Frequency.

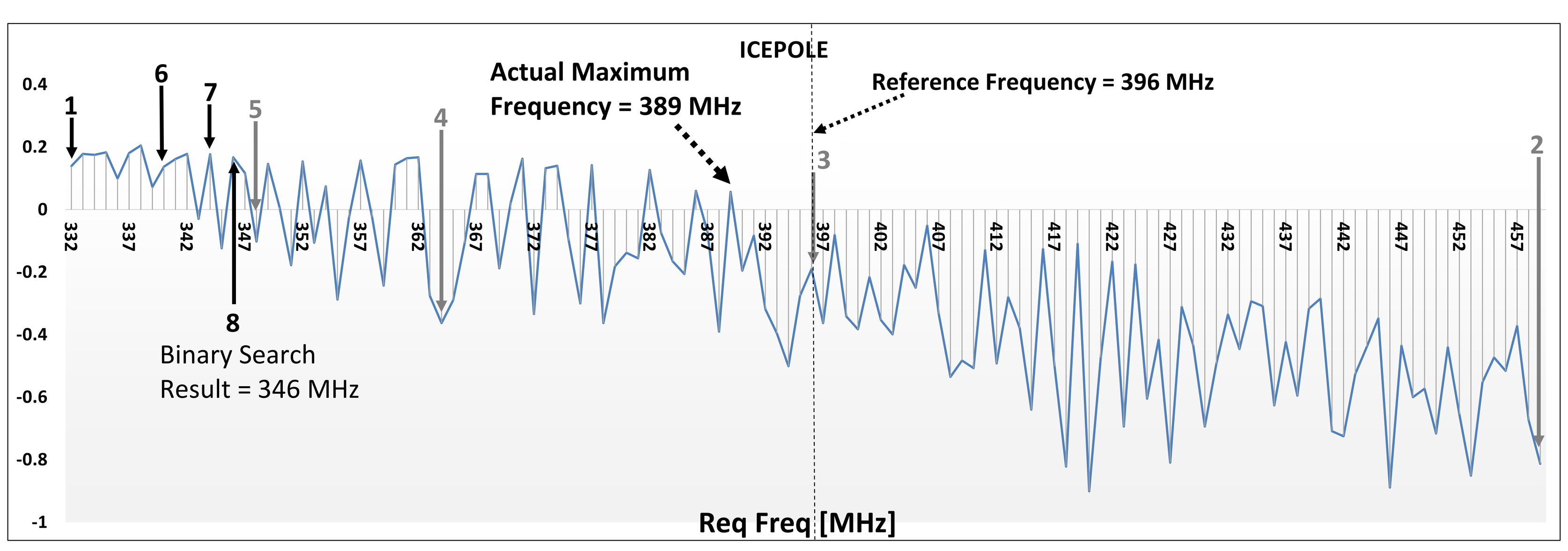
- **High-speed implementation of AES-GCM:**



