

Project Ragnarok: Post-Quantum Cybersecurity with Lightning data

Joanna Zhang, Gianni Bubb, Aidan Nelappana

Faculty Advisor(s): Dr. Siddhartha Bhattacharyya, Dept. of Computer Engineering & Sciences,
Florida Institute of Technology

Motivation

Cryptography needs to constantly evolve to keep data secure. We believe this idea can be extended into the post-quantum age where many of our current cryptosystems are vulnerable to such attacks. Random numbers with low predictability are vital to cryptography as well. The predictability of pseudo-random number generators can be used maliciously attackers.

Other Applications for Data

Random numbers are used in other fields such as game theory, computer simulations, statistical samples, and password generation.

Abstract

Project Ragnarok aims to remedy the pitfalls of current pseudo-random number generation with mathematically proven truly random numbers from natural phenomena such as lightning while meeting NIST standards. This data is used to achieve less predictable randomness. Users can use theoretically proved quantum-resistant encryption and key generation through the website. As well as have access to random numbers through an API. The secured database will be continuously updated with new data to avoid reuse.

Tools Used

- ❖ Server Backend: Rust
- ❖ API: Python FastAPI
- ❖ Database: PostgreSQL
- ❖ Collaboration: Google Suite, GitHub, Discord, Trello
- ❖ Algorithms: Previous encryption schemes developed, and post-quantum encryption algorithms approved by NIST.

Acknowledgements

Dr. Amitabh Nag for providing the lightning data

