FrodoKEM

MOHMMAD QASIM HUSSAINI, LUCA VOLONTERIO, DANDY FABIAN, and DIEGO GUZMAN, Université Bretagne Sud, France

ACM Reference Format:
Mohmmad Qasim Hussaini, Luca Volonterio, Dandy Fabian, and Diego Guzman. 2025. FrodoKEM. 1, 1 (September 2025), 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

This report aims to explain what FrodoKEM cryptography is and how it functions. Post-quantum cryptography focuses on developing secure systems to withstand threats posed by quantum computers. Quantum computers, using algorithms like Shor's Algorithm, can easily break widely used cryptographic methods such as RSA and ECC. These traditional methods depend on problems that are hard for classical computers but solvable by quantum ones, making them vulnerable in the future. To protect sensitive information over the long term, experts are creating quantum-resistant algorithms. These include methods based on lattice structures and learning with errors. The goal is to ensure data security and protect confidentiality and integrity, even if quantum computers become capable of breaking today's systems.

Lattice-Based Cryptography

Lattice-based cryptography is an important approach in post-quantum cryptography. It relies on the difficulty of solving specific problems within high-dimensional lattice structures. Lattices are geometric grids of points in multidimensional space, and their complexity makes them useful for cryptographic systems. A key problem in this field is Learning With Errors (LWE), which is the basis for the security of many lattice-based systems. LWE is considered difficult for both classical and quantum computers, making it one of the strongest candidates for post-quantum cryptography. By focusing on unstructured lattices, FrodoKEM avoids some risks linked to structured ones, offering stronger protection against specialized attacks.

Learning With Errors (LWE)

The LWE problem involves solving equations with added noise, making it computationally difficult. This noise creates randomness, making it hard to reverse-engineer the original secret.

Key Features of LWE:

- Worst-case to average-case hardness: Breaking LWE is as hard as solving the most difficult lattice problems, which provide strong security.
- Unstructured lattices: LWE avoids structures that attackers could exploit, and this makes it resistance to attacks.
- Noise addition: Random noise makes the problem extremely challenging, even for quantum computers.

Authors' Contact Information: Mohmmad Qasim Hussaini, hussaini.e2405625@etud.univ-ubs.fr; Luca Volonterio, volonterio.e2405617@etud.univ-ubs.fr; Dandy Fabian, fabian.e2405622@etud.univ-ubs.fr; Diego Guzman, Guzman.e2405614@etud.univ-ubs.fr, Université Bretagne Sud, Lorient, France.

Manuscript submitted to ACM

In FrodoKEM, LWE is the foundation of its public-key cryptosystem, FrodoKEM.
FrodoKEM Parameters FrodoKEM aligns with NIST's recommended security levels for post-quantum cryptography, offering equivalence to established symmetric encryption methods:

- FrodoKEM-640: Equal to AES-128 (NIST Level 1).
- FrodoKEM-976: Equal to AES-192 (NIST Level 3).
- FrodoKEM-1344: Equal to AES-256 (NIST Level 5).

Each level has two versions based on the pseudorandom generator (PRG) used to produce the matrix A, a key part of the cryptosystem:

(1) AES-based versions: These use AES-128 for matrix generation, optimized for hardware with AES acceleration.
(2) SHAKE-based versions: These use SHAKE128, offering better performance on general-purpose platforms.

All information and analysis presented in the introduction are derived from [3], ensuring accuracy and alignment with the original content.

2 Algorithm description

2.1 What is FrodoKEM

FrodoKEM is a family of key-encapsulation mechanisms that is designed to be secure against attack from both classic and quantum computers. This algorithm is based on a problem called Learning with Error (LWE) problem. [3].
This mechanism is mainly used for two purposes:

- Public-Private Key encryption PKE): Frodo can be used as standard public-private key that is resistant to attack from quantum computer. This purpose is targeting IND-CPA security evaluation
- Key Exchange (KEM): Frodo also can used as key exchange protocol to generate new shared key. This one is targeting IND-CCA security evaluation.

