Unconditional Security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel

Kiyoshi Tamaki *

***Perimeter Institute for Theoretical Physics**

Collaboration with

Masato Koashi **(Osaka Univ, Creat, Sorst),**
Norbert Lütkenhaus **(Univ. of Erlangen-Nürnberg, Max Plank Research Group)*, and***
Nobuyuki Imoto **(Sokendai, Creat, Sorst, NTT)**

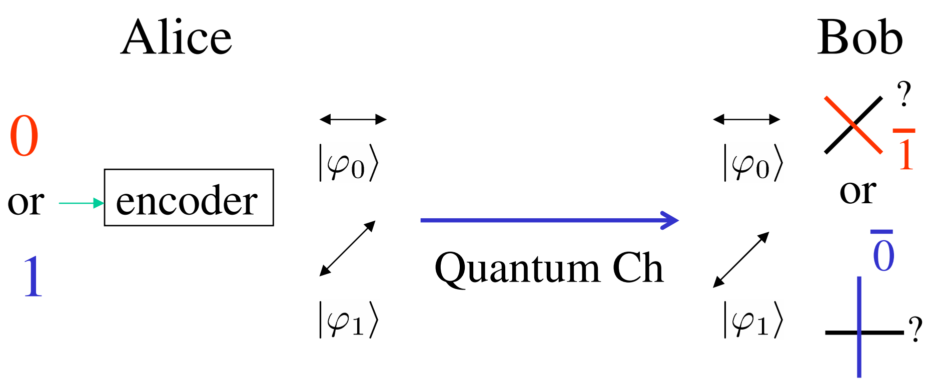
Summary of my talk

- B 92 QKD Protocol
- Outline of the proof
- Examples of the security
- Summary and Conclusion.

K. Tamaki, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **90**, 167904, (2003)

K. Tamaki and Norbert Lütkenhaus, *Phys. Rev. A.* **69**, 032316, (2004)

No Eve, noises and losses case (B92)



$$\mathcal{M}_{\mathrm{B92}} = \{F_0, F_1, F_?\}$$

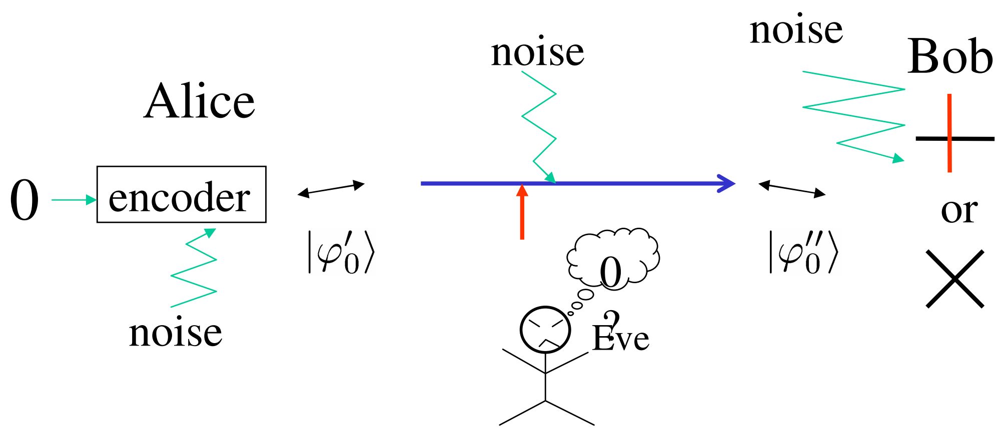
$$F_0 = |\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|/2$$
$$F_1 = |\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|/2$$
$$F_? = 1 - F_0 - F_1$$

0,1: conclusive

Bob tells Alice whether the outcome is conclusive or not over the public ch.

→ Alice and Bob share identical bit values !

The effects of noises or Eve



Noises, Eavesdropping → error, information leakage

For security

All noises are induced by Eve

Security proof of the B92 protocol

Is the B92 really unconditionally secure?

Is the B92 secure against Eve who has unlimited computational power and unlimited technology for state preparations, measurements and manipulations?

Assumptions on Alice and Bob

Alice:	A single photon source.
Bob:	An ideal photon counter that discriminates single photon one hand and multi-photon or single photon on the other hand.

