CEUR-WS.org/Vol-3408/short-s3-02.pdf

Towards a quantum world in cybersecurity land

Manuel A. Serrano[1], Luis E. Sanchez[2], Antonio Santos-Olmo[2], David Garcia-Rosado[2], Carlos Blanco[3] and Eduardo Fernandez-Medina[2]

[1]*Alarcos Research Group, University of Castilla - La Mancha, Ciudad Real, Spain*
[2]*GSyA Group, University of Castilla - La Mancha, Ciudad Real, Spain*
[3]*University of Cantabria, Santander, Spain*

Abstract

Quantum computing is a disruptive new technology that will change the world of computing as we know it. This new programming paradigm promises to solve several currently unsolvable problems, but it also opens up new challenges, such as post-quantum cryptography. In this context, future professionals need to be prepared to face this new framework and new concepts need to be outlined and incorporated into the corpus of cybersecurity education. In this paper we present the main advances in quantum computing and show a small case study similar to the new challenges we face, in order to raise awareness of the need to incorporate quantum cybersecurity in education.

Keywords

Quantum Computing, quantum cybersecurity, quantum optimization, quantum machine learning

1. Introduction

Quantum computing is an emerging technology that has the potential to revolutionize many fields, including cybersecurity. Quantum computers can perform certain calculations exponentially faster than classical computers, which makes them well-suited for applications in areas such as chemistry, medicine, machine learning, and cryptography [1]. Quantum computing is based on quantum theory, which allows for calculations using probability theory and linear algebra. This makes it possible to solve complex problems that classical computers cannot handle, such as encryption and cybersecurity [2].

In the field of cybersecurity, many encryption techniques currently used to secure data could be broken by quantum computing, using new algorithms and approach like the famous Shor's algorithm [3]. This means that new encryption methods will need to be developed to protect against attacks from quantum computers. But also, quantum computing has the potential to revolutionize the field of cybersecurity by enabling the development of new encryption methods that are resistant to attacks from quantum computers. On others research fields, the

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy
Manuel.Serrano@uclm.es (M. A. Serrano); LuisE.Sanchez@uclm.es (L. E. Sanchez); Antonio.SantosOlmo@uclm.es (A. Santos-Olmo); David.GRosado@uclm.es (D. Garcia-Rosado); Carlos.Blanco@unican.es (C. Blanco); Eduardo.FdezMedina@uclm.es (E. Fernandez-Medina)
0000-0003-0962-5659 (M. A. Serrano); 0000-0003-0086-1065 (L. E. Sanchez); 0000-0002-2349-3894 (A. Santos-Olmo); 0000-0003-4613-5501 (D. Garcia-Rosado); 0000-0001-9001-0904 (C. Blanco); 0000-0003-2553-9320 (E. Fernandez-Medina)
© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

advances in quantum optimization [4] and quantum machine learning techniques [5], open new cybersecurity approach to solve hard problems that cannot be solved with classical computers.

By teaching quantum computing in cybersecurity education, future professionals will be better equipped to develop and implement these new encryption methods. Additionally, understanding quantum computing can help cybersecurity professionals better understand the vulnerabilities of current encryption methods and develop more effective strategies for protecting against attacks [6].

Overall, the importance of quantum computing lies in its potential to solve problems using different computational resources to address several tasks, including encryption and cybersecurity, in a way that classical computers cannot handle, and its ability to perform certain calculations exponentially faster than classical computers. In the field of cybersecurity, quantum computing has the potential to revolutionize encryption methods and improve the overall security of digital systems. As such, it is important for cybersecurity education to include quantum computing as a topic of study to prepare future professionals for the changing landscape of cybersecurity.

2. Quantum computing state of the art

In this section we will look at the main advances in quantum computing and their applications to solving cybersecurity problems in the post-quantum era.

2.1. Quantum programming

The paradigm of quantum computing, which takes advantage of reality's quantum physical features, such as superposition and entaglement [7], has the potential to have a significant impact on computers [8]. The development of effective quantum algorithms by Shor [9] and Grover [10] has generated a great deal of interest in the area of quantum programming. Finding novel quantum algorithms is still a very challenging issue, in part because quantum programs are typically written as quantum circuits or in some combinator language that yields functional circuits. The usage of quantum bits (qubits) rather than conventional bits is the first feature that sets quantum programming apart from classical programming.

In addition to syntax-based notations offered by a wide range of quantum programming languages (such as Q# or QASM) that have been proposed to make it simpler to express quantum algorithms, quantum circuits and gates can also be graphically represented, as in Figure 1.

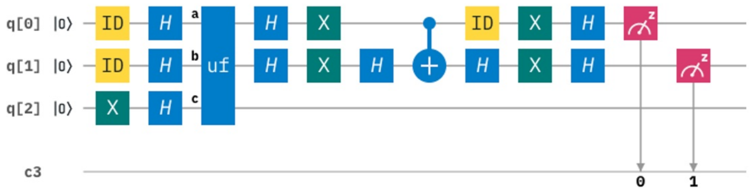

Figure 1: Example of Quantum circuit

2.2. Shor's Algorithm

Shor's algorithm is a quantum algorithm that can efficiently factor large numbers, which is a problem that is believed to be intractable for classical computers [11, 12, 13]. It was developed by Peter Shor in 1994 and is based on the principles of quantum mechanics. The algorithm works by finding the period of a function, which can be used to factor a large number into its prime factors. Shor's algorithm has important implications for cryptography, as many modern encryption schemes rely on the difficulty of factoring large numbers. The algorithm can break the RSA cryptosystem, which is widely used for secure communication, by factoring integers that are the product of two similarly-sized primes [14], which is a problem that is believed to be intractable for classical computers [15]. The algorithm works by finding the period of a function, which can be used to factor a number into its prime factors. The algorithm consists of two main steps: first, it uses a quantum Fourier transform to find the period of a function, and second, it uses classical algorithms to find the factors of the number based on the period.

2.3. Post-quantum cryptography

Post-quantum cryptography refers to cryptographic algorithms that are believed to be secure against attacks by quantum computers [16]. Quantum computers have the potential to break many of the currently used cryptographic algorithms, such as RSA and elliptic curve cryptography, by using Shor's algorithm to factor large numbers and compute discrete logarithms [11]. Post-quantum cryptography aims to develop new cryptographic algorithms that are resistant to quantum attacks, and several candidates have been proposed, such as lattice-based cryptography, code-based cryptography, and hash-based cryptography [16]:

- **Lattice-based cryptography [17]:** It is based on the hardness of finding the shortest vector in a high-dimensional lattice. Examples of lattice-based cryptographic algorithms include NTRUEncrypt, NewHope, and Kyber.
- **Code-based cryptography [18]:** Based on the hardness of decoding certain error-correcting codes. Examples of code-based cryptographic algorithms include McEliece and RQC.
- **Hash-based cryptography [19]:** It is based on the properties of hash functions. Examples of hash-based cryptographic algorithms include XMSS and SPHINCS+.
- **Multivariate cryptography [20]:** This type of cryptography is based on the hardness of solving systems of multivariate polynomial equations. Examples of multivariate cryptographic algorithms include Rainbow and HFE.

The development of post-quantum cryptography is important for ensuring the security of communication and data in the future, as quantum computers become more powerful and widespread. This situation, poses a threat to modern encryption practices because it has the potential to break many of the currently used cryptographic algorithms, such as RSA and elliptic curve cryptography, by using Shor's algorithm to factor large numbers and compute discrete logarithms. Quantum computers can perform these computations exponentially faster than classical computers, which makes them a significant threat to the security of encrypted data [11].

As quantum computers become more powerful and widespread, they could potentially break the encryption used to protect sensitive information, such as financial data, government secrets, and personal information. Therefore, the development of post-quantum cryptography is important for ensuring the security of communication and data in the future.

