# Quantum Algorithms with Potential for New Applications

*Takashi Yamakawa*

**Abstract**

This article outlines a new algorithm devised by NTT for quantum computers (Yamakawa et al. "Verifiable Quantum Advantage without Structure"). Quantum computers are being developed worldwide. However, the types of algorithms that use them are scarce, which may limit their applications. The new algorithm presented in this article is a possible solution to this problem. For the first time, NTT demonstrated a super-fast quantum algorithm that solves a type of difficult problem called "NP (non-deterministic polynomial time) search problem without structure." This algorithm was highly acclaimed in academia as potentially leading to the discovery of new applications for quantum computers.

*Keywords: quantum algorithm, hash function, NP problem*

## 1. Introduction

Quantum computers, which are expected to be the next generation of super-fast computers, have a major challenge. They are currently limited to a narrow range of applications. The greatest advantage of quantum computers is that they are capable of much faster computation than current computers. To benefit from this advantage, it is essential to have algorithms that take advantage of quantum computers to compute efficiently. However, such algorithms are scarce.

It is estimated that at least 5 to 10 years of development are still needed before quantum computers are ready for practical use. In the meantime, if we do not devise many algorithms that can theoretically support fast computation, we may end up with a waste of treasure.

The algorithm developed by NTT has the potential to change this situation because it can solve a type of problem for which quantum speed was not thought possible [1]. Previously, researchers believed that quantum algorithms require a structure to solve problems[*1], but NTT's algorithm is able to solve problems without any structure. A typical example of a quantum algorithm that solves a problem with structure is Shor's algorithm [2], which is well-known for cracking ciphers widely used on the Internet. Shor's algorithm was published in 1994.

NTT's algorithm has been highly acclaimed in academia. The paper describing the algorithm [1] was published at the IEEE Annual Symposium on Foundations of Computer Science (FOCS) 2022, the premier international conference in theoretical computer science, the same conference where Shor's algorithm was presented. Professor Scott Aaronson of the University of Texas at Austin, one of the leading experts in quantum computing, cited it as the latest breakthrough in a talk at the Solvay Conference, known for its historic discussions on quantum mechanics [3]. According to Quanta Magazine, a well-known online scientific publication, many researchers have been inspired by it and have begun exploring the possibility of new applications [4].

## 2. Verifiability

**Figure 1** summarizes the positioning of this new algorithm. Its key feature is that it simultaneously satisfies the properties of verifiability in addition to super-fastness and structureless properties. As the figure shows, there have been super-fast algorithms that can solve structureless problems such as the

*1 Professor Aaronson et al. conjectured that super-fast quantum algorithms exist only for structured problems [3]. The difference is that the target of this conjecture is a decision problem, whereas NTT's quantum algorithm is for a search problem.

