



**HAL**  
open science

# Quantum Minimum Searching Algorithms for Active User Detection in Wireless IoT Networks

Muhammad Idham Habibie, Claire Goursaud, Jihad Hamie

► **To cite this version:**

Muhammad Idham Habibie, Claire Goursaud, Jihad Hamie. Quantum Minimum Searching Algorithms for Active User Detection in Wireless IoT Networks. *IEEE Internet of Things Journal*, 2024, 11 (12), pp.22603-22615. 10.1109/JIOT.2024.3382337 . hal-04818586

**HAL Id: hal-04818586**

**<https://hal.science/hal-04818586v1>**

Submitted on 4 Dec 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Quantum Minimum Searching Algorithms for Active User Detection in Wireless IoT Networks

Muhammad Idham Habibie, *Student Member, IEEE*, Claire Goursaud, *Member, IEEE*, Jihad Hamie, *Member, IEEE*

**Abstract**—The key features of 5G, such as ultra-reliable low latency (URLLC) and massive machine-type communication (mMTC), are designed to address the need for low latency and the ability to connect a large number of devices in the IoT context. To support these constraints, mobile devices transmit information without previously establishing a connection with the base station (BS). This requires the Base Station to detect in real-time the active users (process known as Active User Detection (AUD)). With classical processors, one can employ the Maximum Likelihood (ML) method (the optimal detector, but suffers from high complexity and delay), or suboptimal ones (which are simpler, but less reliable). Meanwhile, quantum algorithms, particularly Durr and Høyer (DHA) algorithm, addressing minimum searching problems, can significantly reduce complexity while keeping good performances. However, these algorithms were designed for generic problems, and their initialization and parameterization are blindly done. Nonetheless, we can have access to prior information on the system's behavior. Therefore, in this paper, we aim to adapt and improve these quantum algorithms by using prior knowledge on the system for the AUD problem. We first propose a novel algorithm, the Improved Iterative Minimum Searching Algorithm (IIMSA) where we define more efficiently the parameters. Then, further enhancements of IIMSA are obtained thanks to a better initialization of the algorithms by exploiting classical preprocessing of the received signals with classical Conventional Correlation Receiver (CCR) or Zero Forcing (ZF). The obtained results show that these proposed algorithms operate more efficiently (i.e., less complexity with better accuracy).

**Index Terms**—5G, Active User Detection, Maximum Likelihood, Quantum Algorithm, Grover's algorithm

## I. INTRODUCTION

The roll out of the deployment of the 5G technology has been ongoing globally for enhanced wireless communication networks, and more specifically for the deployment of IoT. It is capable of handling a large number of users, maintaining a higher capacity than the previous generations, and minimizing latency limitations. The interesting aspect lies in its ability to serve a massive number of users, known as a massive machine-type communication (mMTC), which provides highly scalable wireless connectivity. This extensive connectivity requirement can support various devices such as smartphones, tablets, and Internet of Things (IoT) devices.

The previous generation, Long Term Evolution (LTE), was unable to fulfill these tasks due to the signaling overhead cost

introduced by resources orthogonality [1]. To solve this issue, non-orthogonal multiple access (NOMA) has been proposed to address the high network density for massive connectivity. NOMA's concept allows for devices to access the resource block simultaneously in a non-orthogonal way, even though it may result in inter-user interference in the channel. Despite this interference, this resource access has been proven to enhance Spectral Efficiency (SE), which is one of the main objectives in 5G [2].

Meanwhile, Ultra-reliable low-latency communication (URLCC) aims at achieving a low latency and high reliability network while mMTC handles a large number of users with sporadic traffic [3]. To this aim, 3rd Generation Partnership Project (3GPP) release 16 proposes a grant-free (GF) access scheme on the uplink communication to eliminate all delays by encapsulating all-in-one messages in order to avoid the handshake process [4]. GF uplink transmission allows to transmit message without *grant* from the BS [4].

Consequently, the complexity is deferred to the base station (BS) side. It receives a superposition of signals transmitted by the devices and has to extract the identity of the active users. This process is known as Active User Detection (AUD) which aims to identify and verify the active users in the network. The optimal AUD method is the well-known Maximum Likelihood (ML) decoder [5]. While this method is considered as the most accurate solution, however, it is not pertinent for practical implementation due to its high computation complexity ( $\mathcal{O}(2^N)$  where  $N$  is the number of devices). Herein, an exhaustive search is performed over all the possible user's activity combinations. Yet, some suboptimal methods, such as Parallel Interference Cancellation (PIC) and Successive Interference Cancellation (SIC), Matching Pursuit (MP) or Approximate Message Passing (AMP) algorithms have been proposed, in order to reduce the required computation burden to detect the active users [6]. However, this is at the cost of reduced AUD accuracy.

Meanwhile, quantum computing has emerged as a new computing technology which harnesses the properties of quantum mechanics. It extends classical computing but with a different approach for solving problems. Indeed, one of the quantum attributes, superposition, permits to handle both 0 and 1 states simultaneously, enabling parallelizing processing, i.e. processing data in different dimensions at once.

One of the most famous quantum algorithms is Grover's algorithm. It was designed to search for a specific value in an unsorted database, and extended to function inversion. The interest of this quantum algorithm is that it significantly

Muhammad Idham Habibie, Claire Goursaud, and Jihad Hamie, are with the CITI laboratory, EA3720, Univ Lyon, INSA Lyon, Inria, 69621 Villeurbanne, France (email: claire.goursaud@insa-lyon.fr)

This work has been funded by AEx project QAMUT granted by INRIA France

reduces the complexity. An extension is the quantum minimum searching algorithm (QMSA) family which searches for the minimum value of the database, such as proposed by Boyer, Brassard, Høyer and Tapp (BBHT) and Durr and Høyer (DHA) [7], [8].

In the AUD context, the ML formulation perfectly matches with Grover's algorithm structure. This is thus a promising approach to reduce the complexity while keeping the optimal achieved AUD accuracy. Authors in [9] have implemented BBHT and DHA in the context of multi-user detection (MUD) with a simple case, where the iterations are upper-bounded by  $22.5\sqrt{K/S}$ , with  $K$  the database size, and  $S$  the number of valid solutions. Authors in [10], [11], have compared the classical and quantum performances for several code families for the AUD problem with the original Grover's algorithm implementation, in a specific case. Nevertheless, these works consider Grover's algorithm in a noiseless case. Meanwhile, the ML approach has to be considered to match the AUD case in a noisy scenario. This was done in [12], where the authors have adapted Grover's algorithm to find the minimum for power domain NOMA purpose, when the number of solutions is unknown. Additionally, the authors of [13] have used an improved Quantum Approximate Optimization Algorithm (QAOA) for power domain NOMA purposes. These works were conducted within the power domain NOMA context, whereas in this paper, we focus on the code domain NOMA.

Based on the author's knowledge, the proposal of BBHT and DHA algorithms, which formulate the ML approach, has not yet been used for AUD purposes for the context of NOMA. Besides, the BBHT and DHA algorithms still suffer from high complexity, prompting several researchers to propose new solutions aiming at leveraging this problem [14], [15]. Thus, we propose to adapt the DHA algorithm to find the minimum in the AUD context alongside introducing a novel algorithm called Improved Iterative Minimum Searching Algorithm (IIMSA) to reduce the DHA's complexity. The idea of IIMSA is to exploit the prior knowledge of the system in order to allow for a more efficient search.

Accordingly, the contribution of this paper is summarized as follows:

- 1) Develop a new adapted algorithm of DHA, IIMSA, to improve the performances of DHA. The idea here consists in exploiting the statistical behavior of the communication system in order to estimate the number of solutions.
- 2) Reduce the number of iterations of DHA and IIMSA by merging and adopting the mixed-principle (classical and quantum) strategy. Herein, the initialization processes of the DHA and IIMSA algorithms are performed using classical methods such as CCR and ZF. This mixed-principle strategy conducts in reducing the number of iterations without degrading the final obtained accuracy in our AUD context.

The paper is organized as follows, section II presents the wireless system model with several classical signal processing methods. Section III describes the quantum principle, Grover's algorithm and its attributes, Grover's circuit, and DHA. In section IV, we present our proposed quantum algorithm and

then, section VI discusses the measurement scenarios and the obtained results. Finally, section VII concludes this paper.

## II. WIRELESS AUD SYSTEM MODEL

### A. System Model

Let us consider  $N$  devices (or users) connected to a BS equipped with a single antenna. These devices are assumed to be in sleep mode by default, and active only when they send messages. This network relies on Code-Domain Non Orthogonal Multiple Access (CD-NOMA) approach, where each user is distinguished by its own code. Each codeword is made of  $SF$  chips, where  $SF$  is the spreading factor. The codewords family thus lies in  $\mathbf{C} \in \mathbb{R}^{N \times SF}$ .

As we consider a NOMA system, we assume that  $N \geq SF$  users belong to the network. However, only few of them transmit to the BS simultaneously in one transmission frame. We model the users activity with the set  $\mathbf{b} \in \{0, 1\}^N$  where  $b_i = 1$  corresponds to user  $i$  being active (and  $b_i = 0$  to user  $i$  being inactive). We assume a perfect channel realization (or compensated with a power control loop), by considering  $\mathbf{H} = \mathbf{I}$ . In addition, we consider the presence of Additive White Gaussian Noise (AWGN), with iid realizations on each code component following  $\mathcal{N}(0, \sigma^2)$  distribution, denoted by  $\mathbf{w} \in \mathbb{R}^{SF}$ . The received signal is thus given by:

$$\mathbf{y} = \mathbf{b} \cdot \mathbf{C} + \mathbf{w} \quad (1)$$

The received signal  $\mathbf{y} \in \mathbb{R}^{SF}$  thus depends on three variables, activity user set ( $\mathbf{b}$ ), the codewords messages  $\mathbf{C}$ , and the additive noises ( $\mathbf{w}$ ). In order to evaluate the adaptability of the algorithms, three typical code families are considered in this paper:

- 1) Unipolar  $\mathbf{C} \in \{0, 1\}^{N \times SF}$
- 2) Bipolar  $\mathbf{C} \in \{-1, 1\}^{N \times SF}$
- 3) Random Gaussian Code  $\mathbf{C}/\|\mathbf{C}\| \in \mathbb{R}^{SF}$  with each component of  $\mathbf{C}$  following a Gaussian distribution

Given the received signal and the set of users code, the objective of the AUD process is to recover the set of active users  $\mathbf{b} \in \{0, 1\}^N$ .

