Unconditional security of the Bennett 1992 quantum key-distribution protocol over noisy and lossy channels

Kiyoshi Tamaki

The Graduate Univ. for Advanced Studies
(SOKENDAI), CREST

Collaboration with

M. Koashi, N. Lütkenhaus, and N. Imoto

Summary of my talk

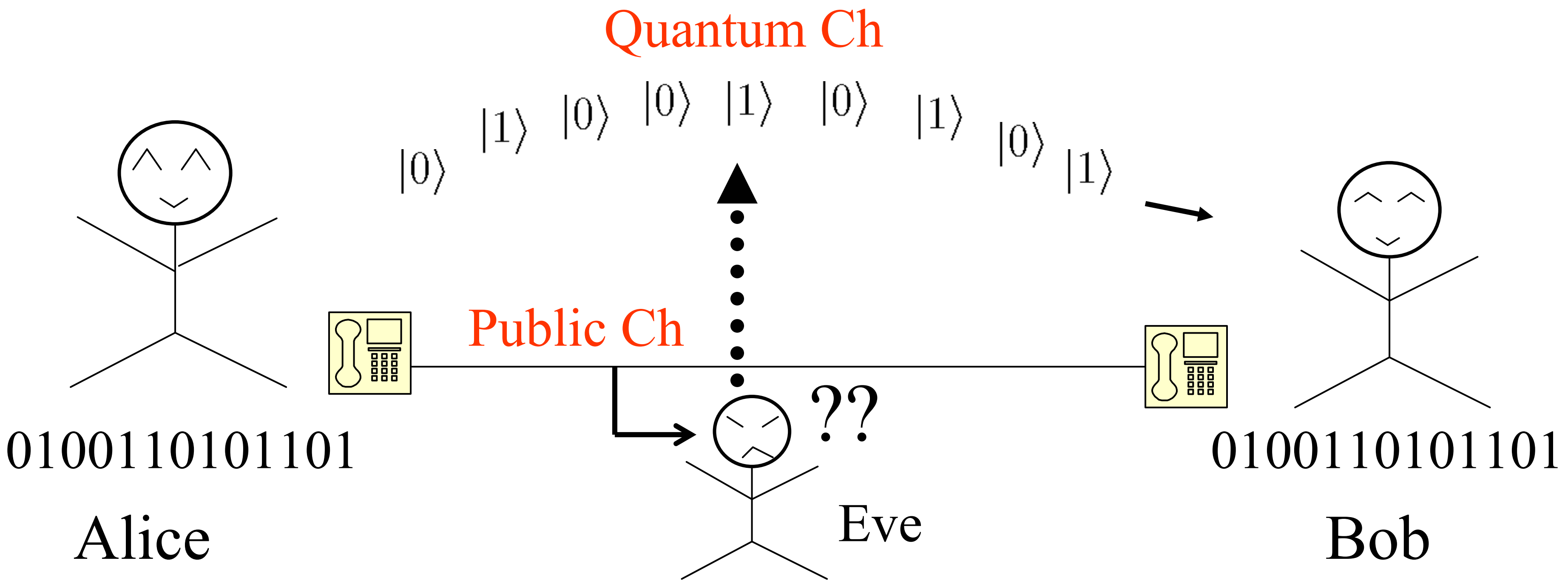
- Motivations for the security proof of the B92
- Introduction to Quantum Key Distribution (QKD)
- Unconditional Security of the B92 protocol
- Summary

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

K. Tamaki, and N. Lütkenhaus, to appear in Phys. Rev A.
quantu-ph/0308048. (over noisy and lossy ch)

Quantum Key Distribution (QKD)

- A way to share a random bit string between Alice and Bob whose info leaks arbitrary small to Eve.


Quantum Ch
$|0\rangle$ $|1\rangle$ $|0\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$ $|0\rangle$ $|1\rangle$
Public Ch
??
0100110101101
Alice
Eve
0100110101101
Bob

B92 (Bennett in 1992): $|\varphi_0\rangle$ and $|\varphi_1\rangle$

BB84 (Bennett and Brassard in 1984): $|H\rangle, |V\rangle, |{+45}\rangle$, and $|{-45}\rangle$

Motivations for security proof of the B92

- The B92 is the simplest QKD.

- Clarifies the role of the nonorthogonality in conveying secret information.

Works related with Coherent Attack

BB84:

D. Mayers, Lec-Notes in Comp Science, **1109**, Springer (1996).

H. Inamori, et.al. quant-ph/0107017.

P. W. Shor and J. Preskill, Phys.Rev.Lett, **85**, 441, (2000).

M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

D. Gottesman and H-K. Lo, quant-ph/0105121.

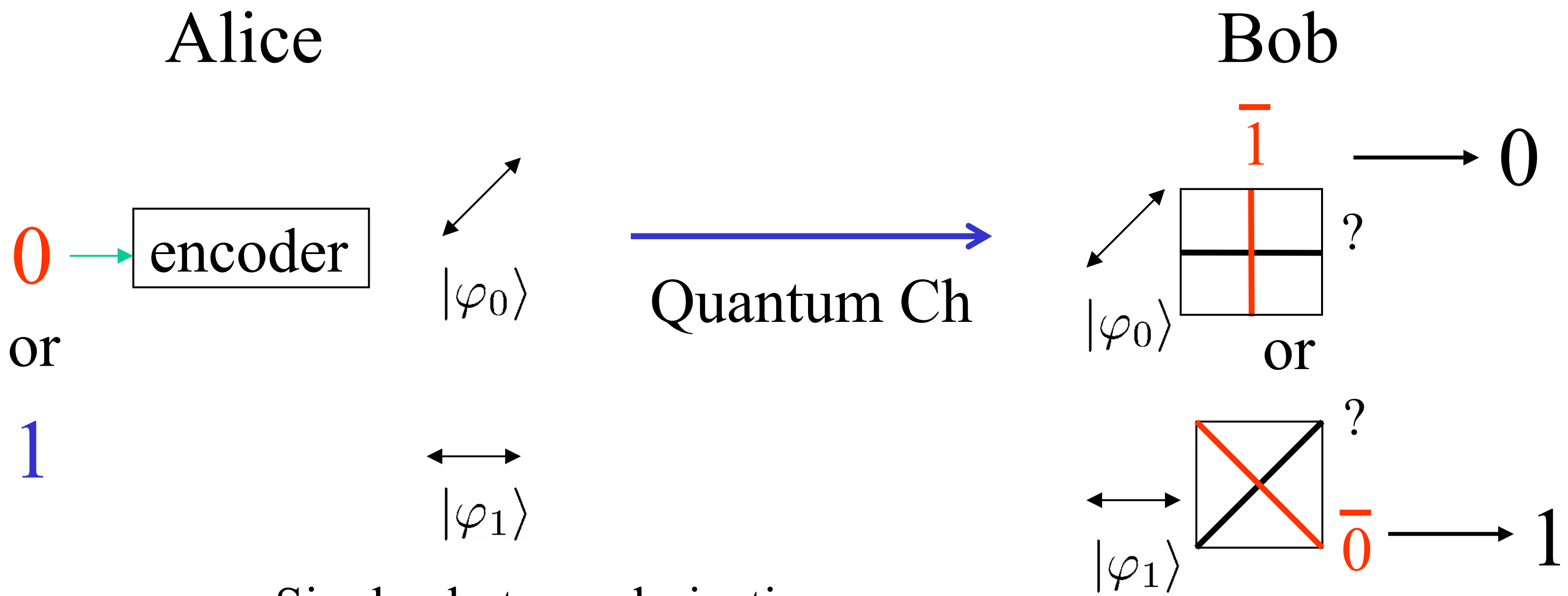
D. Gottesman, H-K. Lo, N. Lütkenhaus, and J. Preskill, quant-ph/0212066 .

B92:

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

K. Tamaki, and N. Lütkenhaus, to appear in Phys. Rev A.

No Eve, noises and losses case (B92)



Alice

Bob

$0 \rightarrow$ encoder

or

1

$|\varphi_0\rangle$

$|\varphi_1\rangle$

Quantum Ch

$|\varphi_0\rangle$ $\bar{1}$ $\longrightarrow 0$?

or

$|\varphi_1\rangle$? $\bar{0}$ $\longrightarrow 1$

Single photon polarization

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

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

$$F_0 = |\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|/2$$

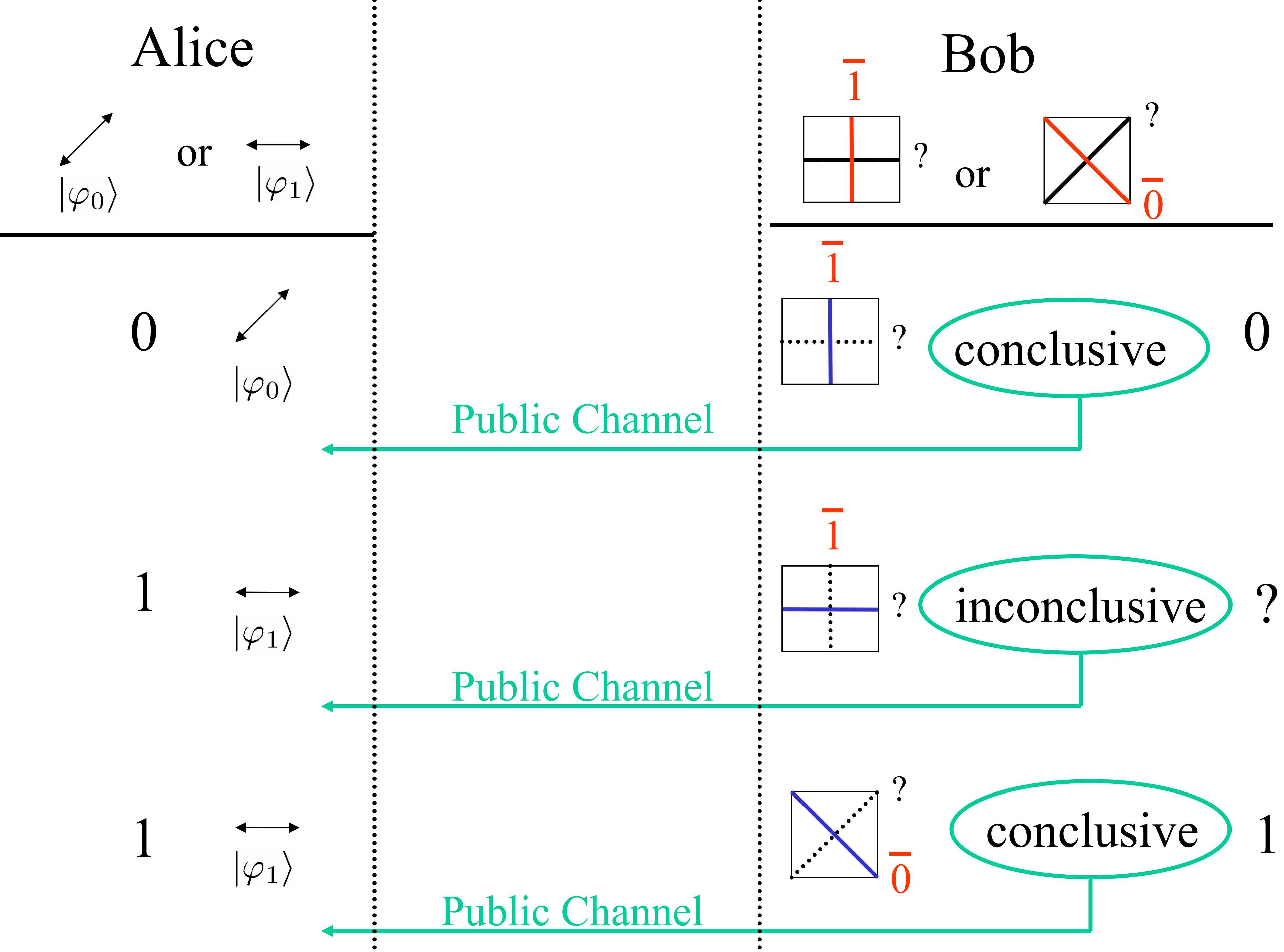
$$F_1 = |\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|/2$$

