A Grover-like Quantum Algorithm for Minimum Distance Decoding of Linear Block Codes

Gangsan Kim and Jong-shick Oh
Directorate of Combat Development,
Korea Army Training and Doctrine Command,
gs.kim@yonsei.ac.kr

Abstract—**In this paper, we propose a Grover-like quantum algorithm for minimum distance decoding of linear block codes. Our algorithm is motivated by the observation that the amplitude of the solution state is amplified even if the initial state of the Grover operation is not on a Hadamard basis. We experimentally derive some parameters of our algorithm. Based on our experimental results, we expect to perform fewer Grover operations on average than algorithms based on the traditional Durr-Hoyer algorithm.**

I. Introduction

With the introduction of the quantum computer, a new paradigm emerged known as quantum algorithms, poised to supplant the traditional Turing machine-based algorithms. Among those, Shor's algorithm [16] stands out, capable of efficiently solving the discrete logarithmic problem and potentially compromising Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptography(ECC), the cornerstones of prevalent public key cryptography. Concurrently, Grover's algorithm [8], [9] exhibited a quadratic acceleration in the unstructured search problem when contrasted with conventional classical computing methods. Furthermore, a range of quantum algorithms, including quantum approximate optimization algorithm (QAOA) [7] and variational quantum eigensolver (VQE) [15], have surfaced, indicating the capacity of quantum computers to solve numerous problems beyond the reach of classical computers [14].

The pursuit of an minimum distance decoding algorithm for arbitrary linear block codes is a fundamental objective in coding theory [10]. Despite its significance, solving the minimum distance decoding problem for random linear block codes has been proven to be NP-complete [4]. Among Turing machine-based approaches, information-set decoding stands out as the fastest known technique. However, this method faces theoretical limitations when exclusively addressed using classical computers.

Recently, there has been attempts to solve the minimum distance decoding problem using the quantum algorithm. Several researchers conducted research to assist information-set decoding with quantum algorithms. In 2010, Bernstein proposed Grover's algorithm-assisted information-set decoding [2]. In 2017, Kachigar and Tillich proposed an information-set decoding algorithm in which Grover's algorithm and quantum walk are appropriately applied [12].

On the other hand, some researchers tried to solve it only with quantum algorithm. Jung, Kang, and Ha introduced a quantum maximum likelihood decoding algorithm founded on the Durr-Hoyer framework [6], [11]. It's worth noting that minimum distance decoding essentially equates to maximum likelihood decoding within a binary symmetric channel. Their algorithm consists of oracle operations of Grover's algorithm, measurements, and random selections. In 2022, Bhattacharyya and Raina also proposed a minimum distance decoding algorithm with a similar concept. [5].

Nevertheless, both the quantum algorithm and the quantum-assisted algorithm fell short of attaining exponential acceleration for the minimum distance decoding problem. This limitation draws attention to McEliece cryptography [13], which is based on the minimum distance decoding problem, is a candidate for post-quantum cryptography(PQC). Consequently, as we await the emergence of an algorithm capable of achieving exponential speedup or definitive proof of its infeasibility, research geared towards enhancing the speed of the minimum distance decoding remains an inherently captivating pursuit.

In this paper, we propose a Grover-like quantum

979-8-3503-1327-7/23/$31.00 ©2023 IEEE

algorithm for minimum distance decoding of linear block codes. Our proposed algorithm is motivated by the observation that the amplitude of the solution state is amplified even if the initial state of the Grover operation is not on a Hadamard basis.

The remain of this paper is organized as follows. Section II introduces minimum distance decoding of linear block code and Grover's algorithm. Section III explain some observations which give the key motivation and shows our proposed algorithm. Section IV presents some future works and concludes this paper.

II. Preliminaries

A. Minimum Distance Decoding of Linear Block Codes

In this paper, the codes we deal with are only binary linear block codes. Given a $[n, k]$ linear block code $C \subset \mathbb{F}_2^n$ and a received word $\mathbf{y} \in \mathbb{F}_2^n$, the minimum distance decoding is selecting a codeword $\hat{\mathbf{c}} \in C$ to minimise the Hamming distance between $\mathbf{y}$ and $\hat{\mathbf{c}}$. i.e. the decoded codeword $\hat{\mathbf{c}}$ satisfies that

