양자정보이론

한국과학기술원 물리학과
양자정보연구실
정 용 욱

순서

- Basic notation & operation
- Entanglement
- Non-locality
- Quantum Cryptography
- Quantum Teleportation
- Quantum Computation
- Implementation

Basic notation

- Qubit: $|\psi\rangle = a|0\rangle + b|1\rangle$

  $|0\rangle = |z+\rangle, |1\rangle = |z-\rangle$
- Notation for many qubits:

  $|i\rangle \otimes |j\rangle = |i\rangle_1 |j\rangle_2 = |i\rangle|j\rangle = |ij\rangle$
- Operation on qubits: $A \otimes B\left(|i\rangle \otimes |j\rangle\right) = A|i\rangle \otimes B|j\rangle$
- Notation for operation: $A \otimes B = A_1 B_2$
- Ex) $A \otimes I = A_1$

Basic Operation(I)

- Single qubit operations: X ,Z, H

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$$

$$Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Basic Operation(II)

- XOR-gate

$$U_{XOR}|i\rangle|j\rangle = |i\rangle|i \oplus j\rangle \Rightarrow \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases}$$

- Universal gates:1-qubit operations+ XOR

Entanglement(pure state)

- Separable State: $|\psi\rangle = |\psi_1\rangle_A \otimes |\psi_2\rangle_B \otimes \cdots$
- Bell states: $$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right)$$ $$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right)$$
- GHZ states: $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|i\rangle_A|j\rangle_B|k\rangle_C - |\bar{i}\rangle_A|\bar{j}\rangle_B|\bar{k}\rangle_C\right)$

Entanglement(mixed state)

- Separable state: $\rho = \sum p_i \rho_i^A \otimes \rho_i^B \otimes \cdots, \; p_i \geq 0$

- Entanglement 구별법?
- Entanglement measure: $E(|\psi\rangle_{AB}) = S(\rho_A)$

Non-locality of entangled state

- Non-local correlation:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|z+\right\rangle_A \left|z-\right\rangle_B - \left|z-\right\rangle_A \left|z+\right\rangle_B\right)$$

$$= \frac{1}{\sqrt{2}}\left(\left|n+\right\rangle_A \left|n-\right\rangle_B - \left|n-\right\rangle_A \left|n+\right\rangle_B\right)$$

- Classical correlation): $\left|z+\right\rangle_A \left|z-\right\rangle_B$

  correlation $\neq$ entanglement

- Entangled state가 갖는 correlation은 local hidden variable theory와 상충!

Non-locality of GHZ-state

- GHZ-state: $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B|0\rangle_C - |1\rangle_A|1\rangle_B|1\rangle_C\right)$
- locality:한편의 측정은 다른 편에 즉각적인 영향을 끼치지 않는다.

$$\sigma_y^A\sigma_y^B\sigma_x^C|GHZ\rangle = +|GHZ\rangle \qquad m_y^A m_y^B m_x^C = 1$$

$$\sigma_x^A\sigma_y^B\sigma_y^C|GHZ\rangle = +|GHZ\rangle \qquad m_x^A m_y^B m_y^C = 1$$

$$\sigma_y^A\sigma_x^B\sigma_y^C|GHZ\rangle = +|GHZ\rangle \qquad m_y^A m_x^B m_y^C = 1$$

$$\sigma_x^A\sigma_x^B\sigma_x^C|GHZ\rangle = -|GHZ\rangle \qquad m_x^A m_x^B m_x^C = -1$$

Quantum Cryptography(I)