Outline of the security proof of the B92

Protocol 1 (Secure)

Key words: Error correction, Bell state,
Entanglement distillation protocol (EDP)

(Equivalent with respect to key distribution)

The B92

Entanglement Distillation Protocol (By CSS Code)

(by Shor and Preskill 2000)

$$\hat{\sigma}_a^s = \hat{\sigma}_a^{s_1} \otimes \hat{\sigma}_a^{s_2} \otimes \hat{\sigma}_a^{s_3} \otimes \cdots \otimes \hat{\sigma}_a^{s_n}, (a = x, z) \text{ and } \sigma_a^0 = 1$$

$$s = (s_1, s_2, \cdots, s_n), \ (s_i = 0, 1)$$

Alice $\rightarrow (e_{bit}, e_{phase}) \leftarrow$ Bob

Syndrome measurement $\{\hat{\sigma}_z^{r_i}\}$ $\xleftrightarrow{\text{Relative bit error position}}$ $\{\hat{\sigma}_z^{r_i}\}$ Syndrome measurement

Public ch

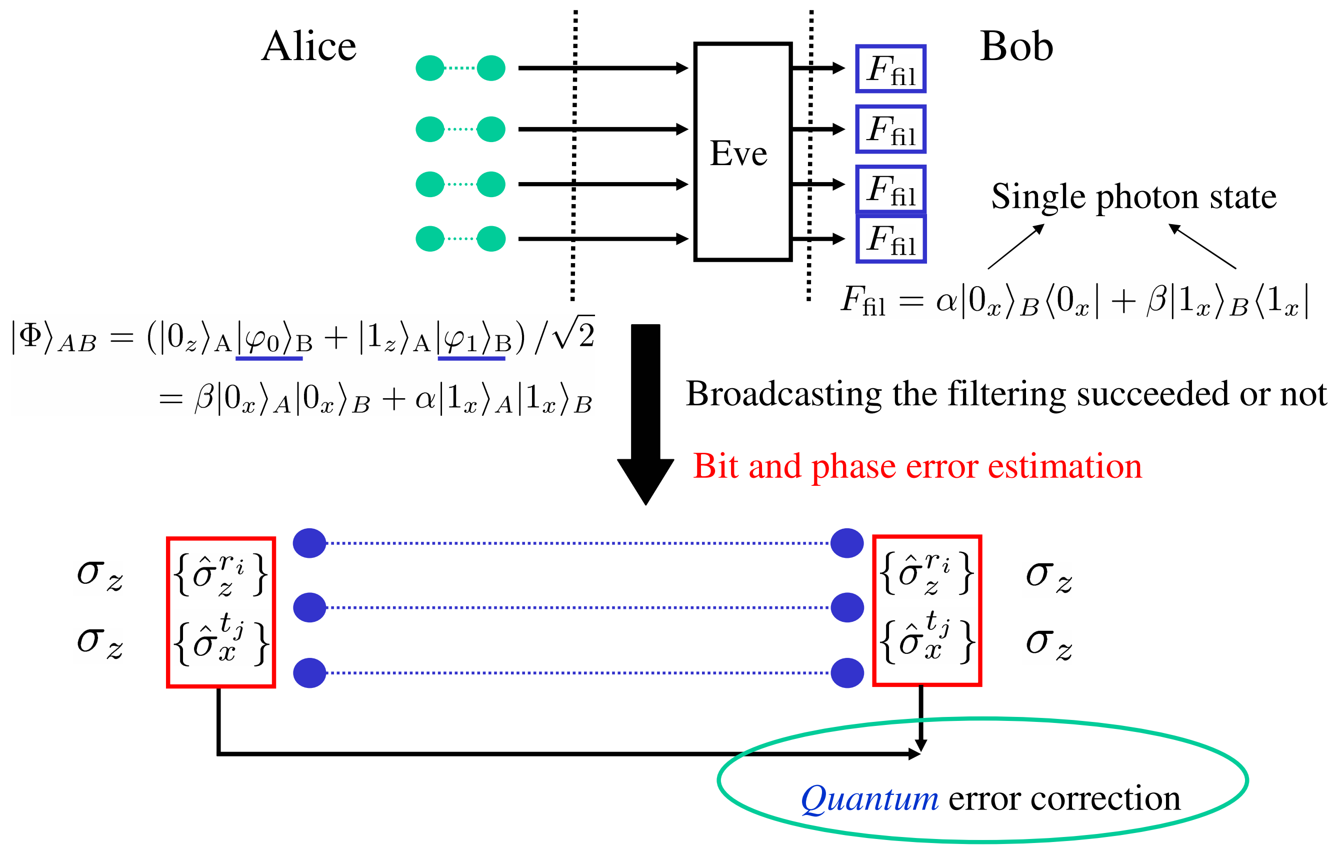
$\{\hat{\sigma}_x^{t_j}\}$ $\xleftrightarrow{\text{Relative phase error position}}$ $\{\hat{\sigma}_x^{t_j}\}$

