On iterated punctured Grover

Cezary Pilaszewicz[1*] and Marian Margraf[1†]

[1*]Department of Mathematics and Computer Science, Freie Universität Berlin, Takustr. 9, Berlin, 14195, Germany.

*Corresponding author(s). E-mail(s): cezary.pilaszewicz@fu-berlin.de;
Contributing authors: marian.margraf@fu-berlin.de;
†These authors contributed equally to this work.

Abstract

Grover's algorithm is a very versatile cryptanalytical tool. Even though it doesn't provide an exponential speed-up, it still changed the cryptographic requirements all over the world. Usually, Grover's algorithm is executed with a fixed well-defined function indicating good states. In this paper, we want to investigate what happens if the function is changed over time to mark less and less good states. We compute the amplitudes after $\mathbf{2^{s/2}}$ steps of an adjusted Grover's algorithm proposed by Zheng et al. in *Nested Quantum Search Model on Symmetric Ciphers and Its Applications (2023)*. We use the amplitudes to reason that such an approach always leads to a worse run-time when compared to the naïve version. We also indicate at which point in Zheng et al. the counterintuitive nature of quantum computation leads to false assumptions.

Keywords: Grover's algorithm, quantum computation, cryptanalysis

1 Introduction

When discussing the power of quantum computers, Grover's algorithm is often treated as an obvious argument to double the key length. The premise, no matter how strong, is simple enough that very little research is conducted in this area. This is even more amplified by the proofs of optimality of Grover's algorithm [2]. This, and the esoteric nature of quantum computation, can often lead to wrong assumptions about its runtime. In this paper, we want to investigate why intuitive arguments fail when discussing Grover's speed-up.

The inspiration for this paper was a publication by Zheng et al. [1]. They suggested an iterated (nested) approach, where for a set of punctured ciphertexts $(z_1, z_2, ..., z_r)$, one investigates the sets of keys $K_1, K_2, ..., K_r$ such that $K_i = \{k : f_i(k) = z_i \wedge k \in K_{i-1}\}$. In this case, a punctured ciphertext is a string created by projecting the ciphertext onto a subset of its bits. One can also consider what changes when we define K_i as $K_i = \{k : f_i(k) = z_i\}$, we will shortly mention this case in section 4. The idea is to begin with a whole key space $K_0 = \{k \in \{0,1\}^n\}$ and start searching for the consecutive key sets using oracles $\mathcal{O}_{z_i}$:

$$K_0 \xrightarrow{\mathcal{O}_{z_1}} K_1 \xrightarrow{\mathcal{O}_{z_2}} K_2 \xrightarrow{\mathcal{O}_{z_3}} ... \xrightarrow{\mathcal{O}_{z_r}} K_r$$

Since for all $i : K_{i+1} \subset K_i$, for a good encryption function the sets will usually drop keys at a constant rate depending on the size of the punctured ciphertext. In fact, for an s-long punctured ciphertext, each round finds $|K_i|$ out of $|K_{i-1}|$ keys with $\frac{|K_{i-1}|}{|K_i|} = 2^s$. The assumption then is that this search with Grover would require $\sqrt{2^s}$ steps. For $r := n/s$ with high probability, K_r consists of a single key that delivers a correct punctured ciphertext for all $i = 1, ..., r$. This results in a runtime of $\sqrt{2^s} \cdot n/s$, which if s is chosen to be 1, gives us polynomial runtime of $n\sqrt{2}$.

We will investigate where the above reasoning founders. The pivotal point is that although at step i, we start the search in a state $|\phi\rangle = \frac{1}{\sqrt{|K_{i-1}|}} \sum_{k \in K_{i-1}} |k\rangle$, the following Grover's steps reintroduce all the keys from $K_0 \setminus K_{i-1}$. Therefore, we do not search in key space of size $|K_{i-1}|$ but in K_0 with non-uniform amplitudes. We will also prove that the resulting non-uniform distribution results in a need for more Grover's algorithm steps.

2 Notation

Let $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be an encryption function with

$$E : (k, p) \mapsto c.$$

Further, for a fixed plaintext-ciphertext pair (P, C), define $F : \{0,1\}^n \to \{0,1\}^n$ with

$$F(k) = E(k, P)$$

and for some index-set $\mathcal{I}$:

$$F_{\mathcal{I}}(k) = \Big(E(k, P)\Big)|_{\mathcal{I}}.$$

In this case $x|_{\mathcal{I}}$ is a projection of x on the bits in $\mathcal{I}$. We are interested in finding a key k' such that $F(k') = C$. This also implies that for any $\mathcal{I} \subseteq \{1, 2, ...n\}$ $F_{\mathcal{I}}(k') = C_{\mathcal{I}}$.

2.1 Grover's algorithm and the iterated version

In this section, we will introduce the notation used for Grover's algorithm and its iterated version from [1]. The original algorithm consists of multiple identical *steps*, each of them consisting of 2 phases:

- for a function f we mark the states $|x\rangle$ which fulfil the clause $f(x) = 1$ using U_f:

  $$U_f |x\rangle |y\rangle = \begin{cases} |x\rangle |-y\rangle, & \text{if } f(x) = 1 \\ |x\rangle |y\rangle, & \text{otherwise,} \end{cases}$$

  and negate their amplitude.
- we apply Grover's diffusion operator.

In our setting the function f will be defined as:

$$f(k) = \begin{cases} 1, & \text{if } F(k) = C \\ 0, & \text{otherwise.} \end{cases}$$

Upon the last step, we can apply the U_f again and measure the second register. When $|-y\rangle$ is measured, we know that all the x values in the first register fulfil the clause f.

For iterated (nested) approach, the algorithm consists of multiple *iterations*. We need a set of punctured ciphertexts $(z_1, z_2, ..., z_r)$, these are valid ciphertexts projected to some subset of bits of the original ciphertext. These can be generated by one or multiple ciphertexts. We will assume they are generated from a single ciphertext (and therefore single plaintext) for the ease of notation, but this must not be the case.

In each iteration, we perform a classical Grover search for a changing function:

- choose an index i
- define U_{f_i} as

  $$U_{f_i} |x\rangle |y\rangle = \begin{cases} |x\rangle |-y\rangle, & \text{if } f_i(x) = 1 \\ |x\rangle |y\rangle, & \text{otherwise,} \end{cases}$$

  for f_i defined as:

  $$f_i(k) = \begin{cases} 1, & \text{if } F_{\mathcal{I}}(k) = z_i \wedge k \in K_{i-1} \\ 0, & \text{otherwise.} \end{cases}$$

  In this case, the $\mathcal{I}$ is a changing subset of bits of the ciphertext C dependent on i which was chosen.
- perform standard Grover search using U_{f_i}.

After sufficiently many steps are repeated, as in classical Grover, we can apply U_{f_i} again and measure the second register to get a distribution of all keys fulfilling the clause $|\phi\rangle = \frac{1}{\sqrt{|K_i|}} \sum_{k \in K_i} |k\rangle$. This concludes the i'th iteration and we move on to the next punctured ciphertext.

3 Comparison of amplitudes in two cases

In this section we will compare the behaviour of the amplitudes in the scenario described in [1] and standard Grover's algorithm. We will prove that a single iteration of the nested approach results in a worse amplitude distribution (needing more follow-up Grover's steps to land at a comparable state) than if we perform the same amount of steps immediately searching for the single correct key.

Let $\mathcal{I} \subseteq \{1, \ldots, n\}$ be a set with s elements. In this case $f_{\mathcal{I}}$ produces a punctured ciphertext of length s. Assume we want to search for a specific key, which maps to a punctured ciphertext $c_{\mathcal{I}}$. Let $K_{\mathcal{I}} := \{k \in K : f_{\mathcal{I}}(k) = c_{\mathcal{I}}\}$.

To find all the keys in $K_{\mathcal{I}}$ we would need $\sqrt{\frac{2^n}{2^{n-s}}} = 2^{s/2}$ steps of Grover's algorithm. In this case, Grover's clause would have the form $f_{\mathcal{I}}(k) = c_{\mathcal{I}}$ and after a measurement the resulting quantum state would be:

$$|\psi\rangle = \sqrt{\frac{1}{2^{n-s}}} \sum_{i \in K_{\mathcal{I}}} |i\rangle \,.$$

Now assume we want to find a specific key k' in $|\psi\rangle$. From [3] we know that the runtime of Grover's algorithm for arbitrary amplitude distribution depends **only** on the average amplitude of the "correct" and "incorrect" keys. In our scenario, the only correct key is k'. Let $\overline{k_{|\tau\rangle}}(t)$ be the average over amplitudes of correct keys at time t for quantum state $|\tau\rangle$, and analogously $\overline{l_{|\tau\rangle}}(t)$ be the average amplitude of the incorrect keys.

For the state $|\psi\rangle$ (achieved after $2^{s/2}$ steps of iterated Grover's algorithm) we have:

$$\begin{aligned}
\overline{k_{|\psi\rangle}}(2^{s/2}) &= 1 \cdot \sqrt{\frac{1}{2^{n-s}}} = \sqrt{\frac{1}{2^{n-s}}} \\
\overline{l_{|\psi\rangle}}(2^{s/2}) &= \frac{\left((2^{n-s}-1) \cdot \sqrt{\frac{1}{2^{n-s}}}\right) + \left((2^n - 2^{n-s}) \cdot 0\right)}{2^n - 1} \\
&= \frac{\frac{2^{n-s}}{\sqrt{2^{n-s}}} - \frac{1}{\sqrt{2^{n-s}}}}{2^n - 1} \\
&= \frac{\sqrt{2^{n-s}}}{2^n - 1} - \frac{1}{\sqrt{2^{n-s}}(2^n - 1)} \\
&\approx \frac{\sqrt{2^{n-s}}}{2^n}
\end{aligned}$$

The value of $\overline{l_{|\psi\rangle}}(2^{s/2})$ is computed as the average of the $2^{n-s} - 1$ incorrect keys in $K_{\mathcal{I}}$ each with amplitude $\sqrt{\frac{1}{2^{n-s}}}$, and the keys in $K_0 \setminus K_{\mathcal{I}}$ with amplitude 0.

Next, we want to compare this result with the state of the register if we would immediately start the search for k' instead of K_1 (this would correspond to performing standard Grover's search over the iterated approach). Let $|\phi\rangle$ be the state of the register after applying $2^{s/2}$ steps of Grover's algorithm with function f instead of $f|_{\mathcal{I}}$. The state at time t can be described as [4]:

$$|\phi_t\rangle = \sin\theta_t \, |k'\rangle + \cos\theta_t \Big(\sqrt{\frac{1}{2^n - 1}} \sum_{k \neq k'} |k\rangle \Big)$$

$$=: \sin\theta_t \left|k'\right\rangle + \cos\theta_t \left|k'^{\perp}\right\rangle,$$

with $\theta = \arcsin\frac{1}{\sqrt{2^n}}$. For small values, we know

$$\sin(x) \approx x, \tag{1}$$

so $\theta \approx \frac{1}{2^{n/2}}$. Further, $\theta_t = (2t+1)\theta$, so for $t = 2^{s/2}$ we have:

$$\begin{aligned}
\theta_{2^{s/2}} &= (2 \cdot 2^{s/2} + 1) \cdot \sqrt{\frac{1}{2^n}} \\
&= 2^{\frac{s-n}{2}+1} + \frac{1}{2^{n/2}} \\
&= \sqrt{\frac{1}{2^{n-s-2}}} + 2^{-n/2} \\
&= \sqrt{\frac{4}{2^{n-s}}} + 2^{-n/2}.
\end{aligned}$$

Using (1) we get:

$$\begin{aligned}
\overline{k_{|\phi\rangle}}(2^{s/2}) = \sin\theta_{2^{s/2}} &= \sin\left(\sqrt{\frac{4}{2^{n-s}}} + 2^{-n/2}\right) \\
&\approx \sqrt{\frac{4}{2^{n-s}}} + 2^{-n/2}.
\end{aligned}$$

This means that $\overline{k_{|\phi\rangle}}(2^{s/2}) > \overline{k_{|\psi\rangle}}(2^{s/2})$ resulting in the higher probability to measure k' in $|\phi\rangle$ than in $|\psi\rangle$ and less following iterations of Grover's algorithm to arrive at the desired state. Further, using Pythagorean trigonometric identity, we know:

$$\begin{aligned}
\cos\theta_{2^{s/2}} = \sqrt{1 - \sin^2\theta_{2^{s/2}}} &= \sqrt{1 - \left(\sqrt{\frac{1}{2^{n-s-2}}} + 2^{-n/2}\right)^2} \\
&\approx \sqrt{\frac{2^s \cdot 2^{n-s}}{2^n}}
\end{aligned}$$

and the average amplitude of an incorrect state is:

$$\begin{aligned}
\overline{l_{|\phi\rangle}}(2^{s/2}) &= \sqrt{\frac{1}{2^n}} \cdot \cos\theta_{2^{s/2}} \\
&\approx \sqrt{\frac{1}{2^n}} \cdot \sqrt{\frac{2^s \cdot 2^{n-s}}{2^n}} \\
&= \frac{\sqrt{2^{n-s}}}{2^n} \cdot \sqrt{2^s}.
\end{aligned}$$

This means $\overline{l_{|\phi\rangle}}(2^{s/2}) \approx \sqrt{2^s} \cdot \overline{l_{|\psi\rangle}}(2^{s/2})$. Counterintuitively this results in state $|\phi\rangle$ needing fewer Grover steps to arrive at the desired distribution. This is caused by the fact that the amplitudes follow the corresponding recurrence:

$$\begin{aligned}\overline{k}(t+1) &= C(t) + \overline{k}(t)\\ \overline{l}(t+1) &= C(t) - \overline{l}(t)\end{aligned}$$

where $C(t)$ is the doubled mean of all the states. Bigger value of $\overline{l_{|\phi\rangle}}(2^{s/2})$ means the updates of $\overline{k}$ increase the amplitudes of the correct states (decrease the amplitudes of the incorrect states) quicker.

4 Discussion

As seen in the previous section, directly searching for the single correct state brings a better result than the iterated approach. An equally distributed amplitude among the incorrect states gives us a higher amplitude amplification for the correct state. Equally important, the amplitude of the correct state after $2^{s/2}$ steps is higher in the case of standard Grover's approach.

First, we want to highlight the faulty intuition when considering the search in a partially collapsed quantum state $|\phi\rangle = \frac{1}{\sqrt{|K_{i-1}|}} \sum_{k \in K_{i-1}} |k\rangle$. Both of Grover's iteration steps, the negation of the correct amplitudes and computation of the mean of all amplitudes, are implemented over the whole register. This means that states $|k\rangle \notin K_{i-1}$ with 0 amplitude will be reintroduced into the superposition. To overcome this, we would have to define Grover's operators over K_{i-1}, meaning we need to know which exact keys are in K_{i-1} defeating the purpose of the previous $i-1$ searches.

Another argument could be the previously mentioned optimality of Grover's search [2]. It states that any algorithm, which accesses the oracle negating the amplitude of the correct states, requires at least as many oracle queries as standard Grover. One could question whether the special structure of the nested approach plays any role. After all, we are dropping keys at a constant rate after each measurement, which is only the case for good cryptographic functions, not for any arbitrary search problem. However, we draw attention to the so-called *Deferred Measurement Principle*. It states that delaying measurements until the very end of a quantum computation does not affect the probability distribution of the final outcome. In other words, the rate at which we drop the keys has no impact on the required amount of Grover's iterations, only the rate of the final correct keys to the whole space.

Finally, we wanted to mention the different behaviour if we define the sets K_i as $K_i = \{k : f_i(k) = z_i\}$. The difference is that now the correct states might also have a 0 amplitude. In fact, for a good cipher, we would on average expect only a few of the states from K_{i-1} to also be in K_i (besides the one correct key). This means that the average over the correct keys would be

$$\overline{k_{|\psi\rangle}}(2^{s/2}) \approx \sqrt{\frac{1}{2^{n-s}}} \cdot \frac{1}{2^{s-\epsilon}}$$

which is significantly smaller than in any other previously mentioned case. This, however, should not be a surprise, since the set of correct keys diverges in each iteration, and the one correct key which is present in each of them has very little influence on the average amplitude of the correct keys.

References

[1] Zheng, Y., Gao, J., Wang, B.: Nested Quantum Search Model on Symmetric Ciphers and Its Applications (2023)

[2] Zalka, C.: Grover's quantum searching algorithm is optimal. Physical Review A **60**(4), 2746–2751 (1999) https://doi.org/10.1103/PhysRevA.60.2746

[3] Biham, E., Biham, O., Biron, D., Grassl, M., Lidar, D.A.: Grover's quantum search algorithm for an arbitrary initial amplitude distribution. Physical Review A **60**(4), 2742–2745 (1999) https://doi.org/10.1103/PhysRevA.60.2742

[4] Michael A. Nielsen, I.L.C.: Quantum Computation And Quantum Information 10th Anniversary Edition, (2012)