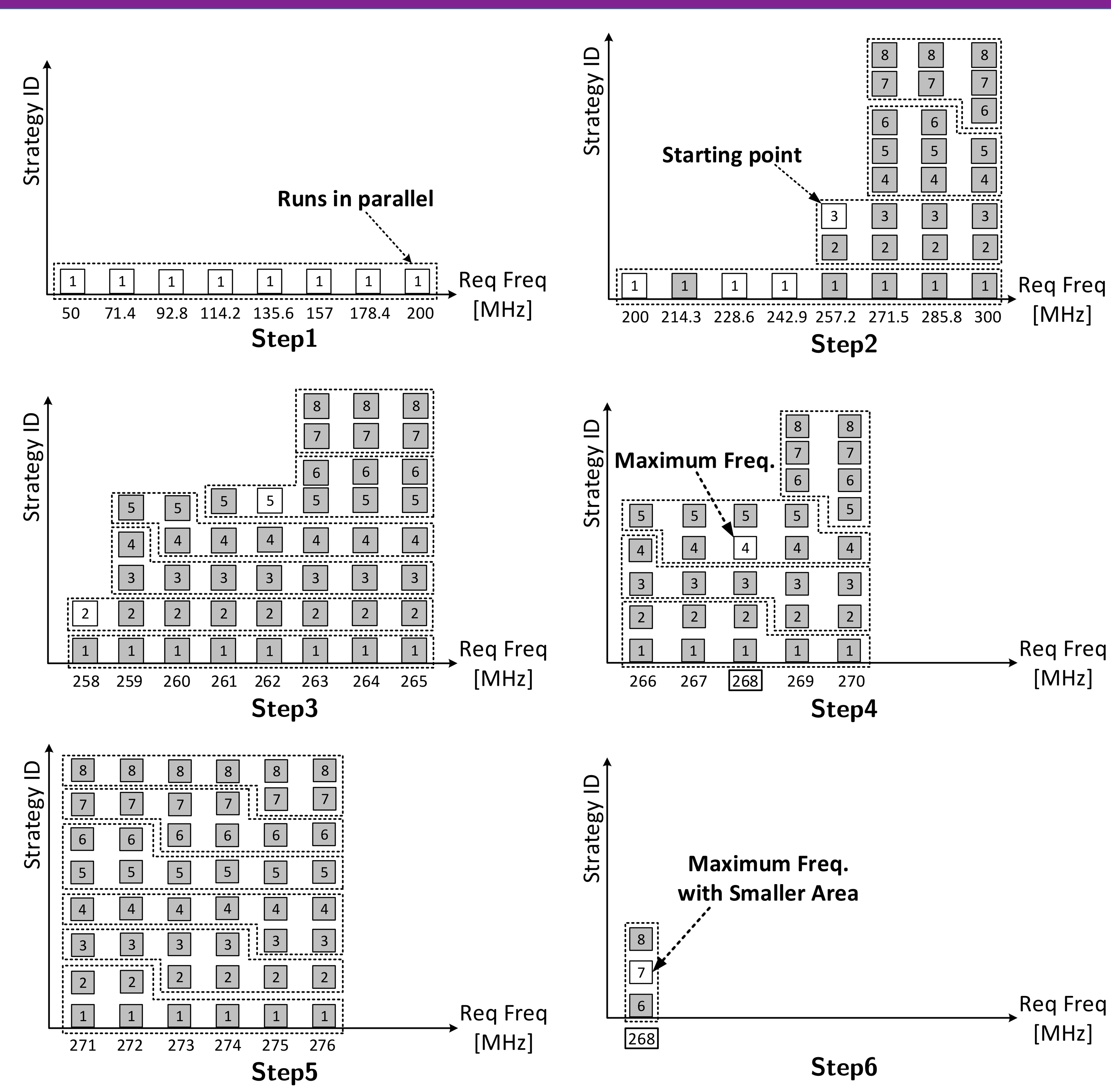
- **High-speed implementation of SCREAM:**