$$F_? = 1 - F_0 - F_1$$

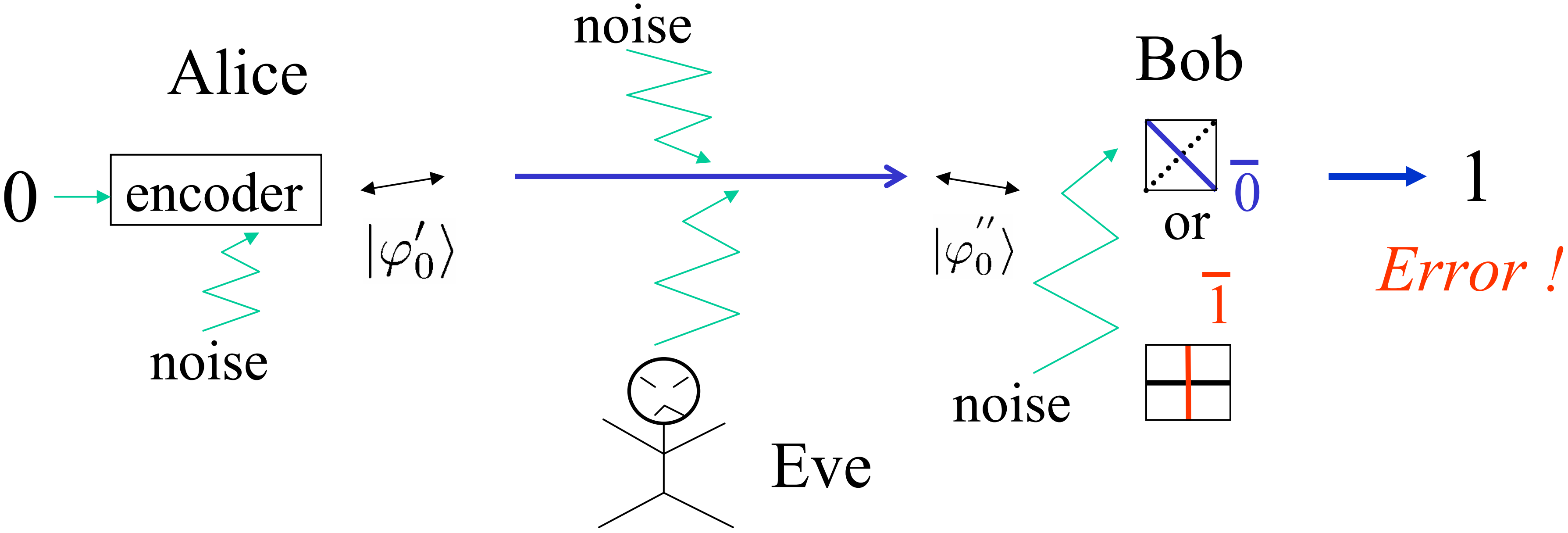
? : inconclusive

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

$\bar{0}$ and $\bar{1}$: conclusive


Alice
$|\varphi_0\rangle$
or
$|\varphi_1\rangle$
Bob
$\bar{1}$
?
or
?
$\bar{0}$
0
$|\varphi_0\rangle$
$\bar{1}$
?
conclusive
0
Public Channel
1
$|\varphi_1\rangle$
$\bar{1}$
?
inconclusive
?
Public Channel
1
$|\varphi_1\rangle$
?
$\bar{0}$
conclusive
1
Public Channel

The effects of noises



Noises, eavesdropping → Errors on the key

- QKD is possible over ideal situations

How to distribute the identical and secure secret key under the existence of eavesdropping, noises and losses?

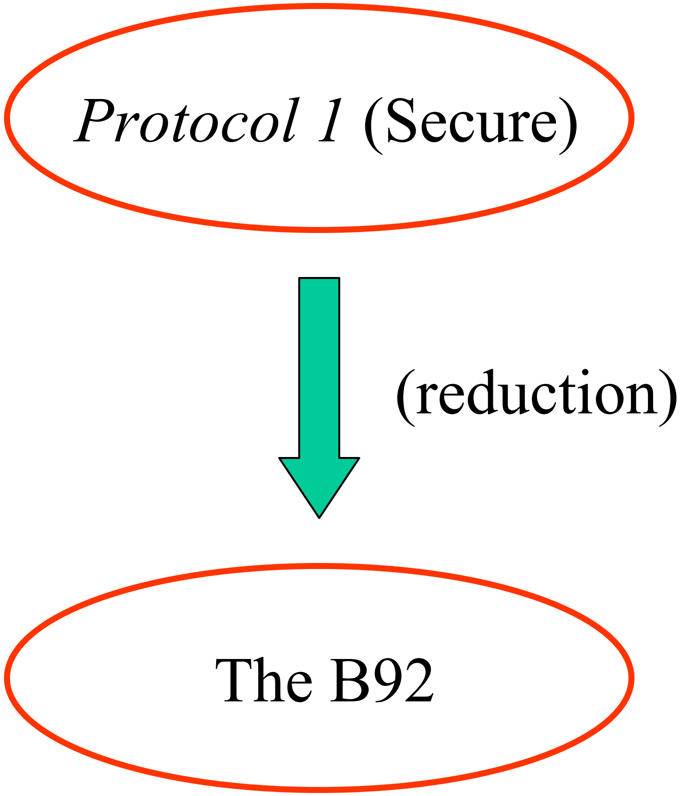
Unconditional Security of the B92 protocol

Security against coherent attacks

Assumptions

- Alice has a perfect single photon source.
- Bob’s detector is ideal (no dark count).
- No channel losses (will be removed later)

Outline of the security proof of the B92



Protocol 1 (Secure)

(reduction)

The B92

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

Basic concept 1 (classical error correction)

(1 bit error case)

