Impact of the malicious input data modification on the efficiency of quantum algorithms

Adam Glos¹,²* and Jarosaw Adam Miszczak¹†

¹Institute of Theoretical and Applied Informatics, Polish Academy of Sciences
Baltycka 5, 44-100 Gliwice, Poland
²Institute of Informatics, Silesian University of Technology,
Akademicka 16, 44-100 Gliwice, Poland
(Dated: 27/02/2017)

In this paper we demonstrate that the efficiency of quantum algorithms can be significantly altered by malicious manipulation of the input data. We exemplify the possibility of attacks on quantum spatial search based on Szegedy walk. We achieve this by proposing a framework suitable for analysing efficiency of attacks on quantum search algorithms. We provide the analysis of proposed attacks for different models of random graphs.

PACS numbers: 03.67.Ac; Keywords: quantum spatial search; exceptional configurations; cyberattacks; quantum hacking

INTRODUCTION

Motivation While the intensive research effort invested in the area of quantum computing is fully justified by groundbreaking theoretical developments [1–3], year by year scientists have discovered new limitations of quantum computing devices [4]. Quantum algorithms have been proved to be susceptible to noise, which may falsify the results of the computation. This fact motivated the development of the theory of quantum error-correcting codes, a new branch of quantum computing. Moreover, unitary operation decomposition provides numerous problems including applications to hardware with fixed topology [5]. These aspects started to play an even more critical role after first commercial quantum computing systems became available. Furthermore, hardware attacks, based on the security holes of conventional electronics, have been discovered for quantum cryptographic protocols [6]. The issues mentioned above demonstrated that the theoretical security confirmed by the laws of physics in the ideal environment could be deceptive in the real-world applications. For the users it is important to be aware that quantum algorithms are inefficient for some types of input data. One of such examples is quantum spatial search, which is inefficient on 2D grid [1]. This case demonstrates that the quantum algorithms are not only unsuitable for some types of problems, but, even for generally optimal quantum algorithms [7], it is possible to construct input data rendering them slow.

These examples show that, while quantum algorithms may be a milestone in computational theory, their realizability and security still need to be carefully checked. From the computational complexity point of view, it remains unknown whether the existing quantum algorithms can provide the speed-up promised by the theoretical results, especially when applied to large datasets. On the other hand, the ability to describe the types of data which render quantum algorithms ineffective can be used to develop post-quantum protocols.

Contribution The main aim of the presented work is to demonstrate that the efficiency of quantum algorithms can be significantly diminished by malicious manipulation of the input data.

Let us consider a classical algorithm QuickSort. The algorithm achieves average-case performance $O(n \log(n))$, where $n$ is the number of elements. However, for simple fixed pivot choice, one can provide malicious input data, which increase computation time up to $O(n^2)$. If no security is considered, choosing such data may considerably increase the computational resources required for running the algorithm. If the computer processes such data, this may result in denial-of-service. Fortunately, there are known solutions to this problem, for example, choosing pivot randomly or searching for it using the median of medians algorithm.

Similar problems arise in the quantum spatial search, which can be based on different models of quantum walks. For the continuous-time quantum walk, the algorithm works very well and securely on many graphs [7–9], achieving efficiency $O(\sqrt{n})$, where $n$ is the graph order. However, there are known examples, such as a two-dimensional grid, for which the algorithm reaches linear complexity only [1]. While the grid graph can be searched much faster for the discrete coined quantum walk, it is known that specific subgraphs of the searched graphs can form so-called exceptional configurations [10] which strongly reduce the efficiency.

In this paper we consider the formation of exceptional configurations as a method of attacking quantum algorithms. We propose a framework enabling the analysis of the attack efficiency based on the expected runtime of the algorithm. We utilize this framework for selected families of random graphs. We take into account different resources available for the attacker.
PRELIMINARIES

Let $G = (V, E)$ be an undirected graph and let $S \subseteq V$ be a set of searched vertices. A quantum spatial search algorithm is a quantum walk, which after $t$ steps finds any marked $v \in S$ with probability $p$. While the classical spatial search is known to have time complexity $\Omega(n)$, it is possible to achieve $\Theta(\sqrt{n})$ for quantum algorithms \cite{1,7,11}. The complexity may depend on a chosen graph \cite{12} or a chosen set $S$ \cite{12}.

Szegedy quantum walk (SzQW) \cite{13,14} is a general quantum walk definable on an arbitrary directed graph. Let $P$ be a graph-preserving stochastic operation. Here, the state of the system $|\psi_t\rangle$ belongs to $\mathcal{H}^G_A \otimes \mathcal{H}^C_B$ system. Let

$$|\phi_v\rangle = \frac{1}{\sqrt{\deg(v)}} |v\rangle \otimes \left( \sum_{w \in N(v)} \sqrt{\langle v|P|w\rangle} |w\rangle \right), \quad (1)$$

$$|\psi_v\rangle = \frac{1}{\sqrt{\deg(v)}} \left( \sum_{w \in N(v)} \sqrt{\langle v|P|w\rangle} |w\rangle \right) \otimes |v\rangle. \quad (2)$$

Furthermore, let

$$R_1 = 2 \sum_{v \in V} |\phi_v\rangle \langle \phi_v| - I, \quad R_2 = 2 \sum_{v \in V} |\psi_v\rangle \langle \psi_v| - I \quad (3)$$

$$Q_1 = (I - 2 \sum_{v \in S} |v\rangle \langle v|) \otimes I, \quad Q_2 = I \otimes (I - 2 \sum_{v \in S} |v\rangle \langle v|). \quad (4)$$

The evolution takes the form

$$|\psi_{t+1}\rangle = R_2 Q_2 R_1 Q_1 |\psi_t\rangle, \quad (5)$$

and the initial state reads

$$|\psi_0\rangle = \frac{1}{\sqrt{|V|}} \sum_{v,w \in V} \sqrt{\langle v|P|w\rangle} |v,w\rangle. \quad (6)$$

The success probability equals

$$p_{S,t} = \sum_{v \in S} |\langle v|\text{Tr}_B(|\psi_t\rangle \langle \psi_t|)|v\rangle|^2, \quad (7)$$

where $\text{Tr}_B$ is the partial trace on subsystem $B$. In this paper we consider $P_v$ representing a uniform random walk.

For another quantum walk, discrete coined quantum walk (DCQW), the search problem with multiple marked vertices can be a hard task for some combinations of marked vertices, known as exceptional configurations \cite{10,12,15}. The existence of an exceptional configuration is demonstrated in two steps. First, the existence of a special stationary state needs to be shown. Second, a bound on the probability needs to be determined, based on the stationary state. Recently, the class of connected subgraphs having the stationary state has been described, which solves the first step.

**Theorem** \cite{10}. Let $G = (V_G, E_G)$ be an arbitrary graph. Let $H \subseteq G$ be connected $(V'_H, V''_H)$-bipartite subgraph. Then $H$ contains a stationary state iff it satisfies

$$\sum_{v \in V'_H} \deg_G(v) = \sum_{v \in V''_H} \deg_G(v), \quad (8)$$

where $\deg_G$ is the degree in graph $G$. If $H$ is not bipartite, then it contains a stationary state.

The exceptional configuration of order 2 (2EC) is a path of length 2, such that the degrees of vertices in the original graph $G$ are equal. The exceptional configuration of order 3 (3EC) is a triangle graph, or a path of length 3, such that the degree of the middle vertex equals the sum of the degrees of the end vertices in the original graph $G$. Wong has shown the equivalence between coined and Szegedy models \cite{14}, hence we are going to focus on the latter, as it is more suitable for numerical analysis.

FRAMEWORK FOR QUANTIFYING THE EFFICIENCY OF ATTACKS

For the purpose of quantifying the efficiency of attacking methods, we introduce the formal description of the family of quantum spatial search algorithms.

**Definition.** Quantum Spatial Search (QSS) is a tuple $(\text{Alg}, t; G, S, \theta)$, where $\text{Alg}$ is a quantum algorithm searching for any vertex $v \in S$ in time $t$, running on graph $G$, and parametrized by the set of parameters $\theta$.

By $p(QSS)$ we denote the success probability of QSS. Note that we do not define $\theta$ precisely, as it depends on the chosen algorithm $\text{Alg}$. For example, for coined quantum walk $\text{Alg} = \text{DCQW}$, the parametrization consists of the set of coin operators. For $\text{Alg} = \text{SzQW}$, the parametrization is the chosen stochastic operation $P$.

In order to compare different quantum spatial search algorithms we propose the following measure of efficiency.

**Definition.** Expected runtime $T_{QSS}$ of quantum spatial search $QSS = (\text{Alg}, t; G, S, \theta)$ is defined as

$$T_{QSS} := \frac{t}{p(QSS)}. \quad (9)$$

The expected runtime is an expectation of the number of steps after which we get the result using Bernoulli process. Such approach has been used in \cite{1,11}, where the complexity was analysed.

Using the formalised description of quantum spatial search algorithms, we can introduce the concept of attack on an algorithm as follows.

**Definition.** Attack on QSS is a function $h$ such that

$$h(\text{Alg}, t; G, S, \theta) = (\text{Alg}, t; G', S', \theta'). \quad (10)$$
It should be stressed that the attack cannot change the evolution model and measure time of QSS. Still we will consider the function altering only some of the elements of QSS. For example, the attacks restricted to graph structure imply that $S = S'$ and $\theta = \theta'$.

If we allow QSS element to be changed, then we will say the element is hackable. Otherwise, it is not hackable. Note that by definition Alg and $t$ are not hackable.

To quantify the efficiency of the attacks we introduce attack efficiency as follows.

**Definition.** Attack efficiency $\text{eff}_{h,\text{QSS}}$ on QSS is defined as

$$\text{eff}_{h,\text{QSS}} := 1 - \frac{T_{\text{QSS}}}{T_{h(\text{QSS})}}. \quad (11)$$

We are interested in such functions $h$ that $\text{eff}_{h,\text{QSS}} \geq 0$. Furthermore, since $t$ is common for both QSS and $h(\text{QSS})$ we have

$$\text{eff}_{h,\text{QSS}} = 1 - \frac{p(h(\text{QSS}))}{p(\text{QSS})}. \quad (12)$$

Let us consider the following scenario. The user is trying to start an algorithm QSS, but the attacker has changed it into QSS'. If the user is aware of the attack and its nature, he can alter the measurement time $t$ in order to minimize the expected runtime. To describe this situation we introduce strong attack efficiency.

**Definition.** Suppose we have $\text{QSS} = (\text{Alg},t;G,S,\theta)$ and $h : \text{QSS} \mapsto (\text{Alg},t;G',S',\theta')$. Strong attack efficiency $\overline{\text{eff}}_{h,\text{QSS}}$ is defined as

$$\overline{\text{eff}}_{h,\text{QSS}} := 1 - \frac{T_{(\text{Alg},t;G,S,\theta)}}{\min \tau \geq 0 T_{(\text{Alg},t;G',S',\theta')}}. \quad (13)$$

This definition captures the best possible defence against the attack.

All of the above definitions were restricted to the fixed spatial search algorithm. Since our aim is to analyse the efficiency of attacks on more general graph classes, we extend the previously defined terms.

**Definition.** Let $Q$ be a set of quantum spatial searches and $h$ be an attack on $Q$. Then maximal attack efficiency on $Q$, $\text{eff}_{h,Q}$, is defined as

$$\text{eff}_{h,Q} := \max_{\text{QSS} \in Q} \text{eff}_{h,\text{QSS}}. \quad (14)$$

Similarly, maximal strong attack efficiency on $Q$, $\overline{\text{eff}}_{h,Q}$, is defined as

$$\overline{\text{eff}}_{h,Q} := \max_{\text{QSS} \in Q} \overline{\text{eff}}_{h,\text{QSS}}. \quad (15)$$

The above definition captures the pessimistic level of robustness against the attack. Similarly, we can define the mean and minimal efficiencies. In practice, we would like to find the dependence between the efficiency and the order of the graph.

Instead of providing deterministic $Q_n$, we will focus on $Q_n$ defined by random graph models $G_n$.

**Definition.** Let $G_n$ be a random graph model, and let for arbitrary $G$ exist a quantum spatial search $QSS(G) = (\text{Alg},t(G);G,S(G),\theta(G))$. Let $h$ be an attack defined on QSS. We say that the efficiency of the attack is almost surely at least $E_n$ iff

$$\mathbb{P}(\text{eff}_{h,\text{QSS}(G)} \geq E_n | G \in G_n) \xrightarrow{n \to \infty} 1. \quad (16)$$

The above definition can be naturally applied to strong efficiency.

**ATTACKS ON QUANTUM SPATIAL SEARCH ALGORITHMS**

We will consider the attacks altering the set of marked vertices only. For quantum spatial search (SzQW, $t;G,\{v\},P_u$), we add marked vertices in such a way that the newly generated set $S' \supset \{v\}$ forms a connected exceptional configuration. As the probability of finding any vertex from EC is much lower than the probability of finding a single marked vertex [10], we decrease the success probability of the algorithm.

Suppose that the algorithm outputs a vertex from $S' \setminus \{v\}$. Since we choose additional marked vertices from close neighbourhood of the original marked vertex $v$, the possible defence against the attack is to make a simple classical search over its neighbourhood, which is efficient for sparse graphs. However, the cumulated success probability of measuring any of $S'$ is small. Hence, the attack is effective.

Let us analyse Erdős-Rényi, Watts-Strogatz, and Barabási-Albert models. For Erdős-Rényi we choose the probability of adding edge $p = \frac{2 \log (n)}{n}$, for Watts-Strogatz we select initial degree $K = \lceil 2 \log n \rceil$ and randomness $\beta = 0.5$ [17], and for Barabási-Albert we set attachment parameter to $m_0 = 3$ [18] [19]. First, we analyse the probability of attacking a random vertex. Next, we analyse its efficiency.

Numerical results demonstrate that for every vertex of Watts-Strogatz graph we can almost surely find an exceptional configuration of order 3 (3EC), see Fig. 1(a). Thus the model can be attacked almost surely for any vertex. This is no longer the case when we allow constructing an exceptional configuration of order 2 only. For Erdős-Rényi and Barabási-Albert models, even 3EC will not provide this kind of advantage for the attacker. Nevertheless, the probability of attacking is still large, and the attacker may be able to construct an exceptional configuration of a higher order.

Another constraint for resources available to the attacker is the distance between the originally marked ver-
FIG. 1. Probability of forming an exceptional configuration with a random vertex for different models of random graphs. (a) Probability of forming 2EC vs probability of forming arbitrary 2,3-EC, i.e. EC of order 2 or 3. (b) Probability of forming arbitrary EC of order 2 or 3 (2,3-EC global) vs probability of forming EC of order 2 or 3 by adding vertices from direct neighbourhood of originally marked vertex (2,3-EC local).

FIG. 2. Attack efficiency and strong attack efficiency for random graph models. Pairs of vertices were chosen at random from the collection of all 2EC. Left plots present the efficiency (the case of unchanged measurement time). Right plots present the strong efficiency (the case with measurement time chosen optimally). While Erdős-Rényi and Watts-Strogatz present similar results, one can observe more robust behaviour for Barabási-Albert model.

In order to assess the impact of the attack on the complexity of quantum spatial search we have calculated the expected runtime for three cases for each random graph.

most equal degrees [20]. This makes finding path graph 3EC impossible, as degree condition from Preliminaries section cannot be fulfilled. We have not observed any dependence for Watts-Strogatz model (see Fig. 1(b)).

For analysing the efficiency of the attack, we have chosen at random two vertices forming an exceptional configuration. We have analyzed 50 graphs for each order \( n = 100, 150, \ldots, 2400 \) for all models, using the optimization algorithm implemented in QUANTUMWALK package [21] with penalty time \( t_{\text{pen}} = \lceil \log(n) \rceil \). Parameter \( t_{\text{pen}} \) is a value which is added to the time, thus changing the expected time into \((t + t_{\text{pen}})/p\). Such adjustment prevents the optimization algorithm from halting at small time. Since \( \log(n) \) is typically much smaller than \( t \), its impact on our results is negligible.
Numerical results presented in Fig. 2 show that the complexity attack should result in the algorithm complexity growth, we have determined numerically the expected time change in the case of common measurement time. The results are presented in Fig. 3. We have assumed that the complexity grows as the power complexity, $\Theta(n^\alpha)$. The tangent of the regression line of the expected run-time in the function of the graph order on the log-log scale provides the approximation of the parameter $\alpha$. The observed growth of the values of $\alpha$, resulting from the attack, demonstrates that the attacker is able to significantly increase the expected run-time of the quantum algorithm. This suggests that the algorithm is vulnerable to the complexity attack, which might result in the denial-of-service of the quantum computer.

SUMMARY AND DISCUSSION

In this paper we have signified the problem of possible vulnerability of quantum algorithms to the complexity attacks. The presented approach is based on the analysis of input data. As such it can be used to discover weaknesses of quantum computers resulting from the application of quantum algorithms on input data unsuitable for processing on quantum machines. This is contrast to the common approach where only the theoretical computational complexity is taken into account.

We have developed the theoretical framework for quantifying the efficiency of the attacks. We have constructed an attack based on exceptional configurations and analysed it in the context of its applicability and efficiency. The analysis confirms that it is possible to decrease the efficiency of quantum spatial search based on Szegedy walk by malicious modification of input data.

One should note that the presented results can be applied for a general class of graphs. This is in contrast to the results from [10], where only special classes of graphs were considered. For those classes it can be shown analytically that the algorithm complexity changes from $\Theta(\sqrt{n})$ to $\Theta(n)$.

It should be stressed that the models of random graphs used for assessing the security of quantum algorithms mimic the structure of real-world data [19]. As such the presented analysis confirms that the theoretical security of quantum procedures can be inadequate when the algo-
Algorithms are applied for specific input data. This includes input data which encode the connections observed in complex networks.

The authors would like to thank Nikolay Nahimov for discussion concerning exceptional configurations and Alexander Rivosh for inspiring the application of this concept in quantum spatial search. This work has been partially supported by Polish National Science Center grant 2011/03/D/ST6/00413. Numerical calculations were possible thanks to the support of PL-Grid Infrastructure.

\* Corresponding author; aglos@iitis.pl
\† miszczak@iitis.pl

[1] A. M. Childs and J. Goldstone, Phys. Rev. A 70, 022314 (2004).
[2] A. W. Harrow and A. Montanaro, Nature 549, 203 (2017).
[3] D. J. Bernstein and T. Lange, Nature 549, 188 (2017).
[4] R. Van Meter and C. Horsman, Communications of the ACM 56, 84 (2013).
[5] M. Saeedi, R. Wille, and R. Drechsler, Quantum Inf. Process. 10, 355 (2011).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Malyarov, Nat. Photonics 4, 686 (2010).
[7] S. Chakraborty, L. Novo, A. Ambainis, and Y. Omar, Phys. Rev. Lett. 116, 100501 (2016).
[8] S. Chakraborty, L. Novo, S. Di Giorgio, and Y. Omar, Phys. Rev. Lett. 119, 220503 (2017).
[9] A. Glos, A. Królewski, R. Kukulski, and Z. Puchała, Quantum Inf. Process. 17, 81 (2018).
[10] N. Nahimovs and R. A. Santos, in SOFSEM 2017: Theory and Practice of Computer Science, LNCS, Vol. 10139 (2017) pp. 256–267, arXiv:1605.05598.
[11] A. Ambainis, J. Kempe, and A. Rivosh, in Proc. 16th ACM-SIAM SODA (2005) pp. 1099–1108, arXiv:quant-ph/0402107.
[12] N. Nahimovs and A. Rivosh, in International Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (Springer, 2015) pp. 79–92.
[13] M. Szegedy, in Proc. FOCS 2004 (IEEE, 2004) pp. 32–41.
[14] T. G. Wong, Quantum Inf. Process. 16, 215 (2017).
[15] N. Nahimovs, R. Santost, and K. Khadiev, (2017), arXiv:1710.04046.
[16] K. Prusis, J. Vihrovs, and T. G. Wong, Phys. Rev. A 94, 032334 (2016).
[17] D. J. Watts and S. H. Strogatz, Nature 393, 440 (1998).
[18] A.-L. Barabási and R. Albert, Science 286, 509 (1999), http://science.sciencemag.org/content/286/5439/509.full.pdf.
[19] R. Albert and A.-L. Barabási, Rev. Mod. Phys. 74, 47 (2002).
[20] B. Bollobás, Cambridge Studies in Advanced Mathematics, 2nd ed., Modern Graph Theory (Cambridge University Press, 2001).
[21] Code available at https://github.com/QuantumWalks/QuantumWalk.jl.