- **High-speed implementation of ICEPOLE:**

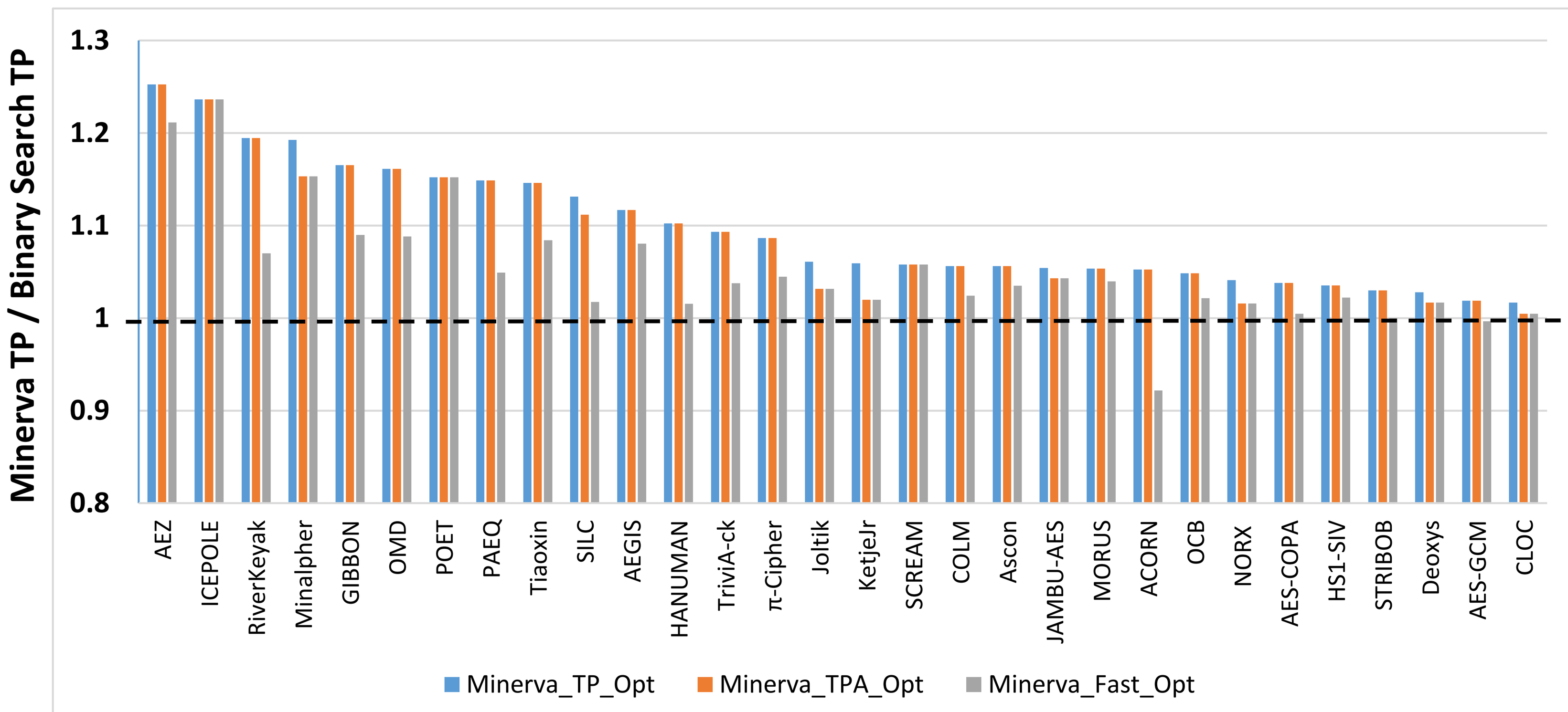


ENVIRONMENT: Graphical Representation of Minerva Frequency Search Algorithm

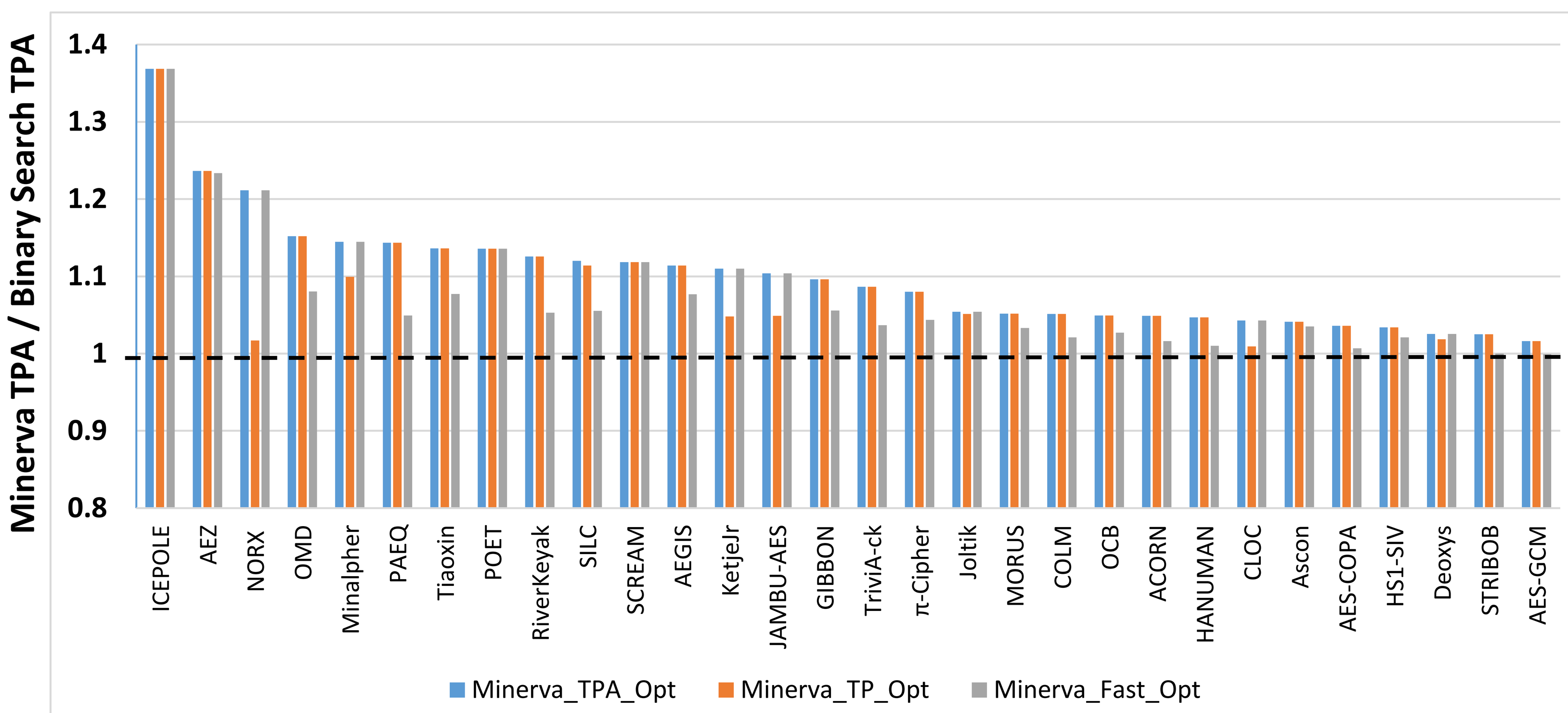


RESULTS: Minerva vs. Binary Search

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

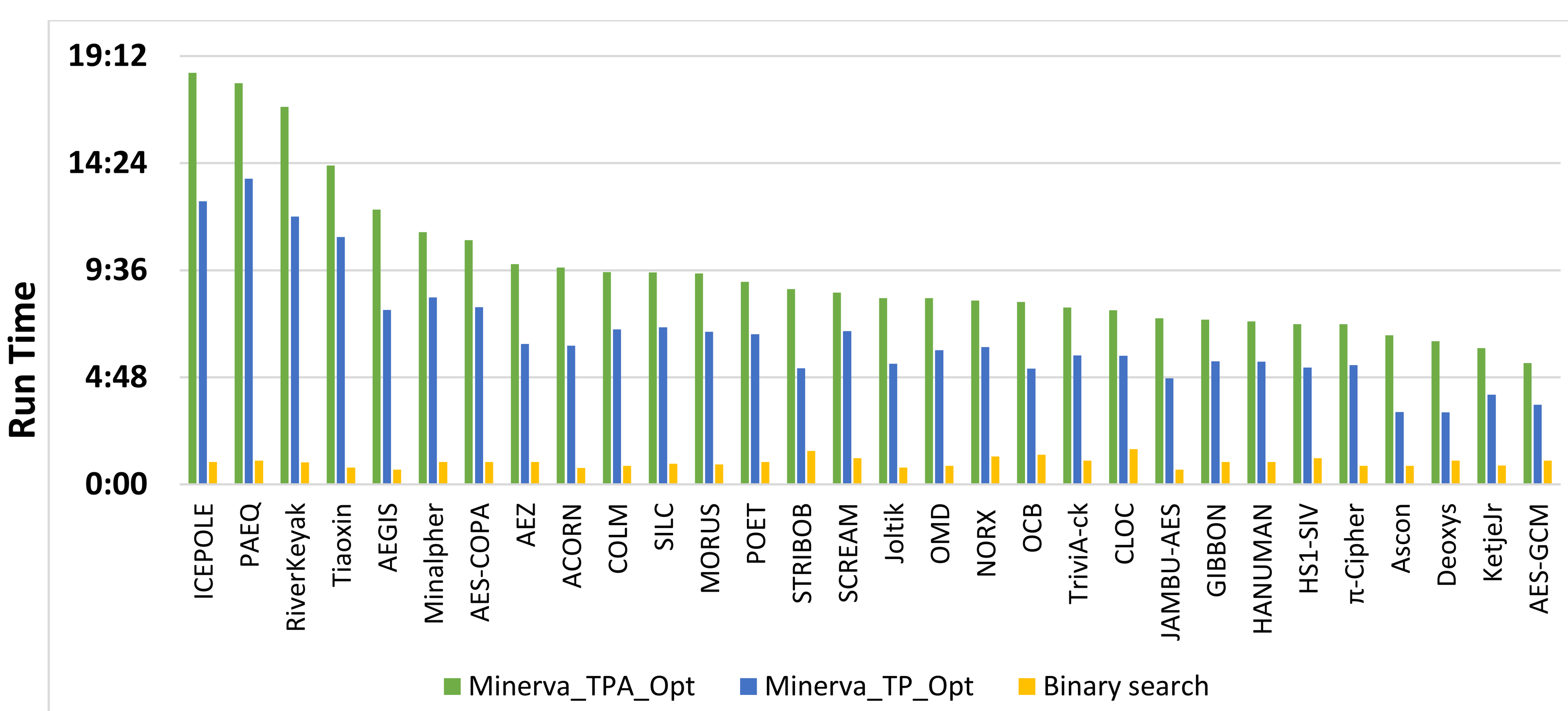


- **Ratios of Minerva TPA / Binary Search TPA for three modes of Minerva frequency search, and 30 authenticated ciphers. Notation: TPA - Throughput/Area ratio**

