양자컴퓨팅 기초세미나 발표

Grover algorithm의 다양한 활용분야

산업경영공학부 김근호 / 전수민 / 조상현

Introduction

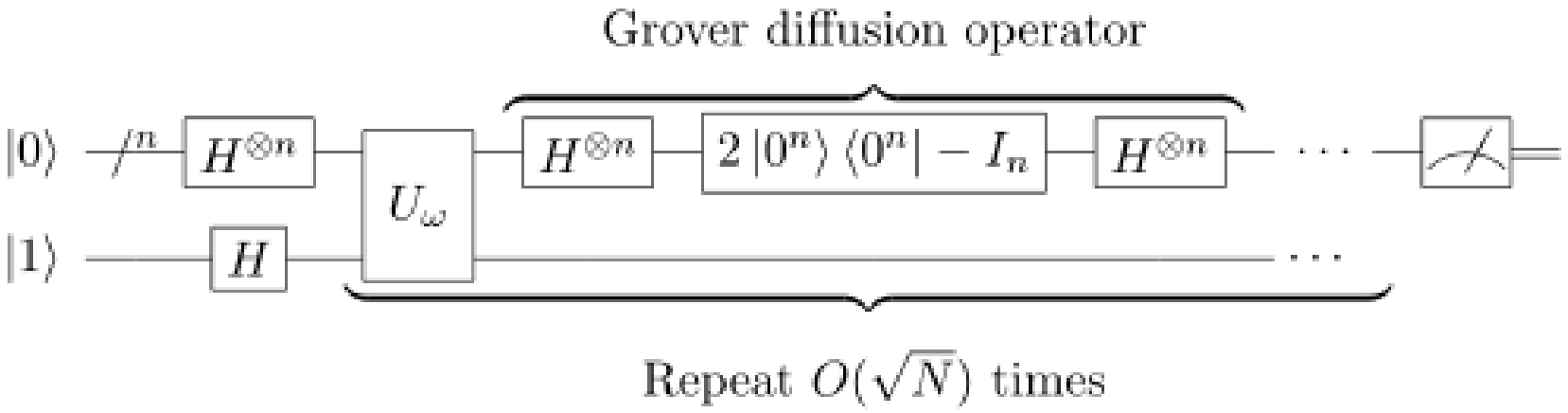
Content

Method

Grover Algorithm 소개

Grover Algorithm이란?

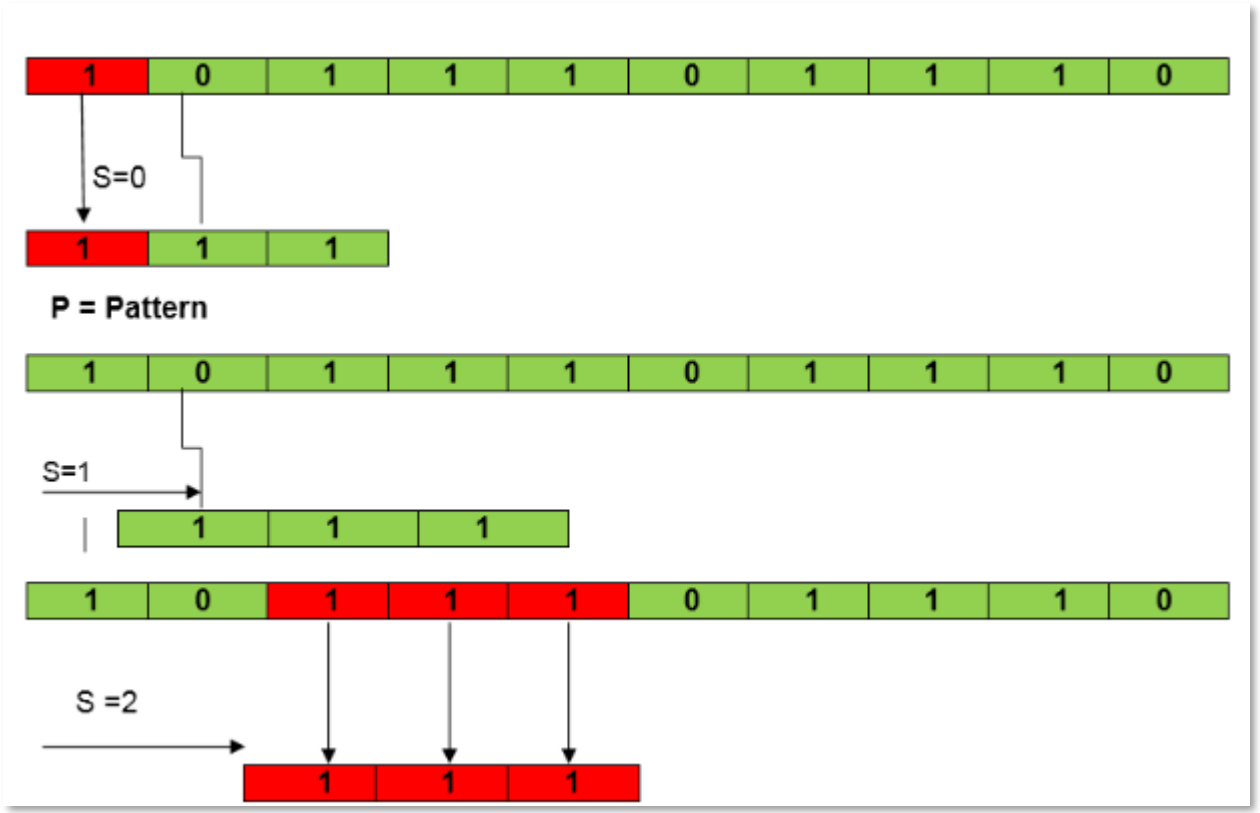
- Quantum Algorithm that finds with high probability the unique input to a black box function that produces a particular output value, using just O($\sqrt{N}$)