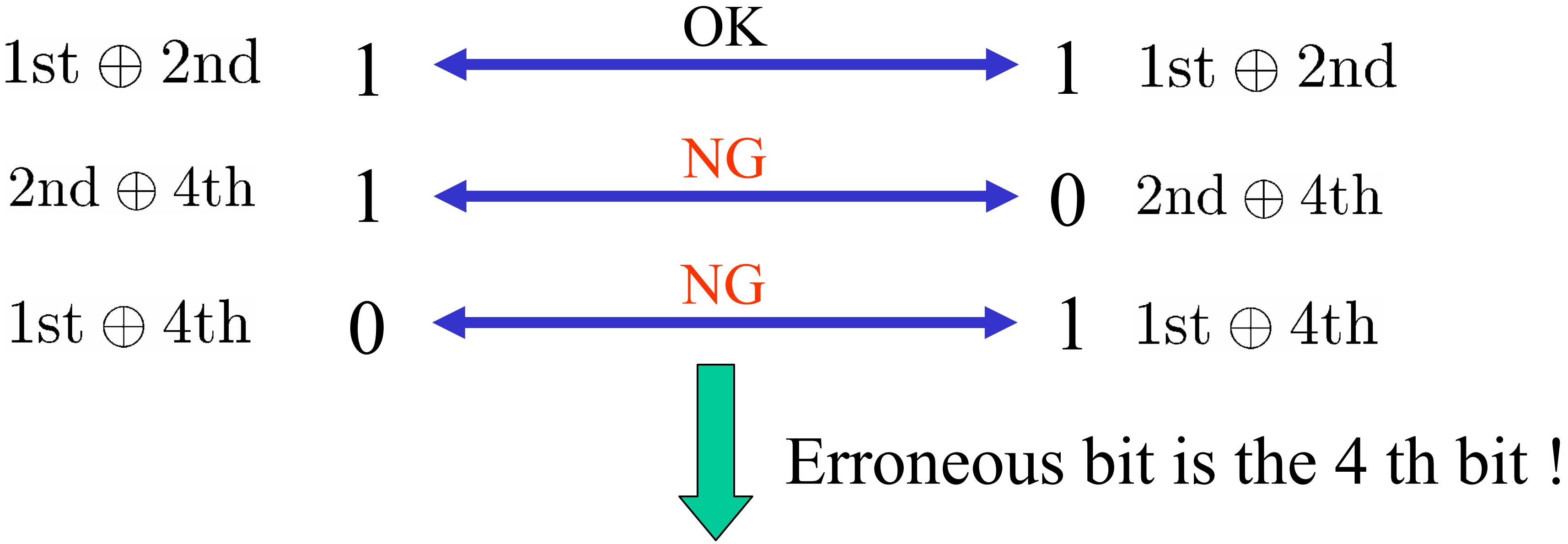
Alice

0110

Bob

0111

Bit Error Syndrome



$1\text{st} \oplus 2\text{nd}$ 1 OK 1 $1\text{st} \oplus 2\text{nd}$

$2\text{nd} \oplus 4\text{th}$ 1 NG 0 $2\text{nd} \oplus 4\text{th}$

$1\text{st} \oplus 4\text{th}$ 0 NG 1 $1\text{st} \oplus 4\text{th}$

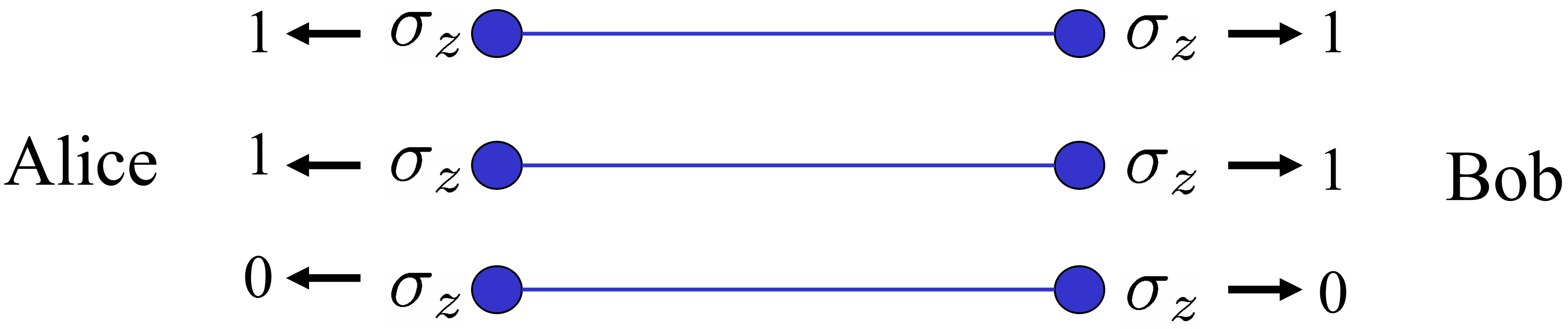
Erroneous bit is the 4 th bit !

0110

0110

Compare the syndrome of the suitably chosen subsets

Basic concept 2 (Bell state)



A Bell State : $\frac{1}{\sqrt{2}}(|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$

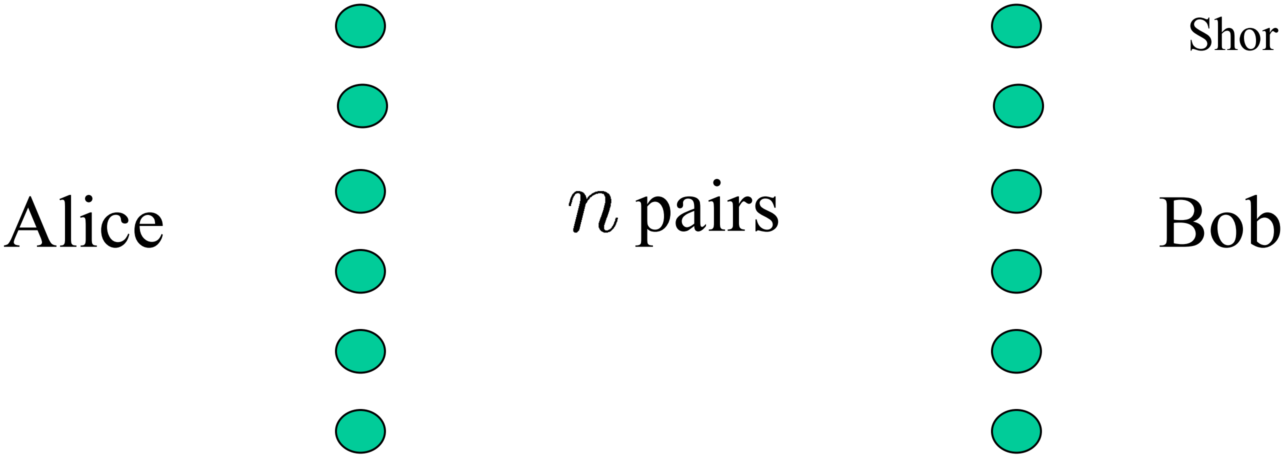
(1) The Bell state is a pure state. (No correlation with the third system)

(2) The bit values are at random.

If Alice and Bob share pairs of the Bell state,
the shared bit values are unconditionally secure.

Basic concept 3 (The EDP based on CSS codes)

Shor and Preskill (2000)



Alice

n pairs

Bob

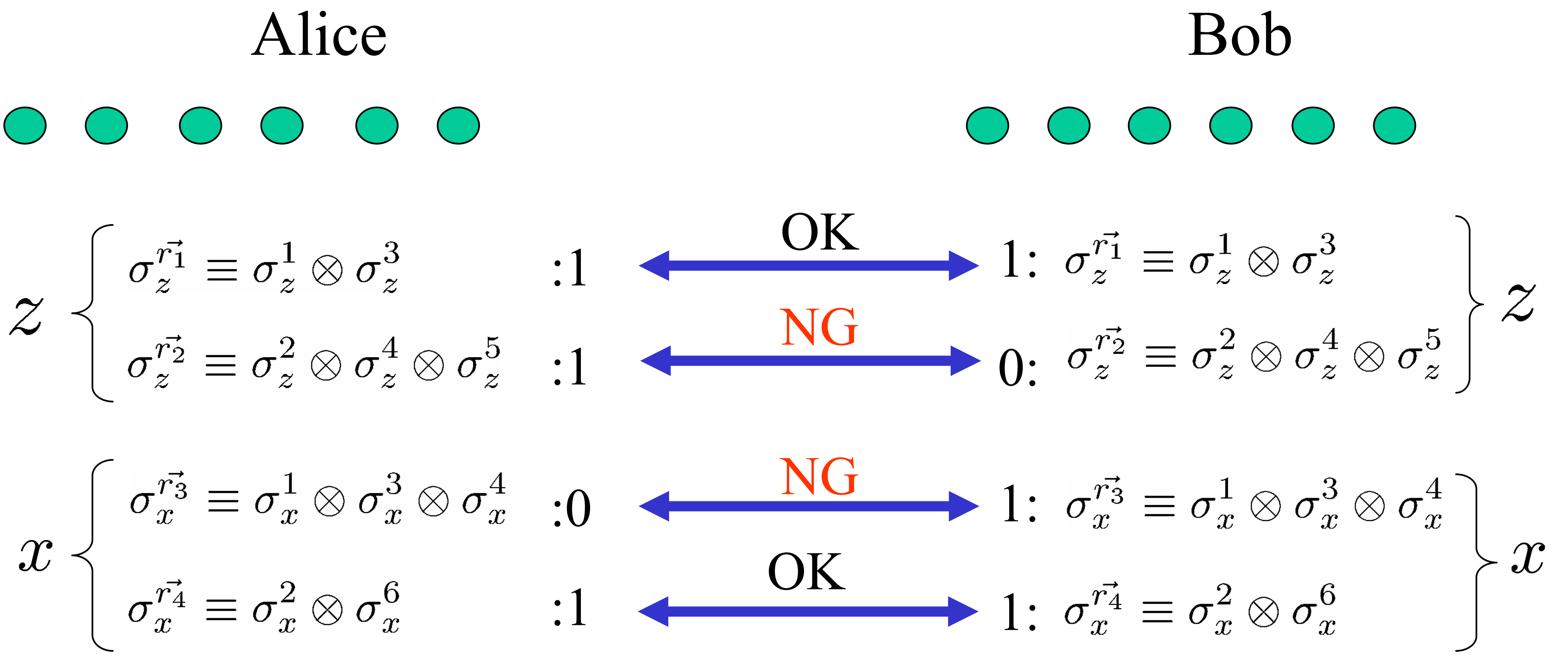
e_{bit} : error rate in $Z(=\{|0_z\rangle,|1_z\rangle\})$ basis (bit error)

e_{phase}: error rate in $X(=\{|0_x\rangle,|1_x\rangle\})$ basis (phase error)

By using CSS codes that correct up to ne_{bit} bit errors and ne_{phase} phase errors, in the limit of large n ,

$n\left[1-h(e_{bit})-h(e_{phase})\right]$ Bell states can be distilled.