Error correction

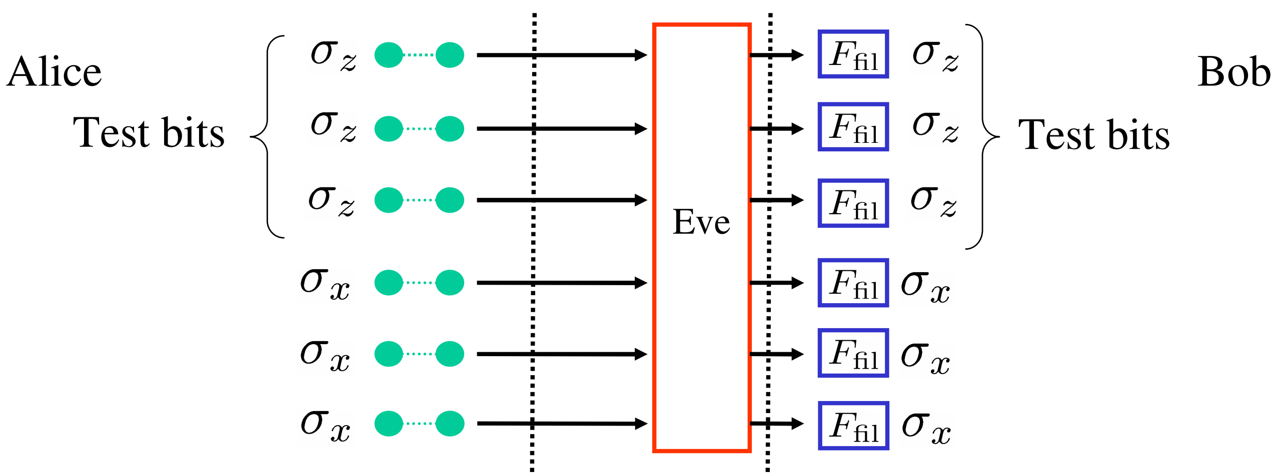
$$\boxed{r_i \in C_1, \ t_j \in C_2, \ C_2 \subset C_1}$$

Sharing $n\,(1 - h(e_{bit}) - h(e_{phase}))$ pairs of a Bell state

Protocol 1 (Secure)



Error estimations on the *Protocol 1*



$$\begin{aligned}
\Pi_{\mathrm{bit}} &= |0_z\rangle_A\langle 0_z| \otimes F_S|1_z\rangle_B\langle 1_z|F_S + |1_z\rangle_A\langle 1_z| \otimes F_S|0_z\rangle_B\langle 0_z|F_S \\
\Pi_{\mathrm{phase}} &= |0_x\rangle_A\langle 0_x| \otimes F_S|1_x\rangle_B\langle 1_x|F_S + |1_x\rangle_A\langle 1_x| \otimes F_S|0_x\rangle_B\langle 0_x|F_S
\end{aligned}$$

$[\Pi_{\mathrm{bit}}, \Pi_{\mathrm{phase}}] \neq 0$

$\Rightarrow$ Phase error rate and bit error rate is not independent

Phase error rate is estimated by bit error rate (the *Protocol 1* is secure)

Outline of the security proof of the B92

Protocol 1 (Secure)

Key words: Error correction, Bell state, Entanglement distillation protocol (EDP)

(Equivalent with respect to key distribution)

The B92

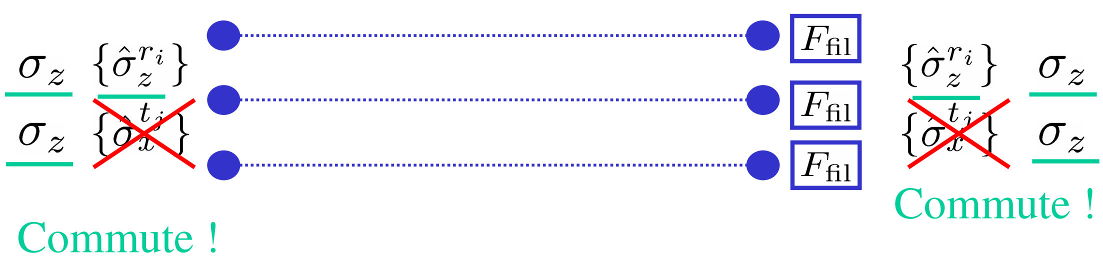
A brief explanation of the equivalence

Main Observation (by shor and Preskill)

Only the bit values are important

□No need for phase error correction

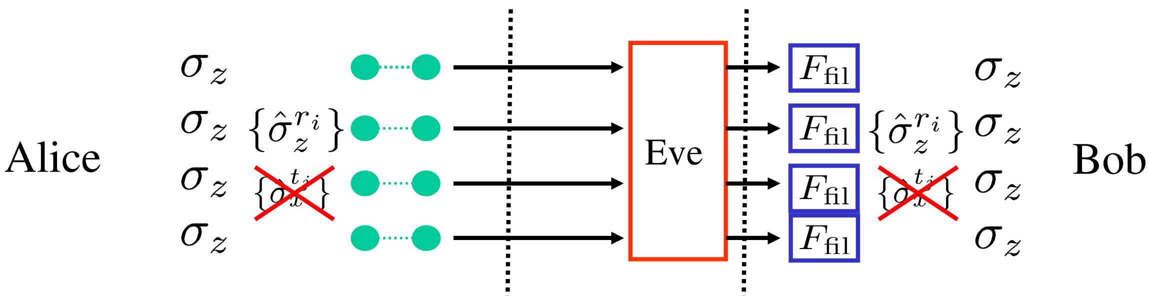
$$\frac{1}{\sqrt{2}}\left(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B\right) \longleftrightarrow \frac{1}{\sqrt{2}}\left(|0_z\rangle_A|0_z\rangle_B - |1_z\rangle_A|1_z\rangle_B\right)$$



Alice and Bob are allowed to measure σ_z before $\{\hat{\sigma}_z^{r_i}\}$.

Protocol 1 (Secure)

No need for phase error correction (Shor and Preskill)

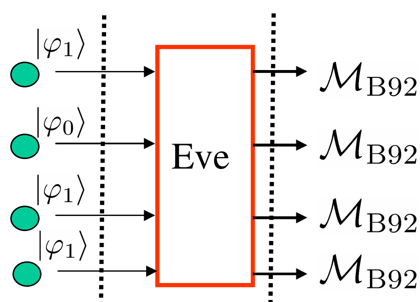


$$|\Phi\rangle_{AB} = (|0_z\rangle_{\mathrm{A}}\underline{|\varphi_0\rangle_{\mathrm{B}}} + |1_z\rangle_{\mathrm{A}}\underline{|\varphi_1\rangle_{\mathrm{B}}})/\sqrt{2}$$
$$= \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B$$

$$F_{\text{fil}} = \alpha|0_x\rangle_B\langle 0_x| + \beta|1_x\rangle_B\langle 1_x|$$

Equivalent !

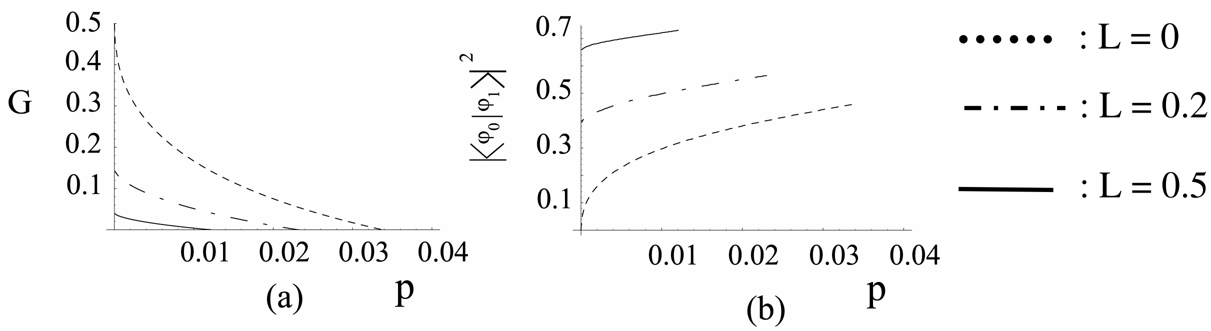
Randomly chosen



Classical data processing
(error correction, privacy amplification)

