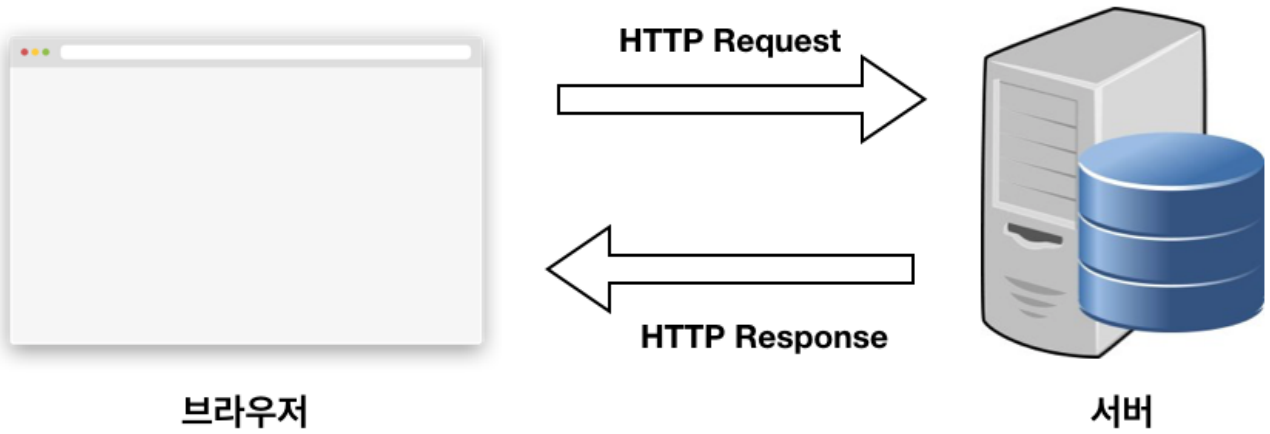
RSA 암호화 탐구 보고서

이민기 / 김연준

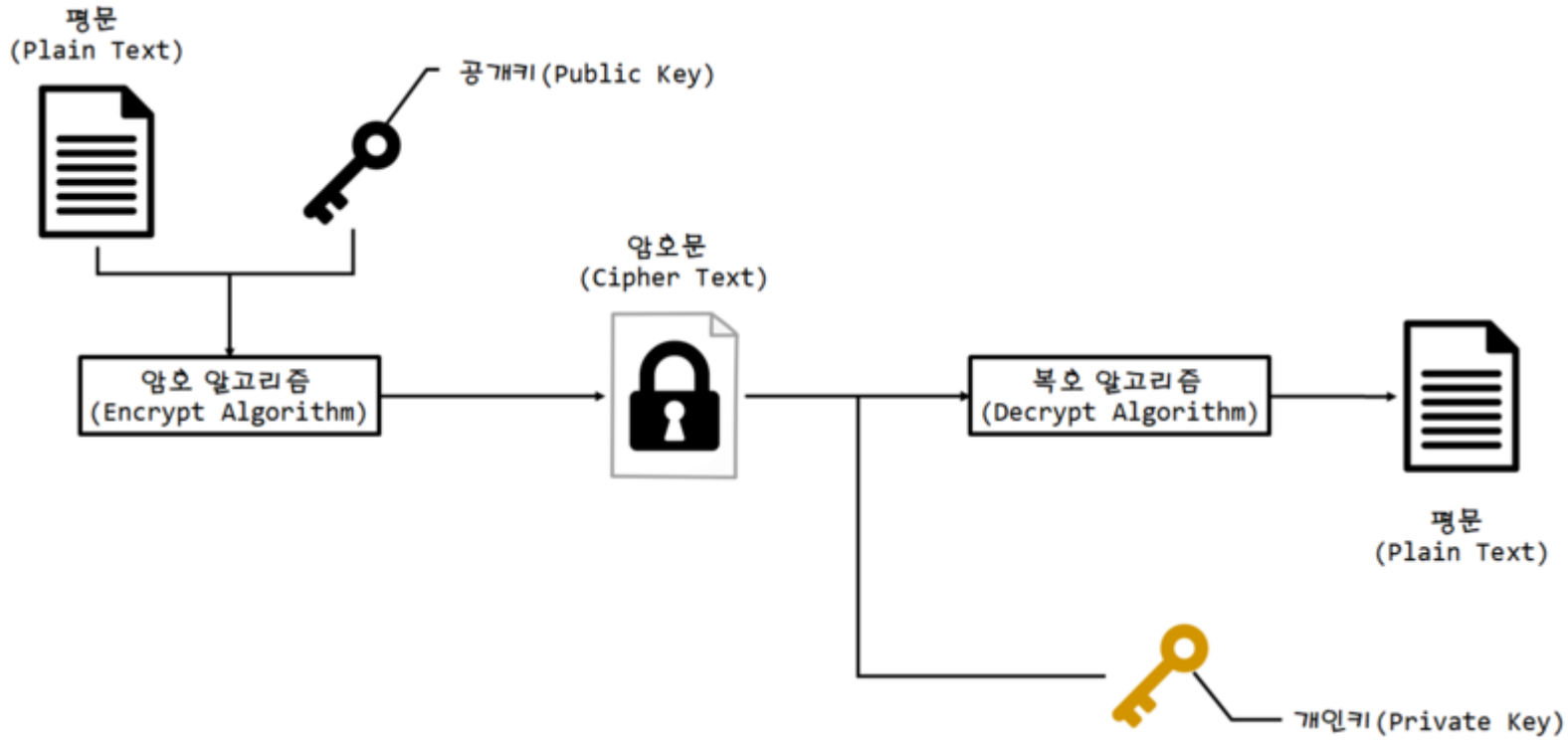
RSA 암호: 현재 SSL/TLS 에서 가장 많이 사용되는 공개 키 암호화 알고리즘



