Project Calliope: Quantum Resistant Encryption Using Asymmetric Numeral Systems

Westemeier, Huxley (School: Saint Paul Academy and Summit School)

Within the next twenty years, modern data encryption methods will become susceptible to quantum attacks due to their limited keyspace and reliance on mathematical factoring-based methods. Project Calliope offers powerful encryption using a probabilistic asymmetric-numeral-system-based approach that simultaneously provides lossless compression. This algorithm encodes using variable-length entropy encoding to create a repetition and pattern-free output revealing no information about the key or original file's nature. Changing any byte in the original key file will result in a unique key, and the keyspace makes it computationally infeasible to break the encryption by brute force. If a theoretical quantum or supercomputer could check a googol of possible key files every second, it would take 10^2,408,239,893 years to brute force a 1GB key file compared to the 10^-23 seconds required to crack the current encryption standard AES. Using Calliope, over ten thousand text files were encrypted in 90 minutes with less than 1GB of memory usage and an average compression ratio of 1.78. This research highlights a promising solution for a low-memory encryptor that is exponentially more secure than existing methods while also providing lightweight compression.

Awards Won: