iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** X **Month of publication:** October 2024

DOI: https://doi.org/10.22214/ijraset.2024.64840

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue X Oct 2024- Available at www.ijraset.com

Unlocking Complexity: D-Wave's Role in Quantum Computing Breakthroughs

Yash Mistry[1], Joy Sata[2], Karan Patel[3]
[1, 2, 3]*Students, Computer Engineering, SAL College of Engineering, Ahmedabad, India*

Abstract: ***In this new era of Quantum Computing, a transformative paradigm is emerging for the enhancement of Cyber Security using the special-purpose systems like D-Wave's quantum annealers which helps the encryption system become more resilient. As quantum computing evolves, it provides new paradigms for breaking the traditional encryption methods, as the recent breakthroughs is accomplished by researchers from Shanghai University that uses D-Wave's quantum annealing capabilities in providing the researchers to successfully demonstrated the potential to compromise widely used encryption systems, including RSA and AES. The usage of quantum annealing (QA) that makes the D-Wave's a specialized quantum system which enables an efficient computation in tackling cryptographic problems, demonstrates the implications for the data security and privacy by applying the quantum-classical hybrid architectures. This research aims to get attention on the urgent need for developing a new security measures in response to the vulnerabilities exposed by the quantum advancements which emphasizes the crucial role of D-Wave's in unlocking the complexities of quantum computing and its implications for the future of cybersecurity.***

Keywords: Quantum Computing, Cybersecurity, D-Wave, Quantum Annealing, RSA, AES.

I. INTRODUCTION

Quantum computing has shown a rapid improvement in the field of cyber security, supporting the principles of quantum mechanics that solves even more complex problems efficiently than the classical computers. Quantum computers are capable of solving many complex mathematical and optimization problems which simulates the quantum systems that breaks certain encryption algorithms, and contribute to advancements in fields like drug discovery, materials science, and artificial intelligence. Moreover, one of the key principles of quantum computing is entanglement., wherein the state of one qubit becomes intrinsically linked to another state, despite the distance amongst them [16]. This interconnection allows the quantum computers to process the information in many ways that traditional computers cannot thus resulting in exponential speedups for some specific calculations [5]. As the quantum figuring innovation progresses security of many existing cryptographic calculations is progressively undermined. Quantum-computers can solve problems like integer factorization (on which RSA is based) and discrete logarithms which are exponentially faster than classical computers, potentially rendering these cryptosystems obsolete.

Furthermore, the D-Wave's quantum computer hardware platform have developed rapidly and steadily as this quantum computer has more than 7,000 qubits and there is also a new topology, Zephyr and a larger energy scale that vastly improves the qubit resource [1]. D-Wave has played a significant role in the advancement of its commercial and practical applications of quantum technology. D-Wave's approach to the quantum annealing is distinct from the famous companies like IBM, Google, and Rigetti. Quantum annealers have emerged as powerful tools for various applications, including logistics and artificial intelligence which provides the short-term advantages in quantum computing. As the capabilities of quantum computing grows, D-Wave's unique position demonstrates its importance in shaping the future of cybersecurity and beyond.

II. QUANTUM ANNEALING

Quantum Annealing is a heuristic optimization method based on adiabatic theory algorithm that takes the advantage of quantum tunneling effect generated by the quantum fluctuations. This algorithm must run near absolute zero at approximately -273.15 degrees Celsius and only on low power consumption of 25kW [2]. Based on the quantum tunneling effect and adiabatic theory the algorithm can escape local suboptimal solutions with a much higher probability of reaching a globally optimized solution [2]. In the public-key cryptography attack the mathematical problem is transformed into a combinatorial optimization problem mapped with the quadratic unconstrained problem Binary Optimization (Quadratic Unconstrained Binary Optimization, QUBO) or Ising form [1]. The quantum bits (qubits) which are the lowest states of energy for the superconducting loops that makes the D-Wave QPU. These states are having a circulating current and a corresponding magnetic field.

As the classical bits, a qubit can be in either 1 or 0 state. The qubit is a quantum object thus it can also be in a superposition of 1 and 0 state at the same time. During the quantum annealing process, an energy barrier is raised, which separates the single minimum energy into two valleys. The probability of a qubit falling into the state of 0 or 1 can be controlled by working on an external magnetic field to bias the qubit to the end in one state over the other; the magnetic field is programmatically controlled via a qubit bias. The real power of the quantum annealing is realized when you link the qubits together so that they can influence each other this can be achieved by a device called a *coupler* [1]. A coupler can correlate two qubits such that they tend to end up in a same classical state either both 0 or both 1 or in the opposite states. The correlation between the coupled qubits is controlled programmatically. Finally, at the end of the quantum annealing process each qubit collapses from its superposition state into either 0 or 1 state.

III. QUANTUM COMPUTING AND CYBERSECURITY RISKS

Cryptography is essential in this modern electronic communication as it ensures the security of activities such as email security, password management, financial transactions and electronic voting. All of these systems must have the important safeguards such as confidentiality, integrity and authentication. Quantum computers pose a significant risk to these goals of security as it can perform the calculations that are beyond the capacity of the traditional computers thus potentially threatening the goal of a secure communication [9]. Their enhanced computing capacity allows them to breach cryptographic keys by extensively searching all possible secret keys which allow unknown actors to intercept the communications between the authorized sender and receiver. According to the National Institute of Standards and Technology (NIST), the emergence of quantum computers proposes a significant threat to the existing public key encryption methods [11].

D-Wave has advanced quantum annealing technology which allows to navigate the complex solution spaces using the quantum tunneling. This ability helps it to bypass obstacles, making it easier to find optimal solutions and not only it does that the D-Wave's quantum annealing also offers a potential threat for cryptographic attacks, this capability not only poses a threat to the existing systems but also lays the groundwork for developing new cryptographic approaches.

Quantum computing poses a real threat to public key cryptography, particularly through its ability to solve the large integer factorization problem that RSA relies on. While traditional computers struggle with this task, quantum computers can handle it much more efficiently. The D-Wave is a dedicated quantum computer which performs the public-key cryptography attacks more efficiently than general-purpose quantum computers. Significant improvements have been made to the penalty term in the dimensionality reduction formula which has led to a new optimized model that have further reduces the local field coefficients and couples the range of these coefficients. Utilizing the D-Wave Advantage, researchers have successfully decomposed the 22-bit integer 2269753 [1] by enhancing the classical algorithms with the quantum tunneling via quantum annealing."