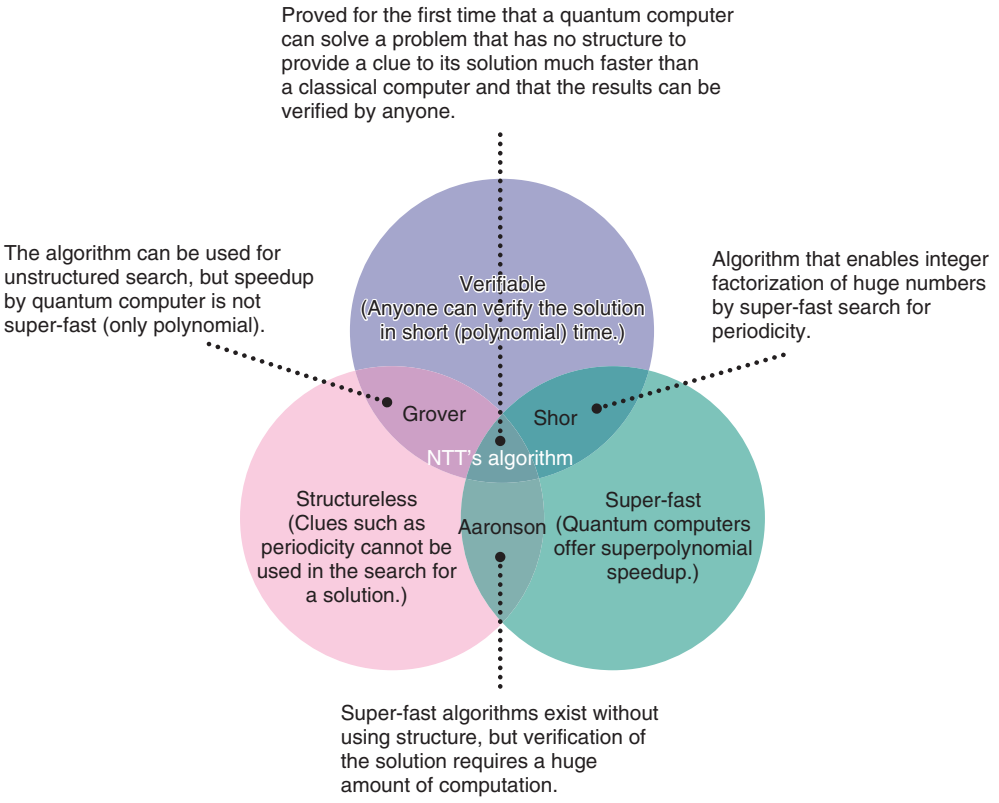



Fig. 1. Positioning of NTT's quantum algorithm.

algorithm proposed by Professor Aaronson [5]. However, these algorithms lack verifiability.

Verifiability means that it is easy to check whether the solution produced by the algorithm is correct. This is usually done using a conventional computer (called a classical computer in contrast to a quantum computer) rather than a quantum computer, and it must be possible to verify the solution in a short time. Current algorithms, however, require extremely long verification times, making it virtually impossible to verify whether the solution they produce is correct. In contrast, NTT's algorithm requires only a short time to verify the result.

Shor's algorithm is intended for integer factorization with large digits. For example, when 39,617 is factorized, the solution is 173 × 229. This is the correct solution, which can be quickly verified by simply multiplying them. When the number of digits is very large, the integer factorization is beyond the capability of a classical computer, but since the result can be verified only by multiplication, it does not take much time even for a classical computer.

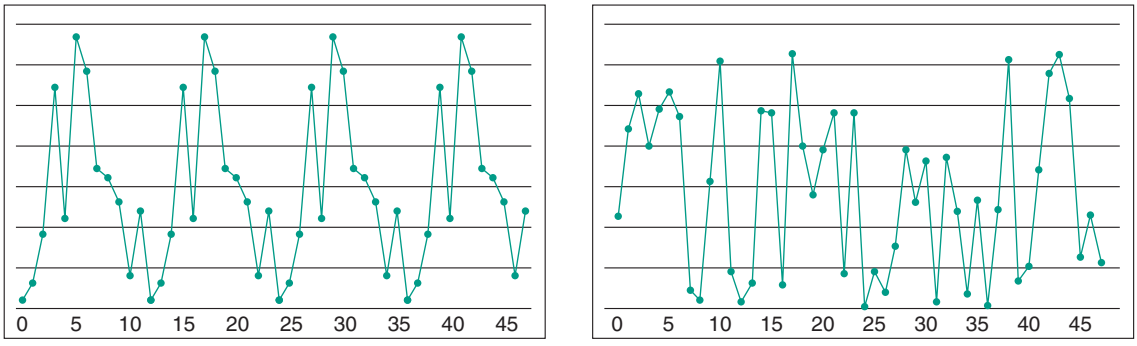
Problems that can be easily verified (in a short time[*2]) are called NP (non-deterministic polynomial time) problems, and the algorithm developed by NTT also targets an NP problem, or more precisely, an NP search problem.