$$h(x)=-x\log_2 x-(1-x)\log_2(1-x)$$



Alice

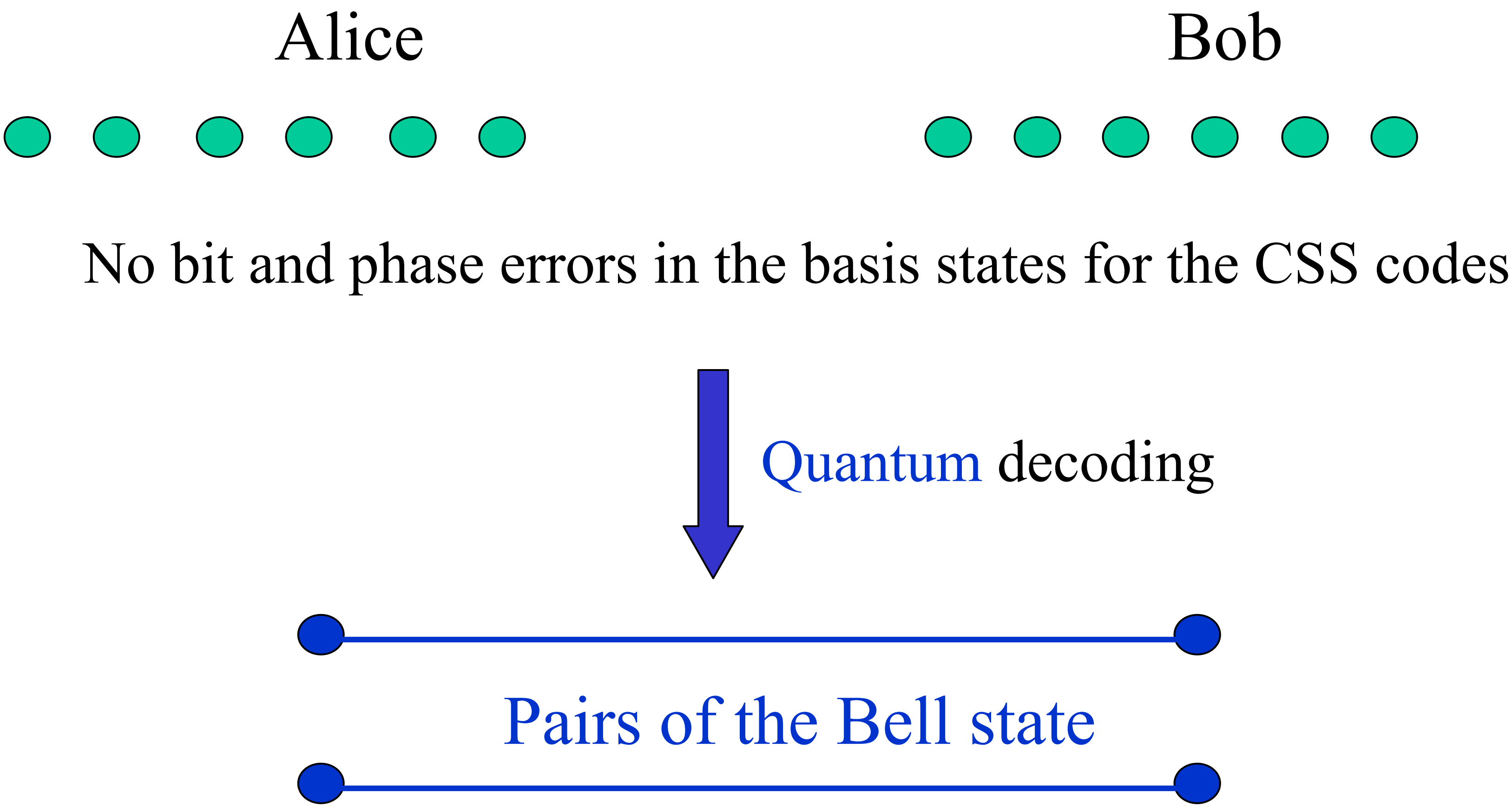
Bob

$$z\left\{\begin{array}{l} \sigma_z^{\vec{r_1}} \equiv \sigma_z^1 \otimes \sigma_z^3 \quad :1 \quad \xleftrightarrow{\text{OK}} \quad 1:\ \sigma_z^{\vec{r_1}} \equiv \sigma_z^1 \otimes \sigma_z^3 \\ \sigma_z^{\vec{r_2}} \equiv \sigma_z^2 \otimes \sigma_z^4 \otimes \sigma_z^5 \quad :1 \quad \xleftrightarrow{\text{NG}} \quad 0:\ \sigma_z^{\vec{r_2}} \equiv \sigma_z^2 \otimes \sigma_z^4 \otimes \sigma_z^5 \end{array}\right\} z$$

$$x\left\{\begin{array}{l} \sigma_x^{\vec{r_3}} \equiv \sigma_x^1 \otimes \sigma_x^3 \otimes \sigma_x^4 \quad :0 \quad \xleftrightarrow{\text{NG}} \quad 1:\ \sigma_x^{\vec{r_3}} \equiv \sigma_x^1 \otimes \sigma_x^3 \otimes \sigma_x^4 \\ \sigma_x^{\vec{r_4}} \equiv \sigma_x^2 \otimes \sigma_x^6 \quad :1 \quad \xleftrightarrow{\text{OK}} \quad 1:\ \sigma_x^{\vec{r_4}} \equiv \sigma_x^2 \otimes \sigma_x^6 \end{array}\right\} x$$

$\boxed{[\sigma_\alpha^{\vec{r_i}}, \sigma_\beta^{\vec{r_j}}] = 0}$ $(\alpha, \beta = x, z,\ i = 1, 2, \cdots)$: CSS Code

By comparing the syndromes in both *z* and *x* basis and after performing Quantum error correction



Alice

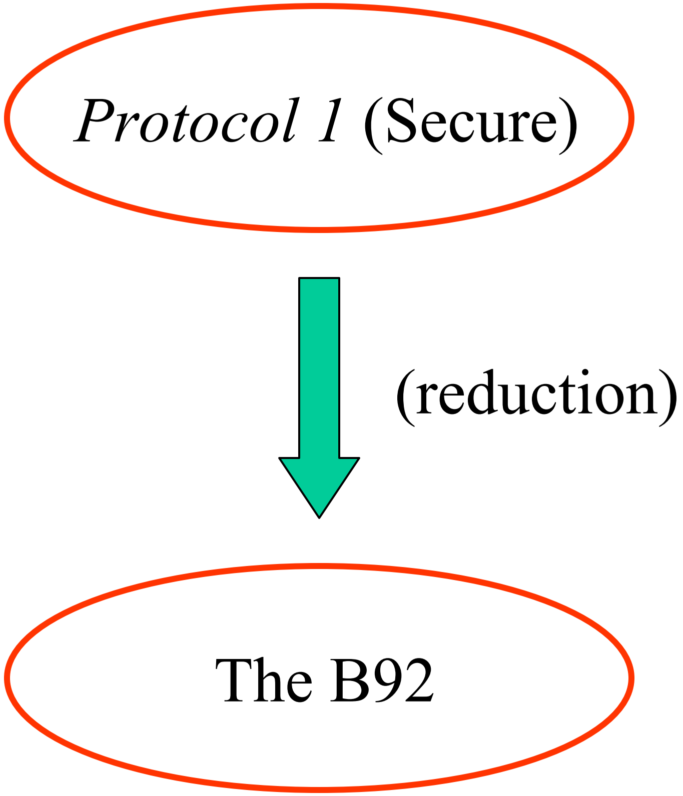
Bob

No bit and phase errors in the basis states for the CSS codes

Quantum decoding

Pairs of the Bell state

Outline of the security proof of the B92



The final purpose of this protocol is to distill pairs of the Bell state for the unconditionally secure key.

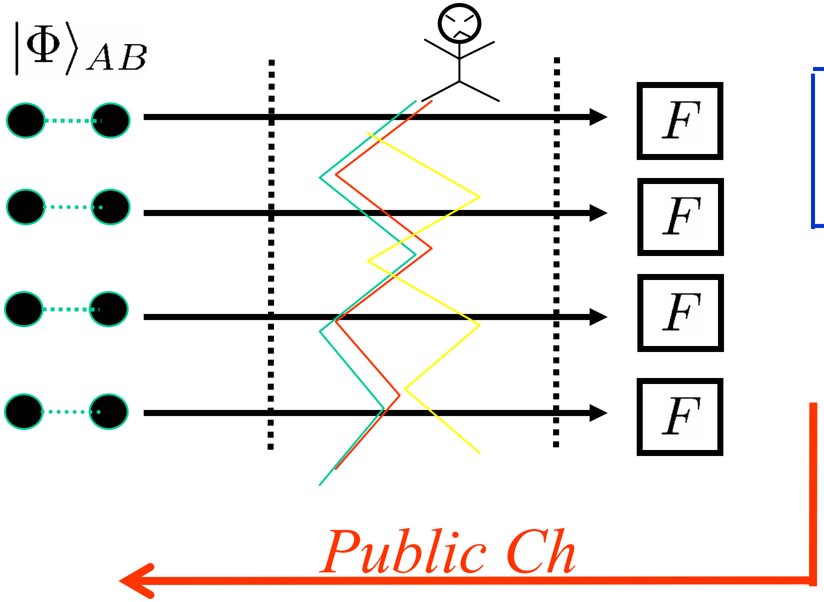
Protocol 1

(1) Filtering operation

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

Alice prepares $|\Phi\rangle_{AB}$: $\frac{1}{\sqrt{2}}(|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B) = \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B$

Alice



$$F = \{F_S, \sqrt{1-F_S^2}\}$$

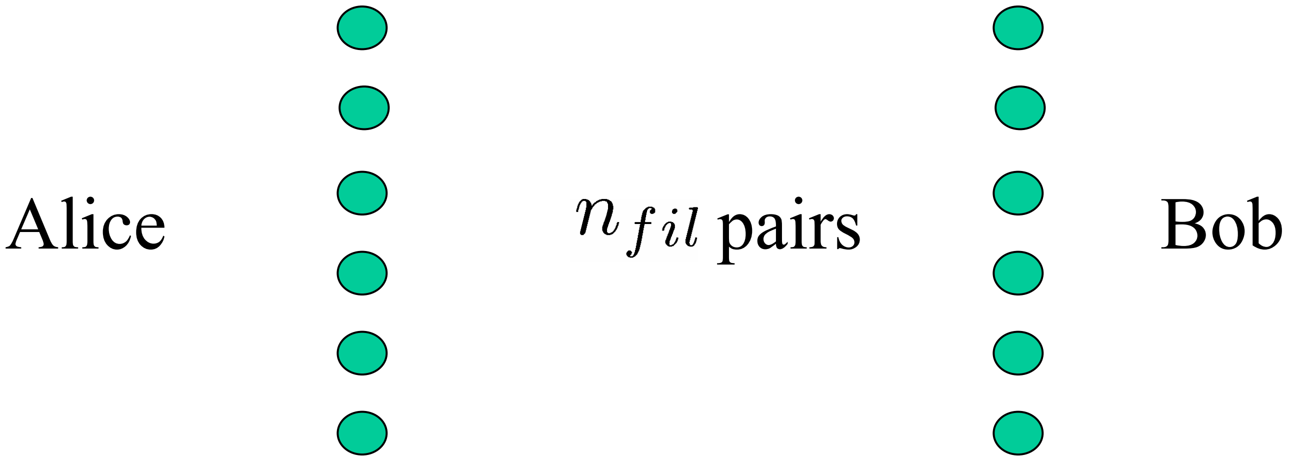
$$F_S = \alpha|0_x\rangle_B\langle 0_x| + \beta|1_x\rangle_B\langle 1_x|$$

Bob

F succeeds or not

Keep the qubit pairs that have passed the filtering

No Eve: $(1_A \otimes F_S)\,|\Phi\rangle_{AB} \propto (|0_z\rangle_A|0_z\rangle_B + |1_z\rangle_A|1_z\rangle_B)$



