Quantum Algorithm : Shor

https://youtu.be/LpwPDTM5RVQ

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Contents

CryptoCraft LAB

1 양자 알고리즘

양자 컴퓨터의 등장과 함께 나타난 새로운 양자 알고리즘

기존 컴퓨터에서 해결하기 어려운 수학적 난제들을 효율적으로 풀어냄

→ 이러한 난제에 기반한 현재 암호시스템들을 위협

암호학계에 끼친 영향 : 양자 컴퓨터에 내성을 가진 암호가 필요하게 되었음 -> Post Quantum Cryptography

2 NIST(National Institute of Standards and Technology) 발표

양자컴퓨터 시대에 대한 현재 암호시스템의 상황

유형	알고리즘	목적	영향
대칭키	AES	Encryption	키 길이 증가 필요
	SHA-2, SHA-3	Hash	출력 길이 증가 필요
공개키	RSA	Signature, Key establishment	더 이상 안전하지 않음
	ECDSA, ECDH	Signature, Key exchange	
	DSA	Signature, Key exchange	
	Diffie Hellman	Key exchange	

CryptoCraft LAB

2 Shor 알고리즘

1994년 수학자 Shor는 기존 컴퓨터에서의 난제인 **소인수분해 문제**를

효율적으로 풀어낼 수 있는 양자 알고리즘을 제안

커다란 두 소수를 곱하는 것은 쉽지만 이렇게 곱해진 매우 커다란 정수를 두 소수로 다시 분해하는 것은,두 소수 중 하나를 모른다면 매우 어려운 일 Ex) N = pq

$$O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right) \xrightarrow[\textit{use Shor's Algoritthm}]{} O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$$

지수 차원의 복잡도 → 다항시간내에 해결

Before *After*

결과 : 이러한 어려움에 기반한 암호시스템들을 무너뜨릴 수 있다. Ex) RSA

CryptoCraft LAB

3 소인수 분해 #1

Problem : 정수 N 에 대하여 소인수분해

N = 15, a = 7

Step 1.

a < *N* 인 난수 *a*를 선택한다.

Step 2.

gcd(a,N)을 구한다. * *gcd : greatest common divisor*

Step 3.

gcd(a,N) ≠ 1 이면, gcd(*a*,*N*) 이 바로 *N*의 인수이다. (소인수분해 완료)

7^1 > 7 mod 15 = 7
7^2 > 49 mod 15 = 4
7^3 > 343 mod 15 =13
7^4 > 2401 mod 15 = 1
7^5 > 16807 mod 15 = 7

Step 4.

그렇지 않은 경우, 주기 찾기 알고리즘을 이용하여

$f(x) = a^x$ mod N 일 때 $f(x+r) = f(x)$ 를 만족하는 차수 r을 구한다.

→ 주기 찾기 문제
(Order Finding)

CryptoCraft LAB

3 소인수 분해 #2

a = 7, r = 4

Step 5.

구해진 *r* 이 홀수이면 Step 1 로 돌아간다. (다시 수행한다.)

Step 6.

구해진 *r* 이 $a^{r/2} = -1 \pmod{N}$ 를 만족하면 Step 1 로 돌아간다. (다시 수행한다.)

Step 7.

그렇지 않은 경우, gcd($a^{r/2}$+1 , N) 과 gcd($a^{r/2}$-1 , N) 이 구하고자 하는 N의 인수이다.

Answer : gcd(50,15) , gcd(48,15)

3과 5 이므로 15 소인수분해 완료

CryptoCraft LAB

3 How?

기존 컴퓨터에서의 난제를 어떻게 해결하였는가?

$$O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right) \xrightarrow[\textit{use Shor's Algoritthm}]{} O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$$

지수 차원의 복잡도 → 다항시간내에 해결

CryptoCraft LAB

3 Where?

Step 1.

$a < N$ 인 난수 a를 선택한다.

Step 2.

gcd(a,N)을 구한다. ** gcd : greatest common divisor*

Step 3.

$gcd(a,N) \neq 1$ 이면, gcd(a,N) 이 바로 N의 인수이다. (소인수분해 완료)

Step 4.

그렇지 않은 경우, 주기 찾기 알고리즘을 이용하여

$f(x) = a^x$ mod N 일 때 $f(x + r) = f(x)$ 를 만족하는 차수 r을 구한다.

→ 주기 찾기 문제 (Order finding)

CryptoCraft LAB

3 How?

Step 4.

그렇지 않은 경우, 주기 찾기 알고리즘을 이용하여

$f(x) = a^x$ mod N 일 때 $f(x + r) = f(x)$ 를 만족하는 차수 r을 구한다.