Application

활용 분야 소개 - Pattern Matching

Pattern Matching이란?



데이터를 검색할 때 특정 문자열이

출현하는지, 또한 어디에 출현하는지 등을 특정하는 방법의 일종

Application

활용 분야 소개 - Pattern Matching

Pattern Matching의 활용분야

- 이미지를 통한 불량품 검사
- 챗봇 알고리즘

Application

활용 분야 소개 – Pattern matching

Pattern Matching Algorithm – Classical Computer

- Brute-Force 알고리즘 → O(MN)
- KMP 알고리즘 → O(M + N)
- Boyer – More 알고리즘 → 일반적으로 O(N)보다 작음

인덱스	0	1	2	3	4	5	6	7	8	9	10	11
텍스트	A	B	C	D	A	B	C	D	A	B	E	E
패턴	A	B	C	D	A	B	E					

[KMP 알고리즘 예시]

Pattern Matching Algorithm – Quantum Computer

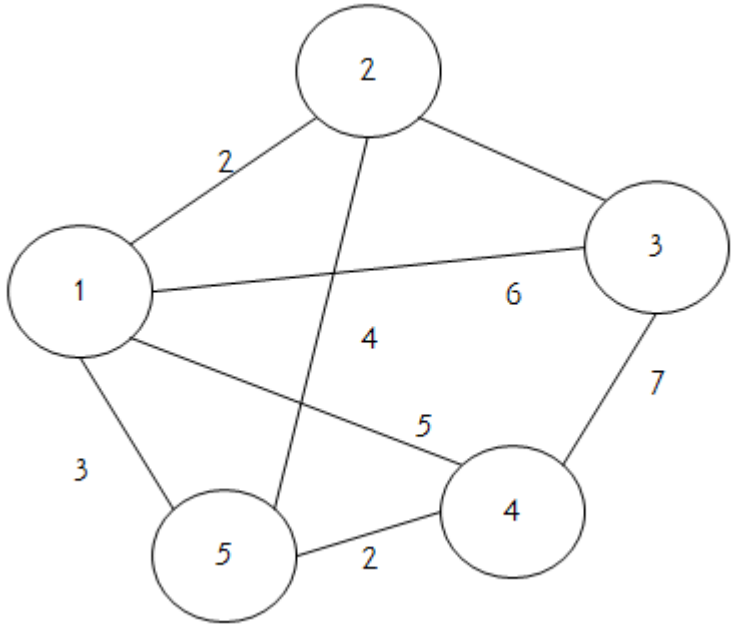
- Grover Algorithm → $O(\sqrt{N})$

Application

활용 분야 소개 – TSP

TSP 란?

- Traveling Salesperson Problem의 약자로, 외판원 순회 문제라고 불리어진다.



Application

활용 분야 소개 – TSP

Traveling Salesperson Problem – Classical Computer

- 선형 최적화 →O((n-1)!)

$$x_{ij} = \begin{cases} 1 & \text{the path goes from city } i \text{ to city } j \\ 0 & \text{otherwise} \end{cases}$$

$$\min \sum_{i-1}^{n} \sum_{j \neq i, j=1}^{n} c_{ij} x_{ij} :$$

$$0 \leq x_{ij} \leq 1 \qquad i, j = 1, \ldots, n;$$

$$\sum_{i-1, i \neq j}^{n} x_{ij} = 1 \qquad j = 1, \ldots, n;$$

$$\sum_{j=1, j \neq i}^{n} x_{ij} = 1 \qquad i = 1, \ldots, n;$$

$$\sum_{i \in Q} \sum_{j \in Q} x_{ij} \leq |Q| - 1 \qquad \forall Q \subsetneq \{1, \ldots, n\}, |Q| \geq 2$$

- MetaHeuristics

Tabu Search → O(n^3)
Simulated Anneling →O(n^2)

Application

활용 분야 소개 – TSP

Traveling Salesperson Problem– Quantum Computer

- Grover Algorithm → $O(\sqrt{N})$

$$\hat{C}\,|T\rangle = e^{i\phi(T)}\,|T\rangle\,,$$

where $\phi(T)$ stands for the overall cost, given tour T

Application

활용 분야 소개 – TSP

Traveling Salesperson Problem– Quantum Computer

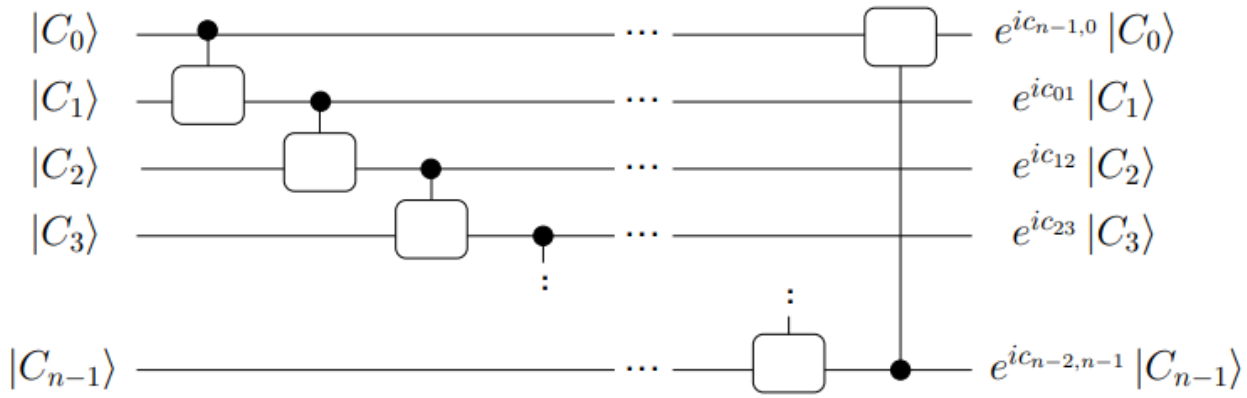


FIG. 1: Simple quantum circuit for cost oracle.

$$|T\rangle = |C_0\rangle \otimes |C_1\rangle \otimes \cdots \otimes |C_{n-1}\rangle ,$$

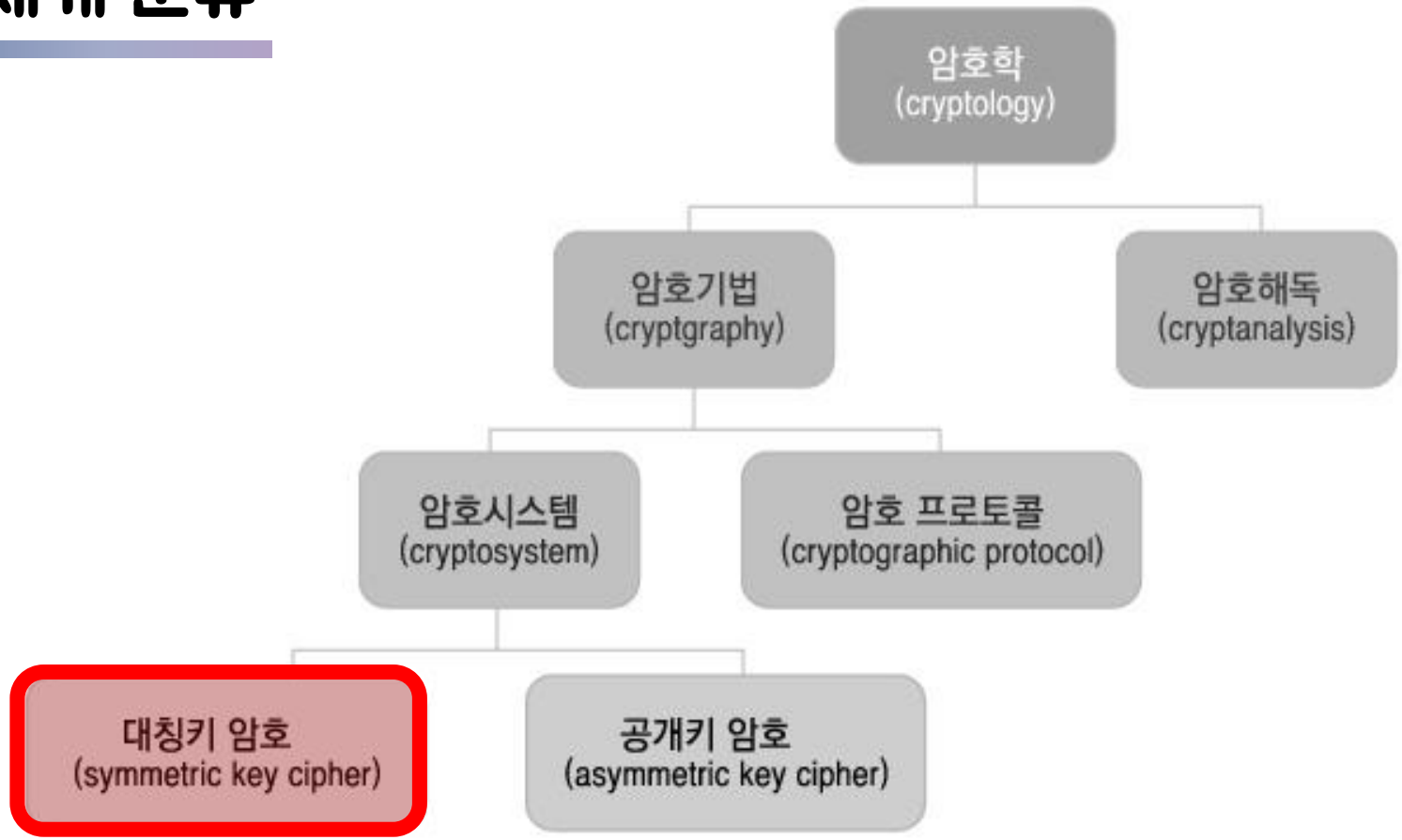
where $|C_k\rangle$ stands for the k-th visiting city, and $|C_0\rangle$ is both the starting city and finally visiting city.

$\hat{P}_{jk}|C_j\rangle|C_k\rangle = e^{ic_{jk}}|C_j\rangle|C_k\rangle$, where c_{jk} denotes the cost from j-th to k-th visiting city.

Application

활용 분야 소개 – 대칭키 암호 해독

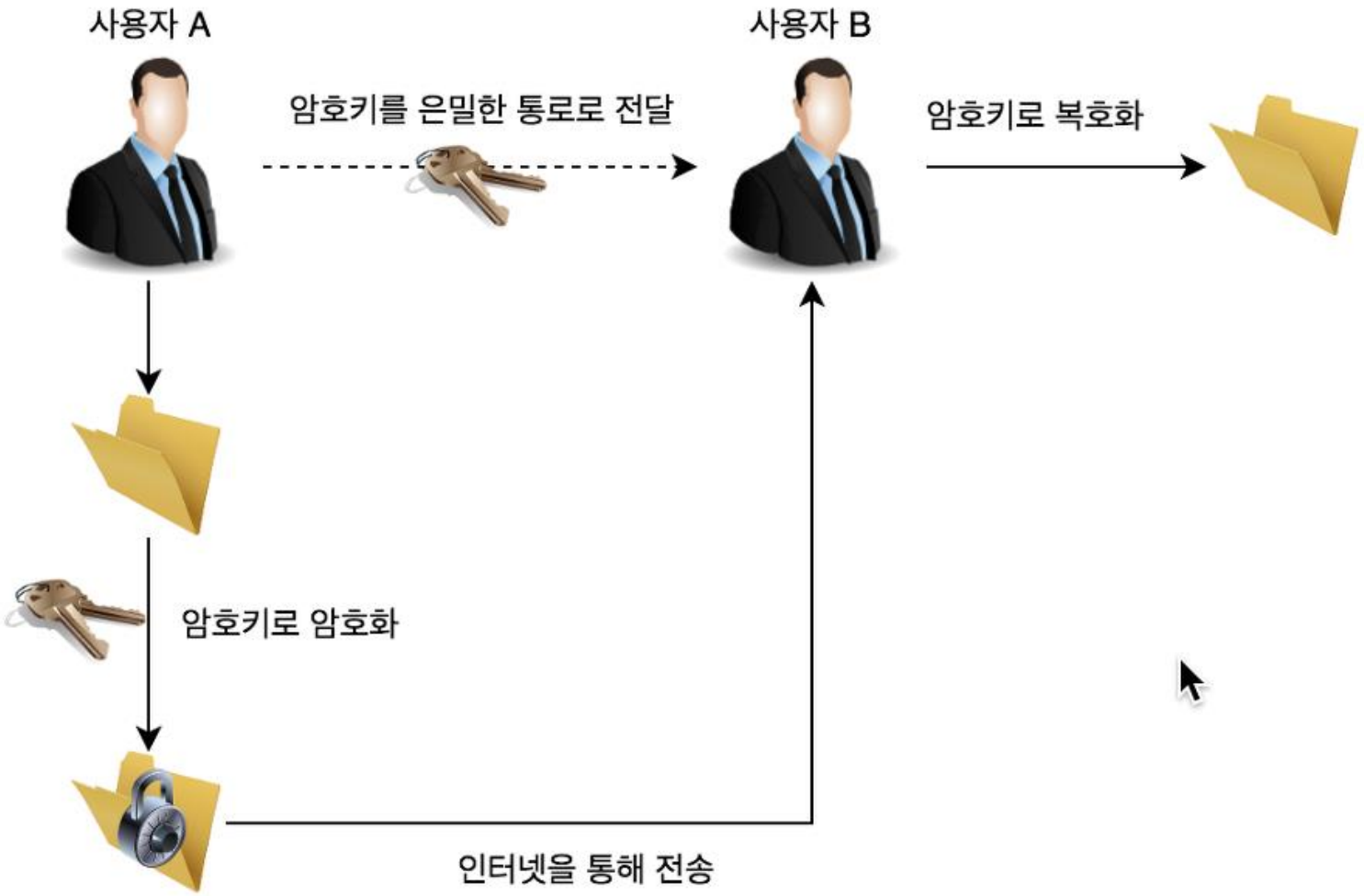
암호의 체계 분류



Application

활용 분야 소개 – 대칭키 암호 해독

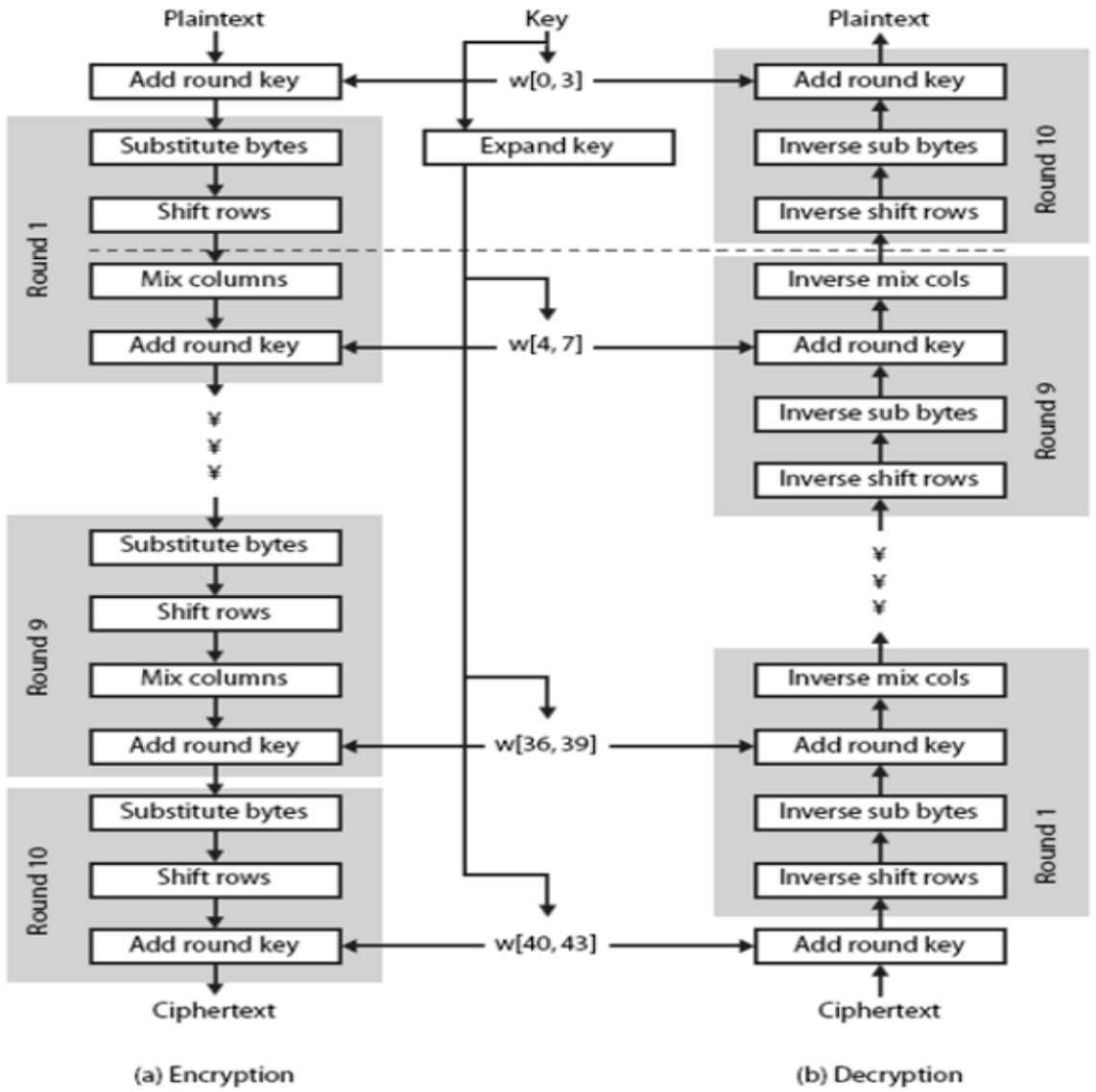
대칭키 암호란?



Application

활용 분야 소개 – 대칭키 암호 해독

AES



Advanced Encryption Standard

Application

활용 분야 소개 – 대칭키 암호 해독

양자암호(QKD) 시스템

Key-bit	0	1	0	1	1	0	1	0
Basis-bit	1	1	0	0	0	0	1	1
Basis	X	X	+	+	+	+	X	X
Photon	↗	↖	→	↑	↑	→	↖	↗

Basis-bit	1	0	1	0	0	1	0	1
Basis	X	+	X	+	+	X	+	X
Photon	↗	↖	→	↑	↑	→	↖	↗
Key-bit	0	0/1	0/1	1	1	0/1	0/1	0

보안 기술 중 하나인 대칭 키 분배 기술을 위하여 개발된 시스템으로
양자 역학적 원리를 근간으로 키를 분배함

양자는 관측시 붕괴되기 때문에 도청자의 도청 시도 여부를 통해 확인 가능

Conclusion

결론 및 의의

의의 및 한계

- 양자 알고리즘 개발 및 연구의 필요성
- 산업공학적 시각의 중요성

Q n A