Password Cracking in The Post-Quantum Era

Ali Alwan
Department of Electrical and Computer Engineering
Villanova University
Villanova, PA

Abstract—**Password cracking has been a critical attack vector for hackers to gain access to a secured system. Hackers typically perform dictionary attacks to run through lists of common and weak passwords until it finds a match with the hashed password. Most user passwords are poorly selected increasing the likelihood of their password being cracked, allowing a malicious user to gain access. Ethical password cracking is organized by companies to test the security of the passwords to their internal systems. However, with the rise of quantum computers and their powerful computational power, this poses a big threat to passwords themselves. Specifically, Grover's algorithm is a quantum algorithm that can speed up an unstructured search problem quadratically compared to that of today's classical computers, making it possible to brute-force passwords. A new approach to ethical password cracking is needed to test a password's vulnerability to a quantum brute-force attack.**

I. INTRODUCTION

Humans typically like to select passwords that are easy to remember and require the least number of keystrokes due to their own convenience. People often tend to use dictionary words to construct their passwords. However, this causes most user created passwords to be poorly selected. Passwords have been a critical attack vector as it can allow a malicious user to gain unauthorized access into a system. Today's password cracking is done by hashing words or strings to find a match with the original hashed password, which can be accessed from a database where they are stored. However, password cracking is not used for only malicious purposes, it can be used by an organization to test the strength of passwords to protected systems to prevent a hacker from exploiting a weak password.

Ethical password cracking is an essential part of an organization's effort to ensuring security within their infrastructure. Ethical hackers main cracking methodology is to perform a dictionary attack on retrieved hashed passwords. This is a targeted form of a brute force attack, where it references a dictionary to run through lists of common words, phrases, and leaked passwords to gain access to a protected system, rather than manually entering a word. However, the hashed password will only be cracked if that password is found in that referenced dictionary. A brute force cracking technique is a definite way to crack a hashed password as this attack runs through all combinations of characters of a predetermined length until it finds a combination that matches the password. The computation time for this attack can become infeasible as it may take years to just crack one password with any of today's classical computers. However, in the near future, the development of quantum computers delivers a huge leap forward in computation to solve certain problems which can allow brute force attacks on passwords to become feasible.

II. PROBLEM: POWER OF QUANTUM COMPUTING

Given the potential computational power of quantum computers, this raises huge concerns for the security industry. Specifically, quantum computers are able to break the existing public-key cryptosystems within seconds, requiring the need for quantum-resistant cryptography algorithms. There is no known quantum algorithm that is able to reverse existing hash algorithms such as SHA, SHA2, and SHA3; however, hashed passwords can still be vulnerable to a quantum attack. Grover's search algorithm is a quantum algorithm that can significantly speed up the computation time to brute-force passwords, so it is important to understand how a quantum computer can be used to conduct password cracking.

A. Quantum Computation

Quantum computers use the properties of quantum physics to store data and perform computations. Quantum computers are able to create massive multidimensional spaces to represent very large problems, which is not possible with the most powerful classical computers. This is done by having quantum bits, or qubits, as the basic unit of memory and connecting them in a state called superposition. Whereas a classical bit can only have two states, a qubit can be in superposition of both states simultaneously. In Figure 1 below, it better illustrates how qubits can be used to create vast computational spaces.

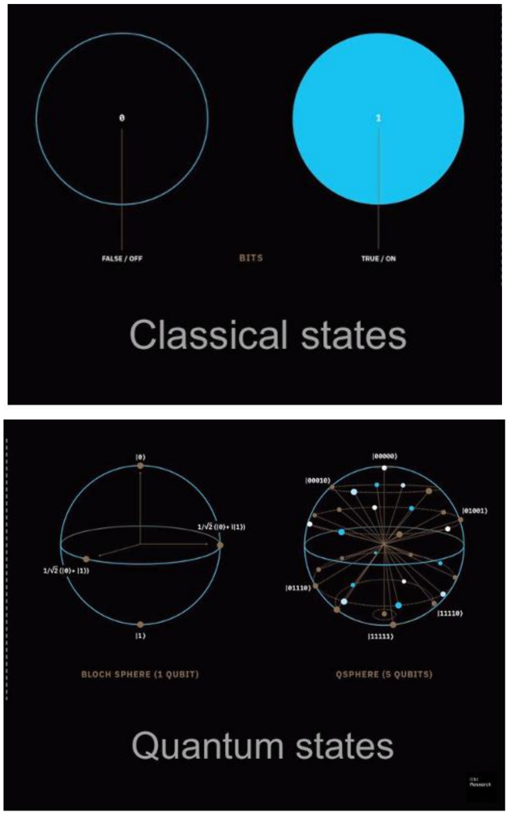


Figure 1: Classical bit vs. Quantum bit

B. Grover's Search Algorithm

Quantum algorithms use the multidimensional space provided by the superposition of qubits to employ quantum wave interference. Grover's search algorithm exploits quantum entanglement, which allows all the qubits to be perfectly correlated with each other. This algorithm provides a quadratic speed up for an unstructured search. For instance, given a large list of N items, it would need to check an average of N/2 items, or worst case all N items, to find a single item using classical computation. However, using Grover's search algorithm, it can find an item in about √N steps, which is a substantial improvement in computation time. In Figure 2 below, it illustrates how Grover's algorithm can be implemented on a two-qubit circuit. The probability displacement in the final state demonstrates the likelihood of each qubit state being the item searched for.

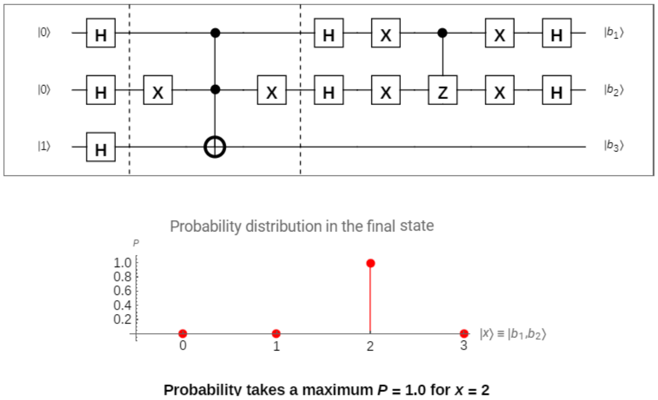
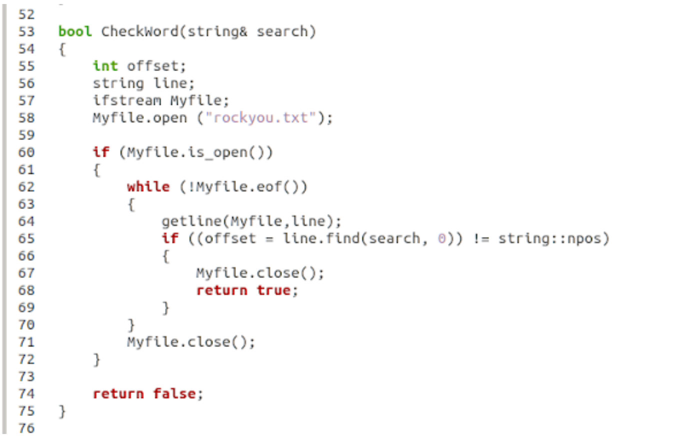

|0⟩
|0⟩
|1⟩
H
X
Z
|b₁⟩
|b₂⟩
|b₃⟩
Probability distribution in the final state
P
1.0
0.8
0.6
0.4
0.2
0
1
2
3
|x⟩ ≡ |b₁,b₂⟩
Probability takes a maximum P = 1.0 for x = 2

Figure 2: Quantum circuit implementing Grover's algorithm

For existing hash algorithms, it is recommended to have a key length of at least 256 bits for security but using Grover's algorithm decreases the effective security quadratically. For instance, SHA-512 in a post-quantum era would have the same effective security as today's SHA-256. This will cause today's key lengths to double to remain secure against a quantum brute-force attack. Passwords themselves would need to be created strong enough that would resist this attack. Therefore, it is important to be aware of this potential attack and how it can massively impact the security of organizations.

III. Solution Design

A new approach to ethically crack passwords is needed to test the security of passwords against a quantum brute-force attack using Grover's search algorithm. It is essential for an organization to find vulnerable passwords to internal systems or employee accounts before a hacker may exploit them. A company can conduct dictionary attacks on the stored hashed passwords to find passwords that were created using dictionary words or common passphrases. A popular dictionary that has over 10 million passwords, RockYou.txt, can be used to instantly crack weak passwords. In the created software program depicted below, it is a working demonstratable model that can be used to test the security of passwords against a dictionary attack and a quantum brute-force attack. In Figure 3 below, this function checks if the inputted password is a common password within the wordlist, causing the password to be cracked instantly.



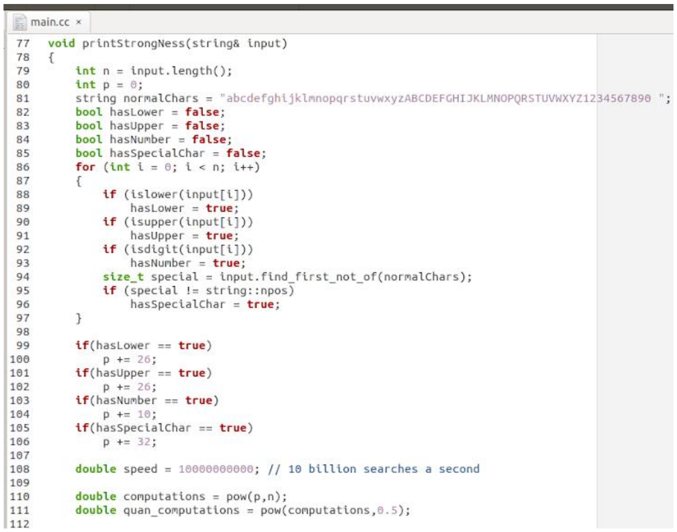
```
bool CheckWord(string& search)
{
    int offset;
    string line;
    ifstream Myfile;
    Myfile.open ("rockyou.txt");

    if (Myfile.is_open())
    {
        while (!Myfile.eof())
        {
            getline(Myfile,line);
            if ((offset = line.find(search, 0)) != string::npos)
            {
                Myfile.close();
                return true;
            }
        }
        Myfile.close();
    }

    return false;
}
```

Figure 3: Function checks password within “RockYou.txt”

To test the security of a password against a brute-force attack using Grover’s search algorithm, the computational time to brute-force is calculated to check if it is within a reasonable time frame. This is done by calculating the total number of combinations for a predetermined length and then applying Grover’s algorithm to get a quadratic speed up over it. Adding uppercase letters, numbers, and special characters increases the complexity of the password by increasing the total number of characters that can be selected to construct the password. The total number of combinations can be determined by taking the complexity of the password and raising it to the power of the length of the password. Since it is possible to stack multiple GPUs, it can multiply the processing power to tens of billions of password cracking attempts per second. Therefore, the computation time to brute-force all combinations can be calculated to determine if this quantum attack is feasible, which can be seen in Figure 4 below.



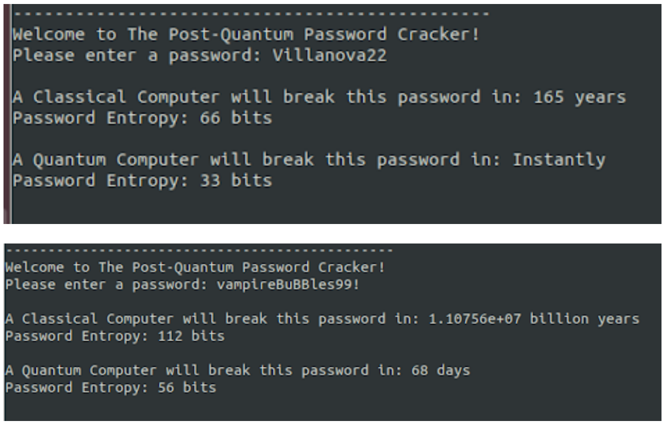
```
void printStrongNess(string& input)
{
    int n = input.length();
    int p = 0;
    string normalChars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 ";
    bool hasLower = false;
    bool hasUpper = false;
    bool hasNumber = false;
    bool hasSpecialChar = false;
    for (int i = 0; i < n; i++)
    {
        if (islower(input[i]))
            hasLower = true;
        if (isupper(input[i]))
            hasUpper = true;
        if (isdigit(input[i]))
            hasNumber = true;
        size_t special = input.find_first_not_of(normalChars);
        if (special != string::npos)
            hasSpecialChar = true;
    }

    if(hasLower == true)
        p += 26;
    if(hasUpper == true)
        p += 26;
    if(hasNumber == true)
        p += 10;
    if(hasSpecialChar == true)
        p += 32;

    double speed = 10000000000; // 10 billion searches a second

    double computations = pow(p,n);
    double quan_computations = pow(computations,0.5);
```

Figure 4: Function tests password security against quantum brute-force attack



```
-----------------------------------------------
Welcome to The Post-Quantum Password Cracker!
Please enter a password: Villanova22

A Classical Computer will break this password in: 165 years
Password Entropy: 66 bits

A Quantum Computer will break this password in: Instantly
Password Entropy: 33 bits
```

```
-----------------------------------------------
Welcome to The Post-Quantum Password Cracker!
Please enter a password: vampireBuBBles99!

A Classical Computer will break this password in: 1.10756e+07 billion years
Password Entropy: 112 bits

A Quantum Computer will break this password in: 68 days
Password Entropy: 56 bits
```

Figure 5: Test cases for inputted passwords

In Figure 5 above, it depicts two different passwords being inputted in the program to test its vulnerability to a brute-force attack. For the first example, “Villanova22” is an 11-character password that would take 165 years for a classical computer to brute-force. However, it can be cracked almost instantly using Grover’s search algorithm. An important observation is that the password entropy decreases by a factor of 2 from using Grover’s algorithm. Password entropy is a measurement of how strong a password is and determines the difficulty of it being cracked through various attack methods. For the second example, “vampireBuBBles99!” is a strong passphrase that is resistant to a quantum brute-force attack. This is mostly due to the length of the password being 17-characters. Adding characters to a password exponentially increases the computational time to perform a brute-force attack, making it crucial to have a long password to remain secure. Therefore, this software model demonstrates how an organization could ethically crack passwords to test its security against a quantum brute-force attack, which will be a critical attack vector once quantum computing is widely available.

IV. Conclusion

In a post-quantum era, the biggest threat to hashed passwords is Grover’s search algorithm, as this provides a substantial increase in computation power. Quantum computers will be able to brute-force passwords if their entropy is not strong enough. A password with 60 bits of entropy is considered strong enough to resist a brute-force attack, which can be achieved by having a password with at least 16 characters in a post-quantum world. Therefore, having strong passphrases are able to resist attacks from a quantum computer. It is essential for organizations to be aware of the capability of a quantum brute-force attack and conduct ethical password cracking tests to ensure security on all password-protected systems.

References

[1] C. G. Almudever et al., "Towards a scalable quantum computer," 2018 13th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS), 2018, pp. 1-1.

[2] P. Shrivastava, K. K. Soni and A. Rasool, "Evolution of Quantum Computing Based on Grover's Search Algorithm," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6.

[3] Fisher, C. (2009, April 2). *IBM: What is Quantum Computing?* IBM Quantum. Retrieved December 6, 2021, from https://www.ibm.com/quantum-computing/what-is-quantum-computing/.

[4] *Grover's algorithm*. IBM Quantum. (n.d.). Retrieved December 6, 2021, from https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm.

[5] *State of symmetric & hash algorithms after quantum computing*. REAL security. (2019, August 19). Retrieved December 6, 2021, from https://www.real-sec.com/2019/08/state-of-symmetric-hash-algorithms-after-quantum-computing/.

[6] Gao, X. (n.d.). *First, what is the post-quantum password?* Post quantum password (anti-quantum password) - Programmer All. Retrieved December 6, 2021, from https://www.programmerall.com/article/38501694136/.