→ 주기 찾기 문제 (Order finding)

Solution !

양자 컴퓨터가 여러 상태에 동시에 존재할 수 있다는 성질을 이용

함수 $f(x)$의 주기를 계산하기 위해서 모든 x 점에서의 함수 값을 동시에 계산한다.

반복이 필요한 주기 찾기 작업을 한 번의 계산으로 가능하게 하여 계산 복잡도를 크게 낮춘다!

→ 쇼어 알고리즘

CryptoCraft LAB

4 Fourier transform

푸리에 변환 : 시간에 대한 신호를 그 신호를 구성하고 있는 주파수로 분해하는 작업

신호(함수)의 크기와 위상을 보기위해 사용되던 공식

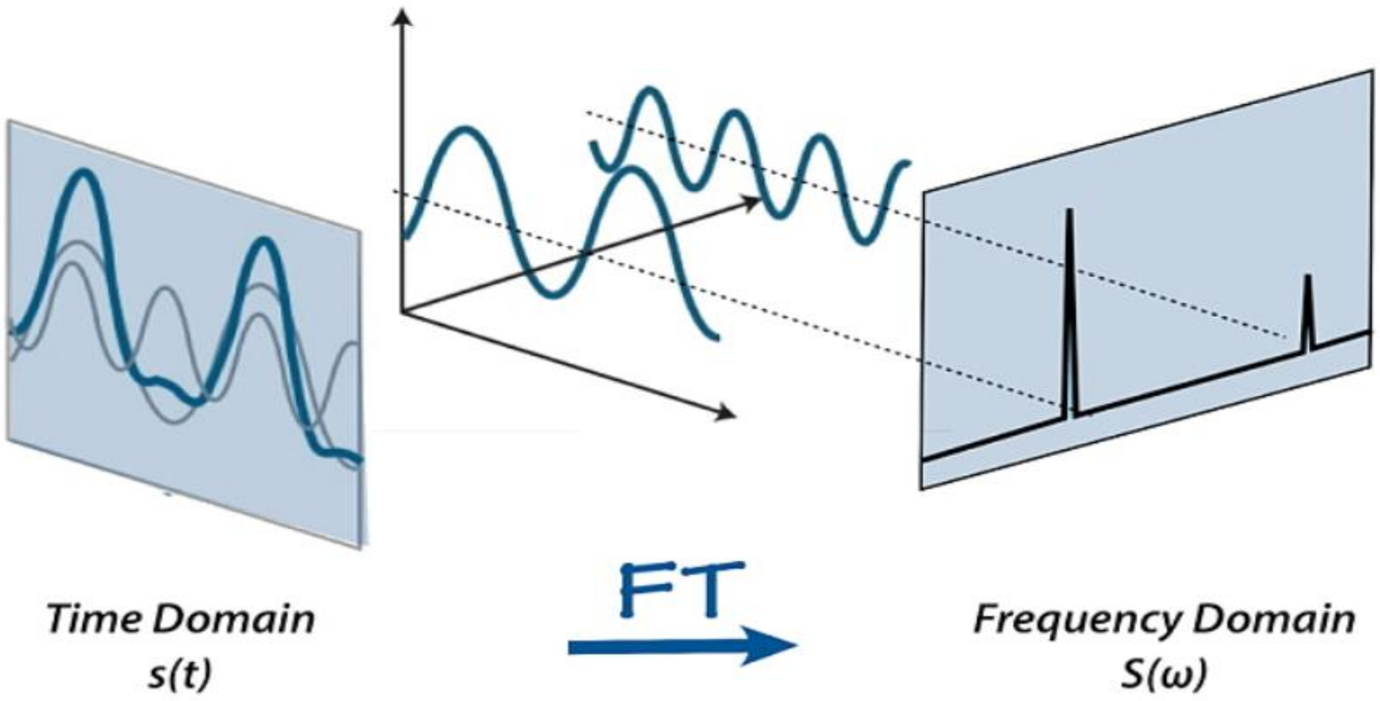
이산 푸리에 변환 : 컴퓨터같은 디지털 장치에서 쓰기 위한 푸리에 변환의 한 종류

이산적인 입력에 대한 신호(함수)를 분석하여 크기, 위상을 확인하는데 사용된다.