$$d_H(\mathbf{y}, \hat{\mathbf{c}}) \leq d_H(\mathbf{y}, \mathbf{c}) \quad \text{for any } \mathbf{c} \in C,$$

where $d_H(\mathbf{y}, \hat{\mathbf{c}})$ is the Hamming distance between $\mathbf{y}$ and $\hat{\mathbf{c}}$. There uniquely exist a message $\hat{\mathbf{m}} \in \mathbb{F}_2^k$ such that $\hat{\mathbf{c}} = \hat{\mathbf{m}}G$ where G is a generator matrix of C. Without loss of generality, we assume that C is a systematic code. i.e. let

$$\hat{\mathbf{c}} = \{\hat{c}(0), \hat{c}(1), ..., \hat{c}(n-1)\} \quad \text{and}$$

$$\hat{\mathbf{m}} = \{\hat{m}(0), \hat{m}(1), ..., \hat{m}(k-1)\},$$

then $\hat{c}(t) = \hat{m}(t) \quad \text{for} \quad t = 0, 1, ..., k-1.$

B. Grover's algorithm

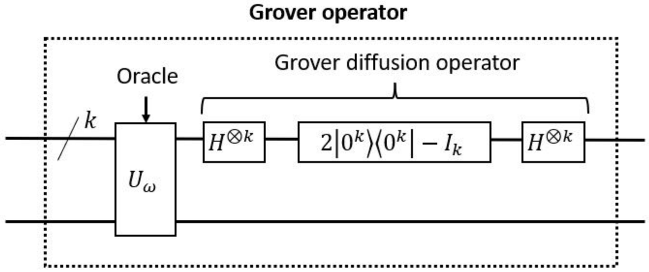

Fig. 1. The Grover operator

Consider a bool function $f : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$. Grover's algorithm is a quantum algorithm that finds one solution of $f(x) = 1$ with high probability. To explain Grover's algorithm, we will first explain the Grover operator.

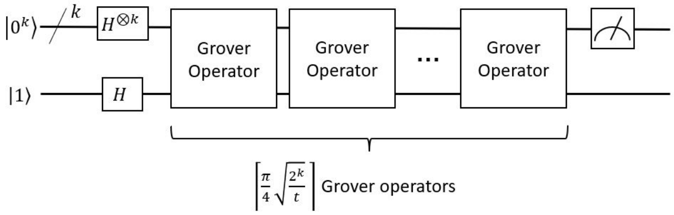

Fig. 2. The Grover's algorithm

The Grover operator is composed of oracle and Grover diffusion operator on the k logical qubits and one ancilla qubit as in Fig. 1. The ancilla qubit is expected to remain in $|-\rangle$ state. Oracle U_ω is defined as

$$U_\omega |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle.$$

The Grover diffusion operator is expressed as the following matrix form

$$H^{\otimes k}\Big\{2\Big|0^k\Big\rangle\Big\langle 0^k\Big| - I_k\Big\}H^{\otimes k} = \frac{1}{2^{k-1}}\times$$

$$\begin{bmatrix} -2^{k-1}+1 & 1 & 1 & \cdots & 1 \\ 1 & -2^{k-1}+1 & 1 & \cdots & 1 \\ 1 & 1 & -2^{k-1}+1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & -2^{k-1}+1 \end{bmatrix}.$$

This operation performs a symmetric inversion of the coefficients of all states to their arithmetic mean.

The Grover operator is defined as serially connecting one oracle and one Grover diffusion operator. When the initial quantum state is $H^{\otimes k}\big|0^k\big\rangle|-\rangle$, the Grover operation amplifies the amplitude of the state corresponding to the solution of $f(x) = 1$, and even if the Grover operation is performed several times, it continues to be amplified up to a certain number of times. The Grover's algorithm performs multiple grover operations on $H^{\otimes k}\big|0^k\big\rangle|-\rangle$ to maximize the amplitude of the state for solutions of $f(x) = 1$ and then, conducts measurement on logical qubits. If it has only t solutions, the number of Grover operations is $\left\lceil \frac{\pi}{4}\sqrt{\frac{2^k}{t}} \right\rceil$ as in Fig. 2.

III. Main Results

A. Key Observations

Before introducing our proposed algorithm, we discuss the key observations that motivated our study. In the previous section, Grover's operation on the initial state $H^{\otimes}\big|0^k\big\rangle|-\rangle$ amplifies amplitude of the state for the solutions of $f(x) = 1$. In facts, Grover operation on the initial state of the other forms can amplify amplitude of the solution state.

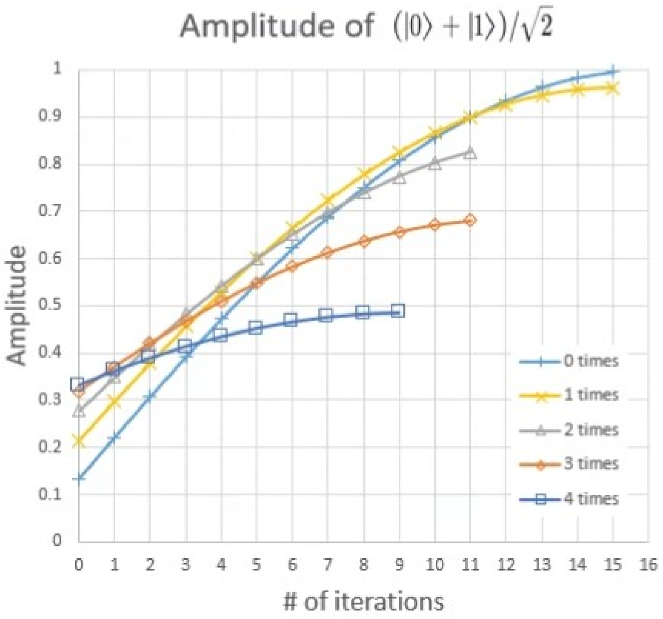

Fig. 3. Amplitude of the solution state of $f(x) = 1$ as the number of Grover operations of f increases after conducting some Grover operations of g

Now, we establish a special initial state not a forms of $H^{\otimes}\big|0^k\big\rangle|-\rangle$. Consider a bool function $f : \mathbb{Z}_{2^k} \to \mathbb{F}_2$, where $\mathbb{Z}_{2^k} = \{0, 1, 2, ..., 2^k - 1\}$. Set our goal to find $\hat{x} \in \mathbb{Z}_{2^k}$ satisfying $f(\hat{x}) = 1$. Consider a function $g : \mathbb{Z}_{2^k} \to \mathbb{F}_2$ satisfying

$$\{x \in \mathbb{Z}_{2^k} \,|\, f(x) = 1\} \subset \{x \in \mathbb{Z}_{2^k} \,|\, g(x) = 1\}.$$

Define an oracle U_{ω_g} of g as

$$U_{\omega_g}|x\rangle|-\rangle = (-1)^{g(x)}|x\rangle|-\rangle.$$

Then, the Grover operator $\mathcal{G}_g$ of g can be expressed as

$$\mathcal{G}_g = H^{\otimes k}\Big\{2\Big|0^k\Big\rangle\Big\langle 0^k\Big| - I_k\Big\}H^{\otimes k}U_{\omega_g}$$

Then, for a given integer M, we establish the initial state $|\psi\rangle$ of grover operator of f as

$$|\psi\rangle = \mathcal{G}_g^M\Big\{H^{\otimes k}\Big|0^k\Big\rangle|-\rangle\Big\}.$$

For a reasonable integer M, not only does $\mathcal{G}_g^M$ already increase the amplitude of the state $|\hat{x}\rangle$ but we also expect that the Grover operator of f will continue to increase the amplitude of $|\hat{x}\rangle$.

Example 1: Let $k = 10$, $f(x) = 1$ only for $x = 0, 1$ and $g(x) = 1$ only for $x = 0, 1, ..., 20$. Consider five initial states $\mathcal{G}_g^M\{H^{\otimes k}|0^k\rangle|-\rangle\}$ for $M = 0, 1, 2, 3, 4$. Note that $\left\lceil \frac{\pi}{4}\sqrt{\frac{1024}{21}} \right\rceil = 6$. Fig. 3 shows, for each initial state, the amplitude of the solution state of $f(x) = 1$ as the number of Grover operations f increases. In all five cases, the amplitude of the solution state tends to increase. However, as M increases, the upper bound on the amplitude becomes lower.

As in Example 1, conducting Grover operator $\mathcal{G}_g$ does not help to find $\hat{x}$. However, we expect that it may be helpful for the case when we don't know exact the number of solutions.

B. Proposed Algorithm

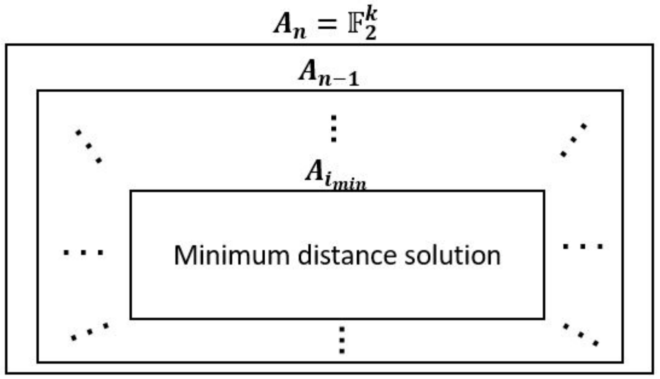

Fig. 4. The Euler diagram of the sets $A_n, A_{n-1}, ...$

Now, we describe the exact statement of the problem we want to solve. For a random systematic $[n, k]$ linear block code $C \subset \mathbb{F}_2^n$ and a random word $\mathbf{y} \in \mathbb{F}_2^n$, our goal is to find $\hat{\mathbf{m}} \in \mathbb{F}_2^k$ satisfying that

$$d_H(\mathbf{y}, \hat{\mathbf{m}}G) \leq d_H(\mathbf{y}, \mathbf{c}) \quad \text{for any } \mathbf{c} \in C,$$

where G is a generator matrix of C. i. e.,

$$\hat{\mathbf{m}} = \underset{\mathbf{m}\in\mathbb{F}_2^k}{\operatorname{argmin}}\, w_H(\mathbf{y} + \mathbf{m}G),$$

where $w_H(\mathbf{y}+\mathbf{m}G)$ is the hamming weight of $\mathbf{y}+\mathbf{m}G$.

For $i = 0, 1, 2, ..., n$, define a bool function $f_i : \mathbb{F}_2^k \to \mathbb{F}_2$ as

$$f_i(\mathbf{m}) = \begin{cases} 1 & \text{if} \quad w_H(\mathbf{y} + \mathbf{m}G) \leq i, \\ 0 & \text{if} \quad w_H(\mathbf{y} + \mathbf{m}G) > i. \end{cases}$$

Let $A_i = \{\mathbf{m} \in \mathbb{F}_2^k \,|\, f_i(\mathbf{m}) = 1\}$ for $i = 0, 1, 2, ..., n$. Observe that $A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_n$ and A_i for some i should be empty set. Let i_{min} be minimum number satisfying $A_{i_{min}} \neq \emptyset$. Then, we can draw Euler diagram of A_n, A_{n-1}, ..., $A_{i_{min}}$ as in Fig. 4. Any element in $A_{i_{min}}$ can be $\hat{\mathbf{m}}$. If we know i_{min}, the problem can be solved by conducting Grover's algorithm of $f_{i_{min}}$.

However, we don't know the exact value of i_{min} since C is a random linear code. Our strategy is to run some

Grover operations of f_n, some Grover operations of f_{n-1}, ..., some Grover operations of f_1, and some Grover operations of f_0, in that order. By key observations in the previous subsection, we expect that the amplitude of $|\hat{\mathbf{m}}\rangle$ keep to increase.

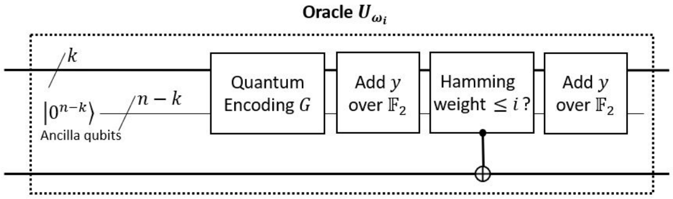

Fig. 5. The oracle U_{ω_i} of the function f_i

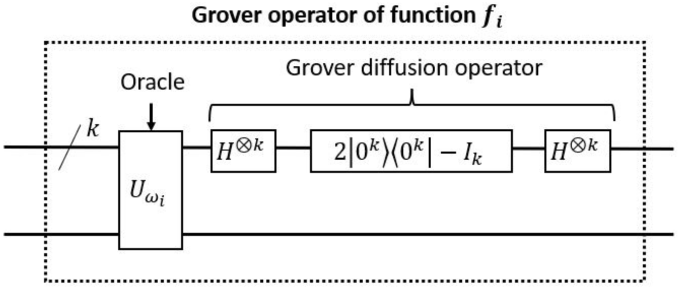
Grover operator of function f_i
Oracle
Grover diffusion operator
k
U_{ω_i}
$H^{\otimes k}$
$2|0^k\rangle\langle 0^k| - I_k$
$H^{\otimes k}$

Fig. 6. The Grover operator of the function f_i

Let U_{ω_i} be the oracle of f_i for $i = 0, 1, ..., n$. First, we have to check that the oracle of f_i can be designed from the quantum circuit. Fig. 5. shows a quantum circuit of the oracle of f_i. Addition over $\mathbb{F}_2$ and checking whether Hamming weight is smaller than or equal to i is obviously easy to construct. Quantum encoding circuit can be constructed by at most $k(n-k)$ CNOT gates (described in [11], Section IV). Then, we can construct the grover operator of the function f_i as in Fig. 6.

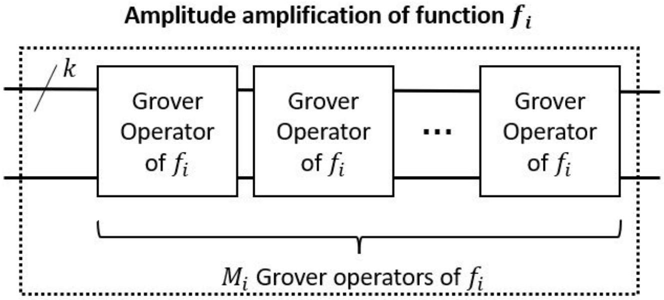

Fig. 7. The amplitude amplification of the function f_i

Let $\mathcal{G}_i$ be the Grover operator of the function f_i. For a given integer M_i, define the amplitude amplification of the function f_i as conducting $\mathcal{G}_i$ M_i times as in Fig. 7. We expect that this operation amplifies the coefficient of the state of A_i.

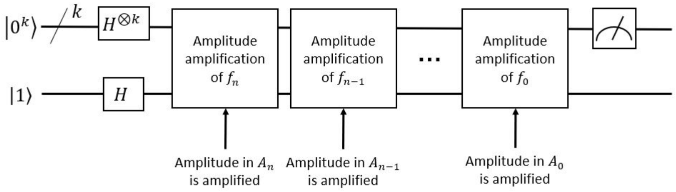
$|0^k\rangle$
k
$H^{\otimes k}$
$|1\rangle$
H
Amplitude amplification of f_n
Amplitude amplification of f_{n-1}
···
Amplitude amplification of f_0
Amplitude in A_n is amplified
Amplitude in A_{n-1} is amplified
Amplitude in A_0 is amplified

Fig. 8. The proposed algorithm

Finally, we propose an algorithm as in Fig. 8. On the initial state $H^{\otimes k}|0^k\rangle|-\rangle$, run an amplitude amplification of the function f_n, an amplitude amplification of the function f_{n-1}, ..., and an amplitude amplification of the function f_0, in that order. And then, conduct measurement on the logical qubits.

Now, our task is to determine M_i for $i = 0, 1, ..., n$ such that the measured state is a minimum distance solution with high probability. In fact, we have not theoretically analyzed what numbers are appropriate as values for $M_0, M_1, M_2, ..., M_n$.

However, we have experimentally found a way to determine the values of $M_0, M_1, M_2, ..., M_n$ that finds the minimum distance solution with reasonable probability. Roughly speaking, we set the total number M_{total} of Grover operations to be approximately

$$0.7 \times \frac{\pi}{4}\sqrt{2^k},$$

where $M_i/M_{total} \approx P(i_{min} = i)$ and $P(i_{min} = i)$ is the probability of $i_{min} = i$ for $i = 0, 1, ..., n$.

The exact way is: Let $M_{total} = \left\lceil 0.7 \times \frac{\pi}{4}\sqrt{2^k} \right\rceil$. Set $M_0 = 0$ and $M_{i+1} = \lfloor M_{total} P(i_{min} \leq i+1) \rfloor - \sum_{j=0}^{i} M_j$ for $i = 0, 1, ..., n-1$, where

$$P(i_{min} \leq i) =$$

$$\frac{1}{|\mathbb{F}_2^n \times \mathbb{F}_2^k||\mathbb{F}_2^n|} \sum_{G \in \mathbb{F}_2^n \times \mathbb{F}_2^k, \mathbf{y} \in \mathbb{F}_2^n} \delta(A_i \neq \emptyset), \quad \text{and}$$

$$\delta(A_i \neq \emptyset) = \begin{cases} 0 & \text{if} \quad A_i = \emptyset, \\ 1 & \text{if} \quad A_i \neq \emptyset. \end{cases}$$

We applied this method to perform Monte Carlo simulations to investigate the average measurement success probability for $n = 50, 100, 150$ and $k = 10, 15$. In each case, we ran 1,000,000 simulations. Table I shows the simulation results.

TABLE I
Simulation Results of the Proposed Algorithm

n	k	average success probability
50	10	0.376
100	10	0.384
150	10	0.389
50	15	0.407
100	15	0.371
150	15	0.358

Roughly speaking, the average success probability is about 0.38. Therefore, for taking the right answer, the expected number M_{total} of Grover operations is about

$$\frac{1}{0.38} \times 0.7 \times \frac{\pi}{4}\sqrt{2^k} \approx 1.45\sqrt{2^k}.$$

The algorithms in [5], [11], which are based on the Durr-Hoyer algorithm, should conduct $4.5\ \sqrt{2^k} \sim 22.5\ \sqrt{2^k}$ times of Grover operations. Therefore, the proposed algorithm is slightly faster than the existing algorithm in terms of the expected value of the number of Grover operations.

IV. Concluding Remarks

In this paper, we propose a Grover-like quantum algorithm for minimum distance decoding of linear block codes. Our algorithm is motivated by the observation that the amplitude of the solution state is amplified even if the initial state of the Grover operation is not on a Hadamard basis. We experimentally decide the values of the parameters $M_0, M_1, ..., M_n$ of our algorithm. Based on our experimental results, we expect to conduct $1.45\sqrt{2^k}$ Grover operations on average while the algorithms in [5], [11] based on the traditional Durr-Hoyer algorithm should conduct $4.5\ \sqrt{2^k} \sim 22.5\ \sqrt{2^k}$ Grover operations. However, we have not shown that it is theoretically a faster algorithm for all n, k. In the future, we would like to build a sophisticated theoretical foundation for our algorithm and derive the optimal values of $(M_0, M_1, ..., M_n)$.

References

[1] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing" *SIAM journal on Computing*, 26(5), pp. 1524–1540, 1997.

[2] D. J. Bernstein, "Grover vs. McEliece," In *Proceeding of Post-Quantum Cryptography: 3rd International Workshop, PQCrypto 2010*, pp. 73–80, 2010.

[3] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemporary Mathematics*, 305, pp. 53–74, 2002.

[4] E. R. Berlekamp, R. J. McEliece, and H. C. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, 24(3), pp. 384–386, 1978.

[5] M. Bhattacharyya and A. Raina "A quantum algorithm for syndrome decoding of classical error-correcting linear block codes," In *Proceeding of 2022 IEEE/ACM 7th Symposium on Edge Computing (SEC)*, pp. 456–461, 2022.

[6] C. Durr and P. Hoyer, "A quantum algorithm for finding the minimum," *arXiv preprint quant-ph/9607014*, 1996.

[7] E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," *arXiv preprint arXiv:1411.4028.*, 2014.

[8] L.K. Grover, "A fast quantum mechanical algorithm for database search," In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219, 1996.

[9] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical Review Letters*, 79(2), pp. 325–328, 1997.

[10] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge university press, 2010.

[11] H. Jung, J. Kang, and J. Ha, "Quantum maximum likelihood decoding for linear block codes," In *Proceeding of 2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 227–232, 2020.

[12] G. Kachigar and J. P. Tillich, "Quantum information set decoding algorithms" In *proceeding of International Workshop on Post-Quantum Cryptography*, pp. 69–89, 2017.

[13] R. J. McEliece, "A public-key cryptosystem based on algebraic," *DSN Progress Report*, 44, pp. 114–116, 1978.

[14] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge university press, 2010.

[15] A. Peruzzo, J. McClean, P. Shadbolt, M-H. Yung, X-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," *Nature communications*, 5(1), 4213. 2014.

[16] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer" *SIAM review*, 41(2), 303–332, 1999.

[17] J. Stern, "A method for finding codewords of small weight," In *Proceeding of Coding Theory and Applications: 3rd International Colloquium Toulon*, pp. 106–113, 1989.