
Kyber Drive
The World's First
Pure Post-Quantum
Lattice-based File
& Disk Encryption
by AMERICAN BINARY

Contact Info: Sales@Ambit.inc

Introduction

This white paper describes a proposed software-only solution for using the Kyber-1024 algorithm to encrypt disk and file storage. This is important because the advent of quantum computers poses a significant threat to the security of current encryption methods. As quantum computers become more powerful, they will be able to break many of the encryption methods currently in use, such as RSA and Elliptic Curve Cryptography (ECC).

To mitigate this risk, post-quantum cryptography research is focused on developing new cryptographic algorithms that are secure against both classical and quantum computers. CRYSTALS-Kyber (Cryptographic Suite for Algebraic Lattices), hereafter "Kyber," is a family of public-key encryption schemes selected by the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) challenge for global standardization.[1] Kyber-1024 is a specific variant of the Kyber family with a public key size and ciphertext size of 1568 bits.

Background on Post-Quantum Cryptography

Post-quantum cryptography aims to develop cryptographic algorithms that are secure against both classical and quantum computers. This is a significant challenge, as quantum computers possess the ability to break many of the encryption methods currently in use. To be considered secure against quantum computers, as well as dequantized quantum algorithms run on classical computers, an encryption method must be resistant to attacks from quantum algorithms such as Grover's algorithm[2] and Shor's algorithm.[3] Additionally, there is a concept in Quantum Information Science called "dequantizing". This is where a Quantum Algorithm is reduced back to a deterministic solution which can be computed on a classical binary computer.

On 23 December 2022, Chinese researchers published "Factoring integers with sublinear resources on a superconducting quantum processor."[4] This paper outlines a near-term (by 2025) method to break upper levels of encryption security (RSA 2048) that safeguards global financial systems. They propose a path to factor large integers more efficiently than Shor's algorithm (a quantum algorithm) that will break RSA 2048 in a timely fashion with 372 qubits. In context IBM claims that they will have 1,000 qubits by 2025.[5] What is more, a paper published on January 26, 2023, titled "Digitized-counterdiabatic quantum factorization."[6] This paper deepens the thesis that we may not need a quantum computer to quickly break upper-levels classical encryption security; This is because the algorithms they're using only exhibits a polynomial speedup in theory in this paper.

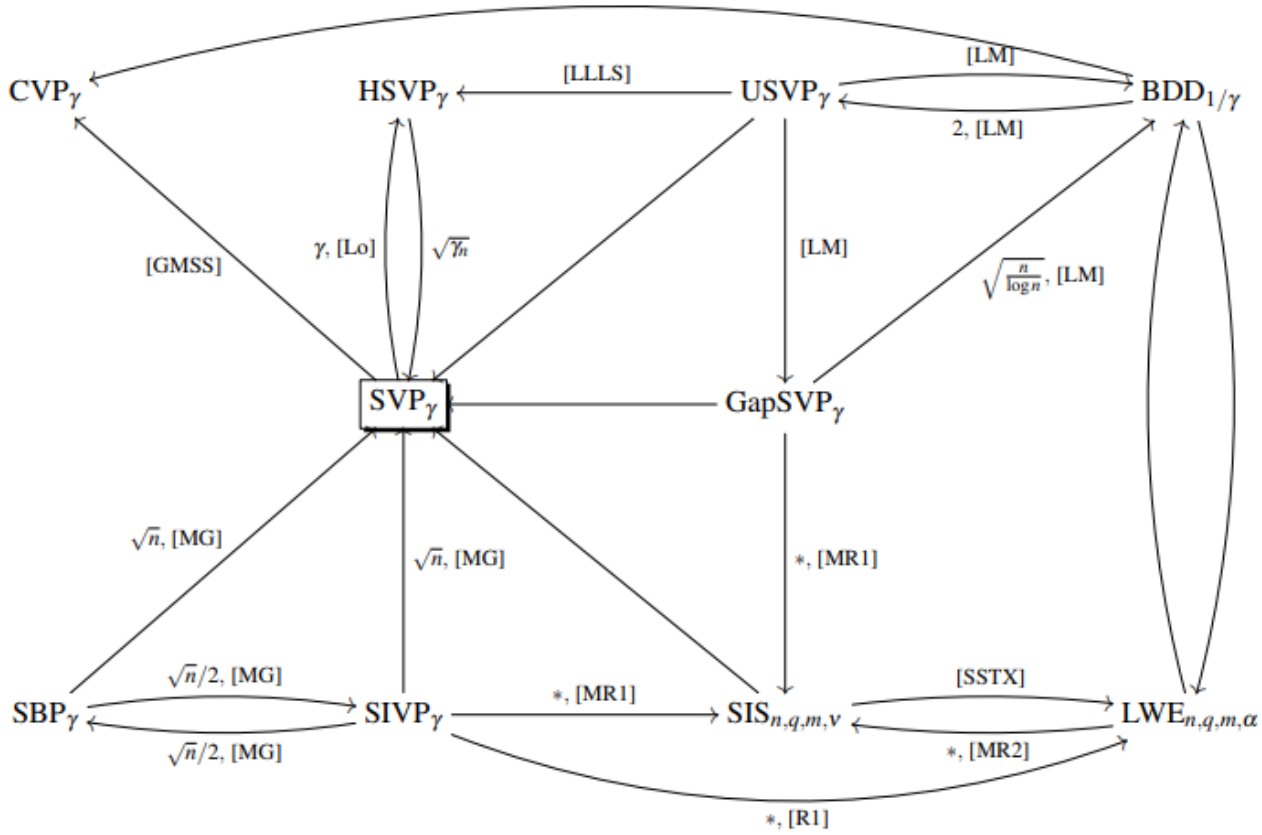
This is all important because RSA 2048 was a backup plan for securing data in the event of near-term advances in computing. There is a larger question, which is out of scope for this paper, to consider. This question is one of geopolitical signaling and their intent when publishing this research in English. It is clear however that the Noisy Intermediate-Scale Quantum (NISQ) era is rushing the need to transition to post-quantum encryption sooner than expected. This highlights the importance of a secure way to secure data at-rest in addition to in-transit.

CRYSTALS-Kyber: A Post-Quantum Encryption Algorithm

The canonical paper which describes Kyber is "CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM."[7]

As a refresher, Kyber is a Key Encapsulation Mechanism (KEM) that is built on the concept of module lattices and is designed to be CCA-secure (indistinguishable against chosen-ciphertext attacks). It is a method for securely generating a shared secret key between two parties, typically used in encryption and authentication protocols. It is based on the Module Learning with Errors (MLWE) problem,[8] a variant of the Learning with Errors (LWE) problem;[9] This variant is believed to be computationally hard for a quantum computer.

LWE is strongly believed to be as computationally hard as GapSVP; GapSVP is NP Hard.
Below is a graph showing the relations among lattice problems.[10] Whether Module Learning with Errors (MLWE) is classically NP Hard is an open question.



Relevant to discussions later are the parameters of Kyber-1024 as seen in table 1 below of "CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM."[11] The number 1024 in Kyber-1024 refers to the lattice dimensions in our MLWE problem. Kyber-1024 is known to have 254 bits of classical security and 230 bits of quantum security (core-SVP hardness). It is a NIST Level 5 security level. This means it is as secure if not more secure than AES 256 classically. Not all modes of AES are post-quantum secure.[12] [13] [14]

Table 1: Parameter sets for KYBER

	n	k	q	η	(d_u, d_v)	δ
KYBER512	256	2	3329	2	(10, 3)	2^{-178}
KYBER768	256	3	3329	2	(10, 4)	2^{-164}
KYBER1024	256	4	3329	2	(11, 5)	2^{-174}

- n is set to 256 because the goal is to encapsulate keys with 256 bits of entropy (i.e., use a plaintext size of 256 bits in KYBER.CPAPKE.Enc). Smaller values of n would require to encode multiple key bits into one polynomial coefficient, which requires lower noise levels and therefore lowers security. Larger values of n would reduce the capability to easily scale security via parameter k.
- We choose q as a small prime satisfying $n \mid (q-1)$; this is required to enable the fast NTT-based multiplication. There are two smaller primes for this property holds, namely 257 and 769. However, for those primes we would not be able to achieve negligible failure probability required for CCA security, so we chose the next largest, i.e., $q = 3329$.
- k is selected to fix the lattice dimension as a multiple of n; changing k is the main mechanism in KYBER to scale security (and as a consequence, efficiency) to different levels.
- The remaining parameters η, d_u and d_v were chosen to balance between security (see Section 4), ciphertext size, and failure probability. Note that all three parameter sets achieve a failure probability of $< 2^{-128}$ with some margin. We discuss this in more detail in Subsections 1.5 and 5.3. Also note that $\eta = 2$ is fixed for all variants, which simplifies implementations.

The failure probability δ is computed with the help of the `Kyber.py` Python script which is available online at https://github.com/pq-crystals/security-estimates. For the theoretical background of that script see [22, Theorem 1].

As we can see, there is a clear and exigent need for a post-quantum secure way to encrypt files and file systems. Enter Kyber Drive.

Proposed Solution: CRYSTALS-Kyber 1024 Encrypted Disk and File Storage

The proposed solution is a software-only program that uses the Kyber-1024 algorithm to encrypt disk and file storage. The program would work by chunking the file into 128-bit blocks and then encrypting each chunk using a single unique public key. The encryption key would be generated using the crystals-kyber1024 algorithm, and then

securely stored on the user's device. There are problems with this approach and will be discussed in the Further Research section.

When a user wants to access an encrypted file or disk, they would decrypt with the private key, which would be used to decrypt the ciphertext. In the Further Research Section, we will discuss introducing a Password Authenticated Key Exchange (PAKE). This would allow a user to enter a password rather than having to directly manage the Kyber-1024 public and private key. The program would also include a key management feature, which would allow users to change their encryption key or password. This feature would ensure that even if a user's encryption key or password is compromised, the encrypted data would still be secure.

Implementation

The program would be implemented entirely in software. The software would handle the encryption and decryption of files and disks, as well as the key management feature. The software would be designed to be user-friendly and easy to use. It would include a simple graphical user interface that would guide the user through the process of encrypting and decrypting files and disks. The key management feature would also be easy to use and would include options for changing the encryption key or password, as well as for revoking access to specific encryption keys.

Performance and Security

The Kyber-1024 algorithm has been shown to have excellent performance characteristics for a post-quantum file and disk encryption solution. The algorithm has a relatively small key size, which makes it more efficient than other post-quantum encryption methods. It also has a very small number of parameters, which makes it easy to verify. Additionally, Kyber-1024 has been shown to be secure against any large-scale fully error corrected quantum computers, also known as Cryptographically Relevant Quantum Computers (CRQC)[15] using Grover's algorithm or Shor’s algorithm.

The proposed software solution for Kyber-1024 encrypted disk and file storage would also be designed with Side Channel Attack (SCA), Fault Injection, and other electromagnetic attack vectors. The key management feature would also be designed to include options for revoking access to specific encryption keys. There is one current challenge and that is, when you chunk a file by 128 bits and encrypt each chunk with a 1536-byte key, you end up with a chunk that has been increased by 65x. In other words, 360KB file will increase to 17.8MB. There are potential solutions to this problem.

Further Research

There is much additional work that is needed to make Kyber Drive widely useful. Presently, there is a 65x overhead from encrypting each 256-bit block. One constraint that we have is that we cannot deviate from the likely standardized path of Kyber. In other words, there is no modifying of Kyber allowed if we are to have a widely

useful and accepted solution. Therefore, we are limited to Pre and Post Processing techniques. Furthermore, these techniques cannot impinge on the Security proofs of Kyber nor any of the primitives that make up Kyber. If we investigate specifically where the bloat is occurring, we find ourselves in the Number Theoretic Transform (NTT) domain.[16]