2.4. Quantum machine learning

Quantum machine learning [21] is an emerging field that combines the principles of quantum computing and machine learning to develop new algorithms that can solve complex problems more efficiently than classical algorithms. Quantum machine learning algorithms leverage the properties of quantum mechanics, such as superposition and entanglement, to perform computations in parallel and explore multiple solutions simultaneously. Some examples of quantum machine learning algorithms include quantum support vector machines, quantum neural networks, and quantum principal component analysis [22]. These algorithms have been applied to various problems, such as image recognition, drug discovery, and financial forecasting. However, the field of quantum machine learning is still in its early stages, and researchers are exploring ways to improve the performance and scalability of these algorithms. The best quantum machine learning algorithms depend on the specific problem being solved and the available quantum hardware. Currently, most quantum machine learning algorithms are designed to run on quantum simulators or small-scale quantum computers, and their performance is limited by the number of qubits and the quality of the quantum gates. As quantum hardware continues to improve, it is expected that quantum machine learning algorithms will become more powerful and applicable to a wider range of problems.

2.5. Quantum optimization

Quantum optimization is a field of quantum computing that focuses on solving optimization problems using quantum algorithms. Optimization problems are those that involve finding the best solution among a set of possible solutions, such as finding the shortest path between two points or the best way to allocate resources. Quantum optimization algorithms aim to find the optimal solution faster than classical algorithms by exploiting the quantum properties of superposition and entanglement. One of the most well-known quantum optimization algorithms is the quantum annealing algorithm [23], which is used in quantum annealers such as D-Wave systems. Another popular quantum optimization algorithm is the quantum approximate optimization algorithm (QAOA) [24], which is a variational algorithm that uses a sequence of quantum gates to approximate the optimal solution. Other quantum optimization algorithms include feedback-based quantum optimization, threshold-based quantum optimization, and warm-starting quantum optimization [25, 26, 27, 28].

The field of optimization algorithms has made great strides in recent years, and quantum adiabatic computing is one of them. In addition to the traditional search algorithms, which have some efficiency and effectiveness issues, new algorithms and approaches have been discovered and developed, which have been gradually raising the effectiveness of this class of techniques.In this regard, adiabatic quantum computation holds out one of the greatest possibilities for addressing challenging NP-complete optimization problems in polynomial time

[29] by representing the problem to be addressed as a superposition of qubits, and through the annealing process, the qubits are collapsed to a classical state that is either 0 or 1, and which represents the lowest energy solution to the given problem. Quantum optimization has potential applications in various fields, such as finance, logistics, and drug discovery, where optimization problems are common and often computationally expensive to solve using classical methods [30].

3. A cybersecurity adiabatic optimization example

In this study, we use a quantum computing methodology to enhance incident response management within a framework for risk assessment and management. The present problem is to select the minimum set of incidents to manage in order to solve all the controls associated to the incidents. The input to the algorithm is a series of incidents, having each of them a severity and an estimated resolution time. In addition, it has a series of associated controls that will have to be reviewed and strengthened in order to consider that the incident has been resolved. These controls can be associated to the resolution of several incidents. To solve the problem, we should select a result in which the minimum set of incidents to be solved is selected, so that we cover all the controls that allow us to solve the other incidents.

We will model this problem as a *Quadratic Unconstrained Binary Optimization (QUBO)* problem, which will represent the objectives and constraints of our problem and can be sent to the solver of the adiabatic quantum computer to find the minimum energy state, which will coincide with the combination of variables, i.e. incidents, that must be selected to find an optimal result to our problem. This kind of problems are specified on the basis of a Hamiltonian, indicating the objective and the constraints to be met by the solution. Our main objective is to minimize the total time of the issues that are part of the solution. In the form of a *BQM*[1] expression we could specify it as follows:

$$\sum_{i=1}^{N}(x_i \times t_i) \tag{1}$$

Being x_i the binary variable that determines whether or not the incident i is selected, and t_i the estimated time related to the incident i. It should be noted that our goal is to minimize this objective.

