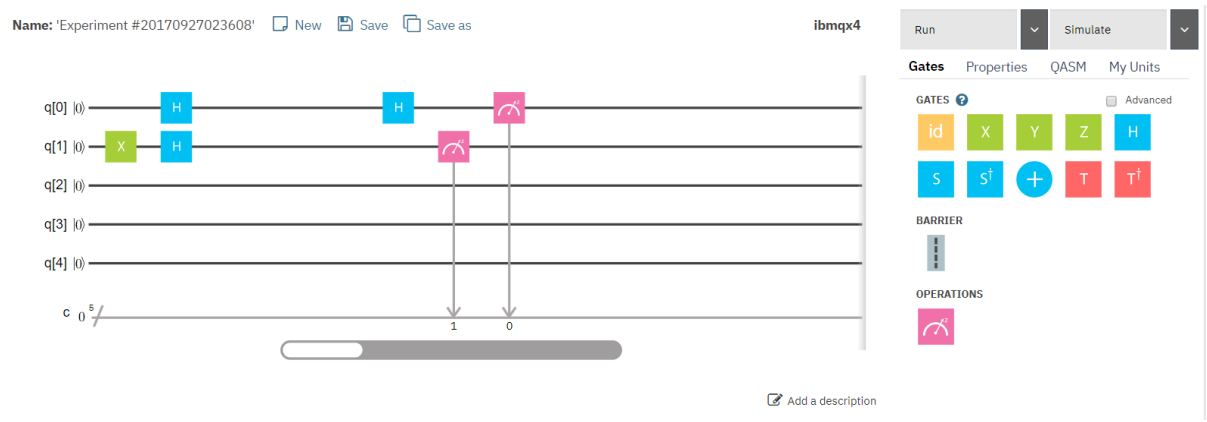
Advanced Information Security HW#2

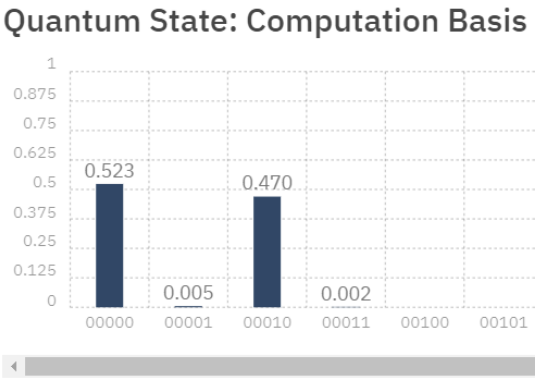
School of Computing, 20173245 Chansu Park

1. IBM quantum experience

IBM quantum experience(QX)는 IBM Cloud를 통해 IBM의 양자 프로세서에 누구든지 접속할 수 있게 하는 플랫폼이다. 사용자들은 QX를 통해 양자 알고리즘 등의 실험을 계획하고 실험할 수 있다.



IBM quantum experience의 composer 탭에 접속하면 보이는 화면이다. 먼저 양자 회로를 위의 GUI로 짜기로 결정했다면, 각 사용자는 최대 5개의 qubit과 최대 80개의 timeslot을 활용해 적절한 양자 게이트를 배치하는 것으로 양자 회로를 구성할 수 있다. 사용자들에 따라서는 양자 어셈블리 프로그래밍 언어나 Python으로 제공되는 API를 이용해서 프로그램을 작성할 수도 있다.



위의 회로를 예로 들자면, q[1]은 먼저 X gate를 통해 |0>에서 |1>로 바뀌었고, Hadamard gate를 거치면서 q[0:1] = $\{\frac{|0>+|1>}{\sqrt{2}}, \frac{|0>-|1>}{\sqrt{2}}\}$ 이 되었고, 이후 q[0]가 Hadamard gate를 한 번 더 거치면서 $\{|0>, \frac{|0>-|1>}{\sqrt{2}}\}$으로 바뀌었다. 그러나 현재의 양자 컴퓨터는 양자 각각이 오차를 가지고 있기 때문에, q[0]가 |0>으로 관측되지 않는 경우가 있음을 확인할 수 있다.

2. Shor's/Grover's Algorithm

Shor의 알고리즘은 주어진 자연수 N의 소인수분해를 기존의 방식보다 빠르게 하기 위해 개발된 알고리즘이다. 알고리즘은 크게 고전적 방법을 쓰는 부분과 양자적 방법을 쓰는 부분으로 나뉜다.

고전적 방법을 쓰는 부분에서는 소인수분해 문제를 함수의 주기를 구하는 문제로 reduce한다. 매 번, 주어진 자연수 N보다 작은 임의의 자연수 a를 선택해서 N과 a의 최대공약수가 1이 아니라면 N이 a로 나누어 떨어지기 때문에 a와 N/a를 소인수 분해하는 두 개의 문제를 풀 수 있다. 그렇지 않다면, N과 a가 서로소이기 때문에 $a^r \equiv 1 \ (mod\ N)$을 만족하는 가장 작은 자연수 $\mathrm{r} \leq \varphi(\mathrm{N})$이 존재한다. 이 r이 짝수이고 $\mathrm{a}^{\mathrm{r}/2} \not\equiv \pm 1 \ (\mathrm{mod}\ \mathrm{N})$을 만족한다면 $\mathrm{a}^{\mathrm{r}/2} \pm 1$과 N의 최대공약수는 1이 아니다. 따라서 이러한 주기 r를 찾는 문제를 푸는 것을 통해 소인수분해 문제를 풀 수 있다. 그러나 고전적 방법을 쓸 경우에는 주기를 찾는 것이 매우 어렵다.

이 때문에 양자적 방법을 통해 주기를 빠르게 찾는 것이 이 알고리즘의 핵심이여, 이 과정에서 사용되는 것이 양자 푸리에 변환(Quantum Fourier Transform)이다. 결론적으로, Shor의 알고리즘은 자연수 N의 소인수분해를 average time complexity $O(\{\log N\}\text{^}3)$ 안에 완료한다.

Grover의 알고리즘은 내부 구조를 모르는 함수가 size가 N인 정의역을 가질 때 $O(\sqrt{N})$번의 시도 안에 1에 가까운 확률로 원하는 출력을 뱉는 입력을 구하는 알고리즘이다. 고전적인 방법으로는 평균 N/2번, 최악의 경우 N번의 시도가 필요하다는 점에서, N의 크기가 매우 큰 문제에 대해 유용한 알고리즘이다. 예를 들어 2^{n}-bit 대칭 키 암호의 경우, brute-force 알고리즘으로는 최대 2^{n}번의 시도를 해야 맞는 키를 찾을 수 있으나, Grover의 알고리즘을 사용하면 1에 가까운 확률로 $2^{\mathrm{n}/2}$번만에 찾을 수 있기 때문에 키의 길이를 늘려야 양자 컴퓨터를 활용한 공격에 안전하다는 결론이 나온 상태이다.

또한 Grover의 알고리즘이 나온 시간대에 Bennett, Bernstein, Brassard와 Vazirani가 위에 제시된 문제를 푸는 어떤 양자 알고리즘도 $O(\sqrt{N})$번보다 asymptotic한 관점에서 작은 계산복잡도를 가질 수 없다는 것을 증명함으로서, 양자 컴퓨팅의 한계를 보여주는 대표적인 알고리즘이 되었다.