One point to make is that compression algorithms do not help us here. If we attempt to use Zstandard, brotli, or any other modern state-of-the-art compression, we find that the data has very little duplication already and therefore there is no size improvement by using these methods. American Binary is investigating viable paths for reducing the number of bits each chunk requires. Indeed, American Binary has some early success on this front which can be discussed in a future paper. With regards to introducing a Password Authenticated Key Exchange (PAKE), there is much literature on the topic.[17] [18]

Conclusion

The advent of quantum computers poses a significant threat to the security of current encryption methods. Post-quantum cryptography research is focused on developing new cryptographic algorithms that are secure against both classical and quantum computers. Kyber is secure against any large-scale fully error corrected quantum computers, also known as Cryptographically Relevant Quantum Computers (CRQC) using Grover's algorithm or Shor’s algorithm.

This white paper describes a proposed software-only solution for using the Kyber-1024 algorithm to encrypt disk and file storage. This solution would allow users to encrypt their entire disk or individual files using a unique encryption key that is generated using the Kyber-1024 algorithm. This software would include a user-friendly graphical interface, key management feature and a feature for securely sharing encrypted files with other users. The program offers a user-friendly graphical interface, key management feature and a feature for securely sharing encrypted files with other users. Additionally, this solution is designed with security in mind, using industry standard cryptographic libraries and protocols for the encryption and decryption process and being resistant to common attacks.

For future research we may want to explore the integration of this software with cloud storage services, as well as investigate the possibility of implementing the Kyber-1024 algorithm in hardware devices such as external hard drives or USB drives. Additionally, further research into the performance and security of the Kyber-1024 algorithm would be beneficial to understanding its capabilities and limitations.

In conclusion, American Binary’s Kyber Drive post-quantum encrypted disk and file storage software will secure data storage in the face of quantum computing threats. It offers an easy to use, secure and efficient way for users to ensure future quantum computers cannot break the encryption and steal their private data. American Binary aims for Kyber Drive to serve as a single global software post-quantum encryption standard for all Disk Encryption and File Storage once the overhead is reduced.

References:

[1] NIST Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/post-quantum-cryptogrphy/post-quantum-cryptography-standardization

[2] Gover's algorithm. https://arxiv.org/abs/quant-ph/9605043

[3] Shor's algorithm https://arxiv.org/abs/quant-ph/9508027

[4] Factoring integers with sublinear resources on a superconducting quantum processor. https://arxiv.org/abs/2212.12372

[5] The IBM Quantum Development Roadmap. https://www.ibm.com/quantum/roadmap/IBM%20Quantum%20Roadmap%202022.zip

[6] Digitized-counterdiabatic quantum factorization. https://arxiv.org/abs/2301.11005

[7] CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM, https://ieeexplore.ieee.org/document/8406610

[8] Short Stickelberger Class Relations and application to Ideal-SVP, https://eprint.iacr.org/2016/885

[9] CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM, https://ieeexplore.ieee.org/document/8406610

[10] Short Stickelberger Class Relations and application to Ideal-SVP, https://eprint.iacr.org/2016/885

[11] CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM, https://ieeexplore.ieee.org/document/8406610

[12] Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation, https://eprint.iacr.org/2016/197.pdf

[13] Quantum Analysis of AES Lowering Limit of Quantum Attack Complexity. https://eprint.iacr.org/2022/683.pdf

[14] Quantum Security Analysis of AES, https://eprint.iacr.org/2019/272.pdf

[15] National Security Agency, Quantum Computing and Post-Quantum Cryptography; Question 2: What is a "Cryptographically Relevant Quantum Computer" (CRQC)? https://meda.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[16] Number Theoretic Transforms, https://link.springer.com/chapter/10.1007/978-3-642-81897-4_8

[17] Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions , eprint.iacr.org/2020/1043.pdf

[18] PAKEs: New Framework, New Techniques and More Efficient Lattice-Based Constructions in the Standard Model, 10.1007/978-3-030-45374-9_14, https://www.iacr.org/cryptodb/data/paper.php?pubkey=30294