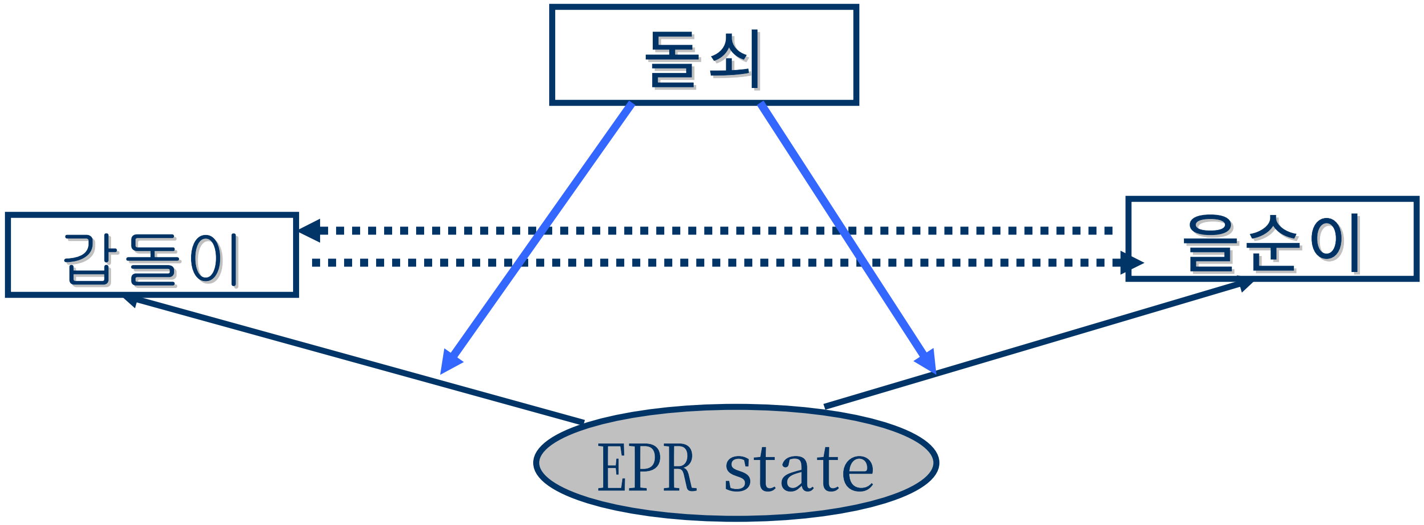
- Secret Key: $\{Z_i\}$
- 원문: $\{Y_i\}$
- 암호문: $\{X_i = Y_i \oplus Z_i\}$

원 문	1	0	0	1	1	1	0	1	0	0
Secret Key	0	1	1	1	0	1	0	0	1	0
암 호 문	1	1	1	0	1	0	0	1	1	0

- Cf) Public key

Quantum Cryptography(II)

- How to share secret key?



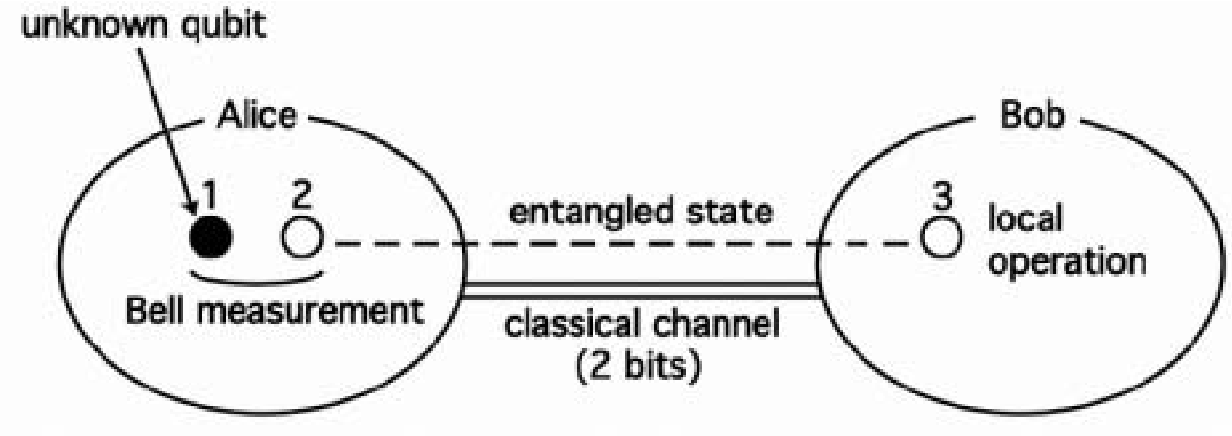
Quantum Cryptography(III)

- EPR-state: $\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|z+\right\rangle_{A}\left|z-\right\rangle_{B} - \left|z-\right\rangle_{A}\left|z+\right\rangle_{B}\right)$

$$= -\frac{1}{\sqrt{2}}\left(\left|x+\right\rangle_{A}\left|x-\right\rangle_{B} - \left|x-\right\rangle_{A}\left|x+\right\rangle_{B}\right)$$

갑돌	측정축	z	x	x	z	z	x	x	z	x	z
	측정결과	+	+	+	–	–	+	–	–	+	–
을순	측정축	x	x	z	z	z	x	z	z	x	x
	측정결과	–	–	–	+	+	–	–	+	–	–
Secret Key		?	0	?	1	1	0	?	1	0	?

Quantum teleportation(I)



- Unknown qubit: $|\psi\rangle_1 = a|0\rangle_1 + b|1\rangle_1$
- Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_2|0\rangle_3 \pm |1\rangle_2|1\rangle_3\right)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_2|1\rangle_3 \pm |1\rangle_2|0\rangle_3\right)$$

Quantum teleportation(II)

- Calculation:

$$\left|\psi\right\rangle_1 \left|\Psi^-\right\rangle_{23} = \left(a\left|0\right\rangle_1 + b\left|1\right\rangle_1\right)\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_2\left|1\right\rangle_3 - \left|1\right\rangle_2\left|0\right\rangle_3\right)$$

$$= \frac{1}{2}\left|\Phi^+\right\rangle_{12}\left(a\left|1\right\rangle_3 - b\left|0\right\rangle_3\right)$$

$$+ \frac{1}{2}\left|\Phi^-\right\rangle_{12}\left(a\left|1\right\rangle_3 + b\left|0\right\rangle_3\right)$$

$$+ \frac{1}{2}\left|\Psi^+\right\rangle_{12}\left(-a\left|0\right\rangle_3 + b\left|1\right\rangle_3\right)$$

$$+ \frac{1}{2}\left|\Phi^-\right\rangle_{12}\left(-a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right)$$

Quantum teleportation(III)

- Fidelity: $F = \left| \langle \psi | \rho | \psi \rangle \right|^2$

- Classical teleportation:

$$\left(1-\text{bit}\ \&\ F = {}^{2}\!/_{3}\right)\ \text{or}\ \left(\infty-\text{bit}\ \&\ F = 1\right)$$

- 측정은 상태에 대한 정보를 파괴한다?

Quantum Computation

- 비교:

	Computer	Quantum Computer
Information	bit	qubit
implementation	electric	2-level system
reversibility	irreversible	reversible
gate	spatially aranged	time orderd

함수연산

- Reversible operation: $U_f |x\rangle|0\rangle = |x\rangle| f(x)\rangle$
- 함수조건부연산: $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$
- Quantum Parallelism:

$$U_f \left(\sum |x_i\rangle\right)|0\rangle = \sum |x_i\rangle| f(x_i)\rangle$$

Quantum algorithm

- Shor's factorization algorithm:

$$\sum |x_i\rangle |f(x_i)\rangle \xrightarrow{Q.F.T} \text{주기}$$

- Grover's search algorithm:

$$\sum |x_i\rangle |f(x_i)\rangle \rightarrow \text{a}=f(x_i) : x_i \; ?$$

- Deutsch's algorithm :

$$\sum |x_i\rangle |f(x_i)\rangle \rightarrow \text{constant ? valence ?}$$

Quantum Error Correction

- Classical code: $0_L = 000, 1_L = 111$
- Quantum code: $|0\rangle_L = |\psi_0\rangle, |1\rangle_L = |\psi_1\rangle$
- Original information: $|\psi\rangle = a|0\rangle_L + b|1\rangle_L$
- Quantum error: $U^i_{error} = \alpha_i I_i + \beta_i X_i + \gamma_i Z_i + \delta_i X_i Z_i$

$$U^i_{error}|\psi\rangle = \alpha_i I_i|\psi\rangle + \beta_i X_i|\psi\rangle + \gamma_i Z_i|\psi\rangle + \delta_i X_i Z_i|\psi\rangle$$