Classical data processing
(error correction, privacy amplification)

Example of the security and estimation



(a) (b)

G : Optimal net growth rate of secret key per pulse

p :depolarizing rate

L: the prob that Bob detects vacuum (Loss rate)

Channel: $\rho \to (1-L)\left[(1-p)\rho + p/3\sum_{a=x,y,z}\sigma_a\rho\sigma_a\right] + L\,\underline{|Vac\rangle\langle Vac|}$

The vacuum state

Summary and conclusion

- We have estimated the unconditionally security of the B92 protocol with single photon source and ideal photon counter.

- We have shown the B92 protocol can be regarded as an EPP initiated by a filtering process.

- Thanks to the filtering, we can estimate the phase error rate.

Future study

- Relaxation of the assumptions.

- Security estimation of B92 with coherent state.

K. Tamaki, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **90**, 167904, (2003)

K. Tamaki and Norbert Lütkenhaus, *Phys. Rev. A.* **69**, 032316, (2004)

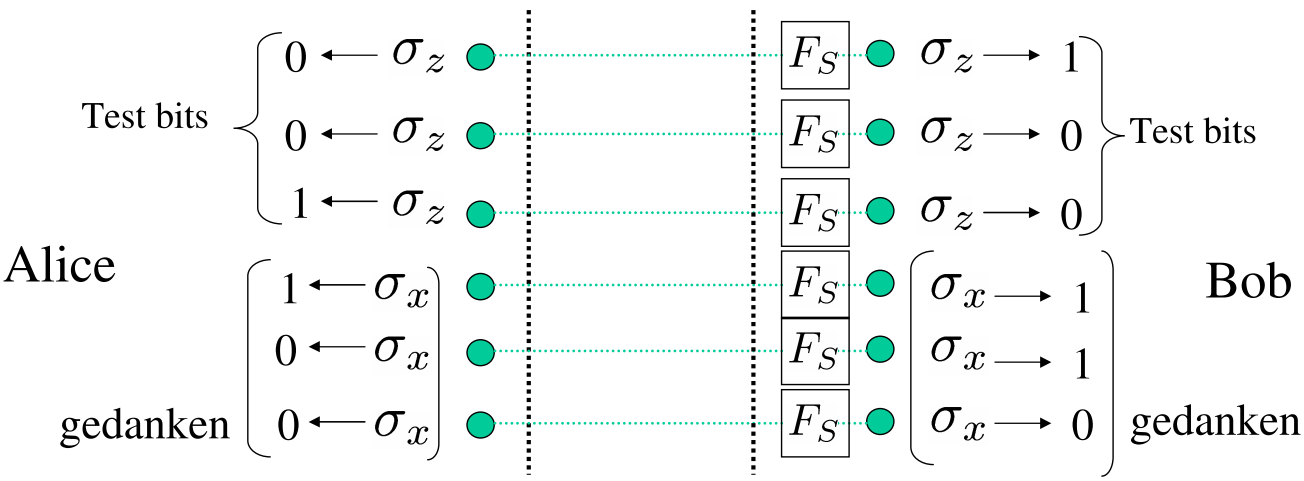
Derivation of the B92 measurement from that in the *Protocol 1*

$$|\varphi_j\rangle \equiv \beta|0_x\rangle - (-1)^j\alpha|1_x\rangle,\ (j=0,1)$$

$$|\overline{\varphi}_j\rangle \equiv \alpha|0_x\rangle + (-1)^j\beta|1_x\rangle,\ (j=0,1)$$

$$\left.\begin{array}{r} F_{\text{fil}}|0_z\rangle_{\text{B}}\langle 0_z|F_{\text{fil}} = |\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|/2 = F_0 \\ F_{\text{fil}}|1_z\rangle_{\text{B}}\langle 1_z|F_{\text{fil}} = |\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|/2 = F_1 \\ 1_{\text{single}} - F_0 - F_1 = F_? \\ 1 - 1_{\text{single}} = F_{\text{multi}} \end{array}\right\} = \mathcal{M}_{\text{B92}}$$