Alice

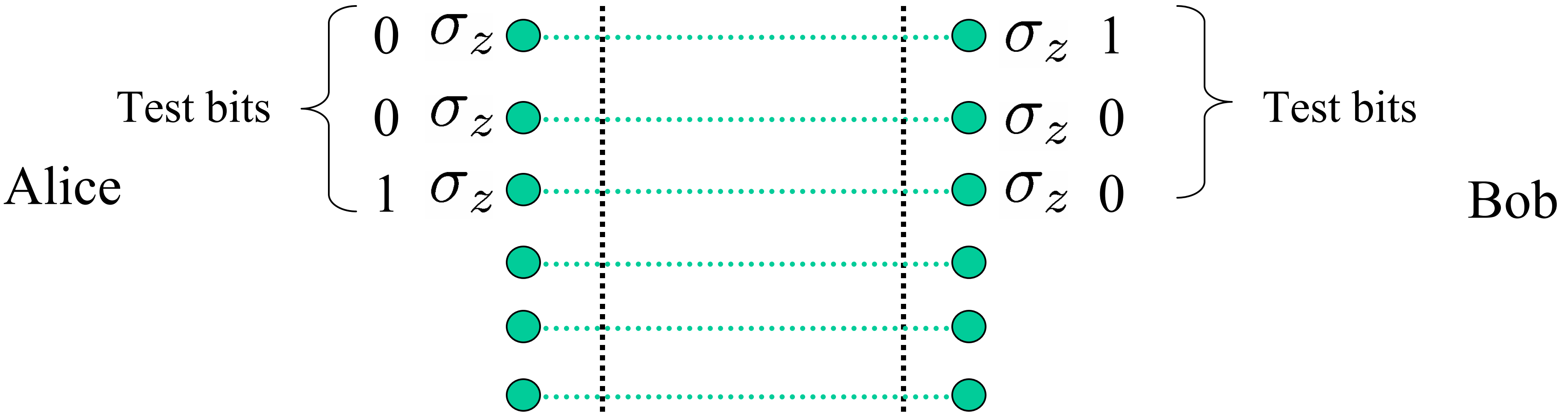
n_{fil} pairs

Bob

n_{fil}: number of the states that have passed the filtering

Randomly permute the pairs of qubit

(2) Bit error estimation



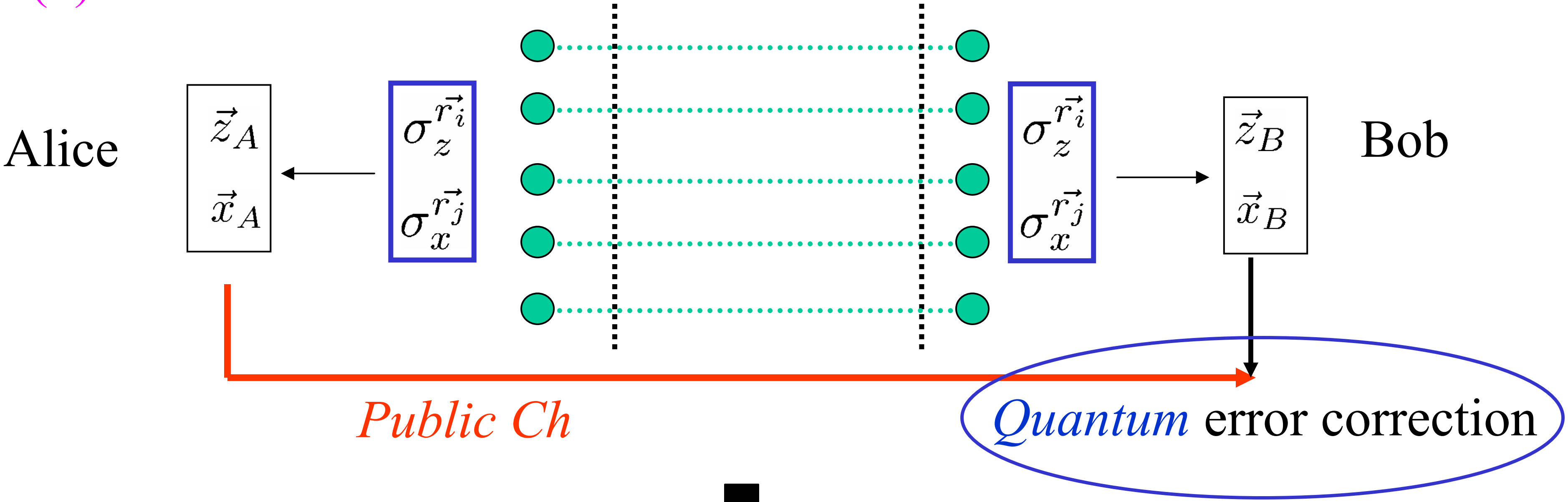
Test bits gives us a good bit error estimation on untested qubit pairs

(2‘) Phase error estimation
(via a property of the Filtering)

If too many errors are detected,
then they abort the protocol

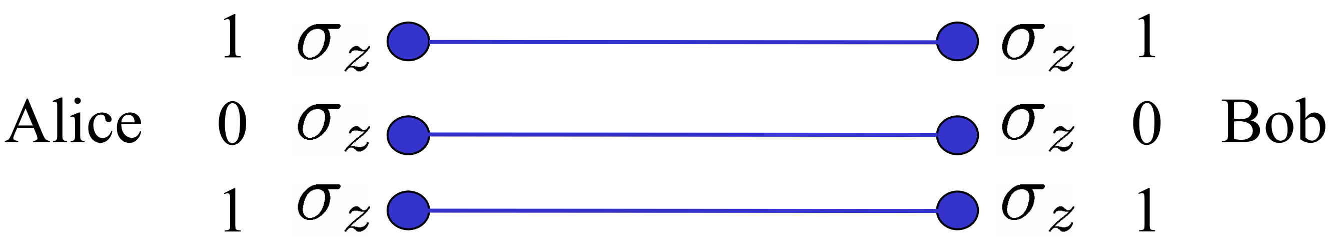
Choose the CSS code that correct up to the estimated errors

(3) The EDP based on CSS codes



(4) Measurements on the Bell states

Quantum decoding



Pairs of the Bell state

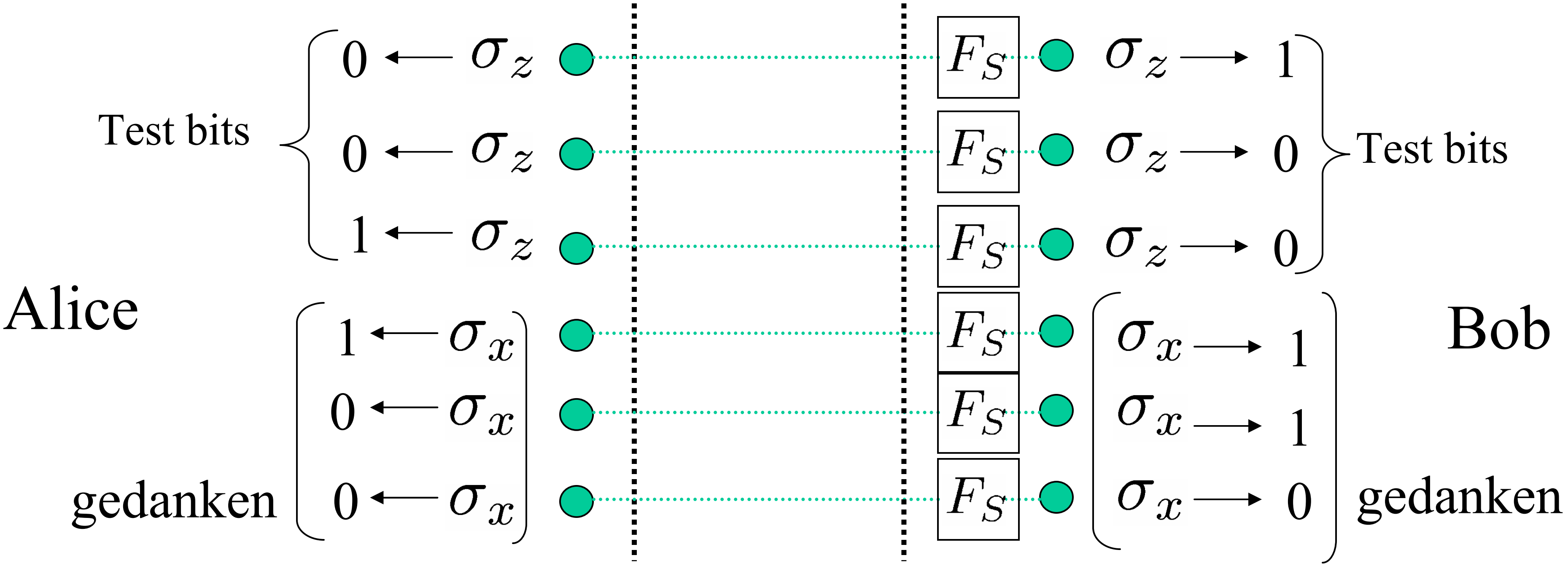
The security of the *Protocol 1* depends on whether they can distill the Bell state or not.

⇓

- *Protocol 1* is secure if the phase error rate estimation for the EDP based on CSS codes is precise.

- The phase error rate has to be estimated from the bit error rate.c

The phase error rate estimation from the bit error rate



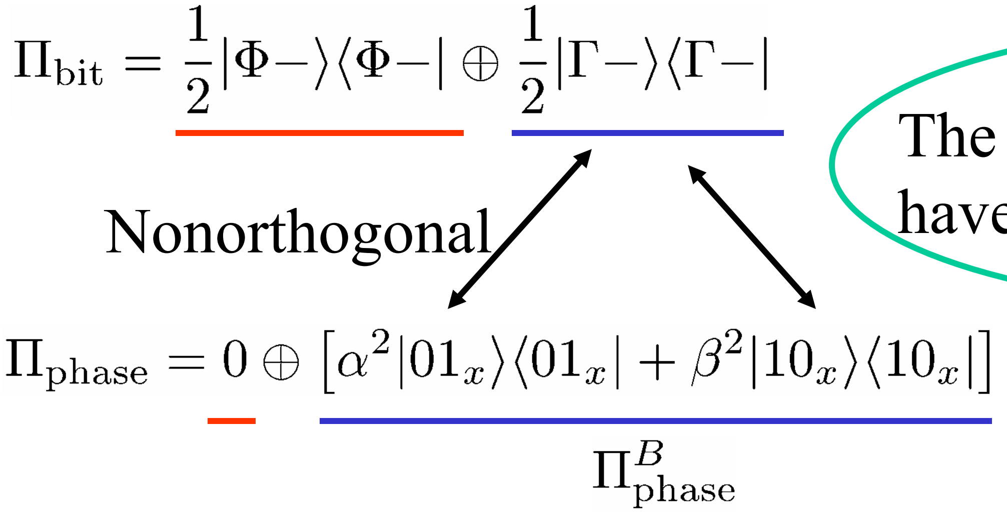
Test bits
$0 \longleftarrow \sigma_z$
$0 \longleftarrow \sigma_z$
$1 \longleftarrow \sigma_z$
Alice
$1 \longleftarrow \sigma_x$
$0 \longleftarrow \sigma_x$
gedanken
$0 \longleftarrow \sigma_x$
F_S
F_S
F_S
F_S
F_S
F_S
$\sigma_z \longrightarrow 1$
$\sigma_z \longrightarrow 0$
Test bits
$\sigma_z \longrightarrow 0$
$\sigma_x \longrightarrow 1$
Bob
$\sigma_x \longrightarrow 1$
$\sigma_x \longrightarrow 0$
gedanken

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

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

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.



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

Nonorthogonal

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

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

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

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

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

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

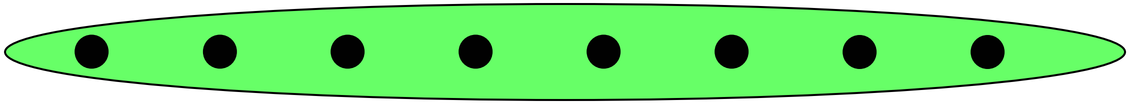
} Qubit space

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

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

Question

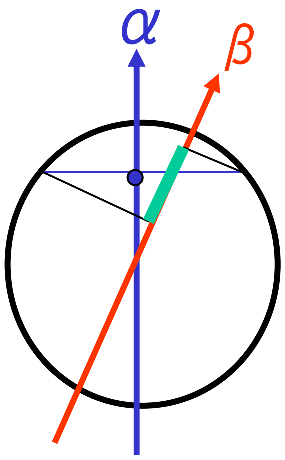
Consider any N-qubit state that is symmetric under any permutation



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

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 !

By using the method, we can estimate the upper bound of the phase error rate from the bit error rate.

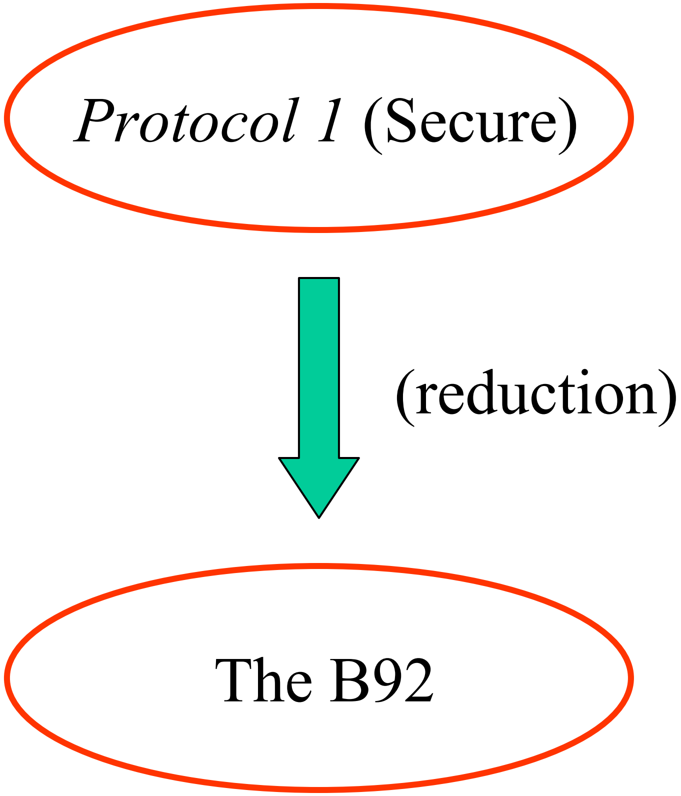
We can distill the Bell states by the EDP based on CSS codes

Protocol 1 is unconditionally secure.

$n_{fil}\left[1-h(e_{bit})-h(e_{phase})\right]$ secret key can be distilled

Outline of the security proof of the B92

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



Protocol 1 (Secure)

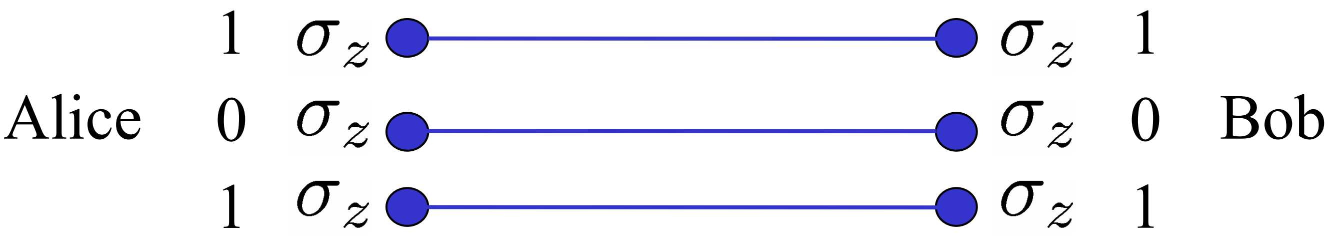
(reduction)

The B92

Observation 1

Shor and Preskill (2000)

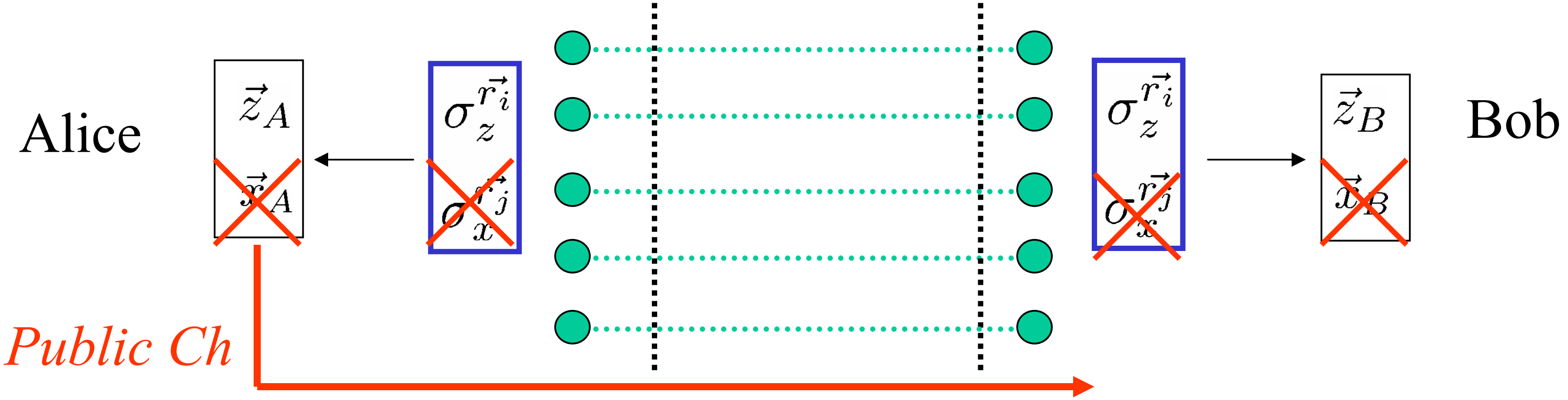
Only the bit values on secret key are important



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

- They do not need to detect phase error positions !

The EDP based on CSS codes



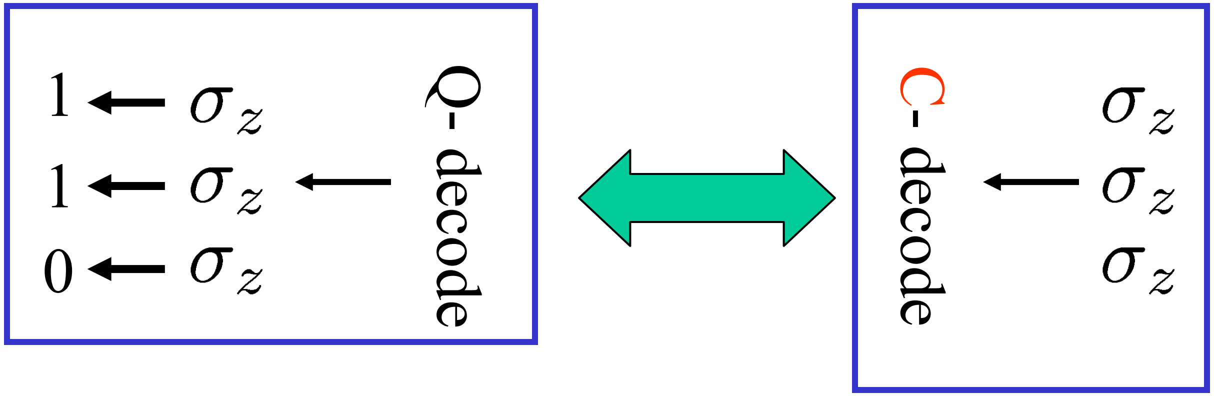
Observation 2

Shor and Preskill (2000)

Due to the property of the Quantum decoding in CSS codes

No need for *Quantum* decode → Classical decode

(*Note*: Phase error rate is still necessary for the decode)



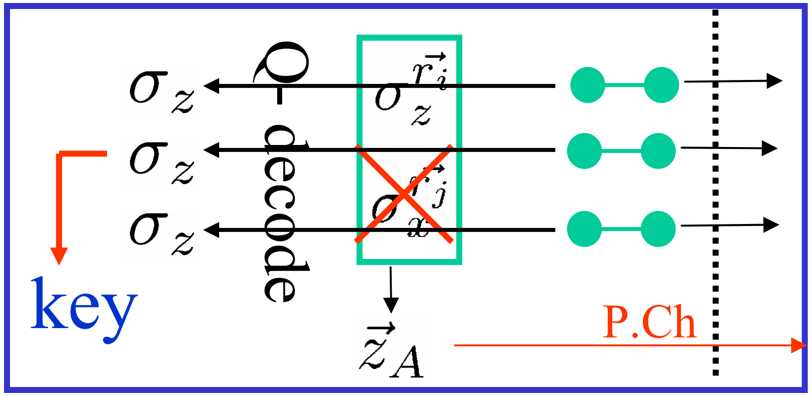
$1 \leftarrow \sigma_z$

$1 \leftarrow \sigma_z \quad \leftarrow$ Q-decode

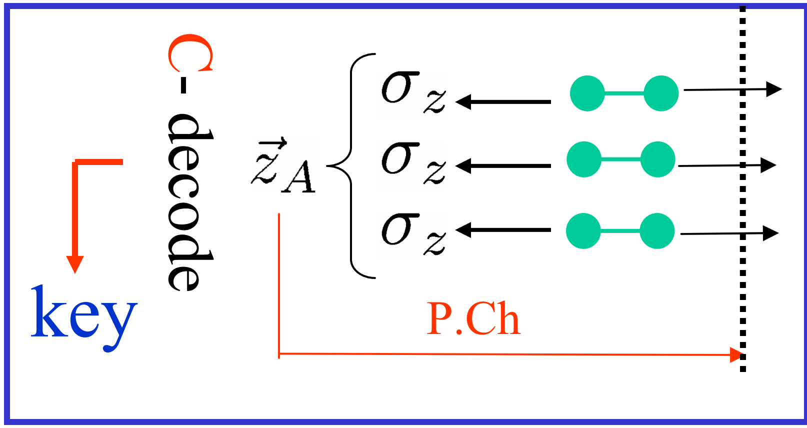
$0 \leftarrow \sigma_z$

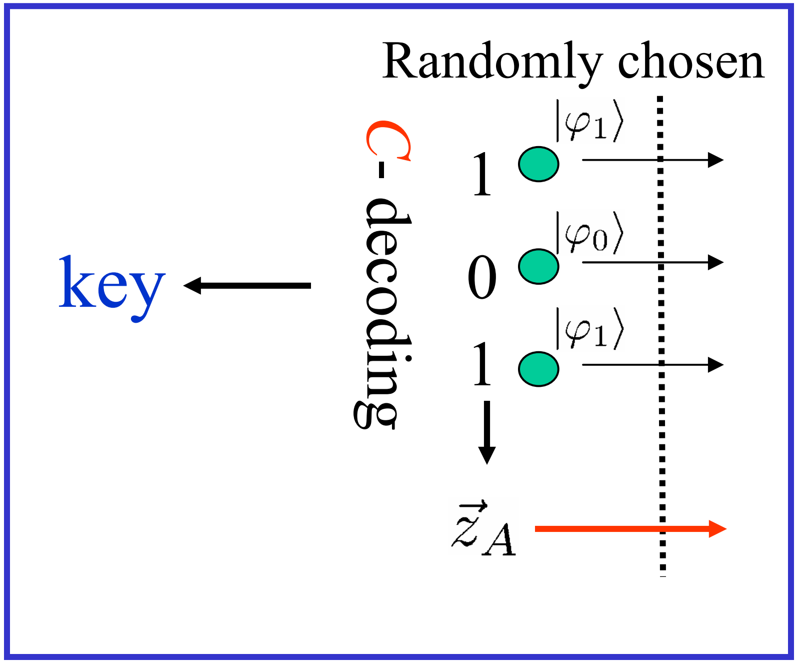
C-decode $\leftarrow \sigma_z \sigma_z \sigma_z$

Reduction to the B92 protocol (Alice's side)



$$\frac{1}{\sqrt{2}}\left(|0_z\rangle_{\mathrm{A}}|\varphi_0\rangle_{\mathrm{B}} + |1_z\rangle_{\mathrm{A}}|\varphi_1\rangle_{\mathrm{B}}\right)$$



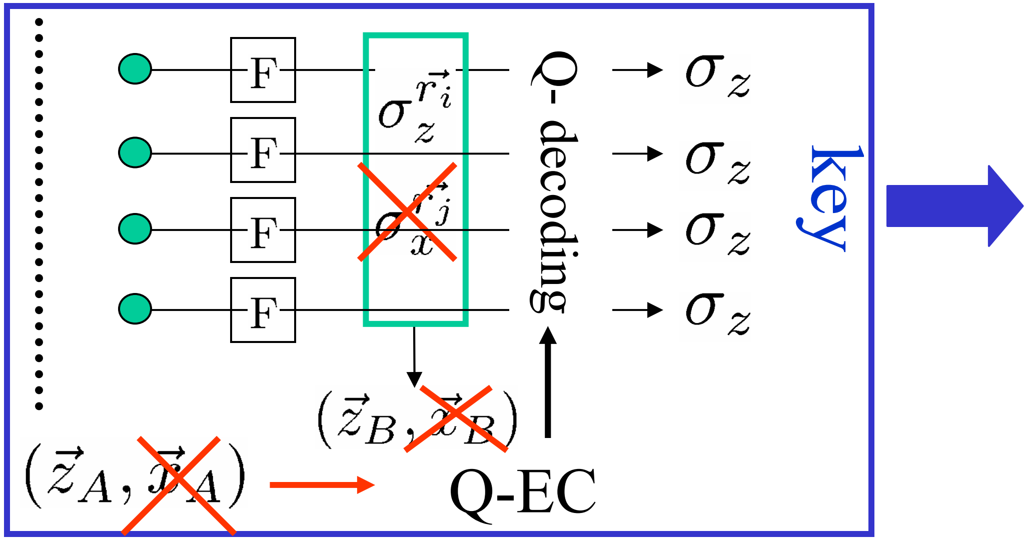


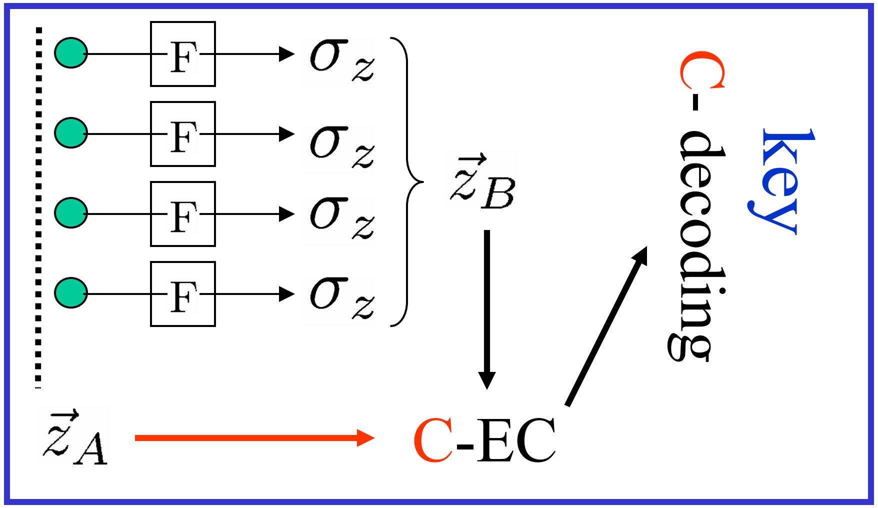
C-decode corresponds to the privacy amplification

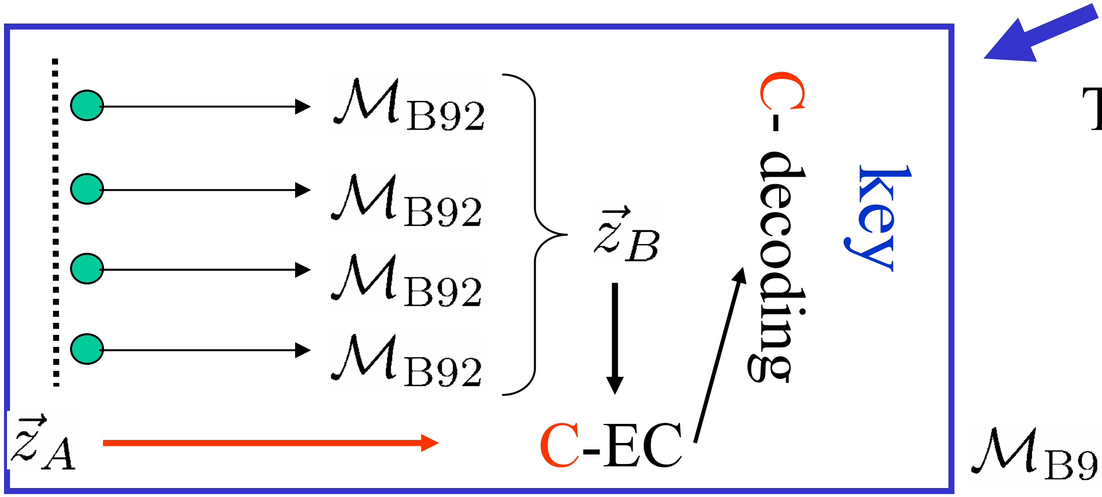
Preparation of the B92 states

Classical bit error correction !!

Reduction to the B92 protocol (Bob's side)







The filtering succeeds or not

⇕

Conclusive or not

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

The B92 measurement and classical error correction !

A derivation of $\mathcal{M}_{\mathrm{B92}}$

$$\left.\begin{aligned} F_S|0_z\rangle_{\mathrm{B}}\langle 0_z|F_S &= |\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|/2 = F_0 \\ F_S|1_z\rangle_{\mathrm{B}}\langle 1_z|F_S &= |\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|/2 = F_1 \\ 1 - F_0 - F_1 &= F_? \end{aligned}\right\} \mathcal{M}_{\mathrm{B92}}$$

$$F_S = \alpha|0_x\rangle_B\langle 0_x| + \beta|1_x\rangle_B\langle 1_x|$$

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

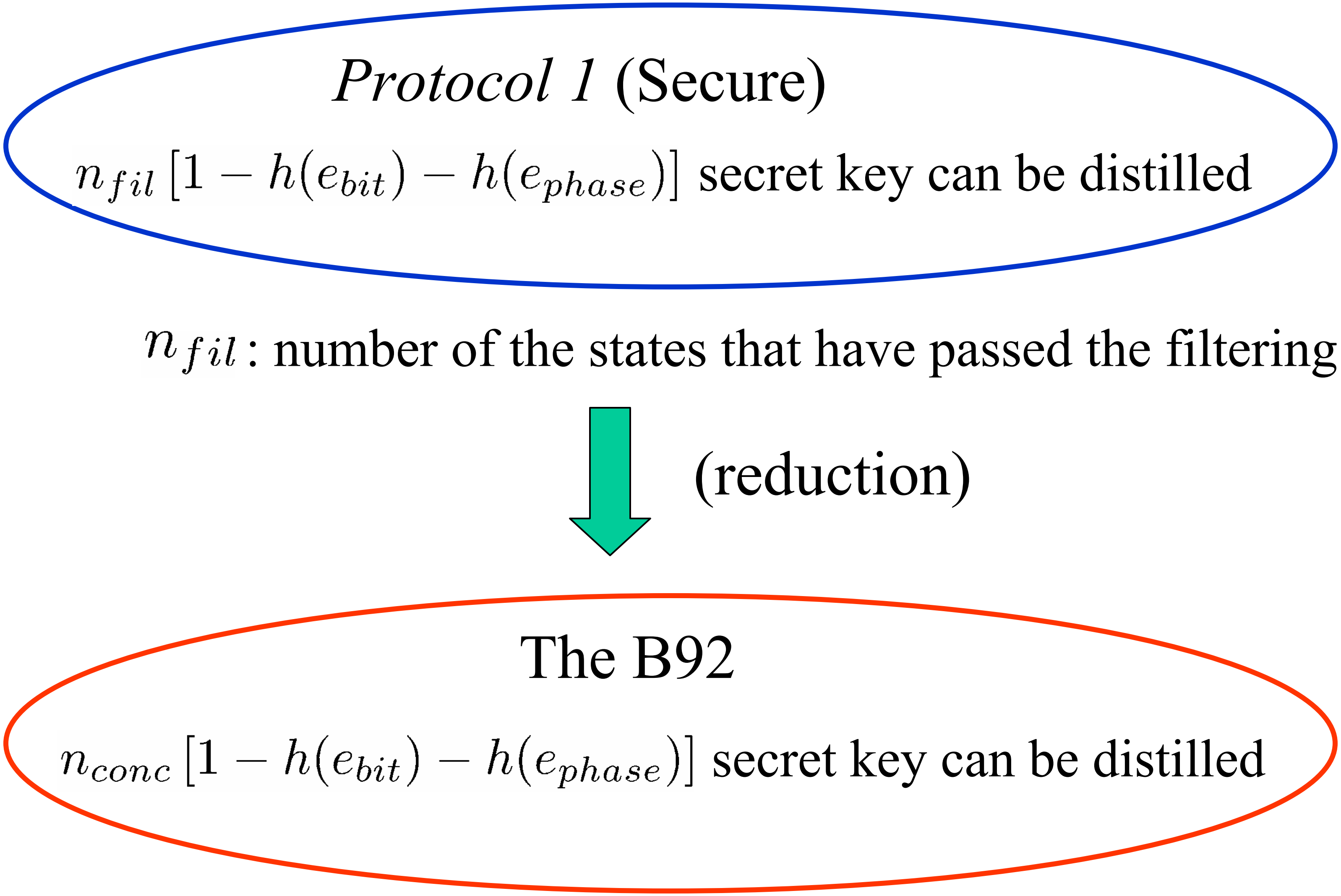
$$\langle\overline{\varphi}_i|\varphi_j\rangle = \delta_{i,j}$$

Success probability of the filtering

||

The probability of obtaining the conclusive event

Summary of our proof



Protocol 1 (Secure)

$n_{fil}\,[1-h(e_{bit})-h(e_{phase})]$ secret key can be distilled

n_{fil}: number of the states that have passed the filtering

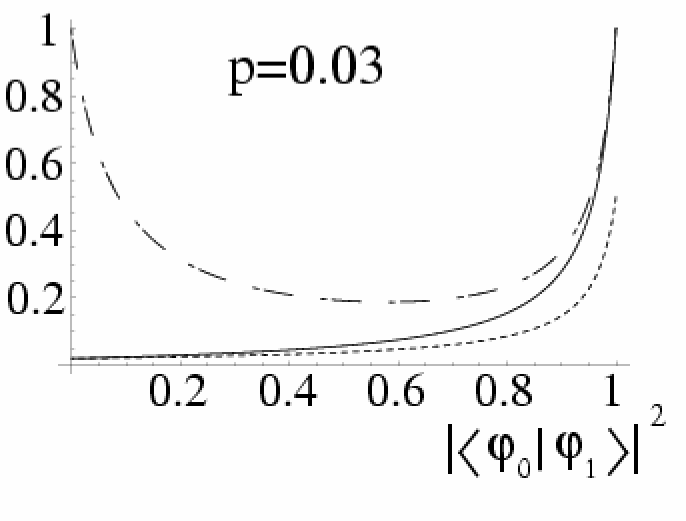
(reduction)

The B92

$n_{conc}\,[1-h(e_{bit})-h(e_{phase})]$ secret key can be distilled

n_{conc}: number of the states that result in conclusive events

Example of the phase error estimation



•••••• :Actual bit error

——— Actual phase error

– · – · · :Estimated upper bound of phase error

Channel: $\rho \rightarrow (1-p)\rho + p/3\sum_{a=x,y,z}\sigma_a\rho\sigma_a$ p : depolarizing rate

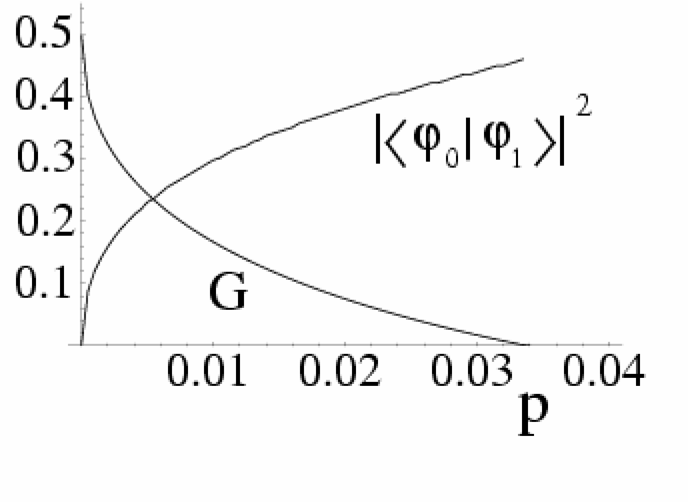
$|\varphi_0\rangle$
$|\varphi_1\rangle$: Two nonorthogonal single photon states

Small $|\langle\varphi_0|\varphi_1\rangle|^2$ makes the estimation poor

↕ Trade-off

Large $|\langle\varphi_0|\varphi_1\rangle|^2$ makes the signal vulnerable to noises

Example of the security



G: Optimal net growth of secret key per pulse p : depolarizing rate

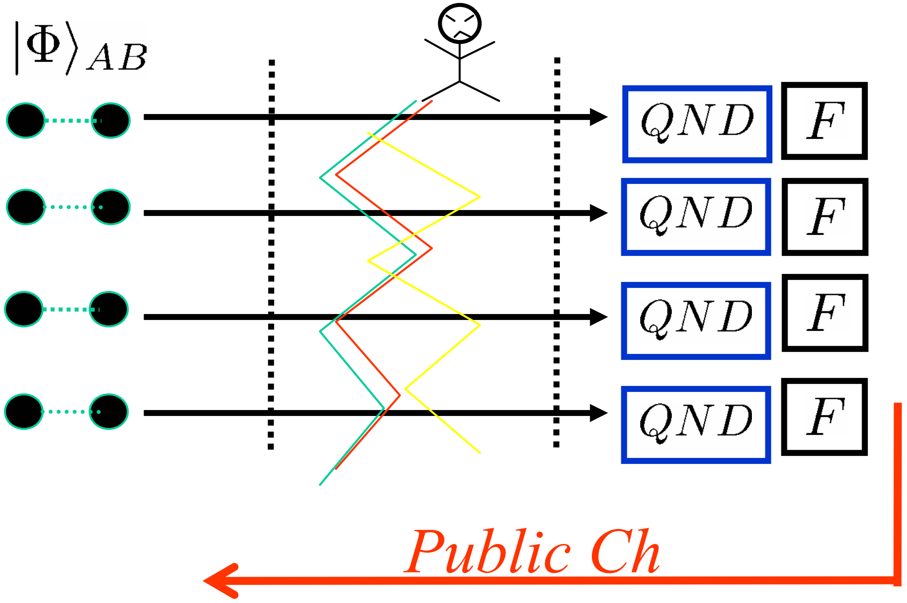
The B92 over loss-free channel is secure up to $p \sim 3.4\%$

c.f The BB84: $p \sim 16.5\%$ (Shor and Preskill , 2000)

The B92 over lossy and noisy channel

Alice prepares $|\Phi\rangle_{AB}$: $\frac{1}{\sqrt{2}}(|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B) = \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B$

Alice



$|\Phi\rangle_{AB}$

QND F

QND F

QND F

QND F

Public Ch

$$F = \{F_S, \sqrt{1-F_S^2}\}$$

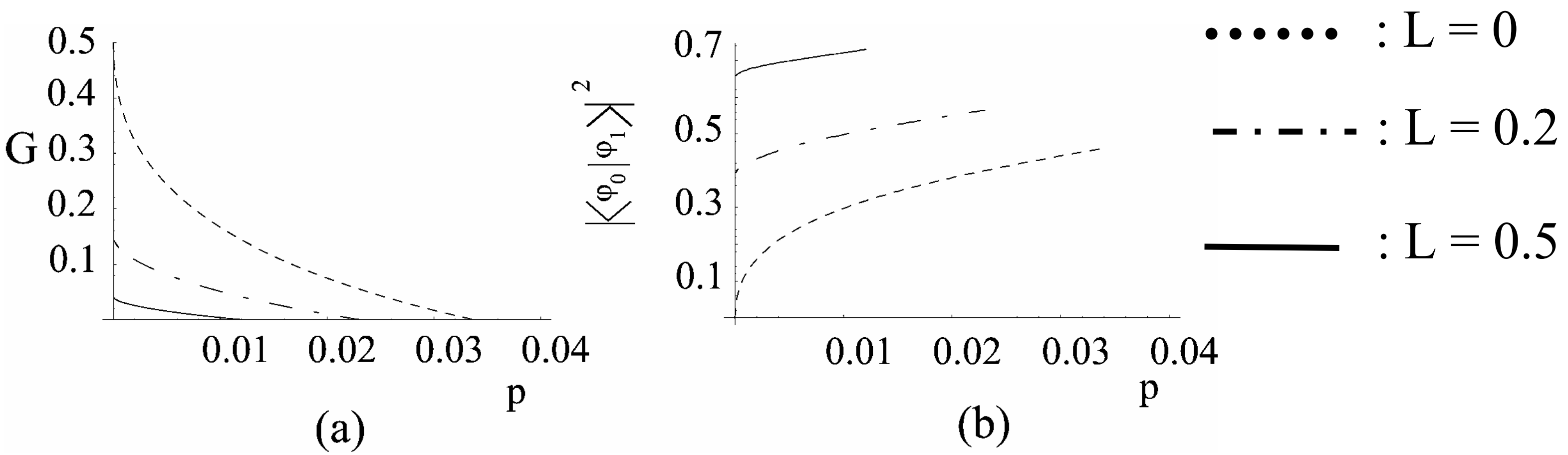
$$F_S = \alpha|0_x\rangle_B\langle 0_x| + \beta|1_x\rangle_B\langle 1_x|$$

Bob

F succeeds or not

$QND \rightarrow n = 1$ and $n \neq 1$

Example of the security and estimation



G : Optimal net growth rate of secret key per pulse

p: depolarizing rate T : the prob that Bob detects single photon

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

The vacuum state

Summary

- We have proven the unconditional security of the B92 over lossy and noisy channel.
  (Assumption:an ideal single photon source, an ideal photon counter that discriminates between single photon and the other states)

- Thanks to the filtering, we can upper bound the phase error rate from the bit error rate.

- Accuracy of the phase error estimation for the EDP based on CSS codes depends on the nonorthogonality. The poor estimation makes the B92 weaker against noises.

K. Tamaki, M. Koashi, and *N. Imoto,*
Phys. Rev.Lett.**90**, 167904 (2003). (ch-loss free)
K. Tamaki, and N. Lütkenhaus, To appear in Phys. Rev A.
quantu-ph/0308048. (over noisy and lossy ch)