IV. CONCLUSION

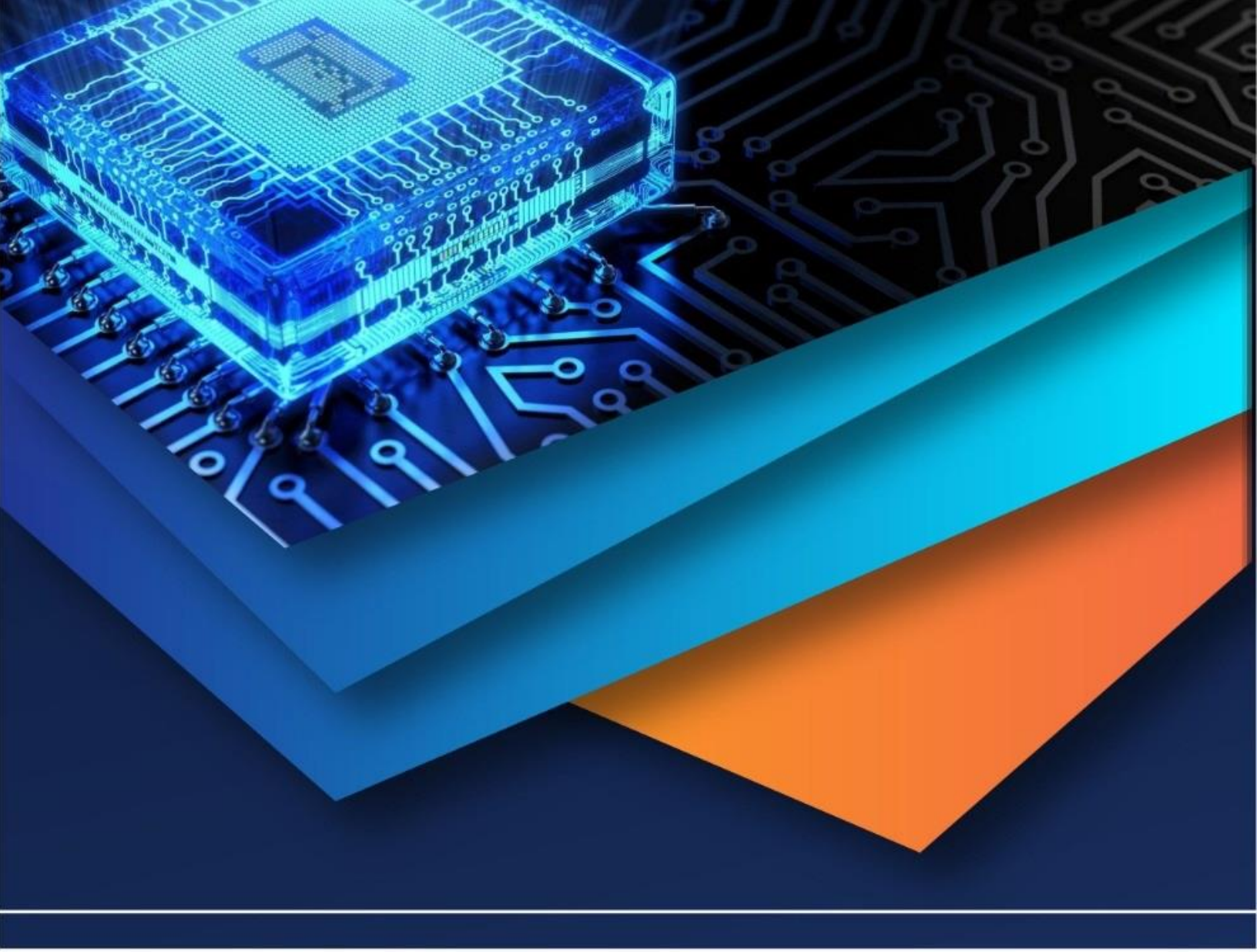
In this paper, the primary objective was to raise awareness of the D-Wave quantum computer that has successfully decomposed the 22-bit ratio special integer 2269753. Quantum computer systems pose a significant risk to both conventional public key algorithms (such as RSA) and symmetric key algorithms (such as AES). The range of integers decomposed is greatly improved, and the local field coefficient is tight and the range of coupling coefficients are significantly reduced. Narrowing the range of coefficients, the coupling strength between qubits can be reduced, and the quantum flipping can be more unified First, it can significantly improve the success rate of annealing.

Quantum algorithms take the advantage of quantum tunneling that poses new challenges towards the field of cybersecurity, especially regarding security features in the upcoming future. The D-Wave quantum computer stands out for its ability to efficiently tackle the large-scale problems, effectively "jumping out" of complex situations. While the current quantum attacks are limited, quantum annealing offers a stable approach for solving the complex problems. D-Wave's advancements position it as a strong contender in RSA and AES cryptographic attacks resulting in the potential risk of its rapidly evolving hardware.

We have verified that D-Wave's realistic attack capabilities via quantum annealing significantly affect RSA cryptography, quantum annealing greatly exceeds that of other types of quantum computers. Many password problems can be turned into combinatorial optimization questions or Exponential solution space solves the problem and solves it using quantum annealing. As an outcome, quantum annealing could potentially be extended to various public-key cryptography along with symmetric cryptography Security Analysis.