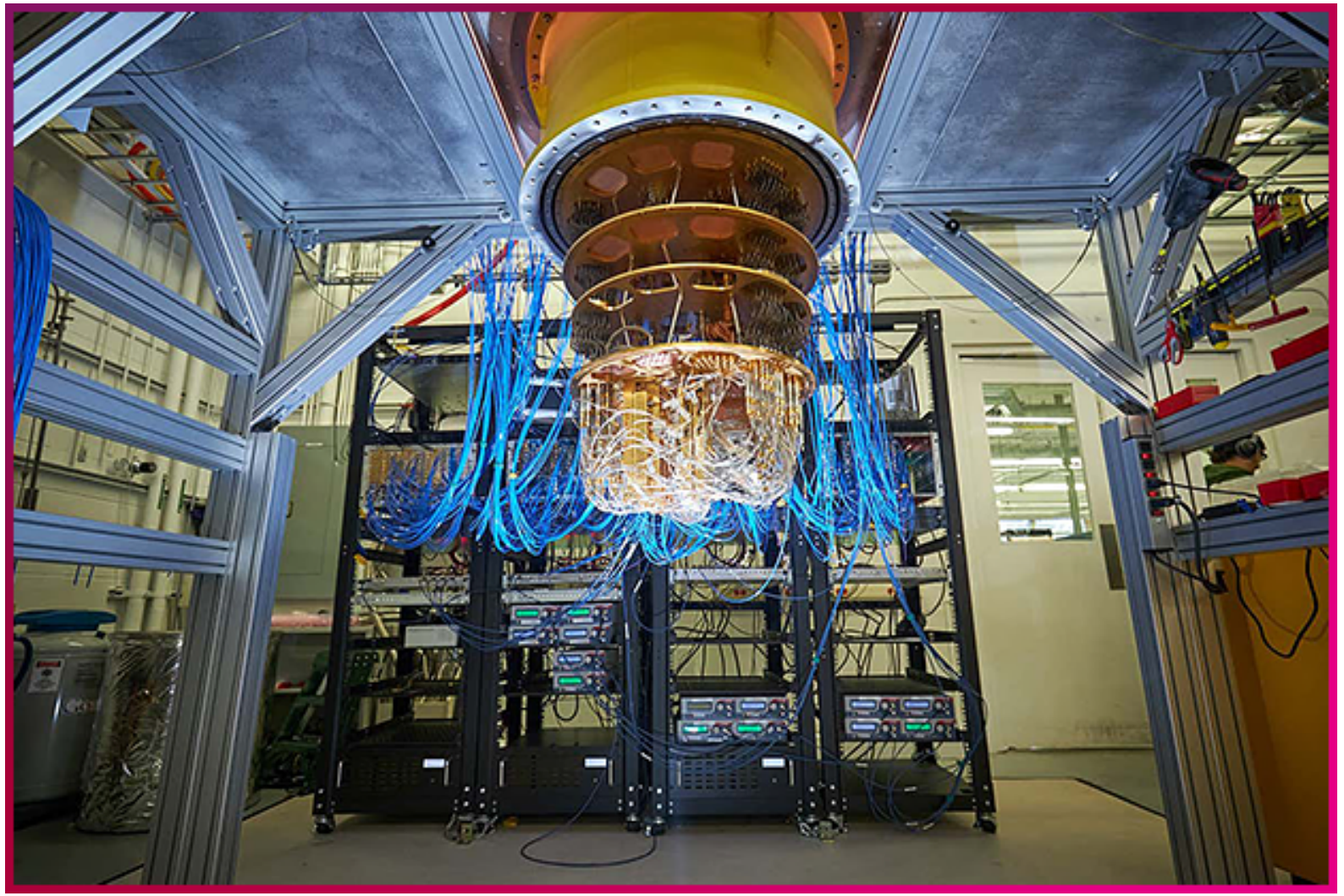
--> 광범위하게 사용되고 있음

RSA 알고리즘의 수학적 원리

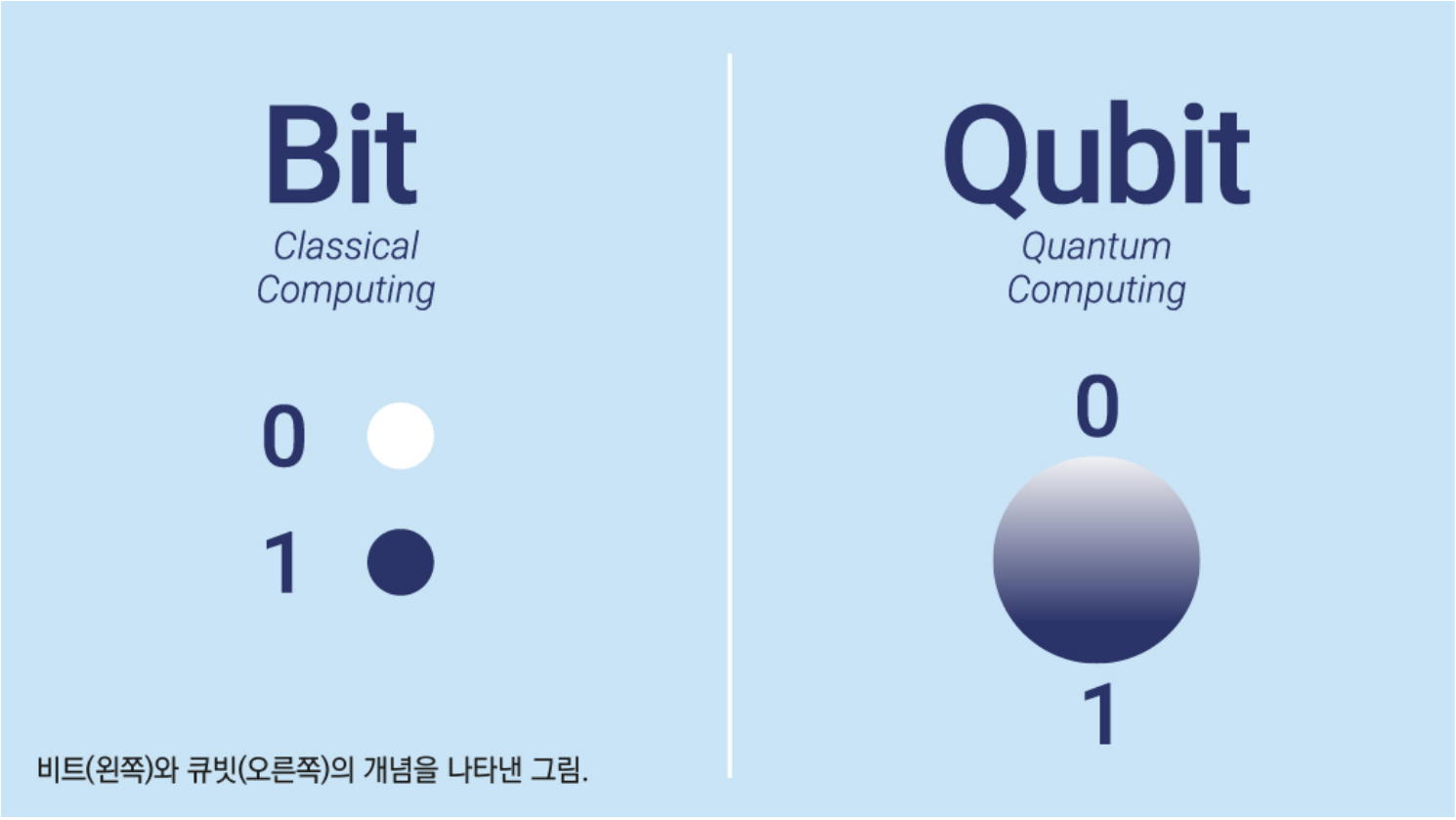
- 큰 소수가 곱해진 수의 인수분해의 어려움을 이용함
- 페르마 소정리
- 오일러 피 함수
- 모듈러 연산



양자컴퓨터는 RSA 암호를 풀 수 있는가



양자 컴퓨터 란



비트(왼쪽)와 큐빗(오른쪽)의 개념을 나타낸 그림.

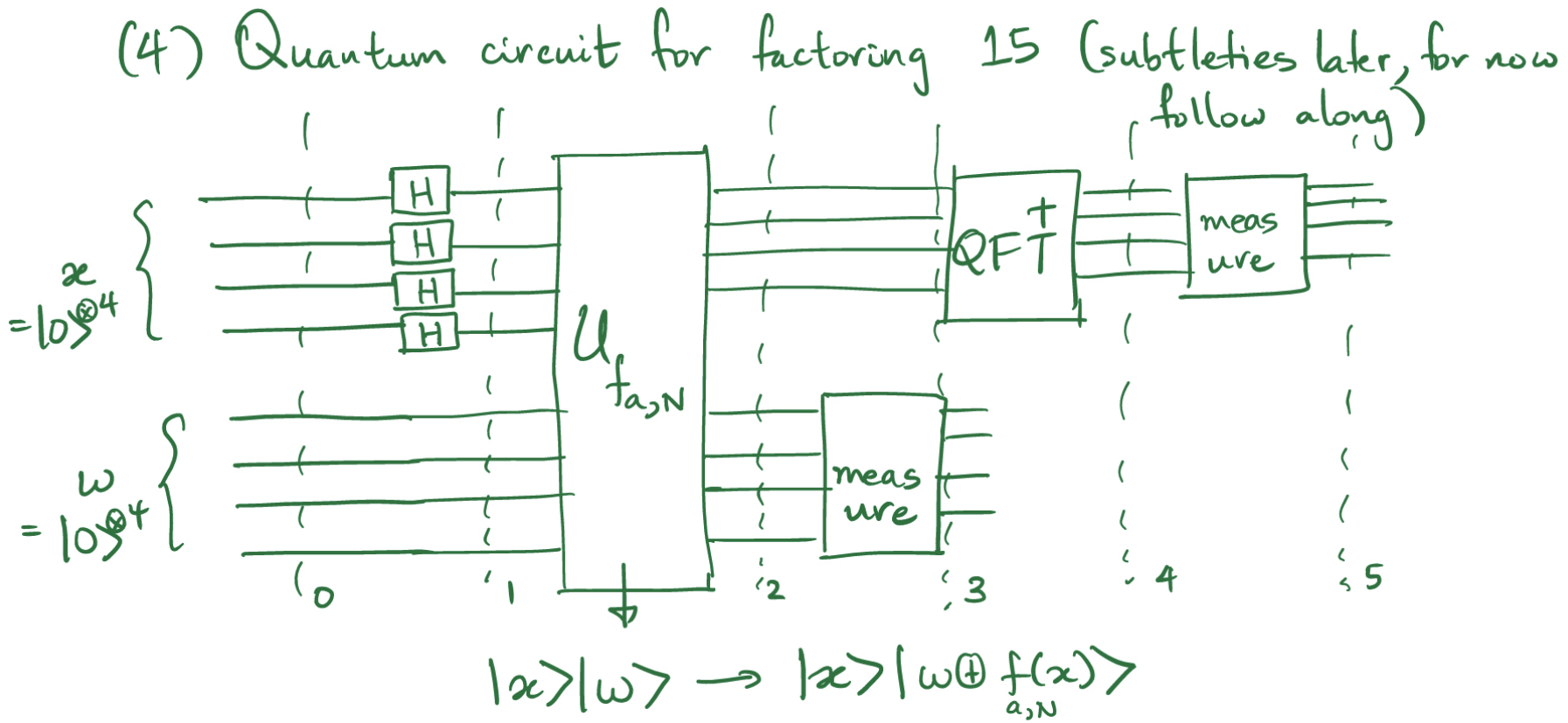
큐비트:: 0 또는 1을 동시에 공존 시킬수 있음

고전 컴퓨터가 천문학적인 시간이 걸리는 문제를 몇분 만에 풀 수 있다.

고전컴퓨터는 소인수 분해를 하려면 2부터 나눠보며 나머지가 0인 값을 저장한 후 다시 그 정수에 대해 2부터 차근차근 나눔.

양자컴퓨터--> **쇼어 알고리즘**

쇼어 알고리즘


(4) Quantum circuit for factoring 15 (subtleties later, for now follow along)
H
H
H
H
$U_{f_{a,N}}$
QFT†
meas ure
meas ure
$|0\rangle^{\otimes 4}$
$|0\rangle^{\otimes 4}$
x
w
0
1
2
3
4
5
$|x\rangle|w\rangle \rightarrow |x\rangle|w \oplus f_{a,N}(x)\rangle$

결론.

- RSA 암호화는 우리도 모르게 인터넷을 사용할때 많이 쓰이고 있다.
- RSA 와 같은 암호학은 수학으로 이루어진 기술이다.
- 양자 컴퓨터는 쇼어 알고리즘을 통해 RSA 암호의 핵심인 소수의 소인수 분해 과정을 무력화 시킬 수 있을것이다.
- 그러므로 수학자,컴퓨터 공학자들은 고전적인 암호화 방식보다 좀더 강력한 암호화 방식을 새롭게 만들 필요가 있을 것 같다.