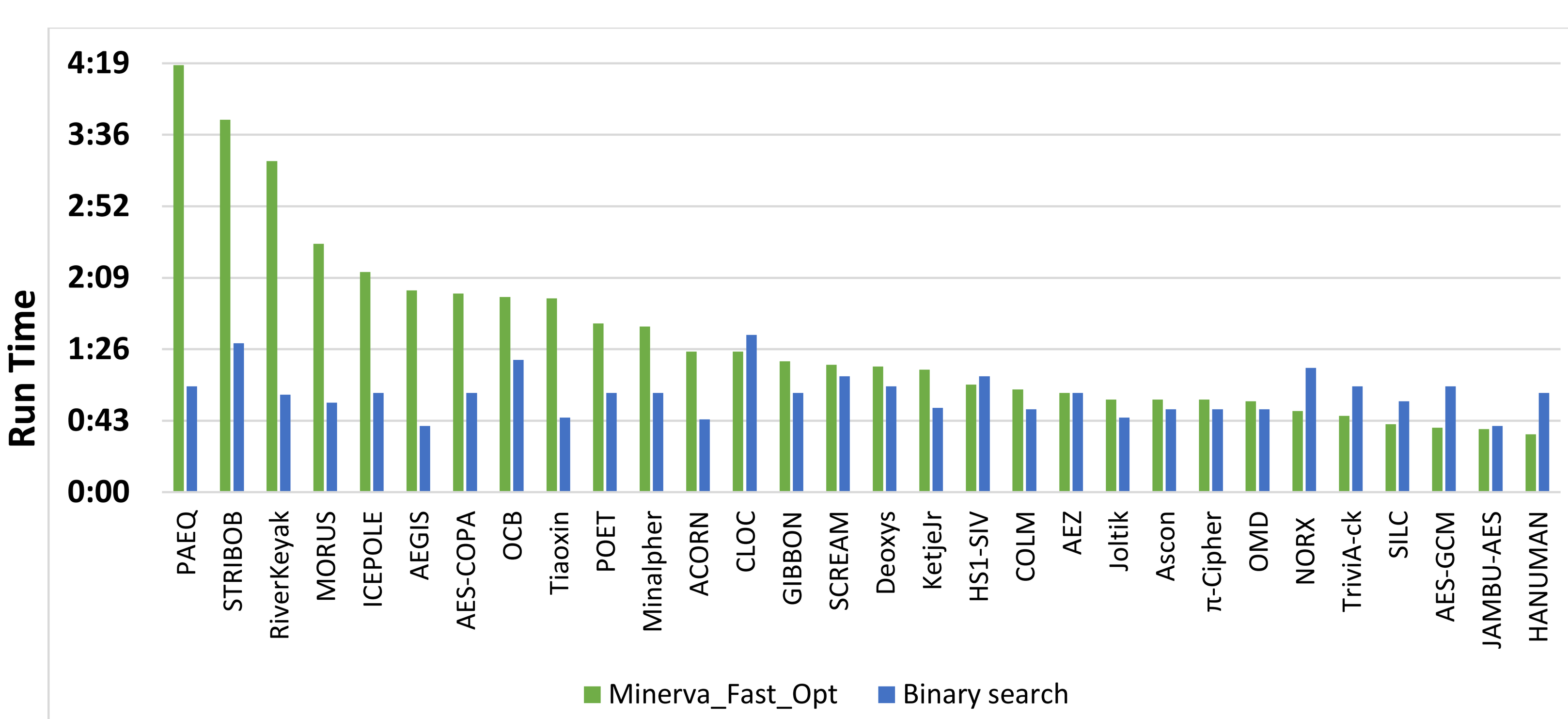


RESULTS: Run Time

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



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



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://cryptography.gmu.edu/athena/index.php?id=Minerva

Acknowledgment

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