## 3. Superpolynomial speedup

As Fig. 1 shows, there are also algorithms that solve structureless problems and still satisfy verifiability. An example is Grover's algorithm, which is a well-known algorithm that appears in quantum-computing textbooks. This algorithm lacks the super-fastness expected of quantum computers. At best, it can only achieve a polynomial speedup compared with the best classical algorithm[*3].

*2 Short time here refers to polynomial time. Polynomial time means that the computation time can be expressed in terms of a polynomial in the size of the problem (e.g., the number of bits to factorize). It increases slower than an exponential function.

*3 Grover's algorithm finds a solution from $n$ candidates. The classical algorithm requires an average of $n/2$ times and maximum of $n$ queries, while Grover's algorithm requires only $\sqrt{n}$ times. Comparing the two algorithms, the speedup is only quadratic.




(a) Remainder of a power of a natural number (periodic)

(b) Output of hash function (no structure such as periodicity)

Fig. 2. Difference between structured and structureless functions.

NTT's algorithm and Shor's algorithm are capable of a significant speedup that can be expressed in terms of mathematical expressions beyond polynomials, such as exponential functions. For example, the integer factorization of a 2048-bit integer used in standard Internet cryptography is a difficult problem that would take tens of thousands of years on a classical computer. However, it is estimated that a future large-scale quantum computer running Shor's algorithm could solve this problem in eight hours [6].

## 4. Finding the input of a random function

What is the structure used by Shor's algorithm? Shor's algorithm solves the integer factorization of a number N by reducing it to another problem. First, a natural number x that is coprime to N is chosen at random, and we consider the remainder of $x^r$ divided by N. As the value of r changes, the remainder changes periodically, as shown in **Fig. 2(a)**. This period is the structure behind the problem.

The factors of N can be easily computed if this period can be found. While classical computers require a large number of computations to find the period, Shor's algorithm uses a method called quantum Fourier transform to achieve super-fast computation.

The structureless problems that NTT's algorithm targets are those that cannot be solved using such clues. The development of quantum algorithms often involves an oracle, which is a black-box that computes a function. An unstructured problem is based on a random oracle, which is an oracle that computes a completely random function. We focus on hash functions[*4] as a concrete example of a random oracle. As shown in **Fig. 2(b)**, there is no rule between the input and output of a hash function, and we can regard the output to be random.

However, hash functions are believed to be secure against attacks by quantum computers. Therefore, we make two modifications. The first is to use a vector of a special form as input, and the second is to apply a hash function, the output of which is one bit for each coordinate of the vector. For the former, we add the condition that the input vector is an error-correcting code[*5] converted from another bit string (**Fig. 3**).

The problem of finding the input from the output in this construction is the target of NTT's algorithm. This is a structureless NP search problem. While a classical computer requires a large amount of computation to solve this problem, we demonstrated that NTT's quantum algorithm can find a solution exponentially faster than a classical computer. The verification of the solution can also be easily implemented on a classical computer. In other words, all three conditions shown in Fig. 1 are satisfied.

## 5. Toward practical application

**Figure 4** shows NTT's algorithm. In quantum computing, algorithms are usually represented as a quantum circuit, which is a combination of quantum gates, as shown in the figure. Although the details are beyond the scope of this article, it can be said that one

*4 Hash function: A function, the outputs of which look random. SHA-2 is a standard hash function used in cryptography.

*5 Error-correcting code: A coding method that converts data into a redundant data so that the original data can be recovered even if there is noise in communication. NTT's algorithm uses a code called Folded Reed Solomon code.