### B. Conventional Correlation Receiver

The simplest user activity detector is the one that detects each specific user independently, with a Conventional Correlation Receiver (CCR) [16]. This detector correlates the received signal  $\mathbf{y}$  to the corresponding code sequences  $\mathbf{C}_i$ . The user is considered active if the correlation exceeds the predefined threshold  $T$ .  $\hat{b}_i^{CCR}$  corresponds to the activity status of user  $i \in \{1, \dots, N\}$  as estimated by the CCR.

It takes a value 0 or 1 as defined by the following rule:

$$\hat{b}_i^{CCR} = \begin{cases} 1 & \text{if } \sum_i \mathbf{y} \cdot \mathbf{C}_i \geq T \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

Note that, in order to estimate the full user activity set, the CCR has to be performed  $N$  times.

### C. Zero Forcing Receiver

The Zero Forcing receiver (ZF) is also a simple and effective detector but it considers all users simultaneously [17]. While the codebook  $\mathbf{C}$  is known, we evaluate the estimated  $\hat{\mathbf{b}}^{ZF}$  by multiplying the inverse code sequences  $\mathbf{C}_C$  with the observed signal  $\mathbf{y}$ . However, one may note that  $\mathbf{C} \in \mathbb{R}^{N \times SF}$  is a rectangular matrix with a full rank of  $SF$ . Thus, to compute this, we can use pseudo-inverse  $\mathbf{C}_C = (\mathbf{C}^T \mathbf{C})^{-1} \mathbf{C}^T$ . The estimated user activity set is thus given by:

$$\hat{\mathbf{b}}^{ZF} = \mathbf{y} \cdot \mathbf{C}_C \quad (3)$$

### D. Maximum Likelihood

Last but not least, the Maximum Likelihood (ML) receiver is the well-known optimal detector for AUD [17]. This detector identifies the most likely active users set  $\hat{\mathbf{b}}^{ML}$ , given the received sequence. For an AWGN channel, the ML is obtained by searching the active user set that minimizes the distance between its expected contribution and the received signal. With  $\mathbf{y}$  and  $\mathbf{C}$ , the received sequence and the set of user's signatures respectively, the ML receiver can be given as follows, in an AWGN channel, and equiprobable activity:

$$\hat{\mathbf{b}}^{ML} = \arg \min_{\{b_i\}_{i \in [N]}} \left\| \mathbf{y} - \sum_{i=1}^N \mathbf{b}_i \cdot \mathbf{C} \right\|_2^2 \quad (4)$$

The ML solution suffers from a high computation complexity  $\mathcal{O}(2^N)$ , as it is based on an exhaustive search over all the existing possibilities. Indeed, the likelihood metric has to be computed for each potential activity set. Even though this metric can be reduced to the distance between the expected received signal and the actual one (as we consider an independent, homogeneous activity, and a gaussian channel), finding the minimum among all distances depends exponentially of the number of users. Thus, the high complexity of the ML detector makes it intractable with classical processors when the number of users increases.

To sum up, with classical receivers, there is a tradeoff between the performance, and the achievability of the processing. This is why, in the following section, we briefly present quantum basics, and some suitable algorithms for our problem, which can permit to alleviate the wireless network from this compromise.

## III. QUANTUM PRINCIPLE

### A. Quantum Notation

Introduced by quantum mechanic which describes the physical properties of atoms and subatomic particles, the quantum principle relies on a new attribute called superposition, where processing 0 and 1 simultaneously is possible. The new type of *bit*, so-called *qubit*, is denoted with a dirac notation  $|\cdot\rangle$ , as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (5)$$

where  $\alpha, \beta \in \mathbb{C}$  are the probability amplitudes that verify  $|\alpha|^2 + |\beta|^2 = 1$ . As the amplitude coefficient are complex numbers, Eq. (5) can also be written as:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (6)$$

where  $0 \leq \theta \leq \pi$  and  $0 \leq \varphi \leq 2\pi$ .

The example above refers to a single qubit with two possible states ( $|0\rangle$  and  $|1\rangle$ ). However, this concept can be expanded to encompass multiple qubits. Thus for two qubits, there are four possible states which can be superposed with a different probability amplitude, and so on. Despite involving numerous qubits, the sum of the probability amplitudes for those states always adds up to 1. For example, if we are using 2 qubits to represent 4 states, we can have:

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle \quad (7)$$

where  $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{C}$  are probability amplitudes that verify  $|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$ .

It is important to highlight that we do not have access to the state amplitudes. The only information that we can have on the system is provided by a measurement of the state  $|\psi\rangle$ . The measure makes a random projection of the state  $|\psi\rangle$  on one of the reference states of the measurement basis (here  $|0\rangle$  and  $|1\rangle$ ). Each state ( $|0\rangle$  and  $|1\rangle$ ) might appear accordingly to its probability amplitude. The following section delves into the workings of Grover's algorithm in the context of modifying these probability amplitudes.

### B. Grover's algorithm

Grover's algorithm has been designed in order to efficiently (in terms of the number of needed operations) search a value in a database. The complexity, defined in this paper as the required number of iterations to find such value, is  $\mathcal{O}(\sqrt{K})$  while classical requires  $\mathcal{O}(K)$ , where  $K$  is the database size.

In a nutshell, to do so, Grover's algorithm relies on two main functions, as illustrated in Fig.1: 1) Oracle (**O**), 2) Diffuser (**D**). The oracle first marks the states which verify the chosen constraint while the diffuser amplifies the states previously marked by the oracle. More precisely, let us assume that we have a value represented by  $N$  qubits. The first step is to initialize the superposed states, denoted as  $|\psi\rangle$ . To do so, we start with all qubits being  $|0\rangle$ , and we multiply each of them with Hadamard operator  $H^{\otimes N}$ :

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=1}^K |x\rangle \quad (8)$$

where  $|x\rangle \in \mathbb{B}^N$  corresponds to the index of the qubit [9], and  $K = 2^N$  corresponds to the number of basis states.

Then, the operation **O** marks the targeted states as follows:

$$\mathbf{O}|x\rangle = \begin{cases} |x\rangle & \text{if } f(x) = \delta \\ -|x\rangle & \text{otherwise} \end{cases} \quad (9)$$

The Oracle **O** is designed with respect to the targeted function and its targeted outcome,  $f(x) = \delta$ , where  $x$  corresponds to any of the  $K$  values to test. Then, this result is amplified by **D** which inverts the probabilities around the mean, thus amplifying the probability for the valid solutions, and attenuating the non-valid ones. This unitary operator can be modeled by:

$$\mathbf{D} = H^{\otimes N} (2|0^N\rangle\langle 0^N| - I) H^{\otimes N} = 2|\psi\rangle\langle\psi| - I \quad (10)$$

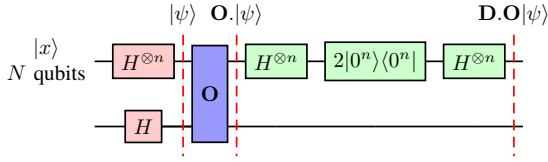


Fig. 1: Grover's scheme

**Algorithm 1: BBHT Algorithm**


---

**Input :**  $K, m, \lambda$   
**Output:**  $x_{out}$

- 1  $m \leftarrow 1, \lambda \leftarrow \frac{6}{5}$  (or  $\lambda \leftarrow \frac{4}{3}$ ),  $L_{BBHT} \leftarrow 1$ ;
- 2 **while**  $L_{BBHT} < 4.5\sqrt{K}$  **do**
- 3     Choose  $j$  uniformly in  $\{0, \dots, [m]\}$ ;
- 4     Initialize the superposition  $|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=0}^{K-1} |x\rangle$  (Eq. (8));
- 5     Apply Grover's algorithm  $j$  times  $|\psi_{out}\rangle = \mathcal{G}^j |\psi\rangle$ ;
- 6     Update  $L_{BBHT} \leftarrow L_{BBHT} + j$ ;
- 7     Measure  $x_{out}$  from  $|\psi_{out}\rangle$ ;
- 8     **if**  $U[x_{out}] = \delta$  **then**
- 9         The solution is found and exit the while loop;
- 10    **else**
- 11       Set  $m \leftarrow \min(\lambda m, \sqrt{K})$ ;
- 12    **end**
- 13 **end**

---

Finally, let us denote Grover's algorithm as  $\mathcal{G}$ , where its full algorithm is written as follows:

$$\mathcal{G}|\psi\rangle = \mathbf{D.O.}|x\rangle = H^{\otimes N} (2|0^N\rangle\langle 0^N| - I) H^{\otimes N} \mathbf{O.}|x\rangle \quad (11)$$

After one iteration, the desired solutions are more likely to be measured than the non-desired ones. However, one may note that the latter can still be obtained.

*C. Grover's optimum iteration: known number of solutions*

Grover's algorithm should be repeated several times, so as to remove as efficiently as possible the non-desired solutions. The number of iterations in Grover's algorithm depends on the database size  $K$  and the number of solutions  $S$ .

The optimal number of Grover iterations has been proven to be  $L_{opt} = \lfloor \frac{\pi}{4} \sqrt{K/S} \rfloor$  where  $\lfloor \cdot \rfloor$  is the floor function [18].

*D. Grover's optimum iteration : unknown number of solutions*

Regardless of the search method, the total number of solutions  $S$  is often unknown, which prevents to accurately evaluate the previous  $L_{opt}$ . As a consequence, there have been efforts to define an effective technique to search a solution in the database when  $S$  is unknown.

Boyer, Brassard, Høyer and Tapp proposed a method called BBHT to find a targeted solution when no prior knowledge is needed [7]. Let us assume that we have a database, denoted  $U$ , with a size of  $K$ . Our objective is to locate the value  $\delta$  within this database. The BBHT's full algorithm is written in algorithm 1.

BBHT's complexity is bounded by  $\frac{9}{2}\sqrt{K}$  as proved by the authors of this algorithm [7]. This complexity is derived by taking the average of the success probability on Grover's algorithm. The algorithm will be stopped if  $U[x_{out}] = \delta$  or if  $L_{BBHT}$  has reached this bound.

**Algorithm 2: DHA's algorithm**


---

**Input :**  $K, m, \lambda$   
**Output:**  $x_{out}$

- 1 Set  $m \leftarrow 1, \lambda \leftarrow \frac{6}{5}$  (or  $\lambda \leftarrow \frac{4}{3}$ ),  $L_{DHA} \leftarrow 1$ ;
- 2 **while**  $L_{DHA} < 22.5\sqrt{K}$  **do**
- 3     Choose  $0 \leq i_x \leq K-1$  with uniform distribution;
- 4     Choose number of iterations  $j$  uniformly from  $\{0, \dots, [m]\}$ ;
- 5     Initiate the superposition  $|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{x=0}^{K-1} |x\rangle$ ;
- 6     Apply Grover's operator  $\mathcal{G}$  with  $j$  iterations resulting in  $|\psi_{out}\rangle = \mathcal{G}^j |\psi\rangle$ , marking states such that  $U[x] < U[i_x]$ ;
- 7     Measure  $x_{out}$  from  $|\psi_{out}\rangle$ ;
- 8     Update  $L_{BBHT} = L_{BBHT} + j$ ;
- 9     Update  $L_{DHA} = L_{DHA} + L_{BBHT}$ ;
- 10    **if**  $U[x_{out}] < U[i_x]$  **then**
- 11       Set  $i_x = x_{out}$  and exit the while loop;
- 12    **else**
- 13       Go back to Step 3;
- 14    **end**
- 15 **end**

---

## IV. AUD DEDICATED QUANTUM ALGORITHMS

In this section, we adapt the DHA algorithm to perform ML decoding for the active user detection problem, and propose a new one.

These advanced search algorithms are inspired by the previous algorithms. Indeed, for Grover's and BBHT's algorithms, the solutions satisfy a *trivial* condition that can be easily checked (for example,  $f(x) < \delta$ ). However, ML does not fall into this category. So, we now take a step further, by considering non-trivial conditions, such as the case where we have to find the minimum, as needed in the ML algorithm.

Besides, as seen in the previous section, we need to consider different approaches depending on whether the number of potential solutions within Grover's search is priorly known. Thus, we present, in this section, two quantum algorithms which search for the ML solution of the AUD problem. In the first case, we consider that we do not have access to the number of solutions for each iterative step, while in the second one, we suppose that we do have access to this information.

*A. Durr and Høyer Algorithm (DHA)*

In this section, we suppose that we have no prior information on the data structure. This means that the search has to be performed in a blind way. Additionally, this algorithm aims to find the minimum value in an unsorted list.

Finding a minimum in a given list can be achieved by selecting an initial value, then iteratively searching for a smaller value than the last one. Once we can not find any new value, the minimum is considered to be found. To do so, the quantum algorithm can process iteratively to find the minimum, by locating the index of a smaller item than the value set by a predetermined threshold index. This algorithm is the one proposed by Durr and Høyer [8], namely DHA, in order to find the minimum of the database. This algorithm finds the index of the minimum value with a probability at least  $1/2$  for a running time  $\mathcal{O}(\sqrt{K})$  [8].

Algorithm 2 illustrates the full steps of DHA to find a targeted value and recover its index. Let us assume a database

$U$  with size  $K$ . The initialization index value  $i_x$  is chosen randomly following a uniform distribution. The objective of DHA's algorithm is to find the minimum value, with the constraint that the solution after Grover's iteration, denoted as  $U[x_{out}]$ , should be less than  $U[i_x]$ . The complexity of this searching procedure is given by  $22.5\sqrt{K}$ .

### B. Improved Iterative Minimum Searching Algorithm

In the previous section, the number of solutions was supposed to be unknown. However, we can suppose that we can have access to this information thanks to a prior off-line study of the system behavior. This knowledge permits to have a better efficiency while running Grover, by doing the appropriate number of iterations, and not a random one. The IIMSA algorithm relying on our system model described in Eq. (1), can be illustrated as follows:

---

#### Algorithm 3: IIMSA Algorithm

---

**Input :**  $\mathbf{C}, K, L_{IIMSA}, \hat{\delta}$

**Output:**  $\delta_x, \mathbf{b}$

- 1  $i \leftarrow \text{choose } (0, K - 1) \text{ uniformly ;}$
  - 2 Choose  $\hat{\delta}(i) \leftarrow \text{corresponds to } i$  ;
  - 3  $\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2 \leq \hat{\delta}$  ;
  - 4  $nb_{it} \leftarrow 1$  ;
  - 5 **while**  $\hat{S} \neq 0$  **or**  $nb_{it} \leq L_{IIMSA}$  **do**
  - 6      $\mathbf{b} \leftarrow \mathcal{G}(L_{opt})$  ;
  - 7      $\delta_x \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2$  ;
  - 8      $\hat{S} \leftarrow \|\mathbf{y} - \mathbf{b} \cdot \mathbf{C}\|_2^2 \leq \delta_x$  ;
  - 9      $nb_{it} \leftarrow nb_{it} + L_{opt}$  ;
  - 10    **if**  $\delta_x < \hat{\delta}$  **then**
  - 11     |  $\hat{\delta} \leftarrow \delta_x$  ;
  - 12    **end**
  - 13 **end**
- 

Firstly, we randomly select an index  $i$  from a uniform range of values between 0 and  $K - 1$ , where  $K$  is the size of the database. Consequently,  $\hat{\delta}$  is here initialized by computing the corresponding distance between the selected set and the received signal. We then evaluate the number of solution  $S$ , i.e. the number of sets whose distance is lower than the current  $\hat{\delta}$ , thanks to the statistical system analysis. If  $S = 0$ , the current  $\hat{\delta}$  is the one that corresponds to the minimum distance. Otherwise, Grover's algorithm  $\mathcal{G}$ , searching for  $x$  such that  $f(x) < \hat{\delta}$  is run, to search for a lower distance. The Grover's output provides a new user activity set, leading to a new  $\delta_x$  and number of solution  $S$ . If  $\delta_x < \hat{\delta}$  (i.e. if the measurement returns a valid solution), we iterate by starting once again  $\mathcal{G}$  but with  $\hat{\delta}$  updated by  $\delta_x$  value. We thus have a smaller set of solutions for the next iteration of  $\mathcal{G}$ .

This principle is applied until we obtain  $S = 0$ . For each Grover's call, the algorithm runs the modified oracle for  $L_{opt} = \lfloor \frac{\pi}{4} \sqrt{\frac{2^N}{S}} \rfloor$  times, to find a lower distance. However, it is important to note that if the number of solutions is bigger than the half of the database size, then the unwanted cases are amplified, pushing the search in the wrong direction. Thus, and also to be in the same conditions than DHA which has a

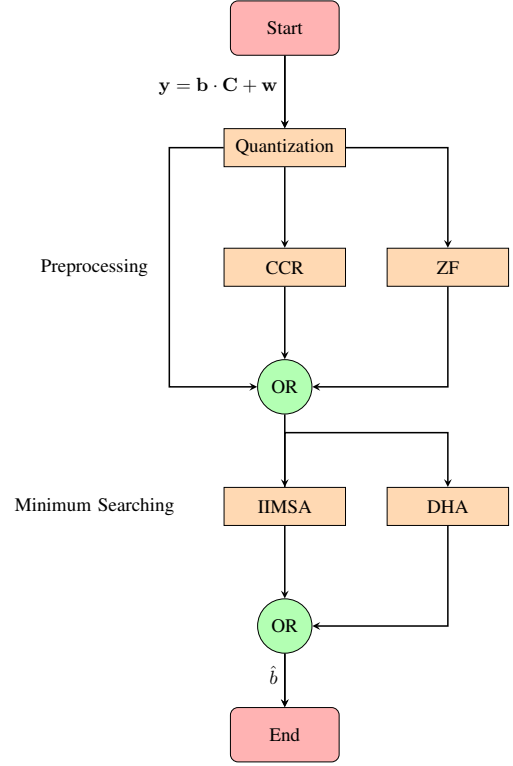


Fig. 2: Proposed algorithms principle

limitation on the number of iterations, we bound the number of unsuccessful trials to  $L_{IIMSA}$ .

### C. Quantum-Classical Hybrid Solution

Finally, to further ameliorate the previous algorithm, we propose to exploit the knowledge that can be easily obtained with classical preprocessing of the received signal. The objective is to initialize accurately the quantum search algorithm, to prevent the case where the number of solutions is too high. Besides, we also expect it to accelerate the search as we might start closer to the targeted solution  $\delta$ . To do so, we propose to evaluate the estimated activity status for each user, by applying CCR (as proposed in II-B) and ZF (as proposed in II-C) to the received signal  $\mathbf{y}$ . The complete algorithms (merging classical pre-processing and quantum search) are called CCR-DHA, ZF-DHA, CCR-IIMSA and ZF-IIMSA.

One may note that this approach requires more classical computations ( $N$  CCRs computations and 1 ZFs computation have to be classically performed), but we expect to significantly reduce the quantum complexity. CCRs and ZFs are expected to identify a *close* solution for the activity set. From this, we compute the distance of this reference set to the received signal, which is called  $\delta_{CCR}$  and  $\delta_{ZF}$  respectively.

## V. SIMULATION SETUP

### A. General setup

This subsection presents the system architecture of the implementation process. As a first step, we start by generating the received signal  $\mathbf{y}$ , which will be then quantized to deliver

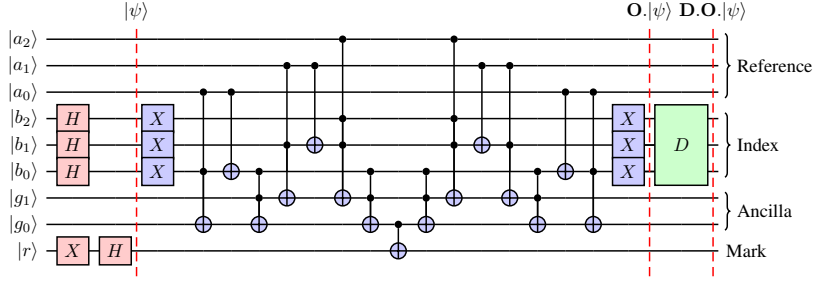


Fig. 3: Grover's Circuit  $n = 3$  qubits  $f(x) < \delta$

Codetype	Spreading Factor $SF$	Number of Users $N$
Unipolar	3	4
	4	5
	5	7
	6	9
	7	11
Bipolar	3	3
	4	5
	5	6
	6	8
	7	10
Gaussian	3	5
	4	6
	5	7
	6	8
	7	9

TABLE I: Parameters  $SF$  and  $N$  for the used code families

a received sequence. Then, the second step is to propose on efficiently target an initialization value by performing classical processing. For example, we chose to exploit CCR and ZF to assist in enhancing the algorithms (i.e. DHA and IIMSA), while also comparing with their original versions without any preprocessing. Overall, we are comparing six possible detectors: DHA, CCR-DHA, ZF-DHA, IIMSA, CCR-IIMSA, and ZF-IIMSA. The goal of these algorithms is to find the set  $\mathbf{b}$  which minimizes the distance between the received signal  $\mathbf{y}$  and  $\mathbf{b} \cdot \mathbf{C}$ . The full system architecture with the various options is presented on Fig. 2.

As for the system parameters, we consider 3 code families (unipolar, bipolar and gaussian which will be detailed in the next section) with various spreading factors (SF), allowing different numbers of users as shown in Table I. As, for these circuits, the required number of qubits is higher than 32 qubits, we simulate Grover's algorithm in MATLAB. As our goal is to keep the same performances, while reducing the computation cost, we evaluate the performance  $P_s$  and the complexity  $nb_{it}$  of the different algorithms, as follows:

- IIMSA vs DHA Analysis (section: V-D1)
- DHA, CCR-DHA, and ZF-DHA Analysis (section: V-D2)
- IIMSA, CCR-IIMSA and ZF-IIMSA analysis (section: V-D3)
- IIMSA vs DHA Analysis w.r.t  $L_{max}$  (section: V-D4)

## B. Implementation Circuit

We present here how we adapted the previous algorithms to the quantum circuit's constraints.

First, to build Grover which relies on oracle  $\mathbf{O}$  and diffuser  $\mathbf{D}$ , as illustrated in Fig. 3, we need four registers: 1) Index register 2) Reference register 3) Ancilla register 4) Mark register. *Index register* contains the argument  $x$  of the function  $f(x)$  to which we compare the targeted value stored in the *Reference register*  $\delta$ . The *Ancilla register* permits to store partial results needed to ensure unitary operators during the processing. Finally, *Mark register* provides the negative sign as stated in (9) in order to mark some of the states.

The whole Grover's circuit is shown in Fig. 3 where  $N$  is the number of qubits on the Hilbert space (1 qubit per potential user). In this figure, we use  $N = 3$  qubits, allowing for eight different computational basis states  $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, \text{ and } |111\rangle$ . The qubits number for the value and reference registers are  $Z$  qubits, corresponding to the number of minimum qubits to operate the function of  $|f(x)\rangle$ , and related to the targeted precision as detailed on next page. The last, *mark register* occupies 1 qubit for the sign  $|-\rangle$ . For example, the authors in [10], [11] show a simpler circuit for  $|f(x)\rangle = |\delta\rangle$ , where the function  $f$  was the identity function.

When searching for a minimum value in a list of databases as proposed by DHA, it is important to redesign the oracle on Eq. (9) so as to mark the states which verify  $f(x) < \delta$ . Hence, the circuit is proposed as illustrated in Fig. 3. The idea is to evaluate the difference between the values coded by two states  $|a\rangle$  and  $|b\rangle$  to compute  $(a - b)$ . From the results, we can deduce that  $a < b$  when the sign is negative.

Thus,  $r = \text{MSB}(a - b)$  acts as a carry, with the condition as follows:

$$r = \begin{cases} 1 & a > b \\ 0 & \text{otherwise} \end{cases} \quad (12)$$

Hence,  $r$  multiplies with  $|-\rangle$  in *mark register* to provide the negative computation to the oracle. In this paper, the qubit  $|a\rangle$  and  $|b\rangle$  correspond to  $|\delta\rangle$  and  $|f(x)\rangle$  respectively, to comply with the oracle theory as proposed in Eq. 9.

Secondly, the received signal  $\mathbf{y}$  components are real values  $\mathbf{y} \in \mathbb{R}^+$ . Nonetheless, in this paper, we consider digital quantum processing and not analog quantum computation. Thus,  $\mathbf{y}$  should be quantized, generating the signal  $\mathbf{y}_q$  that will be processed. The retained integer part of  $\mathbf{y}$  is upper bounded

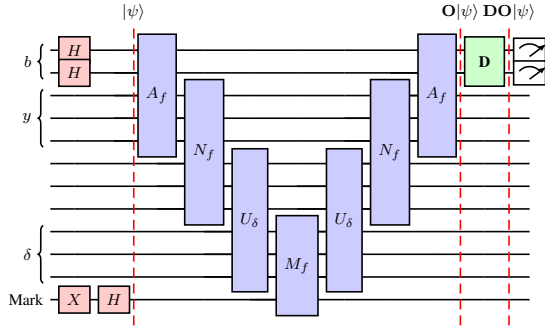


Fig. 4: Quantum Circuit of  $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2 \leq \delta$

by  $2^I - 1$ , where  $I$ , is the number of required qubits for the integer part to span the whole range for possible values for  $f(x)$ .

To represent the decimal part, we define the precision range with the indicator  $p \in \mathbb{N}$ . Indeed, a higher precision  $p$  in the circuit leads to more accurate results. Nevertheless, it requires a larger memory size. At the end, the size of the registers is  $Z = I + p$ . To sum up, the *reference register* in Grover's algorithm is fed with  $\mathbf{y}_q$  as shown in Fig. 3 defined as:

$$\mathbf{y}_q = \min \left( \max \left( 0, \frac{\text{round}(\mathbf{y} \times 2^p)}{2^p} \right), 2^{I-1} \right) \quad (13)$$

In this paper, we use precision  $p = 2$  for the decimal part. After obtaining  $\mathbf{y}_q$ , we modified the Grover's search circuit as  $\mathcal{G}$  in Fig.4. The pre-processed values  $\mathbf{y}$  and  $\delta$  are put into the circuit.

The circuit is composed of four main blocks:

- $A_f$  : stands for *adder function*, it computes  $\mathbf{y} - \mathbf{b}.\mathbf{C}$
- $N_f$  : stands for *norm function*, it computes the norm  $\|\mathbf{y} - \mathbf{b}.\mathbf{C}\|_2^2$
- $U_\delta$  : is the oracle part, identifying the states where the norm is lower than  $f(b) < \delta$
- $M_f$  : marks the previous identified states

These blocks are then repeated in the reverse order for the uncomputation part, before amplifying the amplitude of the solution with the diffuser.

### C. Code families

This section elaborates the adaptation of quantum algorithm to several code families. We consider three families in this paper, *Unipolar Code*, *Bipolar Code*, and *Random Gaussian Code*.

1) *Unipolar Code*: This code family lies on  $\mathbf{C} \in \{0, 1\}^{N \times SF}$ . This codeword is randomly chosen while ensuring non-orthogonality with one or several codes within the family. For example, we can have  $N = 4$  users with  $SF = 3$ . The associated codewords can be  $c_1 = [1, 1, 0]$ ,  $c_2 = [0, 1, 1]$ ,  $c_3 = [0, 0, 1]$  and  $c_4 = [1, 0, 1]$ . In this case, the expected ideal signal is (without noise):

$$f(b_1, b_2, b_3, b_4) = \begin{bmatrix} b_1 + b_4 \\ b_1 + b_2 \\ b_2 + b_3 + b_4 \end{bmatrix} \quad (14)$$

2) *Bipolar Code*: A family code of this codetype utilizes  $\mathbf{C} \in \{-1, 1\}^{N \times SF}$ . The negative computation is done with an *one complement*, where the computation is performed by inverting the bits. Bipolar codes generation is originated by adding together two unipolar codes, one of which is inverted [19]. Quantum operations have been adapted to allow the computation of negative values [11].

3) *Random Gaussian Code*: A random Gaussian code is a code whose each component is randomly generated with a Gaussian distribution, denoted as  $\mathbf{C}$ . In order to ensure equal power between users, this code is normalized by its magnitude. Thus, the used code can be expressed as:  $\frac{\mathbf{C}}{\|\mathbf{C}\|}$  [20]. To implement this function on quantum circuit, the decimals are considered in this circuit. Based on decimal representation in binary with precision  $p = 2$  it helps to identify the corresponding solution.

### D. Performance Analysis

This section discusses the performance comparison between DHA and IIMSA with the contribution of classical methods (CCR and ZF).

To do so, we focus on two parameters:

- 1) The success probability ( $P_s$ )
- 2) The complexity ( $nb_{it}$ )

The success is defined as the case where all active users are detected correctly, and no unactive one is considered active, thus that  $\hat{\mathbf{b}} = \mathbf{b}$ . The variable  $nb_{it}$  represents the total number of Grover's iterations. The  $nb_{it}$  involves an accumulation evaluation identical to that of  $L_{DHA}$  and  $L_{IIMSA}$ . The optimal performance is achieved when there is a high success probability ( $P_s$ ) along with a small number of Grover's iterations ( $nb_{it}$ ). In this paper, we consider small-size code families so as to be able to simulate the proposed quantum algorithms with classical processors, as proof of concept. However, these results can be extended to higher family size. The used configuration of  $SF$  and the corresponding number of users along with code types is given in Table. I.

1) *IIMSA vs DHA Analysis*: First, in Fig. 5, we present the performance  $P_s$  and the number of iterations  $nb_{it}$  of IIMSA and DHA as a function of variance  $\sigma^2$  for the 3 code types. The values of  $L_{IIMSA}$  and  $L_{DHA}$  are both upper-bounded by  $22.5\sqrt{2^N}$ .

These figures, Fig. 5a-5c, demonstrate a clear relationship between the variance  $\sigma^2$  and the success probability  $P_s$ . As the variance increases, the success probability decreases. This is expected as higher noise contamination adversely affects the system's detection performance, leading to errors.

It is important to highlight that each particular SF has a different level of non-orthogonality, resulting in diverse trends among all SF types. Notably,  $SF = 4$  exhibits the highest success probability, followed by  $SF = 3$ . This difference can be attributed to the distinct non-orthogonal components present in the code type for  $SF = 4$ , which results in less non-orthogonality compared to the other SFs, thereby contributing to a higher  $P_s$  compared to the others. The main focus of this study, however, is to compare IIMSA and DHA using



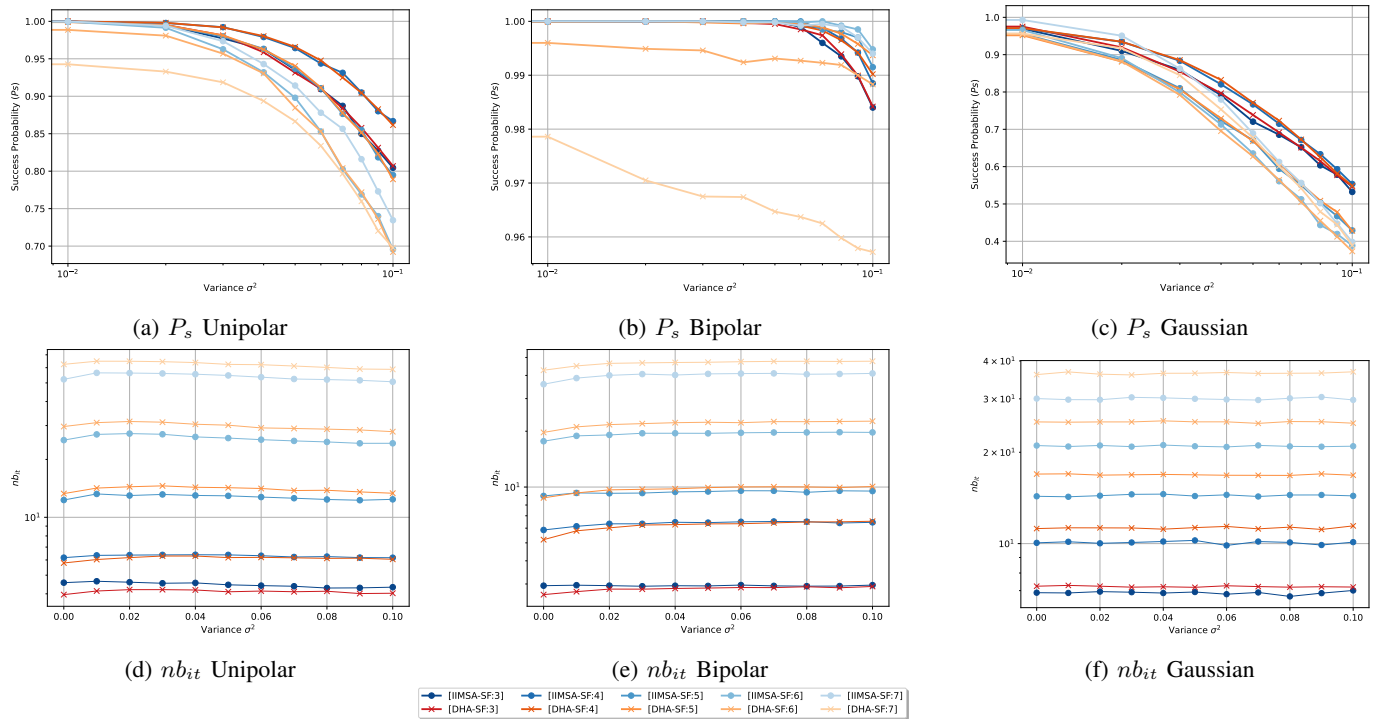


Fig. 5: Success probability  $P_s$  and number of Grover's iterations  $nb_{it}$  w.r.t variance  $\sigma^2$  (IIMSA, DHA)

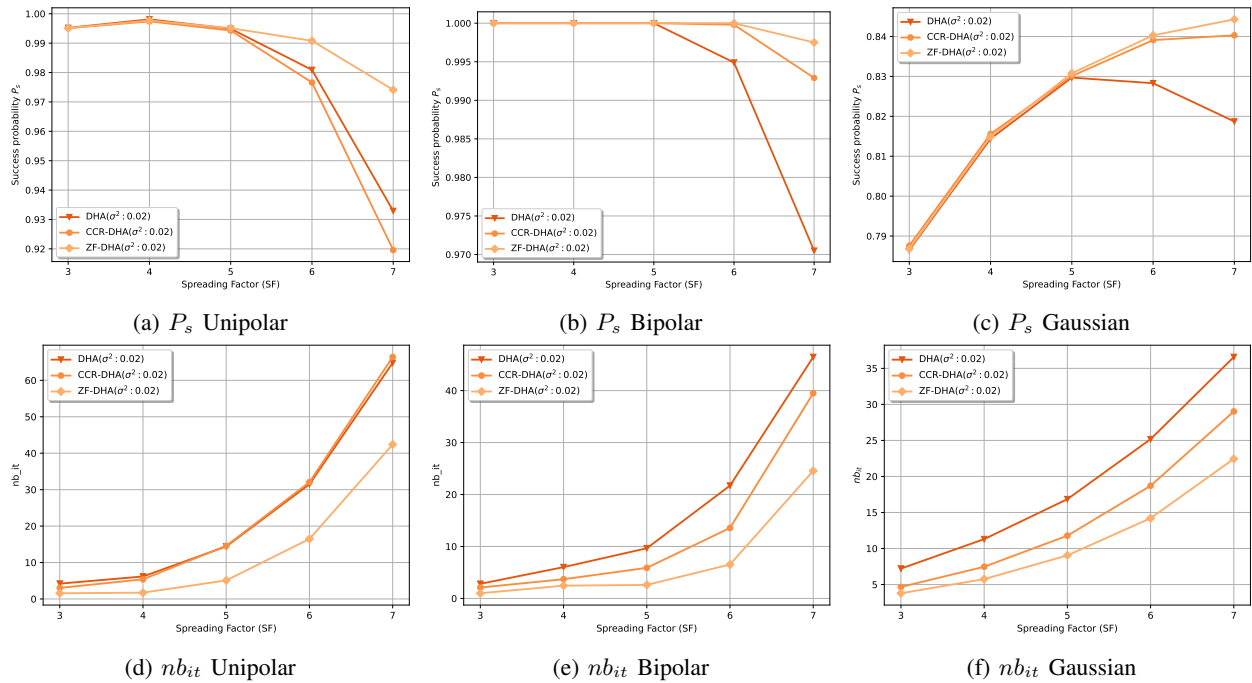


Fig. 6: Success Probability  $P_s$  and number of iterations  $nb_{it}$  w.r.t variance  $\sigma^2$  (DHA, CCR-DHA, ZF-DHA)

the same non-orthogonal code, as described in the subsequent subsection.

The performances show that IIMSA and DHA appear to have comparable and similar performance, especially under a small variance  $\sigma^2$  regime in all code types. However, in the case of bipolar and unipolar, when SF is high, there is a distinct performance between IIMSA and DHA because the bipolar and unipolar are characterized with their high euclidean distance between each component. The IIMSA proves to outperform the DHA when the SF is 6 or 7. This denotes that our proposed algorithm is efficient while handling high variance  $\sigma^2$  with large number of users  $N$  and slots SF.

Let us examine Fig. 5d through Fig. 5f, which depict the evolution of  $nb_{it}$  when varying the variance  $\sigma^2$ . The best efficiency regarding  $nb_{it}$  is reached by the smallest values. These figures clearly show that IIMSA surpasses DHA across all levels of SFs for various variances  $\sigma^2$ , encompassing all code types. As the SF increases, the contrast in IIMSA's superiority becomes more pronounced. It is also important to note that the value of  $nb_{it}$  remains stable across all variance values  $\sigma^2$ ; there is only a slight difference among them. This phenomenon can be attributed to the fact that the number of iterations  $nb_{it}$  characterizes the speed at which convergence occurs toward the nearest active user set. If the level of noise increases, there is a higher probability of encountering an incorrect set, but this only has a minor impact on the convergence speed. Thus, we see only a slight differences for the  $nb_{it}$  as a function of variance  $\sigma^2$ .

Finally, we can also recall that the Unipolar, Bipolar, and Gaussian schemes present varying distances among their components. A greater separation between these components facilitates the detector in distinguishing the group of active users. This phenomenon is clearly illustrated in Figures 5b to 5c. Notably, Bipolar, characterized by a significant Euclidean distance between its components, exhibits a distinct level of  $P_s$  compared to other code types. In this context, the worst success probability (for the considered set of parameters) is 0.96. Conversely, Unipolar and Gaussian schemes exhibit  $P_s$  values of 0.7 and 0.4 respectively. Additionally, we observe varying levels of  $nb_{it}$ , as depicted in Figures 5d through 5f. Notably, Gaussian is the one where the complexity is the smallest thanks to its small Euclidean distance. In contrast, Bipolar, despite its significant distance, converges to a lower level of  $nb_{it}$ . Unipolar attains its highest  $nb_{it}$  when the SF is 7.

In conclusion, our proposed algorithm outperforms the original DHA in terms of both  $P_s$  and  $nb_{it}$  which confirms that the IIMSA can converge more efficiently toward the most likely situation.

2) *DHA, CCR-DHA, ZF-DHA Analysis*: In this section, we now consider the performances of the classically-aided DHA algorithms. We present a comparison between the original DHA and when mixed with classical algorithm (ZF and CCR), to evaluate their efficiency in determining the correct value of  $\hat{b}$ .

In this analysis, we consider the same three code types (i.e Unipolar, Bipolar, and Gaussian).  $P_s$  and  $nb_{it}$  are evaluated as a function of SF for the different algorithms, namely DHA,

CCR-DHA, and ZF-DHA. The configuration is established with an upper-bound for  $L_{DHA} = 22.5\sqrt{2^N}$  with a noise variance  $\sigma^2 = 0.02$ . Results are presented on Fig.6.

First, we can observe that across all codetypes, all algorithms (DHA, CCR-DHA, and ZF-DHA) demonstrate similar  $P_s$  values when SF is small. Interestingly, as the SF value is higher than 6, ZF-DHA outperforms the other DHA types (DHA and CCR-DHA). Then, we can notice that the use of CCR degrades the performances for unipolar code, while it brings improvement for Bipolar and Gaussian codes. This can be explained by the fact that the CCR detects the users activity in a less accurate way for the Unipolar codes, due to the accumulation of positive interference over all chips, thus leading oftenly to an "active" decision. Meanwhile, Bipolar and Gaussian decoding leads to both positive and negative interference, which reduces the risk of false alarm.

Secondly, we have also observe that the success probability ( $P_s$ ) is lower in the Gaussian part due to the closer proximity between components, which makes it more susceptible to noise contamination ( $\sigma^2$ ). Despite the lower  $P_s$  in the Gaussian part, it exhibits a distinct trend when compared to Unipolar and Bipolar curves. This difference can be attributed to the fact that as SF increases, 2 codes are less likely to be confused. However, as the number of users increases, the random generation might lead to have 2 close codewords, thus reducing the performances. The curve shape thus shows the compromise between these 2 effects.

In addition, Fig. 6d - 6f, focus on the evolution of  $nb_{it}$  as a function of SF. It shows that DHA consistently required a higher number of iterations compared to other methods for all code types. We observe that ZF-DHA outruns other DHA types (i.e DHA, CCR-DHA). This is due to the fact that its accurate detection permits to stop the search sooner.

Finally, the trend indicates that at low SF values, the number of iterations ( $nb_{it}$ ) is quite competitive among all algorithms. Particularly, when SF is set to 3, the  $nb_{it}$  values are very close to each other. This closeness in values can be attributed to the fact that with a small SF, the number of Grover's iterations in each step is small, resulting in a closely aligned comparison graph. Moreover, in the Unipolar scenario, CCR-DHA is still less efficient than DHA when the SF value is high. The reason behind this can be attributed to the fact that as seen before, the CCR suffers from high interference in the Unipolar case.

In summary, ZF-DHA exhibits a high success probability while maintaining simplicity with fewer iterations ( $nb_{it}$ ). Thus, it is an interesting way to enhance the performances of the system.

3) *IIMSA, CCR-IIMSA, and ZF-IIMSA Analysis*: Similarly to Section V-D2, this subsection compares the performances between IIMSA, CCR-IIMSA, and ZF-IIMSA. The main objective is to address if the previous conclusions for DHA also apply for IIMSA.

We evaluate the performances  $P_s$  and  $nb_{it}$ , for the same three code types. As done in section V-D2, the upper-bound of IIMSA is set to  $L_{IIMSA} = L_{DHA} = 22.5\sqrt{2^N}$ . Results are presented for a noise variance  $\sigma^2 = 0.02$  on Fig.7.

First, we can note that the success probability  $P_s$  with all evaluated performances (i.e IIMSA, CCR-IIMSA and ZF-

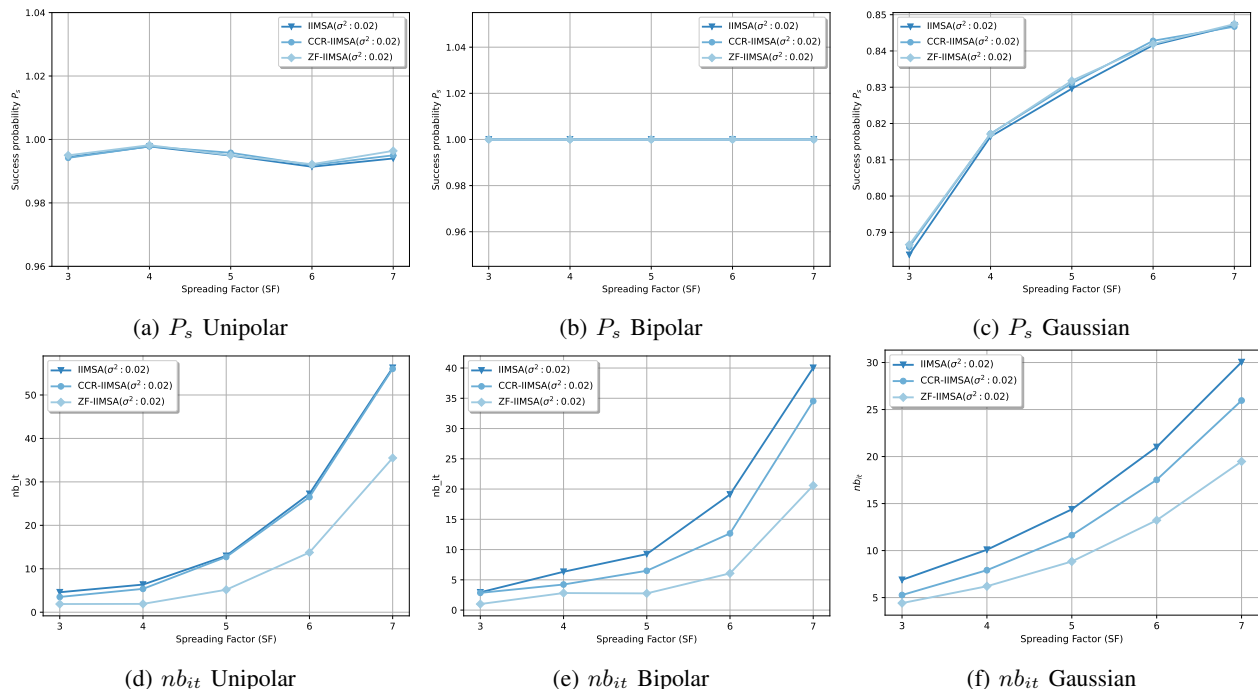


Fig. 7: Success probability  $P_s$  and number of Grover's iterations  $nb_{it}$  w.r.t variance  $\sigma^2$  (IIMSA, CCR-IIMSA, and ZF-IIMSA)

IIMSA) are similar. The Unipolar and Bipolar SFs are close to  $P_s = 1$  among all SFs, while the Gaussian SF exhibits a wider range across the different SF. This is related to the random choice of the Gaussian codes.

Meanwhile, when considering the number of iterations  $nb_{it}$ , there is a contrast different among all IIMSA types. We can observe that ZF-IIMSA outperforms the 2 other IIMSA types (i.e IIMSA and CCR-IIMSA) for all SF. This signifies that the classical ZF has a more accurate detection, making the Grover requires fewer iterations. This performance is followed by CCR-IIMSA with less accurate detection but still can outperform the original IIMSA. The CCR-IIMSA however has a similar performance with IIMSA in unipolar case, but it does outperform the IIMSA on other cases such as Bipolar and Gaussian.

In summary, ZF-IIMSA also exhibits an high success probability while maintaining simplicity with fewer iterations ( $nb_{it}$ ). Despite the success probability has a similarity with other methods, the ZF-IIMSA is still outperforming IIMSA and CCR-IIMSA the  $nb_{it}$  case. This ZF-IIMSA advantage is more important for the high SF range, which is promising for dense IoT networks.

4) *IIMSA vs DHA as a function of  $L_{max}$* : This section finally focuses on examining the influence of the number of allowed iterations denoted by  $L \in \{1, \dots, L_{max}\}$ , where  $L_{max} = 22.5\sqrt{2^N}$ . This analysis is conducted for all code types, and for a noise variance  $\sigma = 0.1$  and  $SF = 6$ . DHA-based curves are plotted in red, and IIMSA ones in blue, to keep the same aspect than in Fig.6 and 7.

First of all, we can observe in Fig. 8, that as  $L$  increases,  $P_s$  increases, and  $nb_{it}$  also increases. This due to the fact that, as we allow for more trials within the algorithms, it is more likely to find the solution, but at the cost of more iterations in

average.

Secondly, as seen in Fig. 8a to Fig. 8c, the success probability ( $P_s$ ) of IIMSA surpasses the DHA's one, when they are both used in the original version, but also when improved with CCR or ZF. This is due to the fact that IIMSA exploits the estimation of the number of solutions at each step to be more efficient in the search. Besides, ZF-IIMSA outperforms all the other algorithms. This trend can be observed for all codetypes.

On the other hand, we observe a distinct performance trend concerning  $nb_{it}$ . In 8d - 8f, it can be seen that DHA with the additional classical algorithm (ZF and CCR) outperforms IIMSA, especially when  $L$  is small. This is due to the fact that in IIMSA, the algorithm starts with a higher number of iterations as it is defined by  $L_{opt}$ , while DHA starts with a random value taken in an interval  $L \in \{0, \dots, \lfloor m \rfloor\}$  as explained in Algo. 2, with  $m$  gradually increasing from 1. As the *while* loop stops when the number of iterations has exceeded the level, DHA statically exceeds this threshold with a smaller value than IIMSA. However, this behavior disappears when  $L$  increases. Indeed, in this case, the *while* loop is more likely to stop because the minimum has been found. Thus, the previous small scale behavior is not dominant anymore. This pattern holds true for all mixed classical algorithms (ZF and DHA).

In addition, it is worth noting that among all code types, Bipolar exhibits a higher success probability ( $P_s$ ) in the high  $L_{max}$  regime when compared to the others, reaching a maximum of  $P_s = 0.88$ . In contrast, Gaussian has a lower success probability, with  $P_s < 0.5$ , while Unipolar achieves a maximum of  $P_s = 0.7$ . This difference can be attributed to the fact that Bipolar code type has larger Euclidean distance  $\mathbf{C} \in \{-1, 1\}$ , leading to more accurate detections and lower

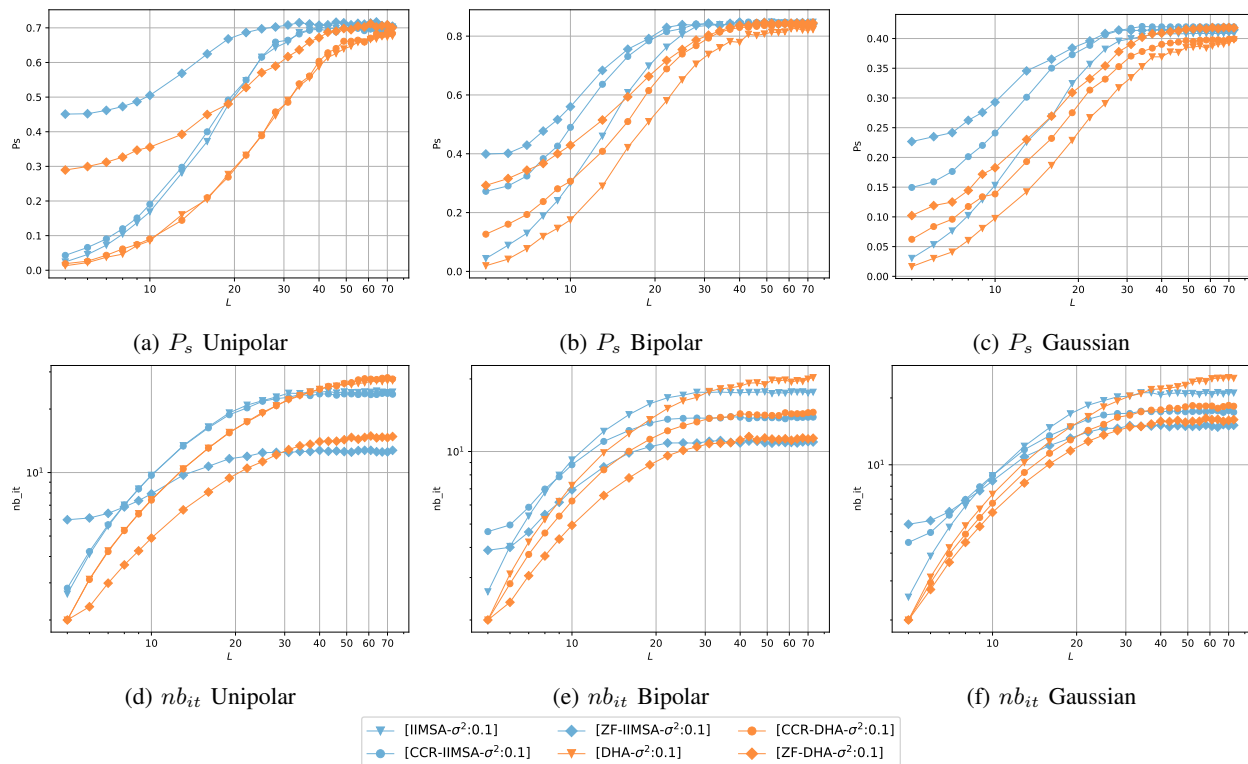


Fig. 8: Success Probability  $P_s$  and number of iterations  $nb_{it}$  w.r.t variance  $L_{max}$

susceptibility to noise contamination. This also applies to the required number of Grover's iterations ( $nb_{it}$ ), where Bipolar requires fewer  $nb_{it}$  compared to other code types. Indeed, the maximum  $nb_{it}$  reached by Bipolar is 18, while Unipolar and Gaussian achieve 29 and 25, respectively. This is due to the fact that, as Bipolar has a higher success probability compared to the other code types, the cases where  $L_{max}$  is reached are less frequent, thus reducing the number of iterations expectation.

As for the classical receiver contribution to the quantum algorithms, while CCR seems to struggle to compete with ZF, it exhibits a higher success probability ( $P_s$ ) compared to the original algorithm. This indicates that CCR contributes positively to the search algorithm initialization, leading to a smaller number of iterations ( $nb_{it}$ ) required for accurate detections. Consequently, CCR performs well and outperforms the original DHA and IIMSA.

Furthermore, it is important to emphasize the significant impact of the classical algorithm (ZF and CCR) in these results. These algorithms notably enhance both the success probability ( $P_s$ ) and the number of iterations ( $nb_{it}$ ). Specifically, for  $L > 20$ , the results demonstrate that ZF-IIMSA exhibits similar performance, but with a smaller  $nb_{it}$  compared to other methods. Following closely is ZF-DHA, which also demonstrates a considerable impact on  $nb_{it}$ . Thus, we can conclude that ZF serves as an excellent method for providing accurate initialization set for the quantum minimum searching algorithms.

To conclude, ZF (and CCR to a lesser extent) is an effective classical method, which permits, when combined with

quantum algorithms to achieve fewer Grover's iterations, while keeping (and even slightly improving) the success probability.

5) *IIMSA and DHA with a noisy quantum hardware*: In this section, we discuss the impact of noisy quantum processors on the performance and the complexity. To evaluate this impact, we modelize the noise effects with the total depolarizing channel (TDCh) [21].

In this model, the current state  $\rho$  is mapped to a maximally mixed state (corresponding to a uniform superposition of all basic states) with probability  $\lambda$  and leaves it unchanged with probability  $1 - \lambda$ .

To assess the performances, we have considered a system with  $\sigma = 0.1$  and  $SF = 6$ . We have evaluated the success probability as a function of the number of the allowed iterations  $L \in \{1, \dots, L_{max}\}$ , where  $L_{max} = 22.5\sqrt{2^N}$ . In addition, we have considered 3 different TDCh coefficients  $\lambda \in \{0, 0.05, 0.1\}$  for both IIMSA and DHA. One may note that the case where  $\lambda = 0$  corresponds to the perfect case as considered in the previous section for reference.

The results are presented on Fig.9.

First, we can observe, as expected, that the noisy quantum hardware tends to reduce the performances of the algorithms, for all types of codes. However, for the DHA, Fig.9a-9f, one can identify 2 main regions. When  $L$  is low, the noisy hardware has neglectible or no impact on the performances, meanwhile, high  $L$  suffer from higher impact. Contrarily, for the IIMSA, Fig.9g-9l, the effect can be observed for the whole range of  $L$  values. This can be explained by the fact that DHA does not rely on any prior information on the number of solutions within each Grover's iteration. Thus, it blindly

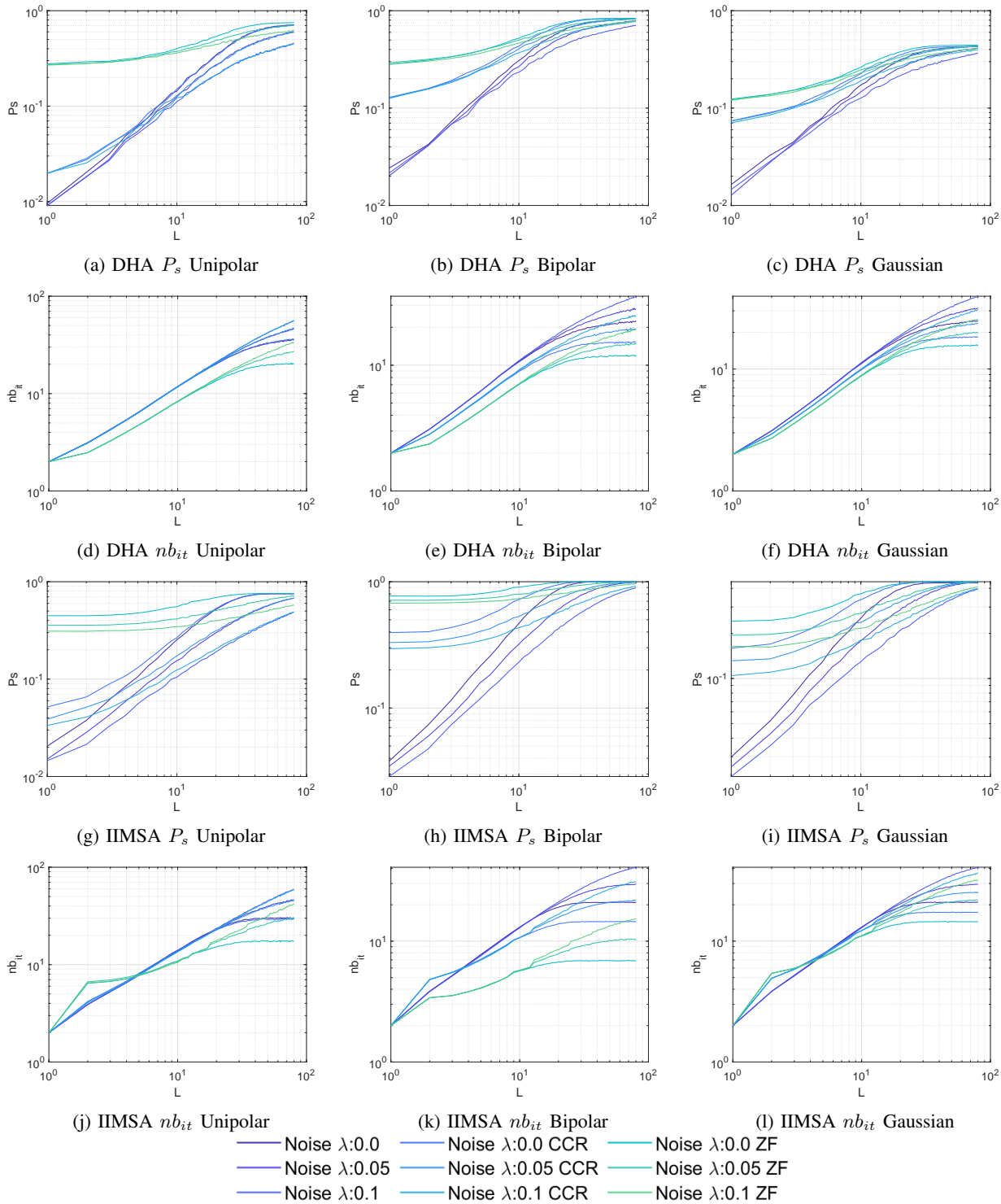


Fig. 9: Performances of DHA and IIMSA on noisy quantum hardware

tests with random chosen values for  $S$ . This approach implies that  $S$  is not always adequate and Grover's algorithm does not provide a valid solution. This happens quite frequently and is important compared to missing a valid solution due to the TDCh noise, especially when  $L$  is low and does not permit to do many trials. On the contrary, IIMSA considers an appropriate number of solutions, and is thus more efficient for each Grover's iteration. Thus, the TDCh errors always have an impact compared to the noiseless case.

In addition, we can observe that, even with the noisy hardware consideration, the IIMSA still outperforms DHA. Similarly, the figures show that initializing the algorithms with CCR or ZF output is still an efficient strategy. Indeed, the noise errors does not change the fact that the accurate initialization and parametrization of Grover's algorithm permits to efficiently target the search, leading to better success probability and lower number of iterations. To conclude, this study shows that, even deployed on a noisy hardware, the ZF-IIMSA is a very promising algorithm.

## VI. CONCLUSION

In this paper, we proposed adaptation and extensions of Grover's algorithm for the active user detection problem. Existing algorithms like DHA can address this kind of problem, but with still a non-neglectible level of complexity. First, we proposed a new algorithm, IIMSA, which exploits the statistical behavior of the system to evaluate the number of solutions. The IIMSA algorithm demonstrated superior performance compared to DHA, particularly in high  $SF$  regimes.

Furthermore, to enhance the performance of DHA and IIMSA, we exploited classical methods such as CCR and ZF to initialize the quantum search criteria in a more accurate way. With this improvement, we were able to reduce the number of iterations required for Grover's algorithm to start at a smaller  $L_{IIMSA}$  value, without degrading the performances (even improving them slightly). Besides, we showed that the gain brought by these light classical computations is increased for high  $SF$  regimes. Thus, this is a promising approach for dense IoT networks. We obtained these interesting results for perfect hardware, but we also showed that this gain is maintained for a noisy quantum hardware deployment. However, one may note that error mitigation strategies could be implemented on top of this algorithm. This will be the next step of this work.

## REFERENCES

- [1] R. C. Kizilirmak, "Non-orthogonal multiple access (noma) for 5g networks," in *Towards 5G Wireless Networks*, H. K. Bizaki, Ed., Rijeka: IntechOpen, 2016, ch. 4. DOI: 10.5772/66048. [Online]. Available: <https://doi.org/10.5772/66048>.
- [2] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jäntti, and Z. Han, "Spectral efficiency optimization for next generation noma-enabled iot networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 284–15 297, 2020. DOI: 10.1109/TVT.2020.3038387.
- [3] S. Wu and Y. Shin, "User Activity Detection for mmWave Grant-free IoT Networks," in *Asia Pacific Conference on Communications*, IEEE, 2022, ISBN: 9781665499279. arXiv: 1312.6114.
- [4] N. H. Mahmood, R. Abreu, R. Böhnke, M. Schubert, G. Berardinelli, and T. H. Jacobsen, "Uplink grant-free access solutions for urllc services in 5g new radio," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, 2019, pp. 607–612.
- [5] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*, 1st ed. Springer Publishing Company, Incorporated, 2008, ISBN: 0387765425.
- [6] G. Xue, J. Weng, T. Le-Ngoc, and S. ene Tahar, "Multiuser Detection Techniques : An Overview 1," no. December, 2013.
- [7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, Jun. 1998.
- [8] C. Durr and P. Hoyer, "A quantum algorithm for finding the minimum," 1996.
- [9] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 990–1000, 2014, ISSN: 00906778. DOI: 10.1109/TCOMM.2014.012514.130615.
- [10] M. I. Habibie, J. Hamie, and C. Goursaud, "Adaptation of grover's quantum algorithm to multiuser detection in an ocdma system," in *2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT)*, 2021, pp. 88–93.
- [11] M. I. Habibie, J. Hamie, and C. Goursaud, "A performance comparison of classical and quantum algorithm for active user detection," in *2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC)*, 2022, pp. 1–5.
- [12] N. I. Masaya Norimoto, *A numerical study of quantum speedup for maximum likelihood detection of power-domain noma*, 2023.
- [13] Q. Xiang, Y. H. Kho, W. K. G. Seah, Y. Tian, R. Fang, and P. Huang, "Quantum Approximate Optimization Algorithm for PD-NOMA User Pairing," in *IEEE International Conference on Communications*, May 2023. DOI: 10.1109/ICC45041.2023.10279755.
- [14] Y. Chen, S. Wei, X. Gao, C. Wang, J. Wu, and H. Guo, *An optimized quantum maximum or minimum searching algorithm and its circuits*, 2019. arXiv: 1908.07943 [quant-ph].
- [15] S. Mondal, M. R. Laskar, and A. K. Dutta, "MI criterion based signal detection of a mimo-ofdm system using quantum and semi-quantum assisted modified dha/bbht search algorithm," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1688–1698, 2021. DOI: 10.1109/TVT.2021.3055537.
- [16] E. V. Rogozhnikov, K. V. Savenko, A. K. Movchan, and E. M. Dmitriyev, "The study of correlation receivers," in *2019 20th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 2019, pp. 155–159.
- [17] K. He, Z. Wang, D. Li, F. Zhu, and L. Fan, "Ultra-reliable mu-mimo detector based on deep learning for 5g/b5g-enabled iot," *Physical Communication*, vol. 43, p. 101 181, 2020, ISSN: 1874-4907. DOI: <https://doi.org/10.1016/j.phycom.2020.101181>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1874490720302585>.
- [18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.
- [19] H.-C. Cheng, E. Wijanto, T.-C. Lien, P.-H. Lai, and S.-P. Tseng, "Multiple access techniques for bipolar optical code division in wireless optical communications," *IEEE Access*, vol. 8, pp. 83 511–83 523, 2020. DOI: 10.1109/ACCESS.2020.2991071.
- [20] D. Duchemin, L. Chetot, J.-M. Gorce, and C. Goursaud, "Coded random access for massive mtc under statistical channel knowledge," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications*

(SPAWC), 2019, pp. 1–5. DOI: 10.1109/SPAWC.2019.8815491.

- [21] I. Cohn, A. L. F. de Oliveira, E. Buksman, and J. G. L. de La-calle, “Grover’s search with local and total depolarizing chan-nel errors,” *International Journal of Quantum Information*, vol. 14, no. 02, p. 1650009, Mar. 2016, ISSN: 0219-7499, 1793-6918. DOI: 10.1142/S021974991650009X. [Online]. Available: <http://arxiv.org/abs/1508.03302>.

## VII. BIOGRAPHY



**Muhammad Idham Habibie** (Student Member, IEEE) completed his undergraduate degree at Uni-versity of Indonesia (UI) in 2013. He obtained his MSc. degree from the University College London (UCL) in United Kingdom carried in industry at Cobham Wireless, UK in 2017. He is currently a Ph.D. student in Institut National des Sciences Appliquées de Lyon (INSA) Lyon under the su-pervision of Claire Goursaud. He published several articles related to Quantum communication, Grover’s algorithm. His research interests include quantum

computation, quantum algorithms and quantum active user detection.



**Claire Goursaud** (Member, IEEE) received the Ph.D. degree in high frequency and optical telecom-munications from the University of Limoges, in 2006, working on signal processing for optical communications. In September 2007, she joined the INSA de Lyon (Institut National des Sciences Appliquées), as an Assistant Professor with the Telecommunication Department and the CITI Labo-ratory. She has published over 60 refereed journal and conference papers, and is an associate editor of two international journals. Her research interests

include massive multiple access for wireless networks, and particularly the use of quantum algorithms and SNN architecture to tackle the signal processing challenge.



**Jihad Hamie** (Member, IEEE) completed his Master degree in Signal, Image, Embedded System and au-tomatic (SISEA) in Telecom Bretagne, Brest-France in 2010. He obtained his Ph.D degree working with CEA-Leti and University of Nice Sophia Antipolis. He also had an experience as research engineer at Telecom ParisTech in the Laboratory of Information, Networking and Communication Sciences (LINCS), Paris, France. Between 2016 and 2020, he was a an assistant professor in the computer engineering department at the AUL university in Lebanon. Then,

Mr. Hamie occupied a position of an assistant professor at INSA Lyon (France) between 2020 and 2022. His main research interests are about the Wireless Sensor Networks (WSN), localization, WBANs, Internet of Things (IoT), the quantum communication, and quantum algorithms for the signal processing areas.