The constraints are somewhat more complicated to model, since the incidents can be fulfilled either because they have been selected, or because the set of controls that form part of it have already been solved by one or more previously selected issues. In order to find a possible solution, let's analyze a small example in Table 1:

In Table 1 we can see that to solve our problem it is not necessary to solve all the incidents *{A,B,C}* since by attending to a subset of them, e.g., *{A,B}*, we cover all the necessary controls. In this problem, we are looking for all the incidents to be solved, and to determine that an incident is solved we look at whether its controls have been selected or not. In other words, we want all controls to have at least one incident related to it that has been selected. If all the controls

[1] Binary Quadratic Model, representing an optimization goal in the form of a binary quadratic polynomial

Table 1
Incidents and controls example

Incident	Controls
A	1, 2
B	3, 4
C	1, 2, 3

have been solved, we know that all the issues will be solved as well. This constraint will be formulated as follows:

$$\sum_{i \in C_k}^{\forall k} (x_i) \geq 1 \tag{2}$$

Where C_k is the set of incidents related to the control k. With this expression we control that at least one of the incidents related to k have been selected. Doing this for all the controls, we obtain:

$$\sum_k \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) \tag{3}$$

In order to construct the final QUBO equation we need to add a penalty coefficient (P), which serves to modulate the weight of the constraints in the Hamiltonian expression. Empirically, it can be calculated that this coefficient P is the highest estimated time among all the occurrences plus 1, so that the penalty still affects the solution. The final simplyfied QUBO equation is as follows:

$$\sum_{i=1}^{N} (x_i \times t_i) + P \times \sum_k \Big(\sum_{i \in C_k} (x_i - 1)^2 \Big) = \sum_{i=1}^{N} (x_i \times t_i) + \sum_k \Big(\sum_{i,j \in C_k} (-Px_i + 2Px_i x_j) \Big) \tag{4}$$

This expression gives us a linear part $(-Px_i)$ and a quadratic part $(2Px_i x_j)$, which will be sent to the quantum annealing solver through a bidimensional matrix generated from the above expression. This Hamiltonian is converted into a QUBO matrix and sent to the quantum sampler annealing for getting the lowest energy solution which represent the optimal solution.

4. Conclusions

Today we are witnessing a new revolution that will change today's computing world and open up new challenges in the field of cybersecurity. Quantum computers are capable of solving complex problems that are intractable with the classical computers we know and that are processed in linear times. These new quantum algorithms dismantle some of the bases of cybersecurity such as cryptographic algorithms and force us to investigate new post-quantum cryptographic algorithms. But they not only offer us challenges but also incorporate new tools to streamline and improve the field of cybersecurity. In this sense, it is important to incorporate all this new knowledge in the curricula of studies so that new professionals are prepared to provide new solutions and face new challenges.

Acknowledgments

This work has been developed within the AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI/10.13039/501100011033, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521), ALBA-UC (TED2021-130355B-C33, id.3611130630-130630-28-521) funded by ”Ministerio de Ciencia e Innovación”, and supported by the European Union’s Horizon 2020 Project “CyberSANE” under Grant Agreement No. 833683.

References

[1] J. S. Clarke, Quantum computing and the importance of interconnects, 2018 IEEE International Interconnect Technology Conference (IITC) (2018) 1–1.

[2] W. Sarada, N. Rajalaxmi, G. S. Reddy, Quantum computing: Applications and future importance, 2021.

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

[4] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, et al., Optimización cuántica mediante algoritmos variacionales en dispositivos cuánticos a corto plazo, Ciencia y tecnología cuánticas 3 (2018) 030503.

[5] P. Wittek, Quantum machine learning: what quantum computing means to data mining, Academic Press, 2014.

[6] S. Shamshad, F. Riaz, R. Riaz, S. S. Rizvi, S. Abdulla, An enhanced architecture to resolve public-key cryptographic issues in the internet of things (iot), employing quantum computing supremacy, Sensors 22 (2022) 8151.