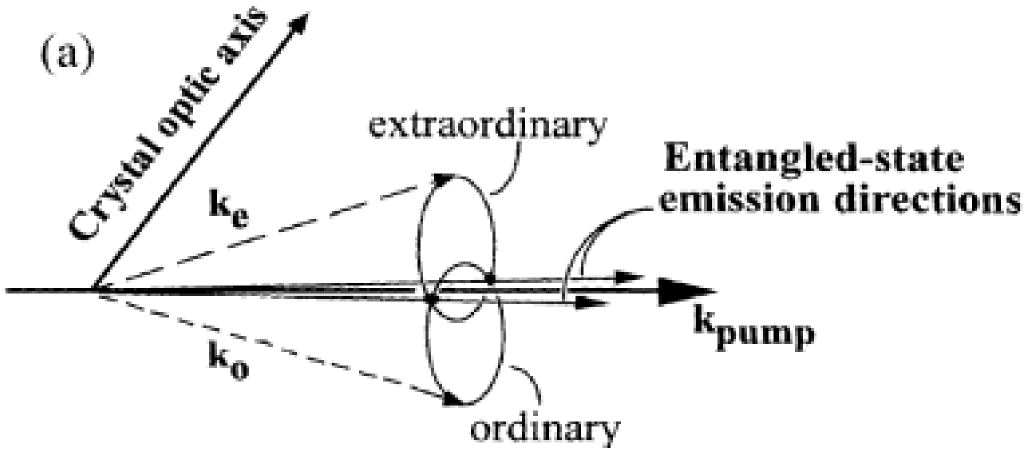
- 원정보가 아닌 오류에 대한 정보만을 측정!

Implementation

- 1)정보의 구현
- 2)초기상태의 준비
- 3)Universal gates의 수행
- 4)결과 읽기

Parametric Down Conversion

- Bell state: $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|H_1, V_2\rangle + e^{i\alpha}|V_1, H_2\rangle\right)$



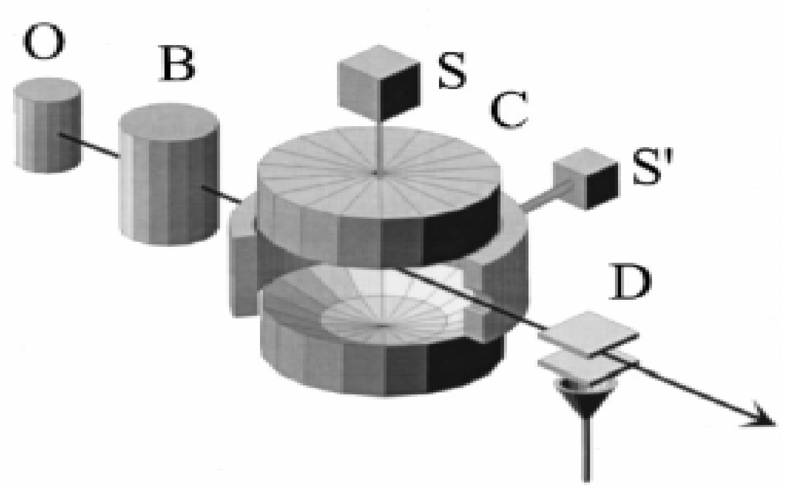
Cavity Q.E.D.

- Hamiltonian: $$H = \hbar\omega_{eg}\sigma_z + \hbar\omega\left(a^+a + \frac{1}{2}\right) - i\frac{\hbar\Omega}{2} f(x)\left(\sigma_+ a - \sigma_- a^+\right)$$
- Interaction: $|e,0\rangle \Leftrightarrow |g,1\rangle$

$$|e,0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|e,0\rangle + |g,1\rangle\right)$$

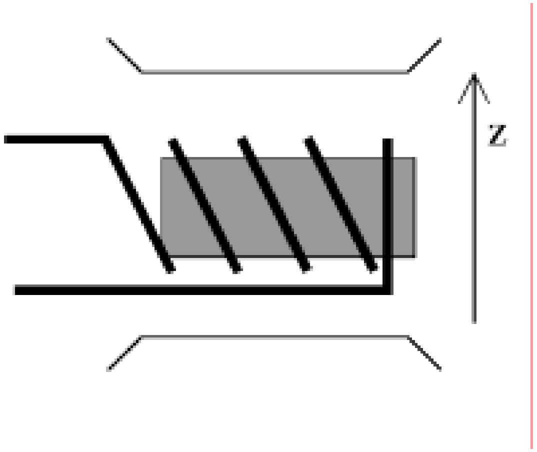
$$\frac{1}{\sqrt{2}}\left(|e,0\rangle + |g,1\rangle\right)|g\rangle$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(|e,0,g\rangle + |g,0,e\rangle\right)$$



N.M.R.

- Hamiltonian: $$\sum_i \omega_i I_{z,i} + \sum_{i,j} 2\pi J_{ij} I_{z,i} \cdot I_{z,j} + \{\sum_i \omega I_{x,i}\}$$



Conclusion

- Quantum Communication
- Quantum Computation
- Implementation