Big Data and Post-Quantum Cryptography

A Performance Benchmark of NIST-Selected Communication Standards with Large Payloads

Arnab Ghosh

Cryptography

- Designing and attacking **secret codes**
- Creating secure channels of communication
- Computerized cryptography is primarily based in **mathematics**
- Modern ciphers use **hard math problems** to guarantee security

Hard Math Problems

- **Nearly impossible** to solve without brute forcing…
- **UNLESS** you have the key!
- Give the key to your partner, and exchange your messages freely

Hard Math Problems

- **Pioneered** by RSA – utilizes the **prime number factorization** problem (Schneier)
- Prime number factorization: how to factor **very large numbers?** (Schneier)
- Nigh unto impossible without brute force; but **easy with a given factor** (Schneier)
- Considered **intractable** – theoretically impossible without brute forcing (Schneier)

Hard Math Problems

- **Elliptic Curve Cryptography** - a new mathematical problem (Dhillon and Kalra)
- Based on the **discrete logarithm problem:**

$$\log_g(h) = x \iff \exists x \in \mathbb{Z} \mid g^x = h$$

Models of Computation

Classical

- **The standard** – nearly all computers in the world
- **Bits** (0s and 1s) to store data
- Makes calculations **individually**
  - (in a theoretical manner)
- **Precise and thorough**

Quantum

- **New** – very few concrete use cases for quantum computing
- **Qubits** – a superposition between 0 and 1
- May do **many calculations at once**
  - (in a theoretical manner)
- **Imprecise and Noisy**

Shor’s Algorithm

- There is currently a **single** concrete use case for quantum computers
- **Shor’s Algorithm** – can solve **BOTH** the prime factorization problem and discrete logarithm problem (Shor)
- Reduce intractable problems to the **order finding problem**; then, solve with order-finding problem (Shor)
- **Greatest threat to modern computing, ever**

Regev’s Algorithm

- Theoretical improvement over Shor’s algorithm (Regev)
- Convert Shor’s algorithm from a 2^{nd}-degree polynomial -> 3/2-degree polynomial time (Regev)
- Published in August 2023
- Severely increases threat posed by quantum computers

Lit Review

- NIST recently standardized three protocols for post-quantum cryptographic communication ("Module-Lattice-Based Key Encapsulation Mechanism Standard")
- One of these, FIPS 203, defines a KEM using Kyber; therefore, we wish to test it ("Digital Signature Standard")
- Kyber works on ARM very well – advantageous in SoC and IoT workloads (Liu and Seo)
- Kyber is **very fast on small computers, with small payloads** - but not tested on big ones (Seyhan et al.)

Are are the NIST-selected post-quantum cryptographic algorithms feasible with large payloads?

The Method

- Benchmark **two algorithms**: Kyber (Post-quantum) and ECC (state of the art)
- Use **KEM** implementations of both algorithms. A KEM is a set of three algorithms…
  - Key generation
  - Encryption
  - Decryption
  - (“Module-Lattice-Based Key Encapsulation Mechanism Standard”)
- Test: Memory usage, Processor usage, **and time taken**
- Memory usage, processor usage less important (as seen later)

Why this Method?

- ECC is the **gold standard** of fast, traditional, state-of-the-art cryptography
- Kyber is **outlined by NIST** as the preferred post-quantum cryptographic algorithm
- Error may be introduced by using our **own implementation**
- Use the **standard, official, NIST-specified** Kyber implementation
- Based on 2018 Pennsylvania State University algorithmic analysis study

Why this Method?

- Other studies about post-quantum cryptographic algorithms **also test Kyber using a KEM**
  - (Ristov and Koceski)
  - (Dhillon and Kalra)

- Combination of more classic studies which **study encryption and decryption separately**
  - 2021 Study of Post-Quantum Cryptographic feasibility on small systems

- Kyber implementation from **official Kyber implementation** in C++

- ECC implementation from **CryptoPP (standard library)**

Results

Benchmark	Payload Size (GB)	Time Elapsed (s)
ECIES	0.5	14
ECIES	1	30
ECIES	2	58
ECIES	4	116
ECIES	8	232
ECIES	16	487
Kyber	0.5	42339

- CPU and Memory was consistent, with **no significant change across different parameters.**
- This is likely due to **segmentation**, which is **inherent to Kyber.**
- We segment ECC as well to **maintain consistency**

Results

- Segmentation **minimizes performance impact…** but also **prevents us from taking full advantage**
- This corroborates Kyber's effectiveness in small systems (**due to segmentation**)
- However… this also **compromises ability with large payloads**
- **Not feasible with large payloads**

Conclusions

- Post-quantum cryptography **as specified by NIST** is not feasible with large payloads

- We **do not** take advantage of parallelization
  - Not part of official specification
  - Non-linear and unpredictable increases/decreases to productivity
  - Future research direction
- We **do not** try to desegment the algorithm
  - Not part of official specification
  - Huge ramifications to overall algorithm family

Works Cited

Bibliography

Akleylek, S., & Soysaldı, M. (2022). A new lattice-based authentication scheme for IoT. *Journal of Information Security and Applications*, *64*, 103053. https://doi.org/10.1016/j.jisa.2021.103053

Blanco-Chacón, I. (2019). *Ring Learning with Errors: A Crossroads Between Post-Quantum Cryptography, Machine Learning and Number Theory.*

Dhillon, P. K., & Kalra, S. (2016). Elliptic curve cryptography for real time embedded systems in IoT networks. *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)*, 1–6. https://doi.org/10.1109/WECON.2016.7993462

Ebrahimi, S., Bayat-Sarmadi, S., & Mosanaei-Boorani, H. (2019). Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT. *IEEE Internet of Things Journal*, *6*(3), 5500–5507. https://doi.org/10.1109/JIOT.2019.2903082

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.*, *74*(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145

Guillen, O. M., Pöppelmann, T., Bermudo Mera, J. M., Bongenaar, E. F., Sigl, G., & Sepulveda, J. (2017). Towards post-quantum security for IoT endpoints with NTRU. *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, 698–703. https://doi.org/10.23919/DATE.2017.7927079

Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing Post-quantum Cryptography for Developers. *SN COMPUT. SCI.*, *4*(4), 365. https://doi.org/10.1007/s42979-023-01724-1

Khalid, A., McCarthy, S., O'Neill, M., & Liu, W. (2019). Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 194–199. https://doi.org/10.1109/IWASI.2019.8791343

Lam, K.-Y., Shparlinski, I., Wang, H., & Xing, C. (Eds.). (2001). *Cryptography and Computational Number Theory*. Birkhäuser. https://doi.org/10.1007/978-3-0348-8295-8

Liu, Z., & Seo, H. (2019). IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. *IEEE Transactions on Information Forensics and Security*, *14*(3), 720–729. https://doi.org/10.1109/TIFS.2018.2856123

National Institute of Standards and Technology. (2023). *Digital Signature Standard (DSS)* (Federal Information Processing Standard (FIPS) 186-5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-5

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd edition). Wiley.

Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2022). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. *Cluster Comput*, *25*(3), 1729–1748. https://doi.org/10.1007/s10586-021-03380-7

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Human Comput*. https://doi.org/10.1007/s12652-017-0494-4

Tiwari, H. D., & Kim, J. H. (2018). Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices. *ETRI Journal*, *40*(3), 396–409. https://doi.org/10.4218/etrij.2017-0220

Westerbaan, B., & Stebila, D. (2023). *X25519Kyber768Draft00 hybrid post-quantum key agreement* (Internet Draft draft-tls-westerbaan-xyber768d00-02). Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00-02