In this section we are going deep into the key generation, encryption and decryption part of FrodoKEM. By understanding this then we can continue with the evolution to key exchange mechanisms (KEM) using Fuji Akamoto Transform method [2]. For KEM, on the key generation, encapsulation as well as decapsulation there are a little difference compare to FrodoPKE such as the additional key component to enable ciphertext validation for IND-CCA security evaluation and cryptographic hash.
For the algorithm to work, some generic primitives need to be defined. The two most important ones are **Sample** and **Gen**. The former outputs a sample from the distribution domain given a random bit string and a distribution table, and is used to generate an error value according to the desired error distribution via inverse sampling, that is performed in constant time to avoid timing side channel attacks. The latter generates a pseudo random matrix given a random seed, by using either AES128 or SHAKE128 depending on the setup, and is used to deterministically generate a matrix from a seed. The *Encode* and *Decode* methods provide a way to convert bit strings into matrices with values in $\mathbb{Z}_q$ and vice-versa.

2.2 Key Generation

The key generation process allows to generate a key pair starting from two random bit seeds. The first seed is used to generate the random A matrix using the *Gen* method (i.e. left size of equation system in the LWE problem) while the second is used for Secret (correct result part of the system) and error (noise added to the result) matrices using the

Sample algorithm.

$$B = AS + E \pmod{q} \tag{1}$$

The public key consists of the seed to generate A and the matrix B, computed by solving the modular system A with parameters S and adding error E. Given just A and B, it is hard to recover S. The secret key is simply the S matrix.

2.3 Encryption & Decryption

The encryption process consists of transforming a plain text message u into a cyphertext $C = (C1, C2)$ where $C1$ and $C2$ are both matrices, using the recipient's public key $pk = (seed_A, B)$.

Similarly to the key generation, matrices A $E^{'}$ and $S^{'}$ are crafted with the *Sample* and *Gen* functions but this time another error matrix $E^{''}$ is generated, using the same *Sample* method. This new matrix is to be added as en error to V, a second matrix that holds the obfuscated version of the recipient's public key.

$$B^{'} = AS^{'} + E^{'} \pmod{q} \tag{2}$$

$$V = S^{'}B + E^{''} \pmod{q} \tag{3}$$

Finally the cyphertext is computed by providing the obfuscated version of A (like key generation) and the obfuscated version of the public key B concatenated with the encoded message u.

$$(C_1, C_2) = (B^{'}, V + Frodo : Encode(u)) \tag{4}$$

Upon getting C_1 and C_2, the receiver can recover $B^{'}$ using its secret key S, and then subtract that from C_2 to obtain the message u.

$$B^{'} = C_1 S \pmod{q} \tag{5}$$

$$u = C_2 - B^{'} \pmod{q} \tag{6}$$

Please note that during all this process, the strings are encoded and decoded with the previously cited *Encode* and *Decode* methods. While they do not directly remove noise in the traditional sense, these definitions plays a crucial role in mitigating the effects of noise introduced during encryption. It's important to note that the noise tolerance is limited by the parameters of the scheme. If the noise level exceeds a certain threshold, the decoding process may fail to recover the correct message. Therefore, the choice of parameters is critical in ensuring the security and reliability of the system.

2.4 Parameters

As mentioned in the introduction, FrodoKEM has 3 different security level that is FrodoKEM-640, FrodoKEM-974, FrodoKEM-1344. The difference in security level is the product of the critical parameters such as matrix dimension (n), modulus for the arithmetic operation (q), standard deviation of the error distribution (σ) and key & ciphertext size (ℓ). The following table 1 shows the parameter on each security level .

In the end these parameters were chosen to consider how optimize the compilation and how secure we want the encryption will be.

3 Security Justification

The security strength of FrodoKEM is grounded in two fundamental principles. One is its robust resistance to cryptanalytic attacks, grounded in the hardness of the LWE problem. Second is its design based on the security reductions from the worst-case problems. A key feature of FrodoKEM is the careful selection of its parameters, ensuring they fall

Table 1. Parameter Sets and Their Characteristics for FrodoKEM

Parameter Set	Security Level	n	q	σ	ℓ	Key Size (Public/Secret)	Failure Rate
FrodoKEM-640	~128-bit	640	2^{15}	Moderate (2.3)	9,952 B	9,568 B / 19,312 B	$2^{-138.7}$
FrodoKEM-976	~192-bit	976	2^{16}	Moderate (2.3)	15,984 B	15,776 B / 31,568 B	$2^{-199.6}$
FrodoKEM-1344	~256-bit	1344	2^{16}	Low (1.4)	22,016 B	21,840 B / 43,760 B	$2^{-252.5}$

within the scope of these established security reductions, providing a theoretical foundation for its strength against both classical and quantum attacks.

3.1 Cryptanalytic attacks

The primary cryptanalytic attacks considered are primal and dual ones, which target different aspects of the LWE structure. Primal attacks aim to recover the secret key directly by solving systems of equations derived from LWE samples, while dual attacks attempt to distinguish LWE samples from uniform random noise. FrodoKEM's parameter sets are specifically chosen to exceed the computational costs of these attacks, providing confidence that they meet the security levels defined by NIST. The scheme's parameters, including the modulus q, matrix dimension n, and error distribution x, are tailored to align with theoretical bounds, ensuring robustness.

The following table [2] provides an estimation of the computational cost required to perform primal and dual attacks on the LWE problem. These costs are presented for different parameter sets (Frodo-640, Frodo-976, Frodo-1344) and are expressed as the base-2 logarithm.

Table 2. Security Levels for Different Attack Modes on Frodo Schemes

Scheme	Attack Mode	Classical	Quantum	Plausible
Frodo-640	Primal	150.8	137.6	109.6
	Dual	149.6	136.5	108.7
Frodo-976	Primal	216.0	196.7	156.0
	Dual	214.5	195.4	154.9
Frodo-1344	Primal	281.6	256.3	202.6
	Dual	279.8	254.7	201.4

A key aspect of FrodoKEM's approach is its reliance on the core-SVP hardness as a baseline for assessing cryptanalytic difficulty. Core-SVP measures the exponential cost of solving the Shortest Vector Problem (SVP) in a lattice, which is closely linked to LWE. Although core-SVP focuses on first-order costs and omits secondary factors like memory overheads, it provides a conservative estimate of security. This approach ensures that FrodoKEM's parameters remain resilient even against potential advancements in cryptanalytic techniques.

3.2 Security reductions

A security reduction connects the difficulty of breaking FrodoKEM to solving a well-established, hard problem in the lattice theory. Therefore FrodoKEM remains secure as long as the hardest instances of these lattice problems remain computationally intractable.

Most security reductions rely on two important concepts. The first is the Random Oracle Model (ROM), an idealized

function that provides truly random output for every unique input, consequently simulating a perfect cryptographic hash. And the other one is the Indistinguishability (IND), which means that an attacker cannot determine whether two ciphertexts correspond to two distinct plaintexts or to the same plaintext.
Additionally, we can extend these concepts and say that a scheme is considered IND-CCA secure if it provides indistinguishability under the conditions of a chosen-ciphertext attack. And that a scheme is considered IND-CPA-secure if it prevents an attacker from distinguishing ciphertexts, even when they can adaptively choose plaintexts to encrypt.
With these concepts in mind, the following summarize the five security reductions for FrodoKEM, which provide rigorous mathematical guarantees about its security.

(1) FrodoKEM is an IND-CCA-secure KEM against classical attacks in the classical random oracle model, under certain considerations.
(2) FrodoKEM is an IND-CCA-secure KEM against quantum attackers in the Quantum Random Oracle Model (QROM), under different considerations. As stated in [4], the QROM is an extension of the ROM that is adapted for adversaries with quantum capabilities that can exploit the quantum parallelism to query the oracle more efficiently.
(3) FrodoPKE is an IND-CPA-secure public-key encryption scheme under the assumption that the uniform-secret LWE decision problem is hard for the same parameters, for either classical or quantum adversaries.
(4) Changing the distribution of matrix A from a truly uniform distribution to one generated from a public random seed does not affect the security of FrodoKEM or FrodoPKE.
(5) The uniform-secret LWE decision problem is hard under the assumption that the worst-case bounded-distance decoding with discrete Gaussian samples problem (BDDwDGS) is hard for related parameters.