The phase error rate estimation from the bit error rate



$$\Pi_{\text{bit}} = |0_z\rangle_A\langle 0_z| \otimes F_S|1_z\rangle_B\langle 1_z|F_S + |1_z\rangle_A\langle 1_z| \otimes F_S|0_z\rangle_B\langle 0_z|F_S$$

$$\Pi_{\text{phase}} = |0_x\rangle_A\langle 0_x| \otimes F_S|1_x\rangle_B\langle 1_x|F_S + |1_x\rangle_A\langle 1_x| \otimes F_S|0_x\rangle_B\langle 0_x|F_S$$

Given $\langle \Pi_{\text{bit}} \rangle_{obs}$, how much is the upper bound of $\langle \Pi_{\text{phase}} \rangle_{obs}$?

Note: It is dangerous to put some assumptions on the state.

$$\Pi_{\text{bit}} = \underbrace{\frac{1}{2}|\Phi-\rangle\langle\Phi-|}\oplus\underbrace{\frac{1}{2}|\Gamma-\rangle\langle\Gamma-|}$$

The bit error and the phase error have a correlation !!

Nonorthogonal

$$\Pi_{\text{phase}} = \underbrace{0}\oplus\underbrace{\left[\alpha^2|01_x\rangle\langle 01_x| + \beta^2|10_x\rangle\langle 10_x|\right]}_{\Pi^B_{\text{phase}}}$$

$(|\Phi-\rangle \equiv \alpha|00_x\rangle - \beta|11_x\rangle)$

$(|\Gamma-\rangle \equiv \beta|01_x\rangle - \alpha|10_x\rangle)$

— : subspace H_L spanned by $\{|00_x\rangle, |11_x\rangle\}$

— : subspace H_R spanned by $\{|01_x\rangle, |10_x\rangle\}$

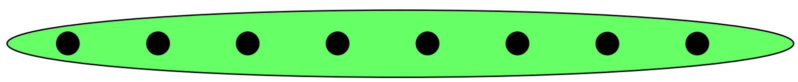
Qubit space

$$\begin{cases} \langle\Pi_{\text{bit}}\rangle_{obs} = \underline{p_{\text{Red}}\langle\Phi-\rangle_{obs}} + \underline{(1-p_{\text{Red}})\langle\Gamma-\rangle_{obs}} \\ \langle\Pi_{\text{phase}}\rangle_{obs} = \underline{p_{\text{Red}}\,0} + \underline{(1-p_{\text{Red}})\langle\Pi^B_{\text{phase}}\rangle_{obs}} \end{cases}$$

Upper bound of $\langle 01_x\rangle_{obs}$ for given $\langle\Gamma-\rangle_{obs}$?

Question

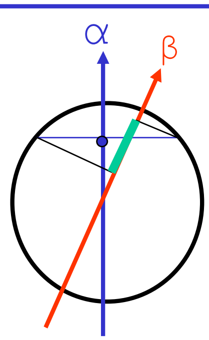
Consider any N-qubit state that is symmetric under any permutation



$\underbrace{\sigma_\alpha \quad \sigma_\alpha \quad \sigma_\alpha \quad \sigma_\alpha}_{\text{Test bit}} \quad \underbrace{\sigma_\beta \quad \sigma_\beta \quad \sigma_\beta \quad \sigma_\beta}_{\text{Untested bit}}$

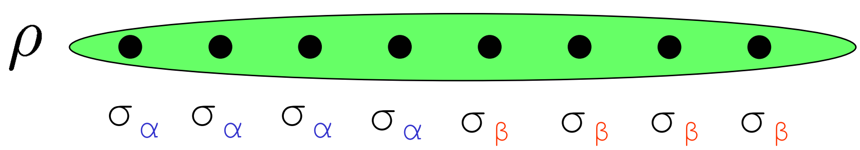
For given $\langle \sigma_\alpha \rangle_{obs}$, how much is the upper bound of $\langle \sigma_\beta \rangle_{obs}$?

ANS,



$(N \to \infty)$

For the estimation, we are allowed to regard the state as having stemmed from Independently and Identically Distributed quantum source !



S_p : unitary operator corresponds to permutation of M qubit

$S_p \cong \bigoplus_\lambda \mathbf{1} \otimes \tilde{\pi}_\lambda(p)$

M qubit state ρ that is symmetric under any permutation

$$\rho \cong \bigoplus_k (p_k/d_k^{\mathcal{V}}) \rho_k \otimes \mathbf{1}$$

M qubit space can be decomposed as $\mathcal{H}^{\otimes M} \cong \bigoplus_\lambda \mathcal{U}_\lambda \otimes \mathcal{V}_\lambda$

S_p : unitary operator corresponds to permutation of M qubit

$S_p \cong \bigoplus_\lambda \mathbf{1} \otimes \tilde{\pi}_\lambda(p)$

M qubit state ρ that is symmetric under any permutation

$$\rho \cong \bigoplus_k (p_k/d_k^{\mathcal{V}})\rho_k \otimes \mathbf{1}$$

● ● ● ● ● ● ● ●

σ_α σ_α σ_α σ_α σ_β σ_β σ_β σ_β

		j=0	j=1
$n_{b,j}$:	b=α	$\{\|\alpha,0\rangle,$	$\|\alpha,1\rangle\}$
	b=B	$\{\|\beta,0\rangle,$	$\|\beta,1\rangle\}$

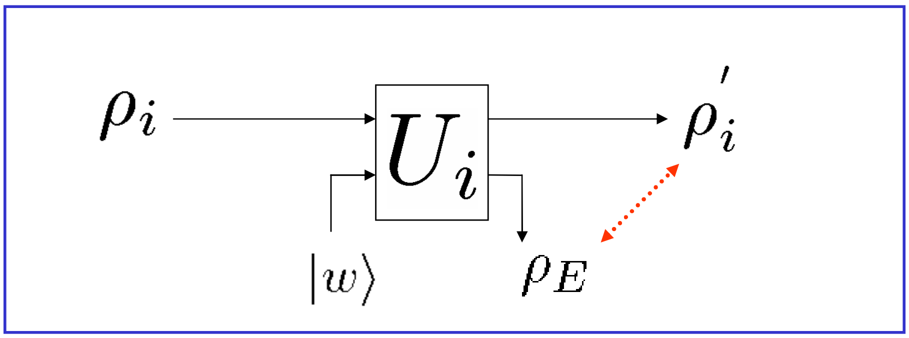
M_b : number of qubits measured in b basis

$$|\chi\rangle \equiv \bigotimes_{b,j} |b,j\rangle^{\otimes n_{b,j}}$$

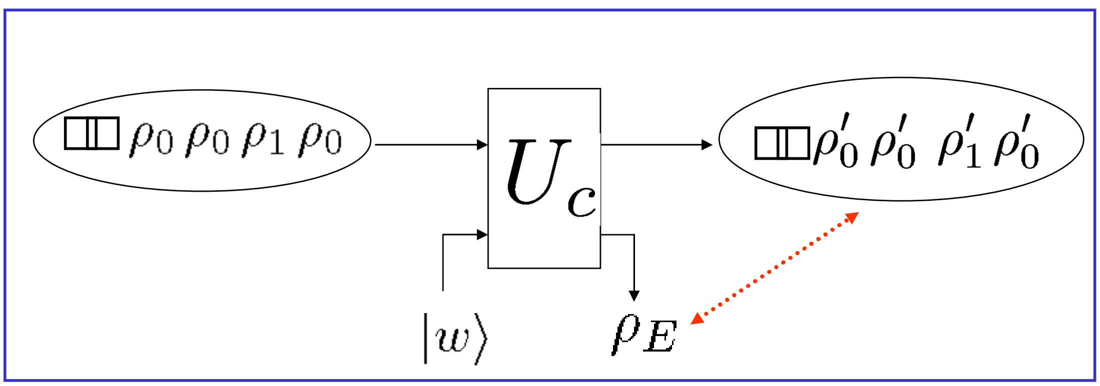
$$p(\delta_0,\delta_1) = \langle\chi|\rho|\chi\rangle \prod_{b=0,1} \frac{M_b!}{n_{b,0}!n_{b,1}!} \leq poly(M)\exp[-M \min R]$$

The class of the eavesdropping

Individual Attack



Coherent Attack (General Attack)



U_i , U_c , and Eve's measurement is arbitrary.

Quantum Key Distribution (QKD)

□A way to share a random bit string between sender (Alice) and receiver (Bob) whose info leaks arbitrary small to Eve.