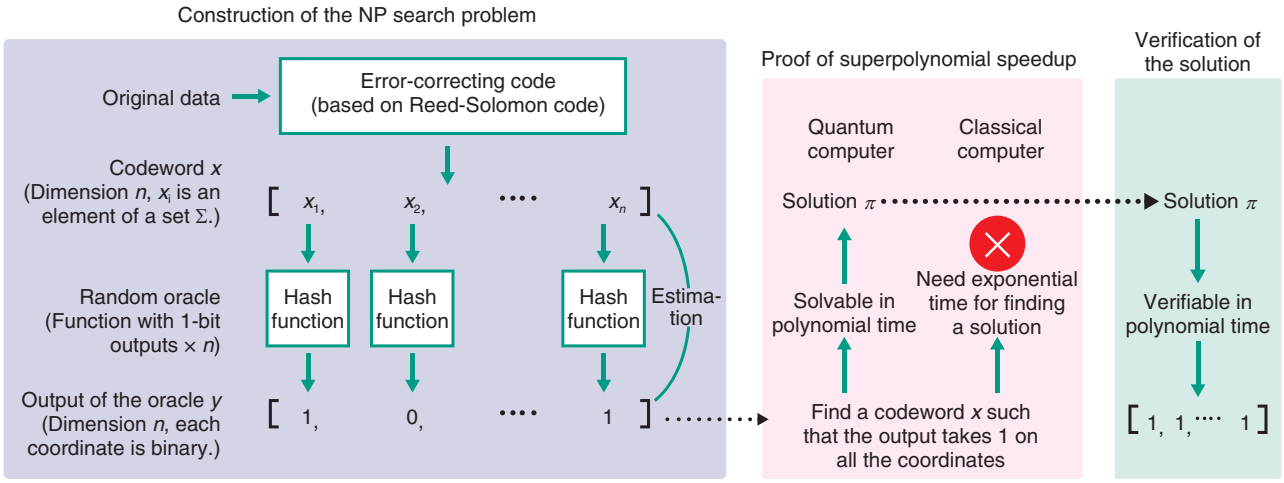



Fig. 3. The target NP search problem and the methods of proving and verification.

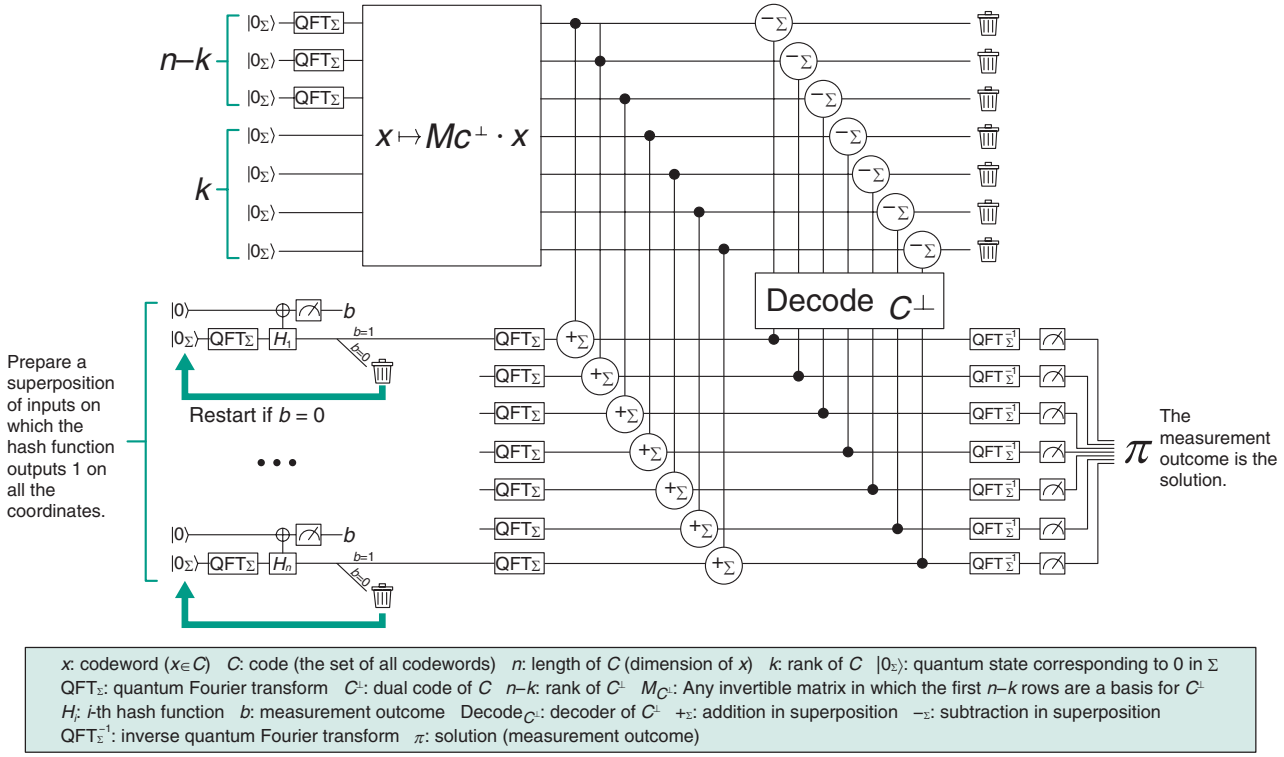



Fig. 4. Quantum algorithm that finds a solution.

of the key points of speedup is the quantum Fourier transform, indicated with QFT in the figure. Unlike Shor's algorithm, however, it is not used to find a structure.

What is the use of this algorithm? The problem solved in this study is intended only to explore the possibilities of quantum computers and has no specific application. The search for algorithms to solve realistic problems in the new direction presented in this article is a major challenge for researchers

around the world, including at NTT.

Peter Shor, who developed Shor's algorithm, recalls that a paper by Daniel R. Simons at a conference was a major inspiration [7]. The algorithm presented in the paper was for an unrealistic problem, and despite the support of Shor, who was a member of the program committee, the paper was rejected at the conference. We hope that the next Shor's algorithm will emerge from the many researchers who read our paper.

## References


[1] T. Yamakawa and M. Zhandry, "Verifiable Quantum Advantage without Structure," Proc. of 63rd IEEE Annual Symposium on Foundations of Computer Science (FOCS 2022), pp. 69–74, Denver, CO, USA, Nov. 2022. https://doi.org/10.1109/FOCS54457.2022.00014

[2] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proc. of 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS 1994), Santa Fe, NM, USA, Nov. 1994. https://doi.org/10.1109/SFCS.1994.365700

[3] S. Aaronson, "How Much Structure Is Needed for Huge Quantum Speedups?", arXiv:2209.06930, Sept. 2022. https://doi.org/10.48550/arXiv.2209.06930

[4] M. Rorvig, "Quantum Algorithms Conquer a New Kind of Problem," Quanta Magazine, July 2022. https://www.quantamagazine.org/quantum-algorithms-conquer-a-new-kind-of-problem-20220711/

[5] S. Aaronson, "BQP and the Polynomial Hierarchy," Proc. of 42nd ACM Symposium on Theory of Computing (STOC 2010), Cambridge, MA, USA, pp. 141–150, June 2010. https://doi.org/10.1145/1806689.1806711

[6] C. Gidney and M. Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," Quantum, Vol. 5, p. 433, Apr. 2021. https://doi.org/10.22331/q-2021-04-15-433

[7] P. W. Shor, "The Early Days of Quantum Computation," arXiv:2208.09964, Aug. 2022. https://doi.org/10.48550/arXiv.2208.09964



**Takashi Yamakawa**

Distinguished Researcher, NTT Social Informatics Laboratories.

He studied cryptography at the Graduate School of Frontier Sciences, The University of Tokyo and received a Ph.D. in 2017. He entered NTT in the same year. He has been a distinguished researcher at NTT Social Informatics Laboratories since 2022 conducting research on quantum cryptography. He was a visiting scholar at Princeton University from 2020 to 2021 conducting joint research with Mark Zhandry, a leading scientist in this field. His papers have been accepted for presentation at Eurocrypt and CRYPTO sponsored by the International Association for Cryptologic Research (IACR), STOC sponsored by Association for Computing Machinery (ACM), FOCS sponsored by the Institute of Electrical and Electronics Engineers (IEEE), and other conferences.