[7] R. S. Sutor, Dancing with Qubits: How quantum computing works and how it can change the world, Packt Publishing Ltd, 2019.

[8] IBM, The Quantum Decade. A playbook for achieving awareness, readiness, and advantage, 2021. URL: https://www.ibm.com/downloads/cas/J25G35OK.

[9] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, Ieee, IEEE Comput. Soc. Press, Santa Fe, NM, USA, 2002, pp. 124–134. doi:10.1109/SFCS.1994.365700.

[10] L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Physical Review Letters 79 (1997) 325–328. doi:10.1103/PhysRevLett.79.325.

[11] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, C. N. Asogwa, An overview of quantum cryptography and shor’s algorithm, International Journal of Advanced Trends in Computer Science and Engineering (2020).

[12] L. M. Baker, L. M. Ogren, Quantum algorithms from a linear algebra perspective, 2017.

[13] L. M. Baker, Digital wpi major qualifying projects (all years) major qualifying projects april 2017 quantum algorithms from a linear algebra perspective, 2019.

[14] S. Nehal, M. Farhan, Quantum cryptography-breaking rsa encryption using quantum computing with shor’s algorithm, 2020.

[15] M. Imran, An exact version of shor's order finding algorithm and its applications, ArXiv abs/2205.04240 (2022).

[16] J. A. Buchmann, K. E. Lauter, M. Mosca, Postquantum cryptography, part 2, IEEE Secur. Priv. 16 (2018) 12–13.

[17] D. Micciancio, O. Regev, Lattice-based cryptography, Post-quantum cryptography (2009) 147–191.

[18] N. Sendrier, Code-based cryptography: State of the art and perspectives, IEEE Security & Privacy 15 (2017) 44–50.

[19] D. Butin, Hash-based signatures: State of play, IEEE security & privacy 15 (2017) 37–43.

[20] J. Ding, A. Petzoldt, Current state of multivariate cryptography, IEEE Security & Privacy 15 (2017) 28–36.

[21] R.-Z. Li, J. Xu, J. Yuan, D. Li, An introduction to quantum machine learning algorithms, 2020.

[22] M. Scekic, S. Scepanovic, S. Mitrović, Implementation of quantum machine learning algorithms: A literature review, 2022 11th Mediterranean Conference on Embedded Computing (MECO) (2022) 1–4.

[23] E. Crosson, E. Farhi, C. Y.-Y. Lin, H.-H. Lin, P. Shor, Different strategies for optimization using the quantum adiabatic algorithm, arXiv preprint arXiv:1401.7320 (2014).

[24] J. Choi, J. Kim, A tutorial on quantum approximate optimization algorithm (qaoa): Fundamentals and applications, in: 2019 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2019, pp. 138–142.

[25] N. N. Hegade, X. Chen, E. Solano, Digitized counterdiabatic quantum optimization, Physical Review Research 4 (2022) L042030.

[26] A. B. Magann, K. M. Rudinger, M. D. Grace, M. Sarovar, Feedback-based quantum optimization, Physical Review Letters 129 (2022) 250502.

[27] J. Golden, A. Bärtschi, D. O'Malley, S. Eidenbenz, Threshold-based quantum optimization, in: 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), IEEE, 2021, pp. 137–147.

[28] D. J. Egger, J. Mareček, S. Woerner, Warm-starting quantum optimization, Quantum 5 (2021) 479.

[29] V. Černý, Quantum computers and intractable (np-complete) computing problems, Phys. Rev. A 48 (1993) 116–119. URL: https://link.aps.org/doi/10.1103/PhysRevA.48.116. doi:10.1103/PhysRevA.48.116.

[30] P. Niroula, R. Shaydulin, R. Yalovetzky, P. Minssen, D. Herman, S. Hu, M. Pistoia, Constrained quantum optimization for extractive summarization on a trapped-ion quantum computer, Scientific Reports 12 (2022).