4 Advantages & Limitation

4.1 Ease of implementation

One of the advantages of FrodoKEM is its design simplicity and compactness, which allow for straightforward implementations that run in constant time. The basic operation of FrodoKEM, matrix computation, enables easy scaling to different dimensions n. Additionally, FrodoKEM uses a modulus q that is always less than or equal to 2^{16}. Combining these aspects facilitates the reuse of matrix functions across different security levels (640, 976, and 1344) by adjusting parameters at build time. Moreover, implementing arithmetic modulo q is straightforward because q is always a power of 2, allowing operations to be performed efficiently on modern computer architectures. Furthermore, the dimension values were chosen to be divisible by 16 to optimize vectorization and simplify the integration of AES128 to generate matrix A, taken from [1].

4.2 Compatibility with existing deployments and hybrid schemes

One key aspect to analyze is how FrodoKEM can be integrated into existing cryptographic systems and its impact on already widespread software. While FrodoKEM has larger public key and encapsulation sizes compared to RSA and elliptic curve cryptosystems, these sizes are still small enough to remain compatible with many existing deployments. For example, developers successfully tested FrodoKEM with common software frameworks, such as the TLS 1.2 implementation in OpenSSL, incorporating both hybrid and non-hybrid cipher suites. The modified library was then integrated with the Apache HTTP server, and the results showed no compatibility or performance issues in practical

Internet applications. Further details of these tests are available in [26].
In the short term, deployments are expected to use hybrid schemes combining post-quantum and traditional cryptography. This approach ensures that the improvements in post-quantum algorithms are incorporated with minimal impact on existing deployments, particularly in terms of latency and throughput.

4.3 Hardware implementation

For hardware implementations Ring-LWE schemes are often preferred because they allow for polynomial multiplication. In contrast, LWE-based schemes (like FrodoKEM) use matrix operations. While matrix multiplication is not as specialized as polynomial operations, it is a well-studied problem in hardware design, and efficient implementations for FPGAs already exist. This balances trade-offs between required area, energy consumption, and performance and it is the foundation for feasibility of hardware implementations of FrodoKEM.

5 Conclusion

FrodoKEM is a conservative but practical approach to post-quantum cryptography, which is based on the hardness of the LWE problem. Its design emphasizes simplicity, security, and compatibility with existing infrastructure. FrodoKEM's security is supported by well-established worst-case to average-case reductions and rigorous cryptanalysis, ensuring robustness against both classical and quantum attacks. The implementation settings of FrodoKEM, such as matrix-based operations and the use of power-of-two modulo, simplify its deployment and facilitate efficient, constant-time operations resistant to side-channel attacks. Moreover, its adaptability across various security levels (640, 976, and 1344) and compatibility with hybrid schemes enable FrodoKEM to address both near-term and long-term cryptographic needs. While its key and encapsulation sizes are larger than existing cryptographic standards, they remain manageable within modern frameworks, ensuring its integration for current real-world applications.

References

[1] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. 2016. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE. Cryptology ePrint Archive, Paper 2016/659. https://doi.org/10.1145/2976749.2978425

[2] Eiichiro Fujisaki and Tatsuaki Okamoto. 1999. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings (Lecture Notes in Computer Science, Vol. 1666)*. Springer, 537–554. https://doi.org/10.1007/3-540-48405-1_34

[3] FrodoKEM team 2017–2023. 2023. *FrodoKEM: Practical quantum-secure key encapsulation from generic lattices.* Retrieved November 30, 2024 from https://frodokem.org/

[4] Takashi Yamakawa and Mark Zhandry. 2020. Classical vs Quantum Random Oracles. Cryptology ePrint Archive, Paper 2020/1270. https://eprint.iacr.org/2020/1270