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N} kn}, \quad k = 0, \ldots, N-1$$

CryptoCraft LAB

4 Fourier transform



CryptoCraft LAB

4 Quantum Fourier transform(QFT)

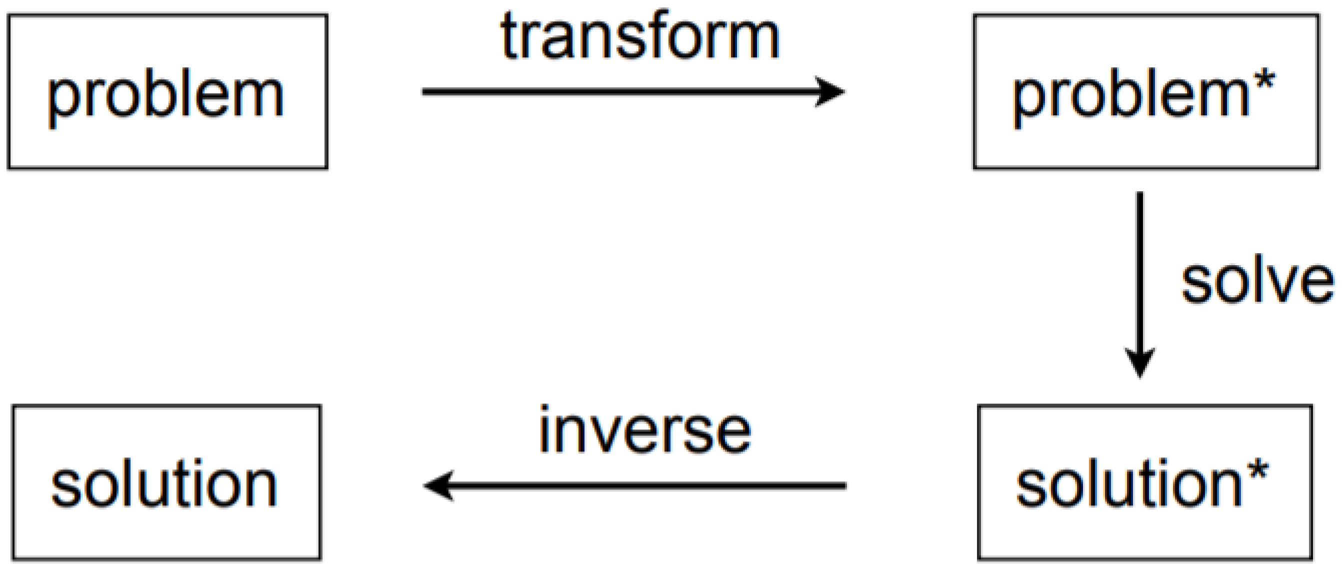
양자 푸리에 변환 : $$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi ijk/N}\alpha_j$$

기존 푸리에 변환을 양자역학에 적용한 것

Shor 의 소인수분해 알고리즘은 이 양자 푸리에 변환의 성질을 핵심원리로 이용

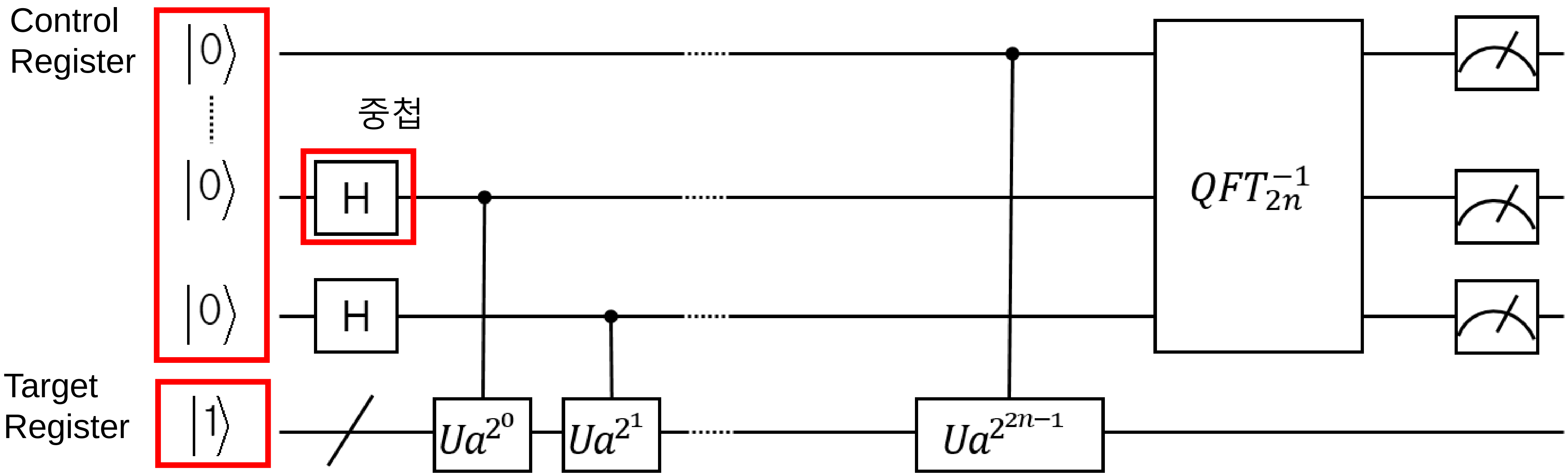
CryptoCraft LAB

4 Quantum Fourier transform(QFT)



CryptoCraft LAB

5 Shor 알고리즘 : Order Finding



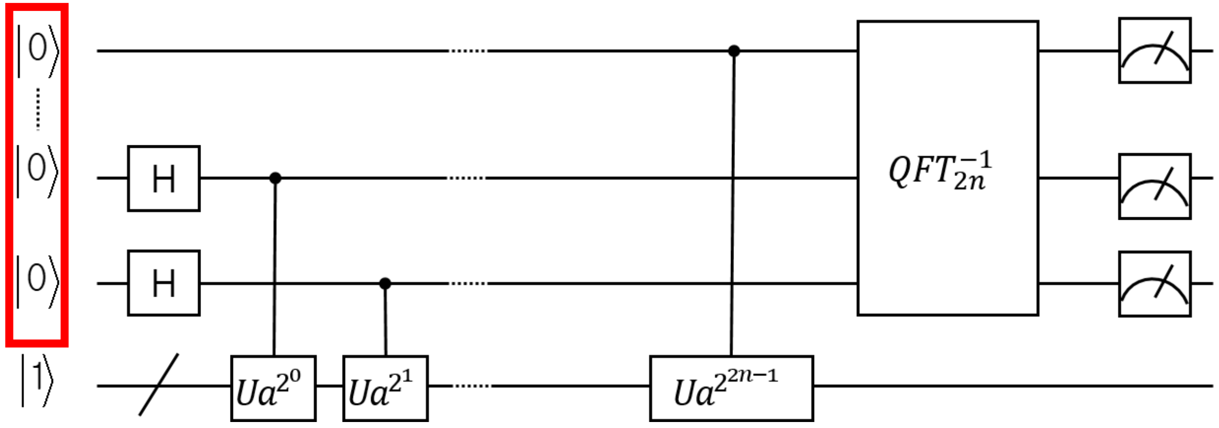
CryptoCraft LAB

5 Control Register

첫번째 레지스터(Control register)에 입력 데이터를 저장한다.

Ex) n = 15?

4개의 큐비트가 필요



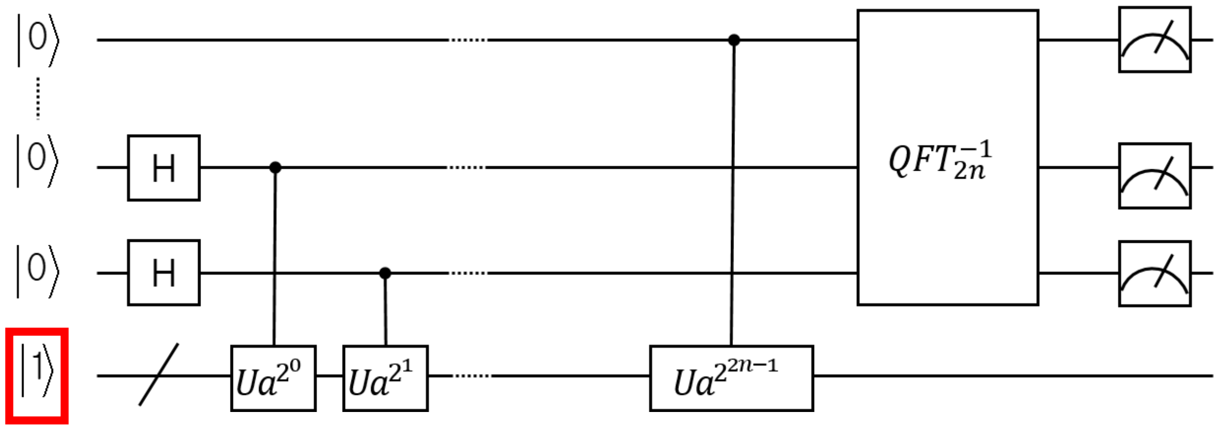
CryptoCraft LAB

5 Target Register

두번째 레지스터(Target register)에 출력 데이터를 저장한다.

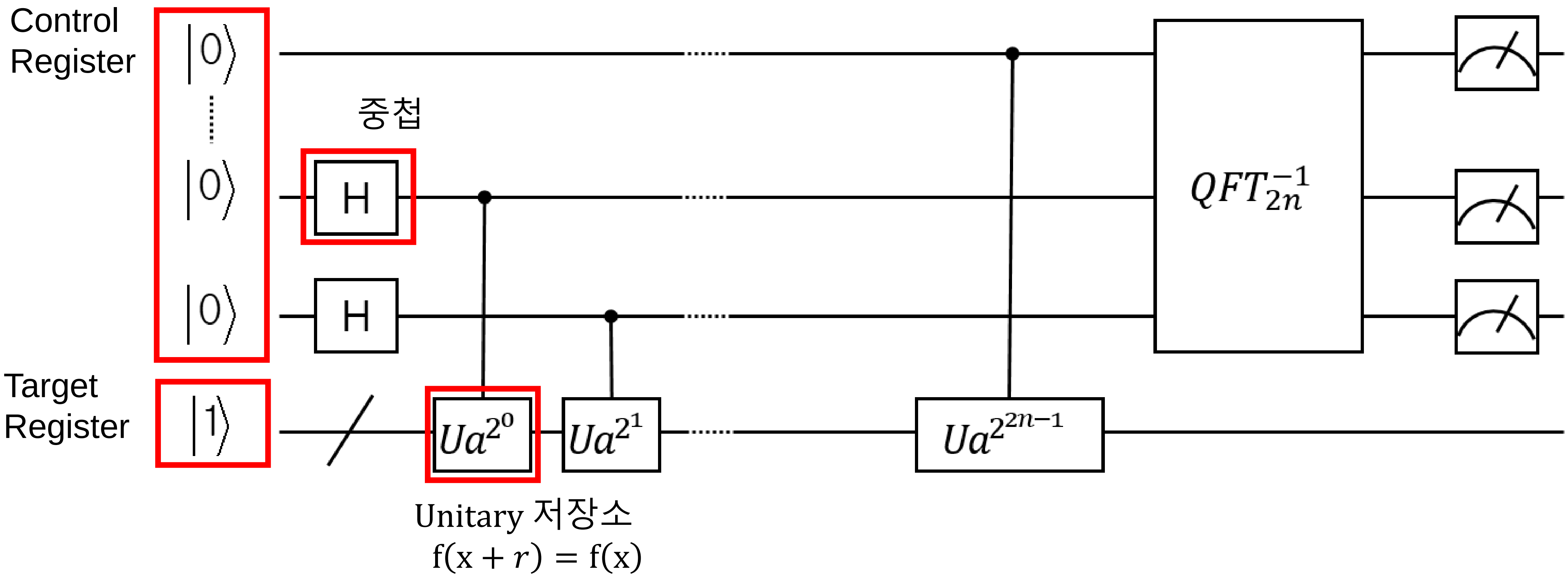
Ex) f(x) = f(x+r)

중첩 상태를 이용한 모든 입력에 대한 함수 결과값을 구현한다.



CryptoCraft LAB

5 Shor 알고리즘 : Order Finding



CryptoCraft LAB

5 Unitary

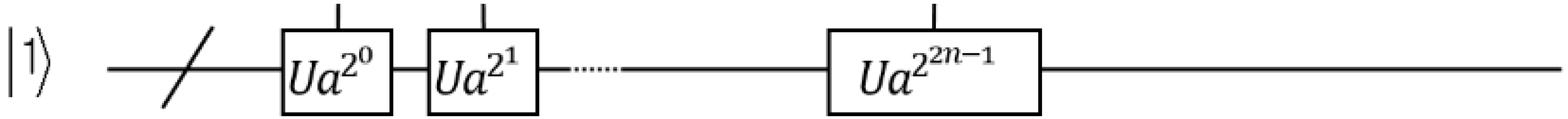
모든 입력 값의 중첩(Superposition)을 준비할 수 있고, 그 함수 계산을 단지 한번 작용함으로써 모든 함수 값에 관한 정보가 들어있는 양자상태를 구현할 수 있다.

→ **자연스러운 양자 병렬처리**

유니터리는 양자를 행렬로 변환했을 때 역행렬이 항상 존재한다는 의미

즉 양자에 어떤 변환을 가했을 때 역변환이 항상 성립해야 한다는 것이다.

결과값으로부터 입력 값을 다시 찾는 것이 가능 해야함 **그러나** Ex) $x^2 = 1$?



CryptoCraft LAB

5

1. $|0\rangle\,|u\rangle$ **Initiialize**

2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,|u\rangle$ **SuperPosition**

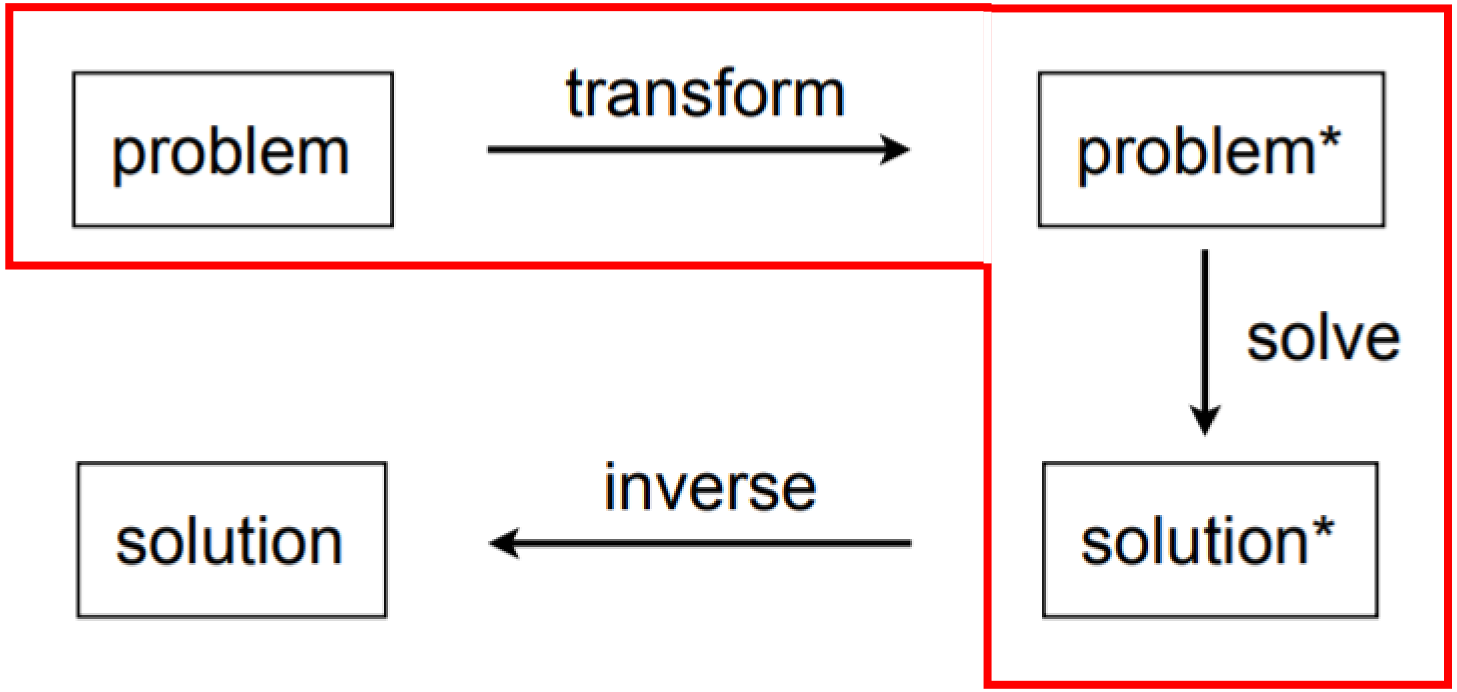
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j\,|j\rangle\,U^j\,|u\rangle$ **Apply U box**

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} x_j e^{2\pi i j \varphi_u}\,|j\rangle\,|u\rangle$$

양자 푸리에 변환 : $\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} \alpha_j$

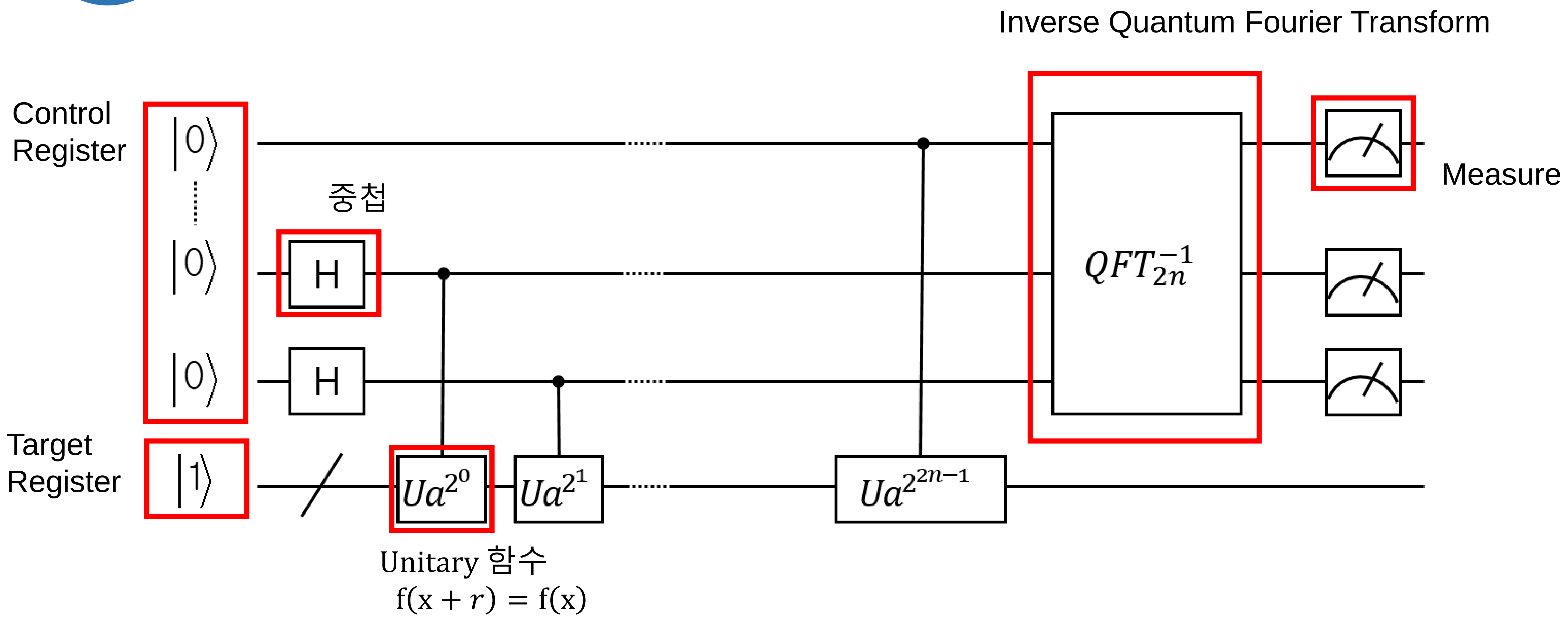
CryptoCraft LAB

5



CryptoCraft LAB

5 Shor 알고리즘 : Order Finding

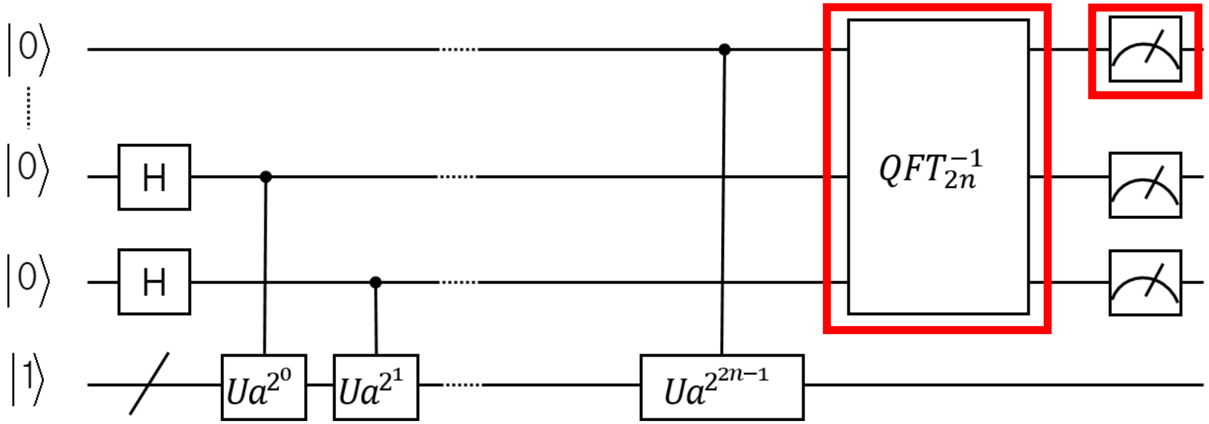


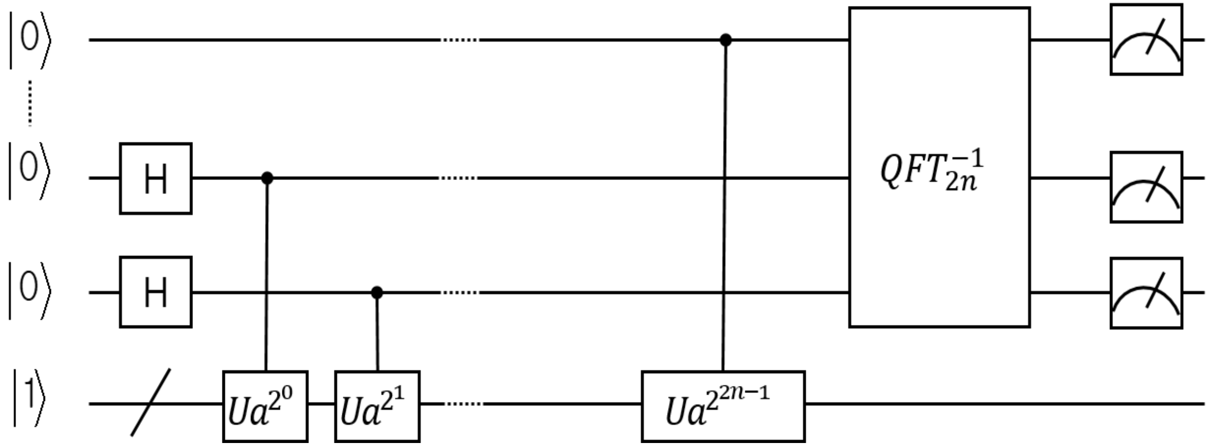
CryptoCraft LAB

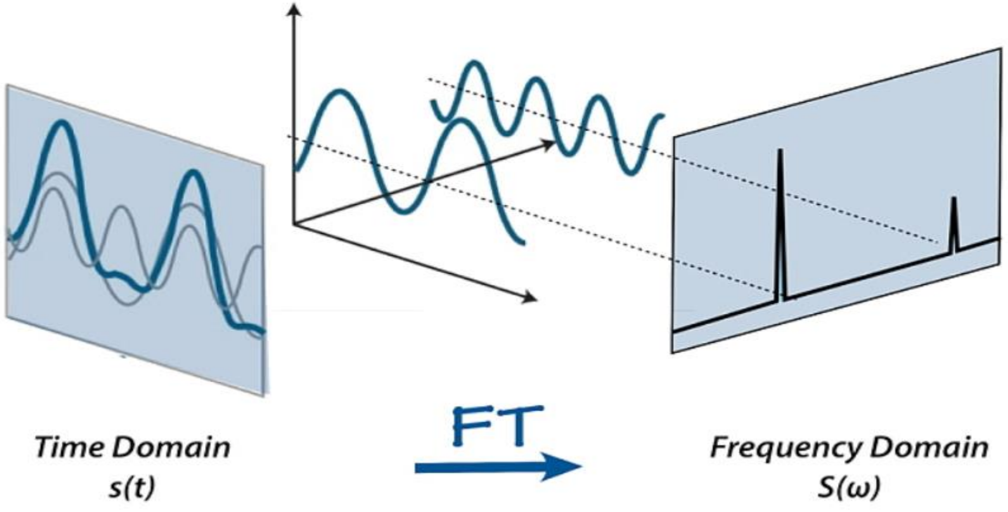
5 Quantum Fourier Transform (QFT)

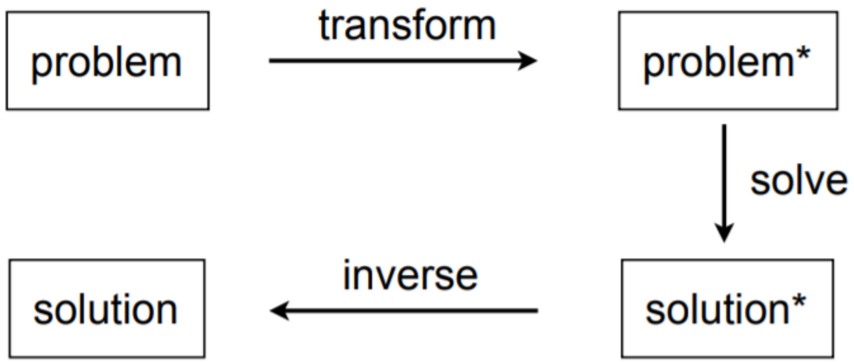
양자 푸리에 변환 : 기존 푸리에 변환을 양자에 적용한 것

입력 큐비트에 **역 푸리에 변환**을 통해서 위상에 대응하는 수치를 정량적으로 표현합니다.









어떠한 양자 측정도 그 모든 계산 된 값을 전부 추출할 수는 없으나

함수의 출력 값의 광역적인 성질에 대해서 → 주기

그 함수에 대한 정보를 얻어낼 수 있는 방법이 존재한다는 것

Thank You

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB