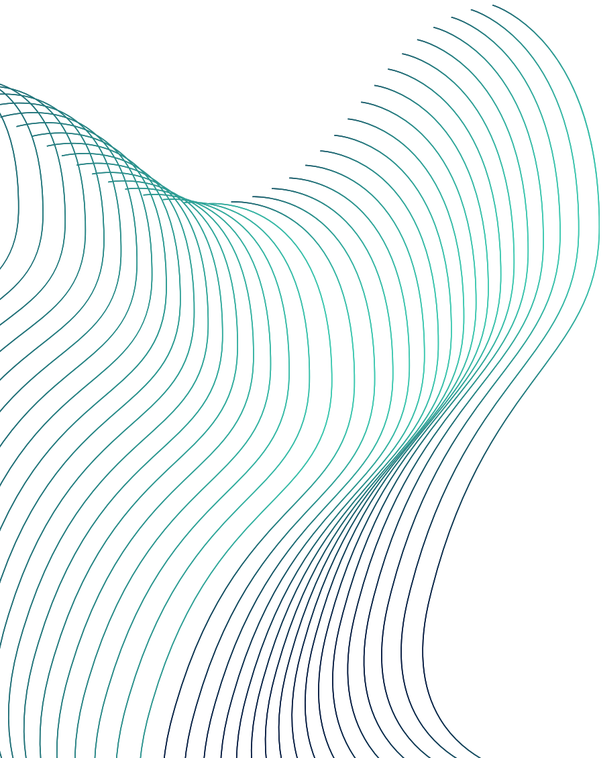
Performance Benchmarking
CRYSTALS-Kyber

CS 199 Group Q
Bugaoisan, Denver Earl Paul S.
Serrano, Nuan Patricia S.

Outline



1. Rationale
2. Statement of the Probkem
3. **Materials and Methods**
    a. **Machines Used**
    b. **Programs Used**
    c. **Research Paradigm**
4. **Results and Discussion**
5. **Conclusion**
6. **Scope and Delimitation**
7. **Recommendations**

Rationale

Threat to commonly used cryptography algorithms

- cryptography algorithms can easily be broken through **Shor's algorithm** using Quantum Computers

NIST

- opened a call for **quantum-resistant algorithms**

Rationale

CRYSTALS-Kyber

- NIST finalist
- General Encryption
- Key Encapsulation Mechanism
- based on **Module Learning with Errors (MWLE) over lattices**

Objectives

- broaden tests using different hardware architectures
- provide insights on feasibility and compatibility of deploying quantum-resistant algorithms in different machines

Problems

How do factors like the programming language and machine used affect Kyber run time?

Problem 1

C vs Python implementation

Problem 2

Better “machines” = faster runtime?

Problem 3

Different machine configurations (RAM, Clock Speed)

Materials & Methods

Machines Used and their Specifications

1. Desktop PC
   - **CPU –** Ryzen 3600
   - **Storage –** 1 TB NVMe SSD
   - **RAM –** 32 GB DDR4-3200
   - **OS** - Windows 11
   - **BASE CLOCKRATE:** 3600 MHz

2. Laptop
   - **CPU –** Ryzen 3500U
   - **Storage –** 500 GB NVMe SSD
   - **RAM –** 10 GB DDR4-2400
   - **OS** - Windows 11
   - **MAX BOOST CLOCK:** 3700 MHz

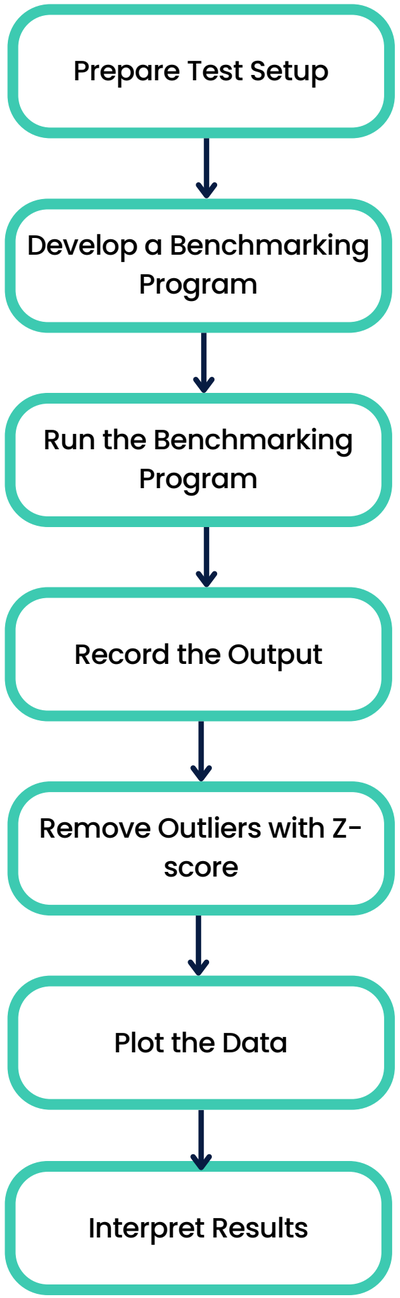
3. Macbook Pro M1 2020
   - **CPU**: Apple M1 chip with 8-core CPU
   - **Storage**: 256 GB SSD
   - **RAM**: 16 GB unified memory
   - **OS**: MacOS Sonoma 14.0
   - **MAX BOOST CLOCK:** 3200 MHz

4. DOST-ERDT High Performance Cluster
   - **CPU**: 2x AMD EPYC 7513 32-Core Processor
   - **RAM**: 16x 16GB DRAM
   - **OS**: CentOS Linux
   - **NODES USED:** 4
   - **CLOCKRATE**: 2600 MHz

Programs Utilized

Kyber Original Implementation (in C)
Kyber Python Implementation

Research Paradigm



1st Sem Results

C Implementation

- 2 machines (desktop and laptop)

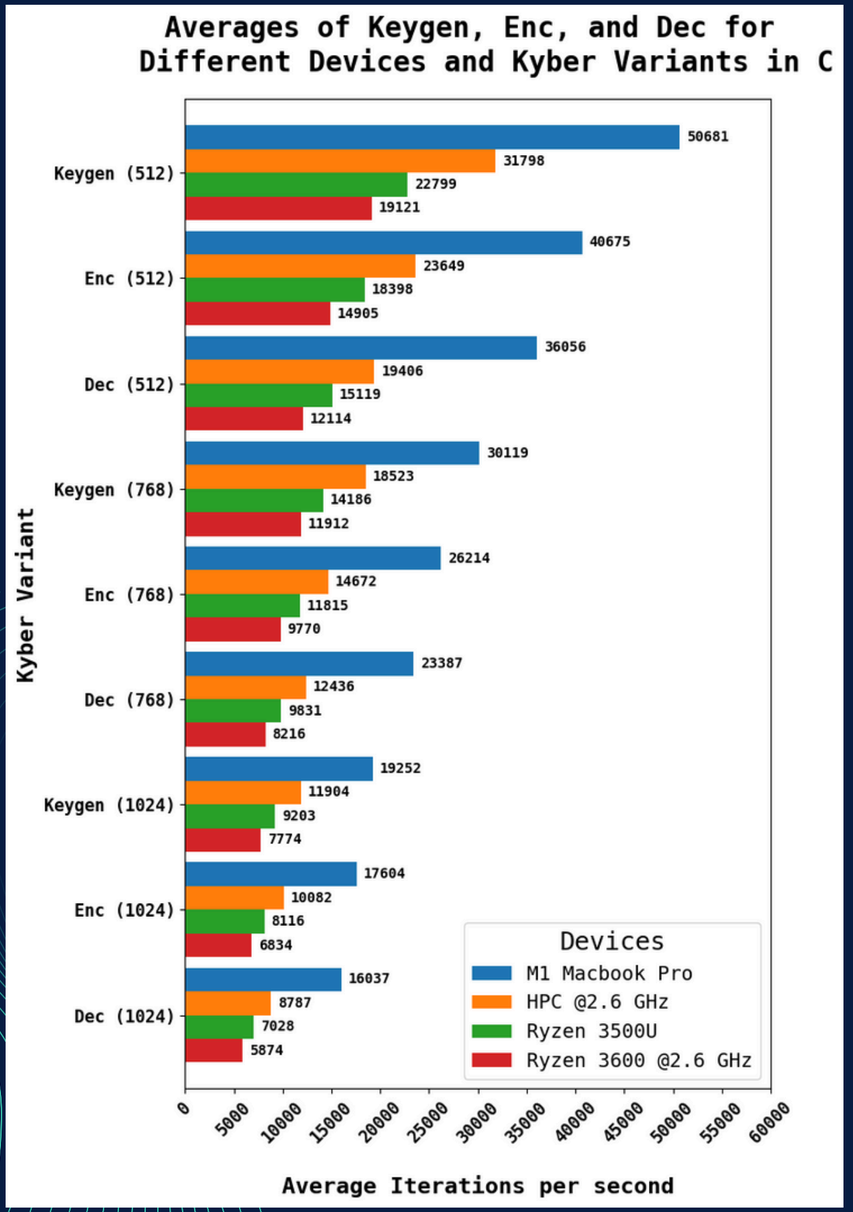
Python Implementation

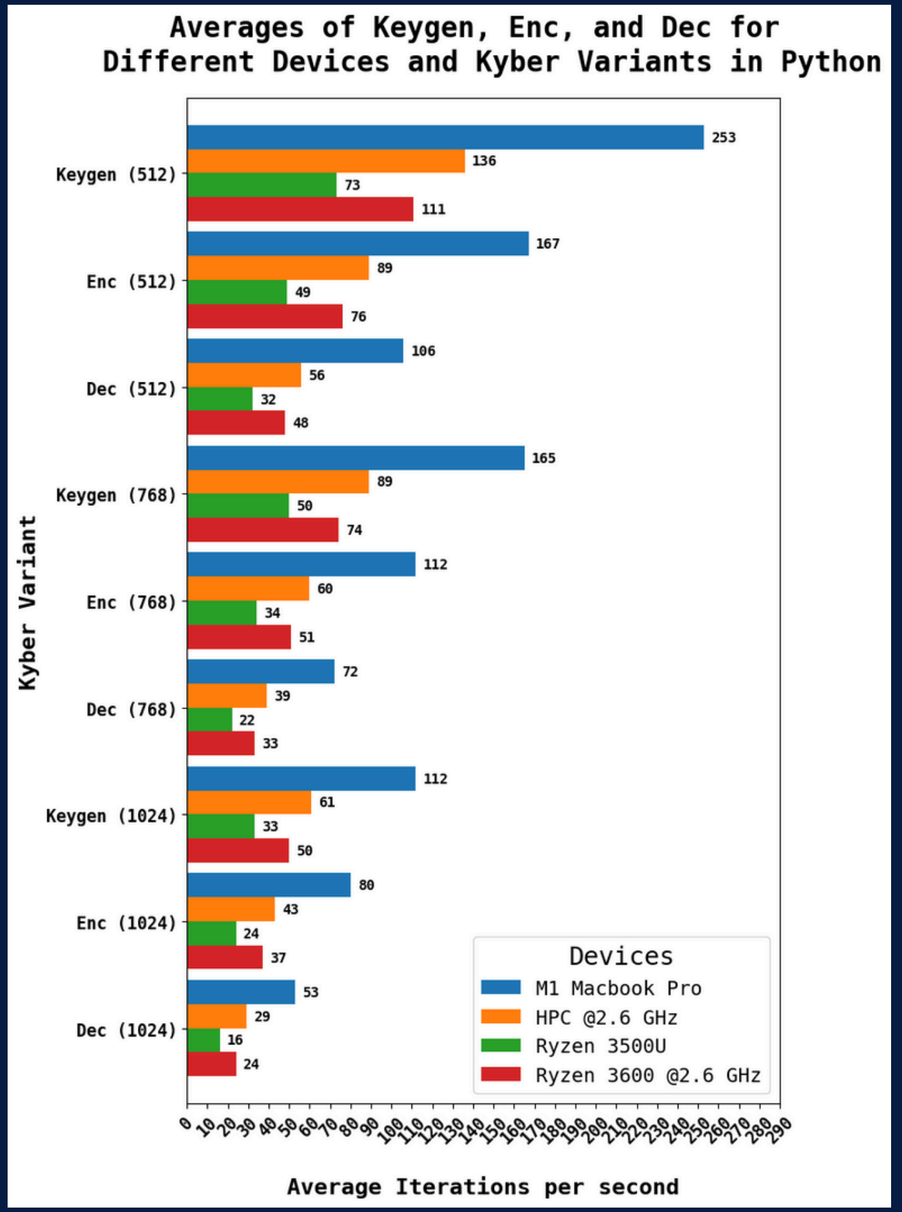
- 3 machines (desktop, laptop and macbook)

- average time it took per iteration (per operation)

Results

Fastest Operation:
Key Generation

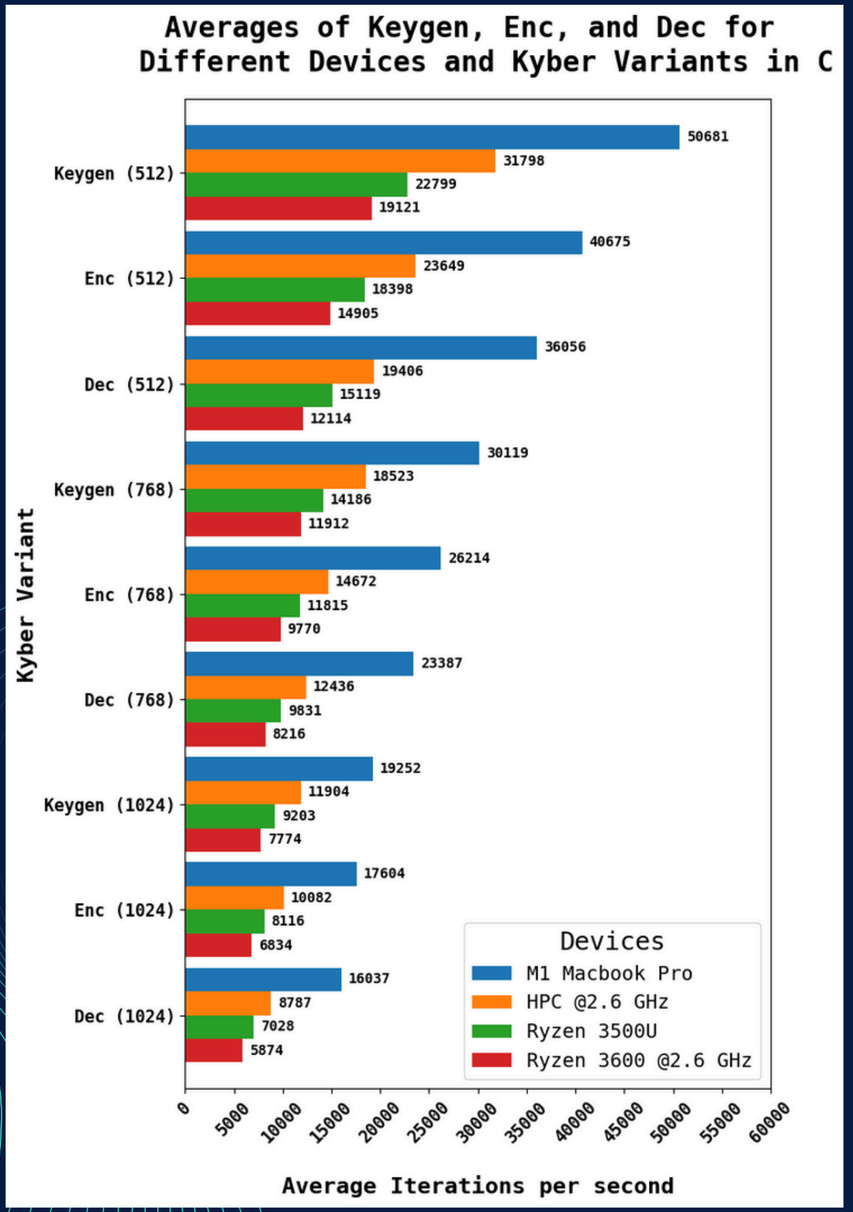


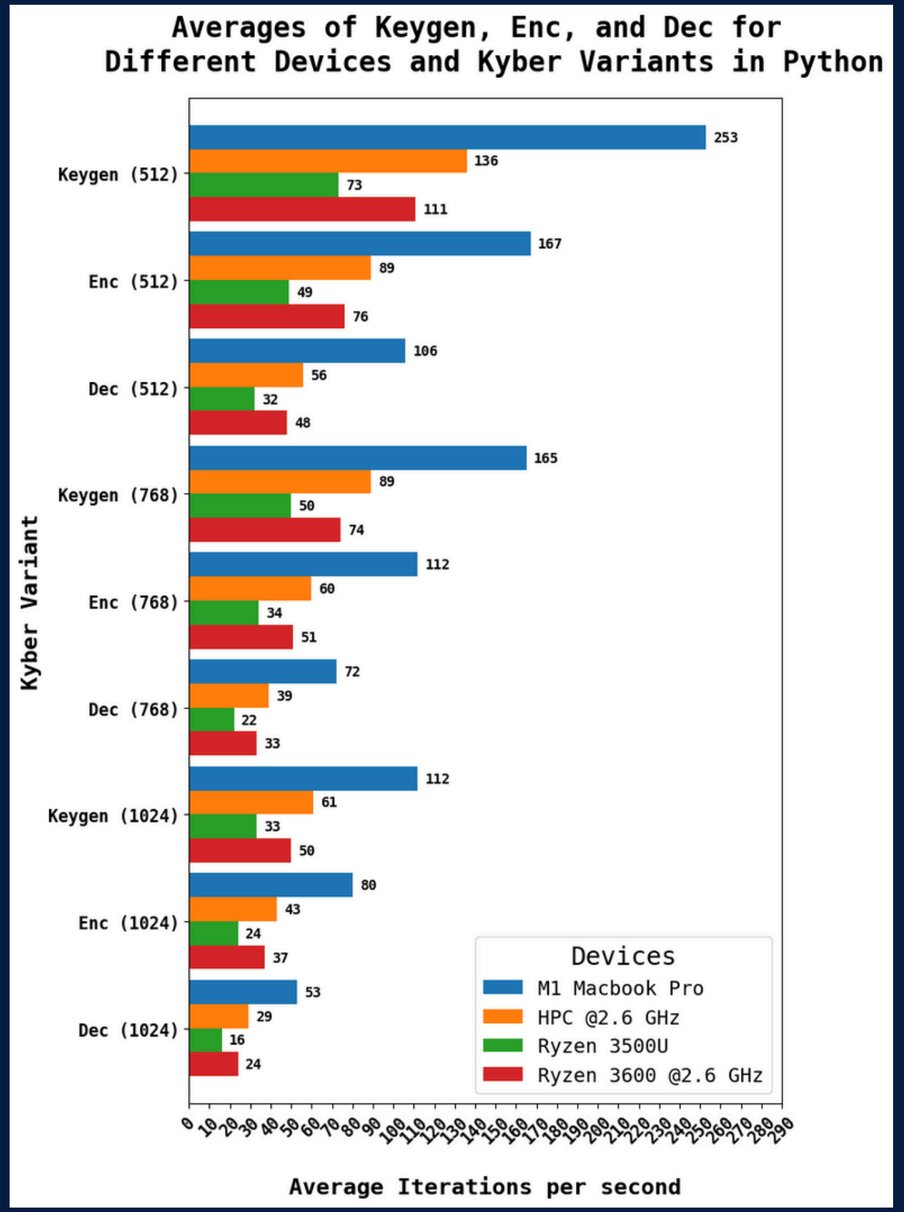


Results

Fastest Variant:

Kyber512

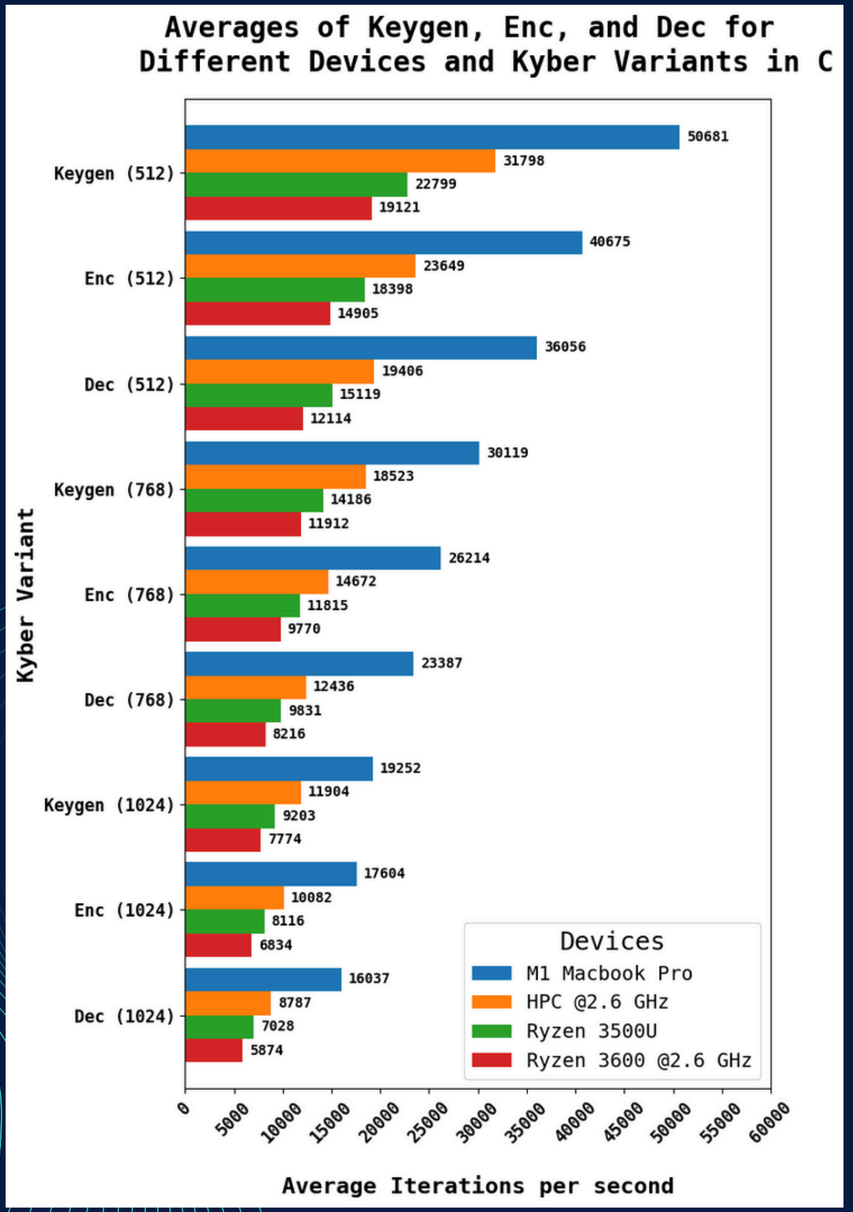


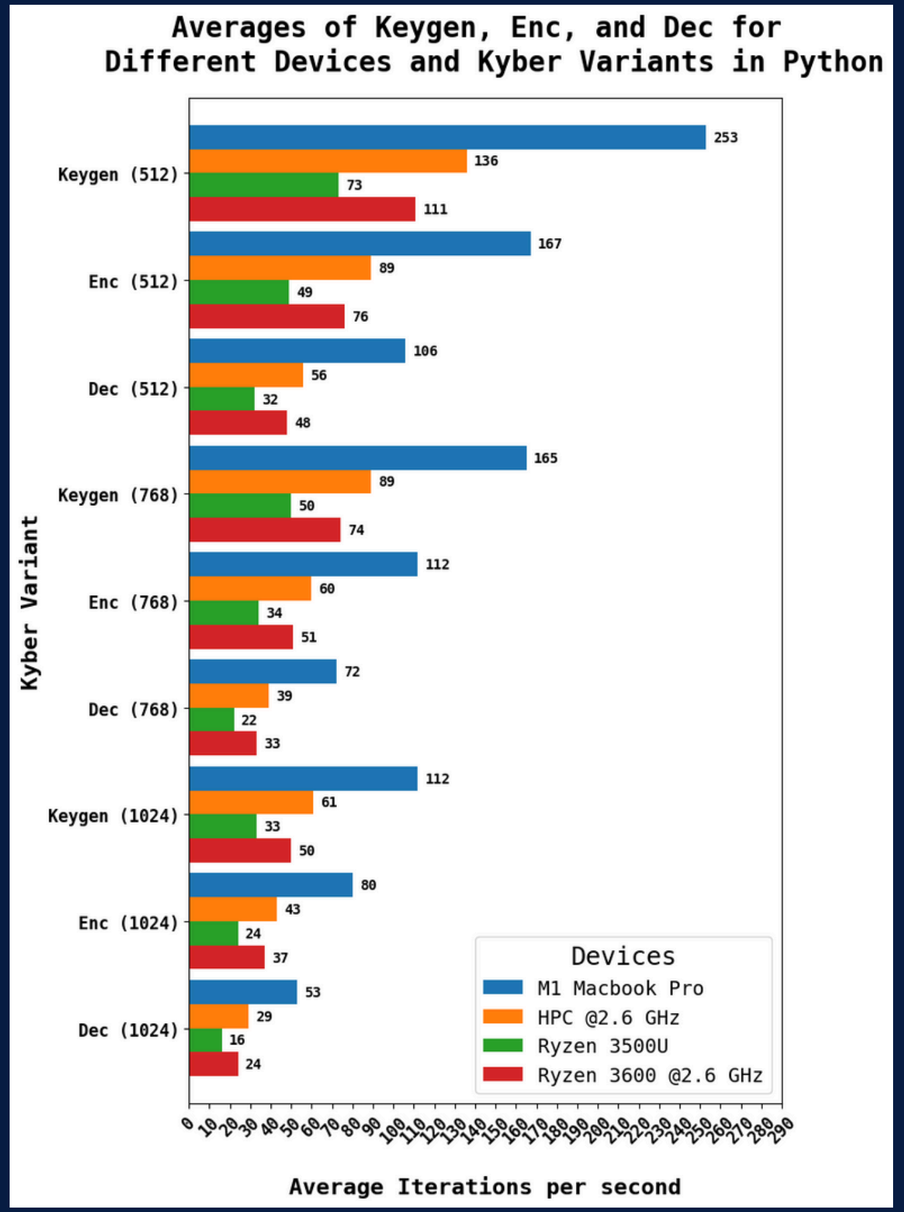


Results

Fastest Programming Language:

C

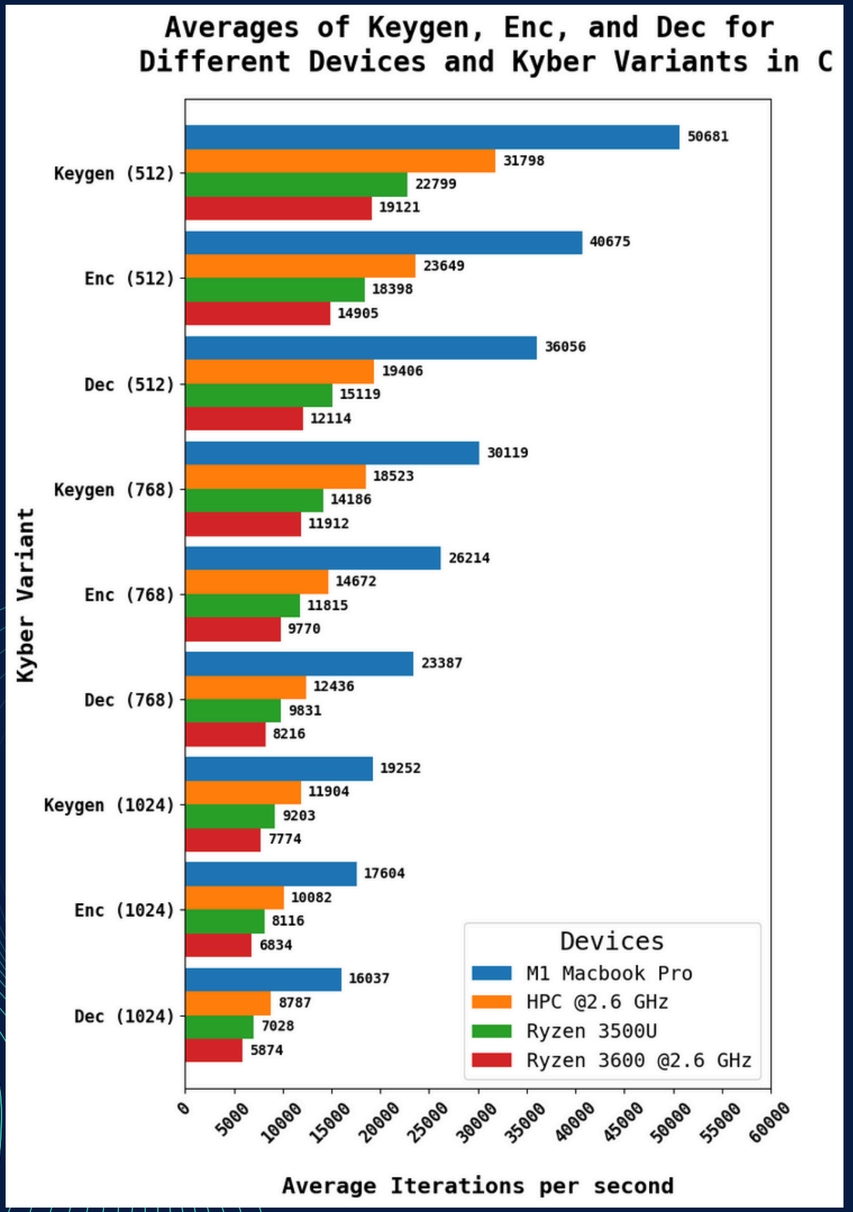


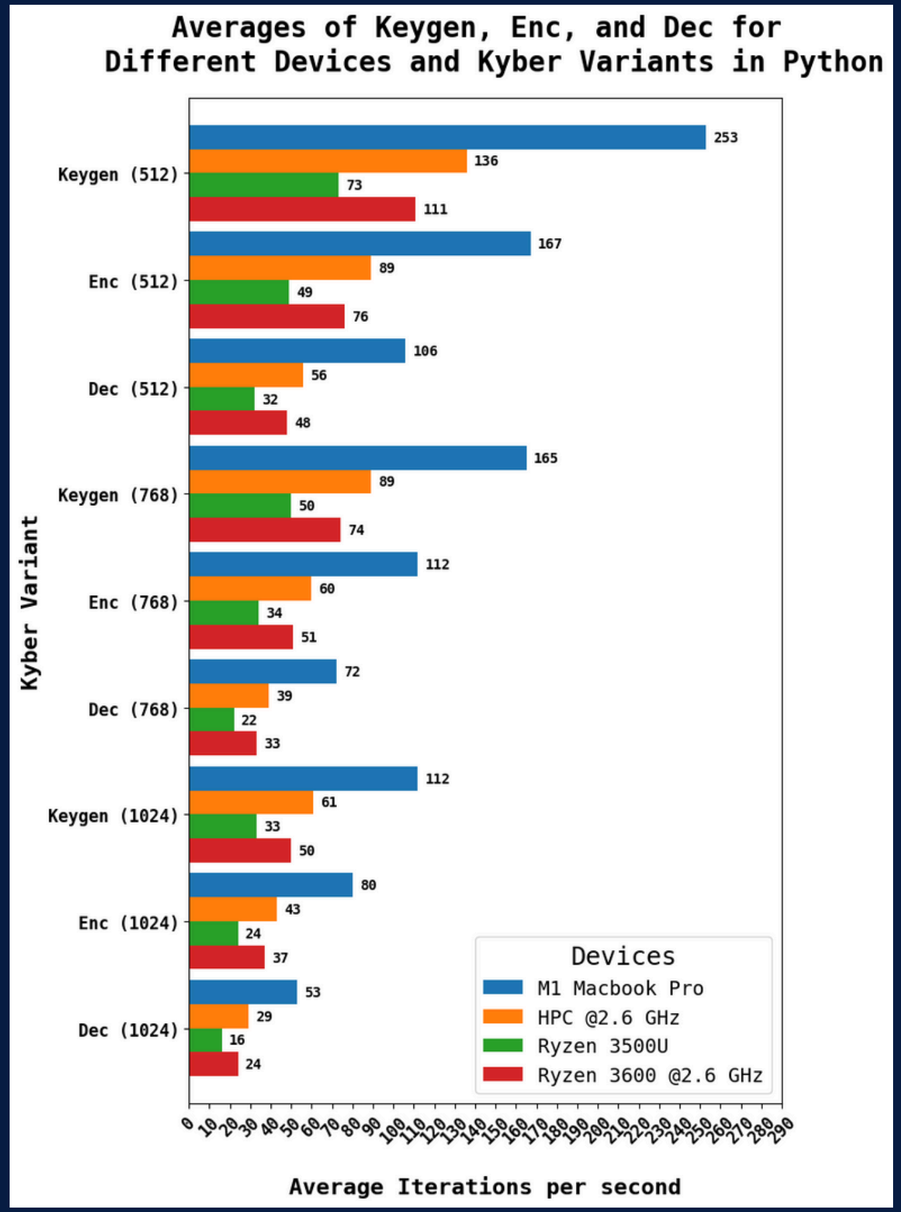


Results

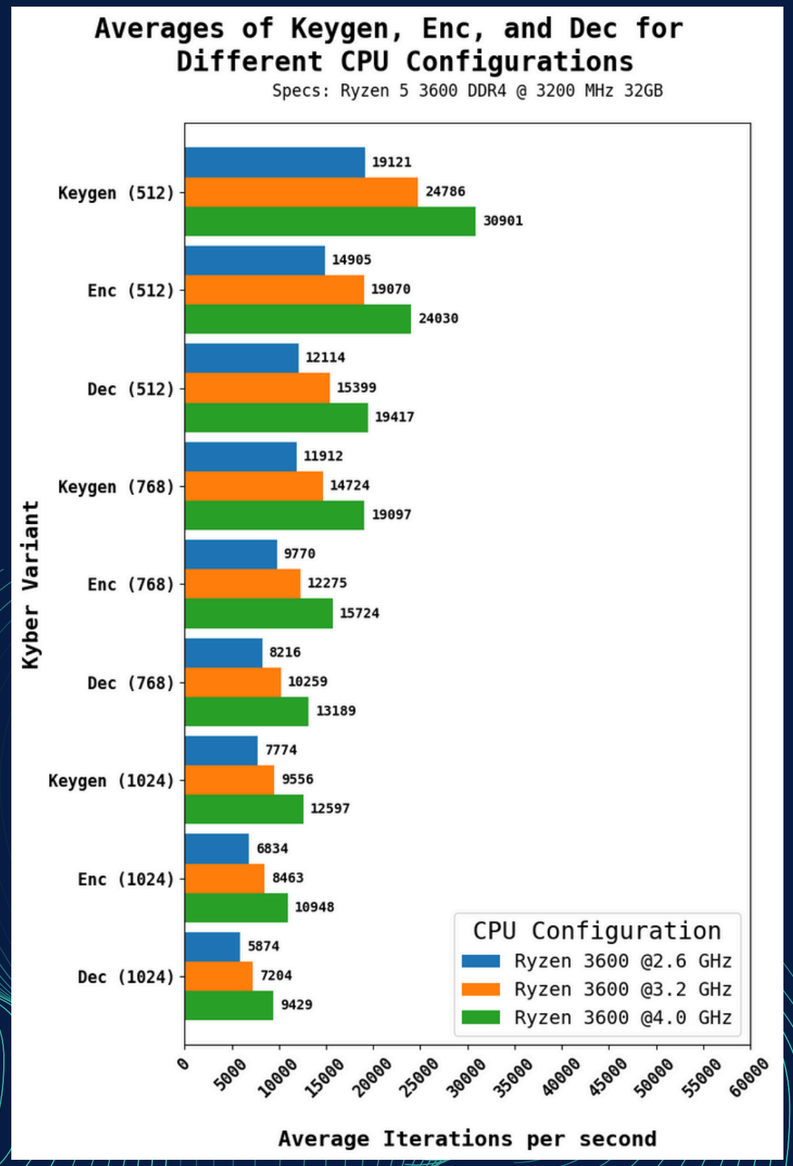
Fastest Machine:

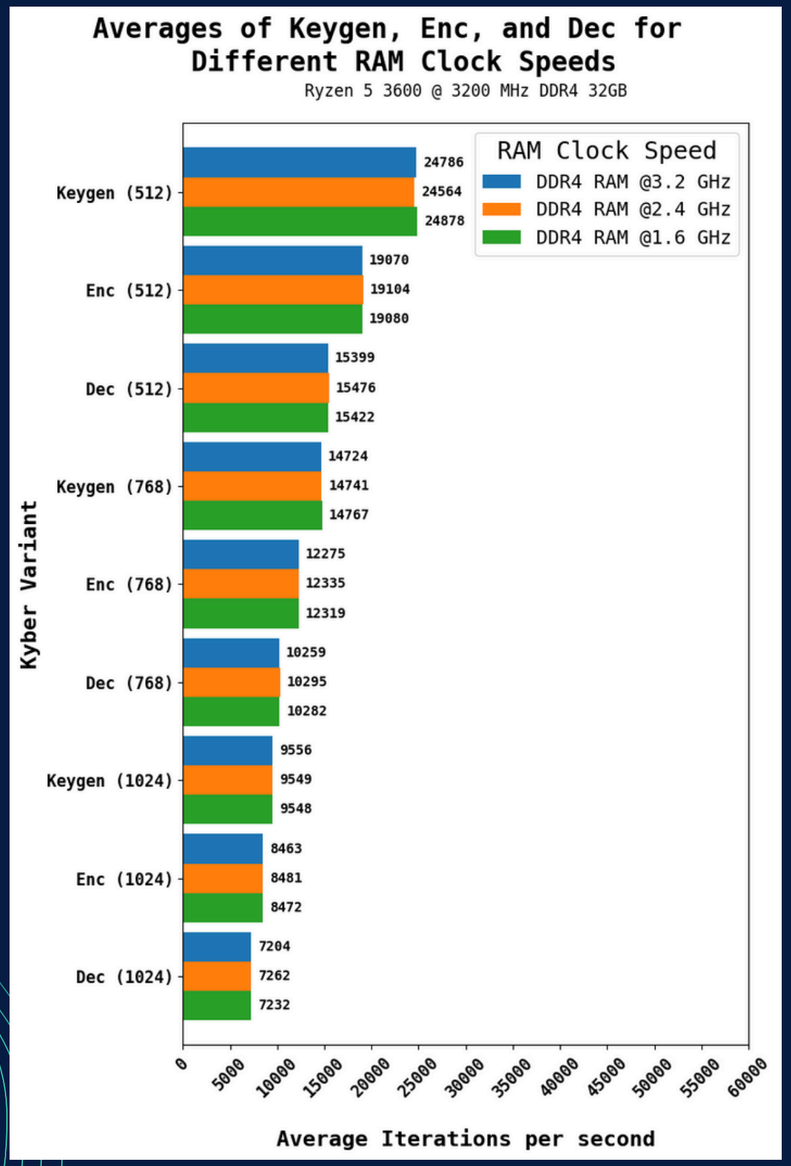
M1 Macbook Pro

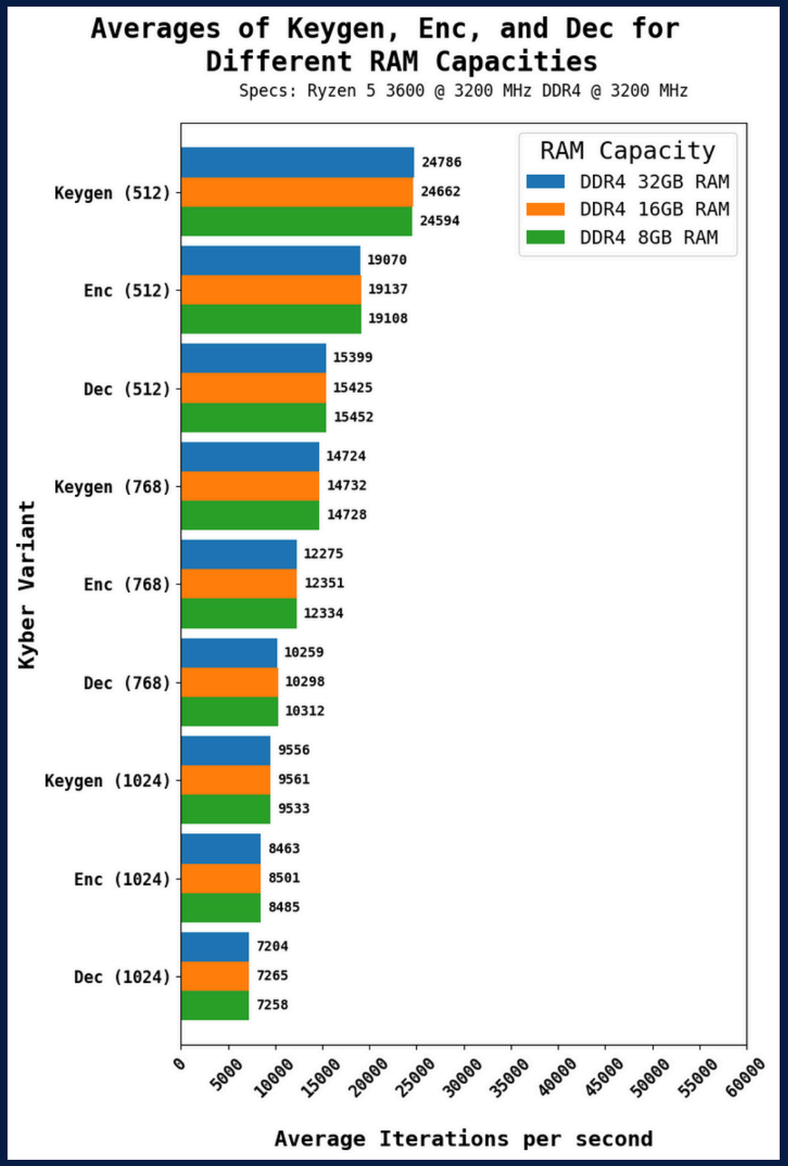




Different Configuration of the Ryzen 3600 Desktop



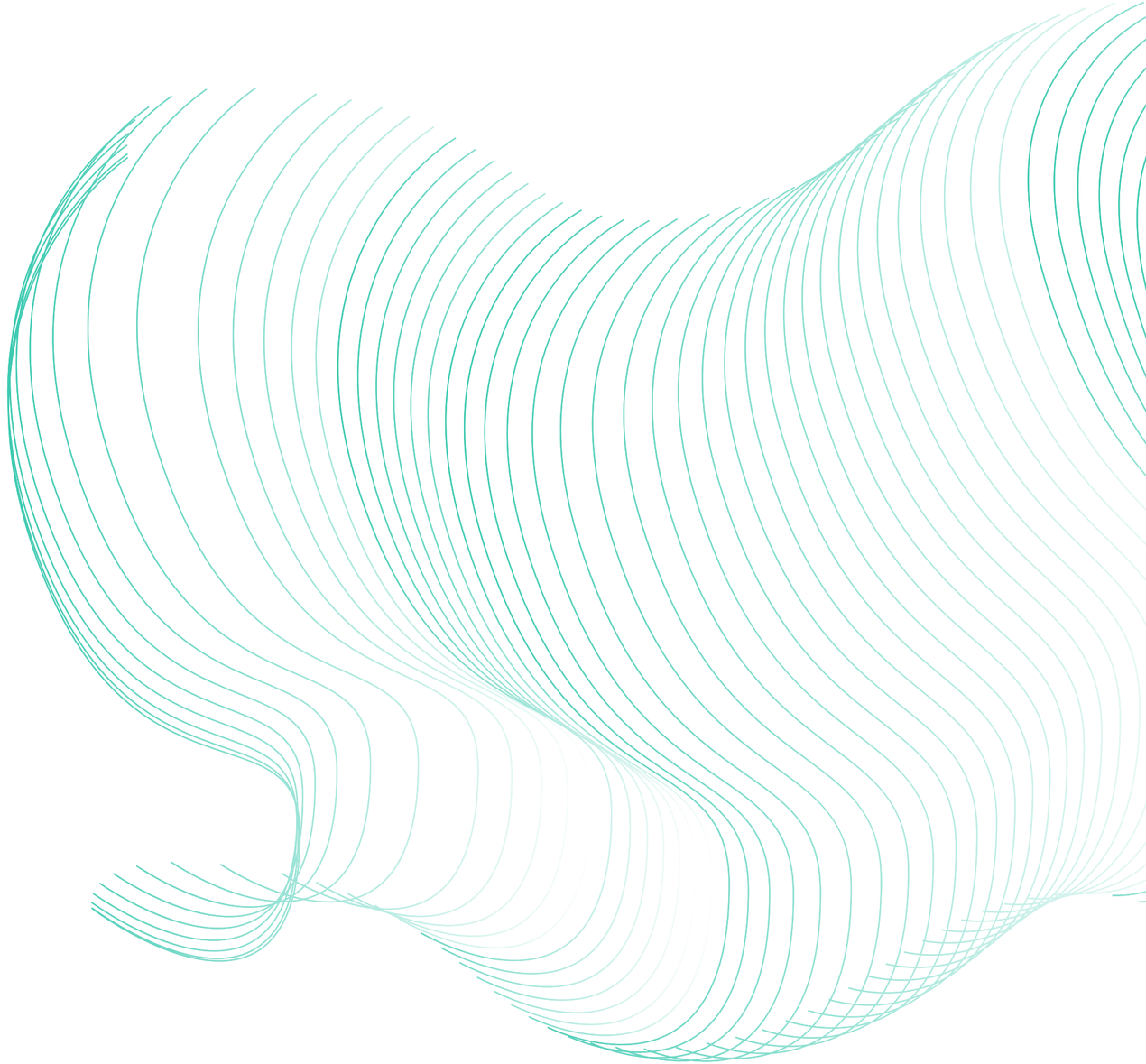




Conclusion

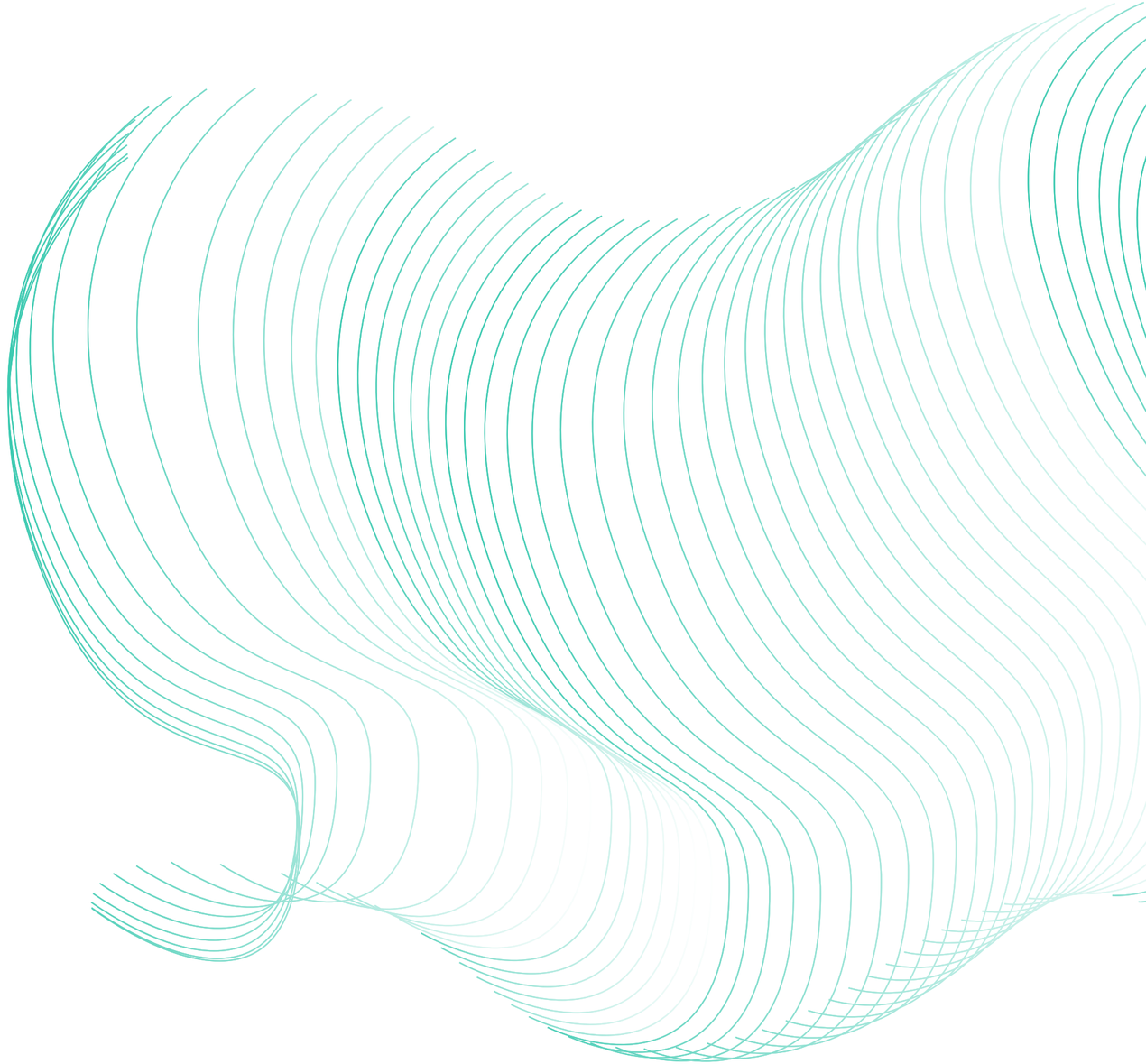
- how the type of operation, Kyber variant, programming language, and hardware architecture **influence** the performance of the Kyber algorithm.

- CPU architecture and CPU clock rate can also significantly impact runtime.



Scope & Delimitation

- Tested on:
  - 4 machines (HPC, PC, Laptop, Macbook M1)
  - 3 OS (Linux, MacOS, Windows (WSL))
  - 2 implementations (Original in C, and Python)



Recommendations

- extend tests (different devices and implementations)
- use of parallelization
- comparison of other KEM algorithms
- standardize tests (dependency versions)
- test the security and efficacy of the algorithm

Thank you!

CS 199 Group Q

Bugaoisan, Denver Earl Paul S.
Serrano, Nuan Patricia S.

References:

D. Liu, Next Generation SSH2 Implementation: Securing Data in Motion, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/B9781597492836000039

O. G. Abood and S. K. Guirguis, “A survey on cryptography algorithms,” International Journal of Scientific and Research Publications, 2018.

A. Gupta and N. Walia, “Cryptography algorithms: A review,” International Journal of Engineering Development and Research, 2014.

N. Singh, Cracking Quantum Computing Interview: A Comprehensive Guide to Quantum Computing Interview Preparation. self-published, 2023.

J. Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017.

R. Grimes, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today’s Crypto. John Wiley Sons, Inc., 2020.

National Institute for Science and Technology. Nist announces first four quantum-resistant cryptographic algorithms. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
Cryptographic Suite for Algebraic Lattices (CRYSTALS). Kyber: Introduction. [Online]. Available: https://pq-crystals.org/kyber/index.shtml

R. Avanzi et al., “Kyber,” https://github.com/pq-crystals/kyber, 2021.

G. Pope, “Crystals-kyber python implementation,” https://github.com/GiacomoPope/kyber-py, 2023. 12