REFERENCES

[1] Wang Chao, Wang Qidi, Hong Chunlei, Hu Qiaoyun, Pei Zhi, "Quantum Annealing Public Key Cryptographic Attack Based on D-Wave Advantage", Chinese Journal of Computers, Vol-47, Issue-5, May 2024.
[2] Atanu Rajak, Sei Suzuki, Amit Dutta, Bikas K. Chakrabarti, "Quantum Annealing: An Overview", The Royal Society Publishing, arXiv:2207.01827v4, Jan 2023.
[3] Girish Dave, Yogendra Patel, Bijal Parmar, Neha Mistri, Nidhi H. Divecha, "Introduction of Quantum Computing - International Journal for Scientific Research & Development, Vol-7, Issue-2, 2014.
[4] Hitesh Singh, D.L. Gupta, A.K Singh, "Entropy Security in Quantum Cryptography", International Journal of Computer Applications, Vol-81, Issue-5, Nov 2013.
[5] Marufa Rahmi, Debakar Shamanta, Ayesha Tasnim, "Basic Quantum Algorithms and Applications", International Journal of Computer Applications, Vol-56, Issue-4, Oct 2012.
[6] Abhishek Pradhan, Sushree Soujanya Padhi, B.Giridhar, Mr Chandan Kumar Giri, "Improvising Security Issues Using Quantum Cryptography", International Journal of Computing and Technology, Vol-1, Issue- 9, Oct 2014.
[7] Santosh Kumar Das, Hari Ram Swamy, B.Giridhar, Mr Chandan Kumar Giri, "Integration of Quantum Cryptography", International Journal of Computing and Technology, Vol-1, Issue- 9, Oct 2014.
[8] Seema S. Kute, Chitra G. Desai, "Quantum Cryptography: A Review", Indian Journal of Science and Technology, Vol-10, Issue-3, Jan 2017
[9] Joshua J. Tom, Nlerum P. Anebo, Bukola A. Onyekwelu, Adigwe Wilfred, Richard E. Eyo, "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems", International Journal of Engineering and Advanced Technology, Vol-12, Issue-5, June 2023.
[10] Abhinandan Joshi, "The Impact of Quantum Computing on Cybersecurity", International Journal of Innovative Science and Research Technology, Vol-8, Issue-5, May 2023.
[11] Nandini Bhiva Metkari, Ruchi Vinod Shukla, "The Influence of Quantum Computing on Existing Cryptography", International Journal for Scientific Research & Development, Vol-9, Issue-6, 2021.
[12] Shamuvel. V, Raja Kumar. B, Vinothkumar. M, "A Novel Approach on Side Channel Threats Attack in Quantum Computing", International Journal of All Research Education and Scientific Methods, Vol-12, Issue-6, June 2024.
[13] Sohaib Shafqat Marazi, "Decrypting Cryptography: Exploring the Impact of Grover's Quantum Search Algorithm on Cryptanalysis", International Journal of All Research Education and Scientific Methods, Vol-12, Issue-8, Aug 2024.
[14] Suryanadh Kumar Ganisetti, "Quantum Computing Applications in Cryptography: Enhancing Security and Identifying Vulnerabilities", International Journal of Science and Research, Vol-13, Issue-6, June 2024.
[15] Harish Kumar Reddy Kommera, "Adaptive Cybersecurity in the Digital Age: Emerging Threat Vectors and Next-Generation Defense Strategies", International Journal for Research in Applied Science & Engineering Technology, Vol-12, Issue-9, Sep 2024.
[16] Bhanu Sankhyan, Anupam Baliyan, Abhishek Kumar, "Design of a Hybrid Security Protocol based on Cryptographic Algorithms", International Journal for Research in Applied Science & Engineering Technology, Vol-12, Issue-3, Mar 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY