Mathematical Aspects in Current Quantum Information Theory 2019 at Seoul National University

Structure of Sequential State Discrimination

Min Namkung and Younghun Kwon
Department of Applied Physics, Hanyang University

한양대학교
HANYANG UNIVERSITY

Index

Part I : Theory

- Scenario of sequential state discrimination
- Constructing optimization problem
- Comparison with other scenarios

Part II : Application

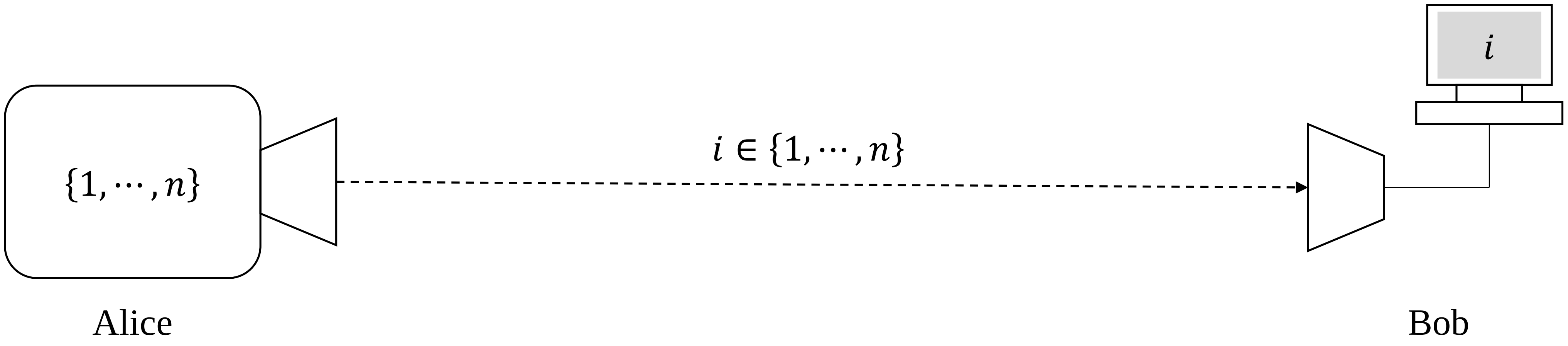
- Realistic QKD
- Implementing sequential state discrimination
- Sequential state discrimination in noisy channel
- Comparison with probabilistic cloning strategy

Part I

Theory

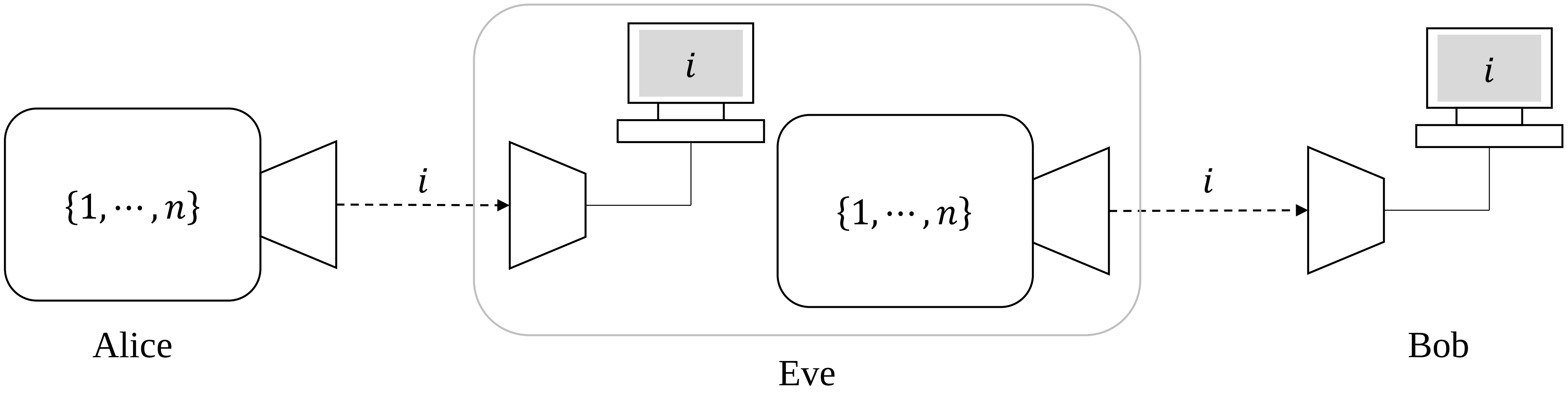
Scenario of sequential state discrimination

Classical scheme of communication



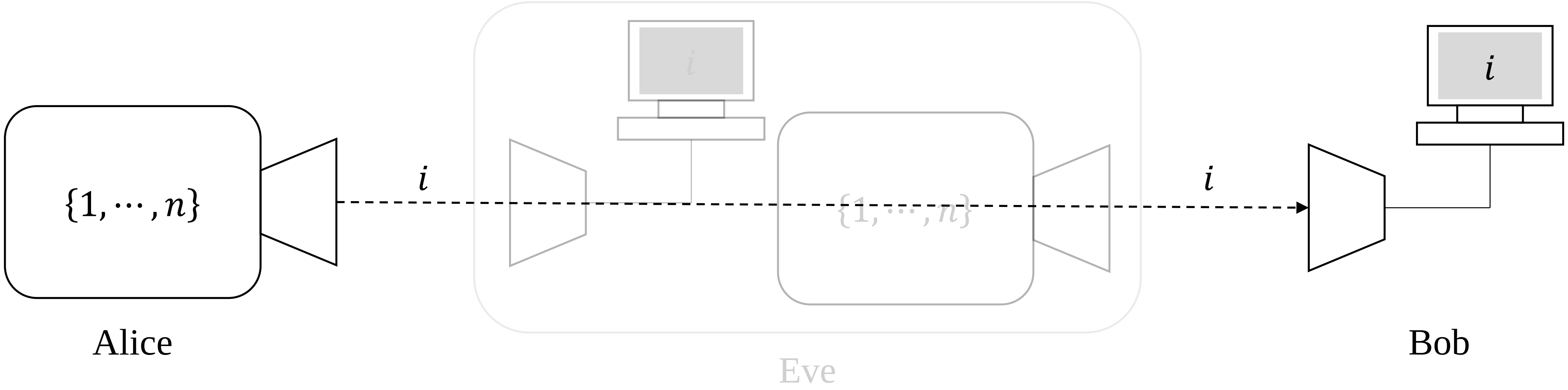
Scenario of sequential state discrimination

Classical scheme of communication



Scenario of sequential state discrimination

Classical scheme of communication



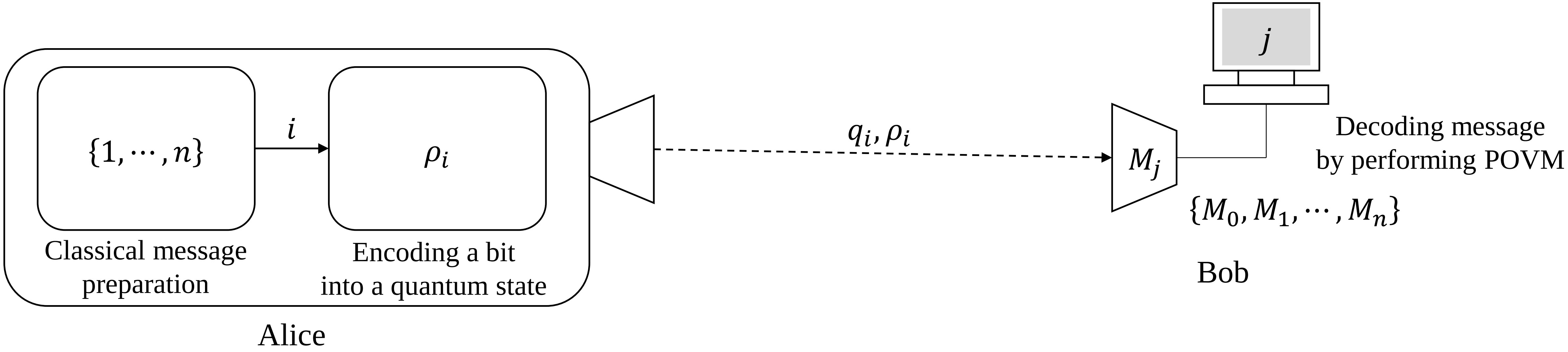
Insecurity of classical scheme

Even Eve eavesdrops secure message during Alice and Bob communicate,
Alice and Bob cannot notice Eve.

HYU 한양대학교 HANYANG UNIVERSITY

Scenario of sequential state discrimination

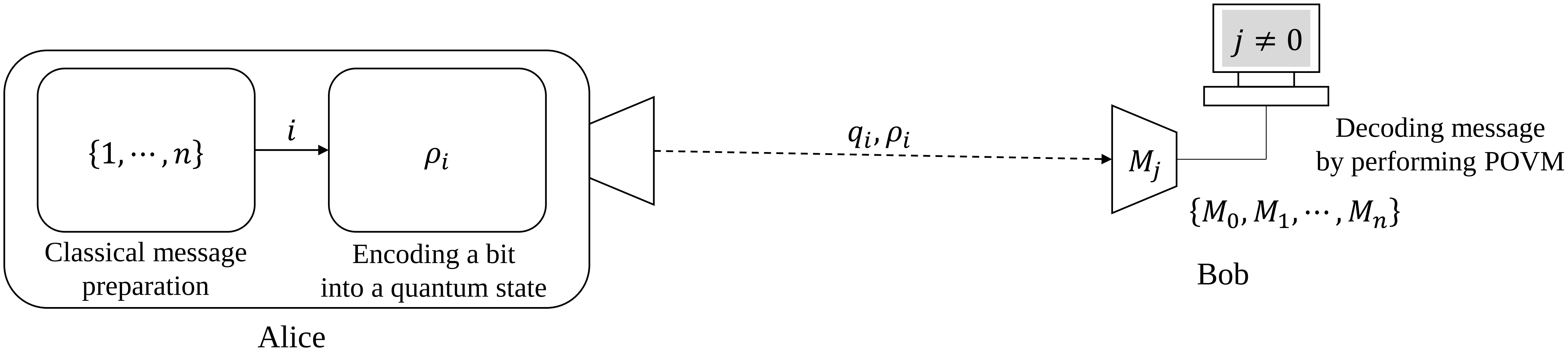
Quantum key distribution



G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

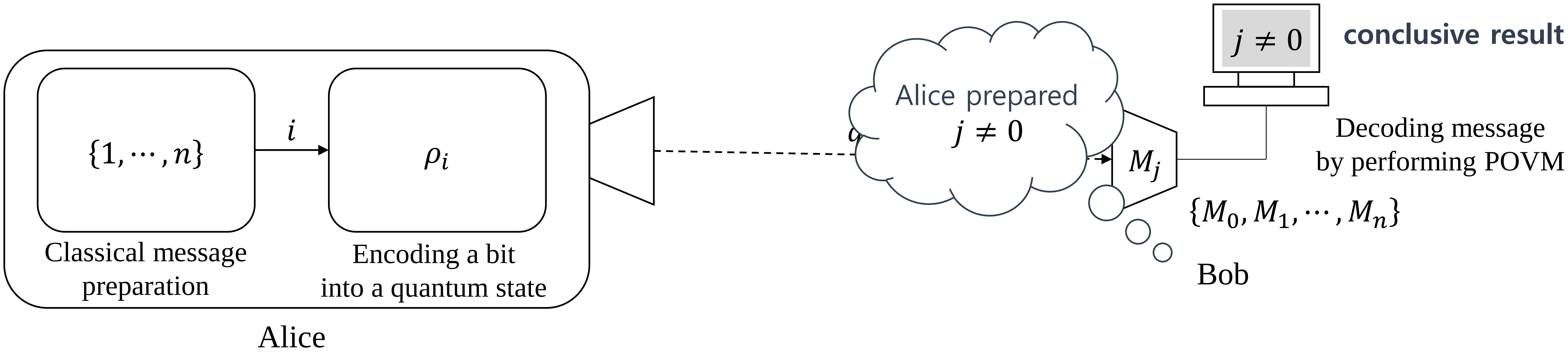
Quantum key distribution



G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

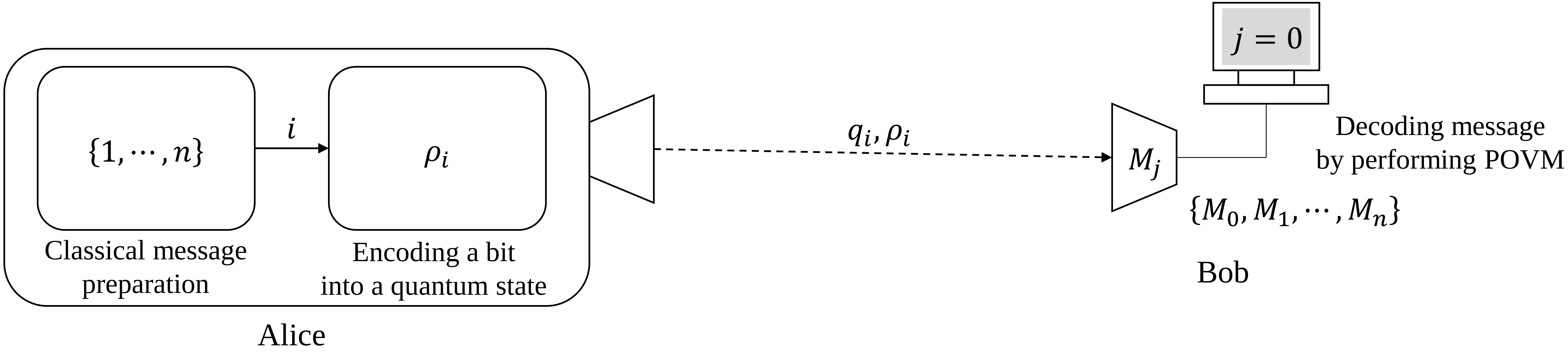
Quantum key distribution



G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

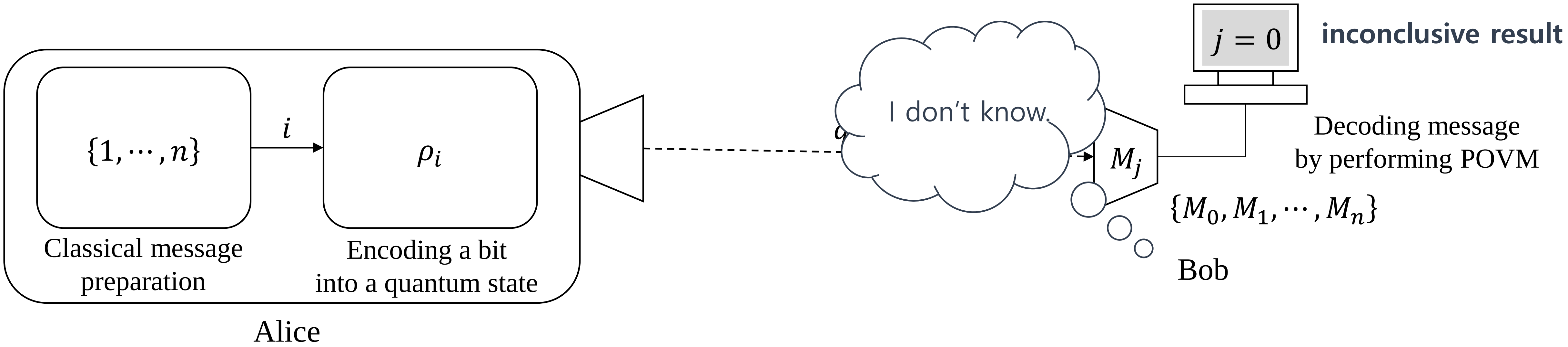
Quantum key distribution



G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

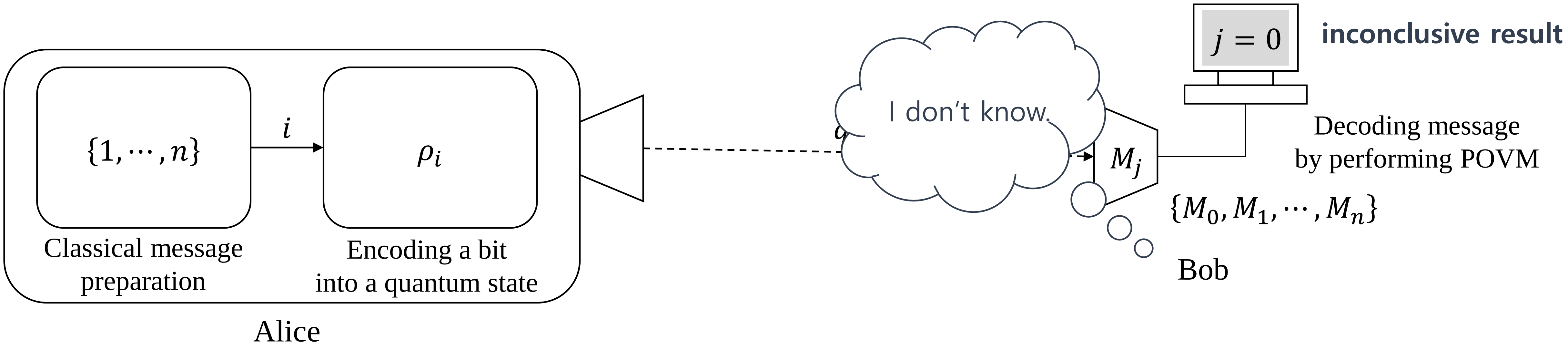
Quantum key distribution



G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

Quantum key distribution



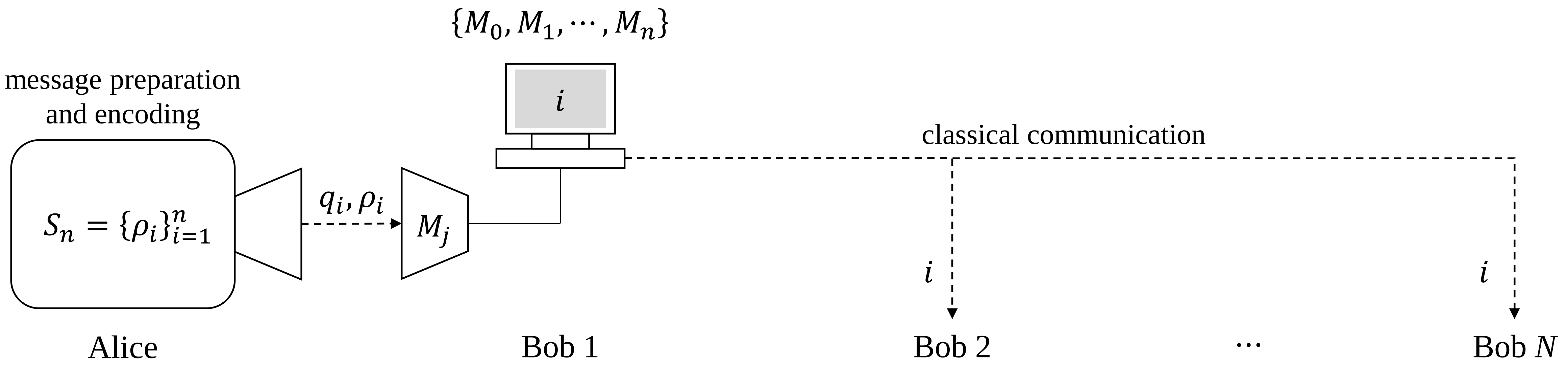
General structure of quantum key distribution

Quantum key distribution can be expressed as quantum state discrimination. For example, if Alice and Bob perform B92 protocol, then this scenario can be expressed as unambiguous discrimination.

G. Cariolaro, *Quantum Communications* (Springer, 2015).
C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

Scenario of sequential state discrimination

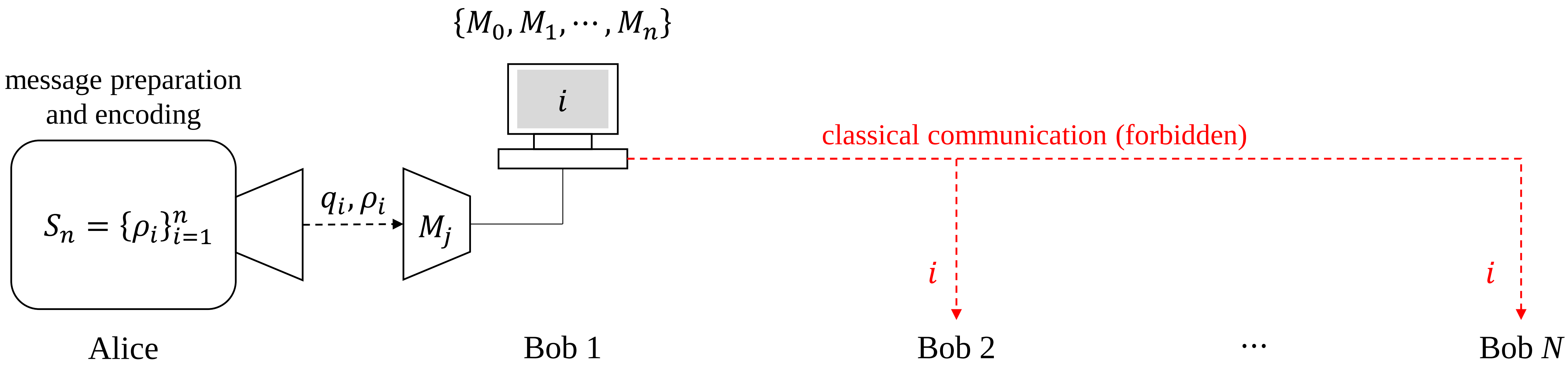
Multiparty QKD based on sequential state discrimination



HYU 한양대학교 HANYANG UNIVERSITY

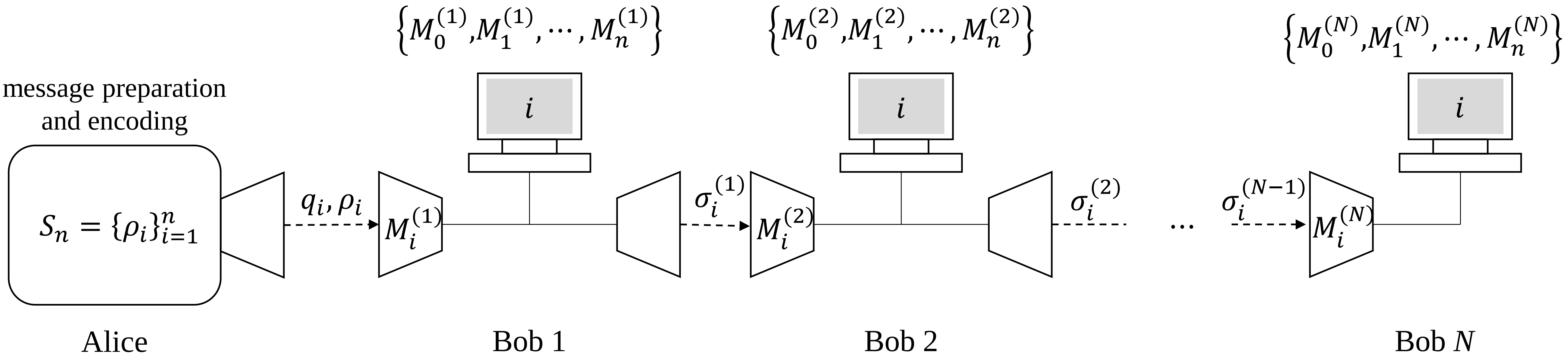
Scenario of sequential state discrimination

Multiparty QKD based on sequential state discrimination



Scenario of sequential state discrimination

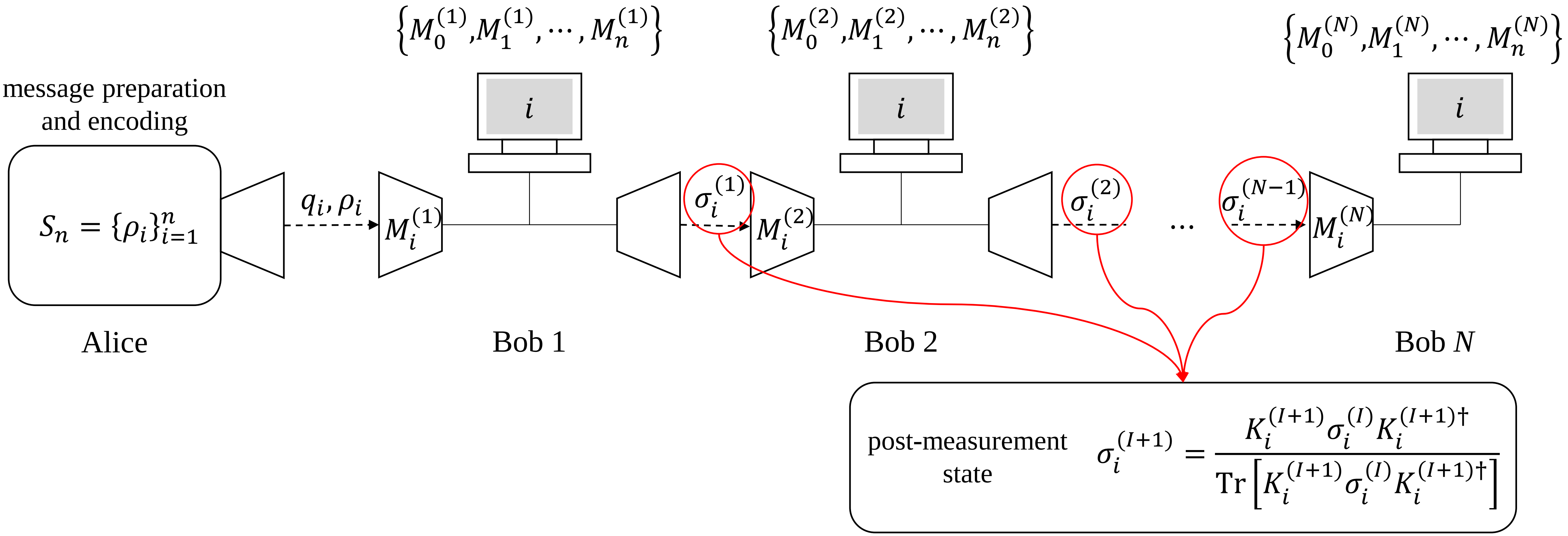
Multiparty QKD based on sequential state discrimination



J. A. Bergou et al., Extracting information from a qubit by multiple observers: Towards a theory of sequential state discrimination, Phys. Rev. Lett. 111, 100503 (2013).

Scenario of sequential state discrimination

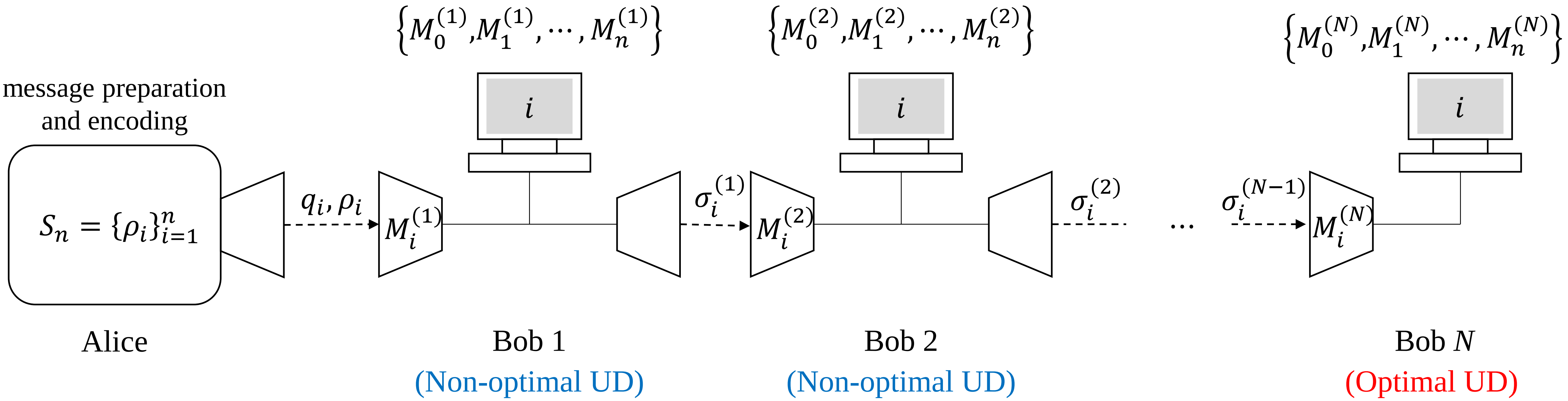
Multiparty QKD based on sequential state discrimination



J. A. Bergou et al., Extracting information from a qubit by multiple observers: Towards a theory of sequential state discrimination, Phys. Rev. Lett. 111, 100503 (2013).

Scenario of sequential state discrimination

Multiparty QKD based on sequential state discrimination



J. A. Bergou et al., Extracting information from a qubit by multiple observers: Towards a theory of sequential state discrimination, Phys. Rev. Lett. 111, 100503 (2013).

HYU 한양대학교 HANYANG UNIVERSITY

Constructing optimization problem

POVM for unambiguous discrimination

$$p(j|i) = \mathrm{Tr}\rho_i M_j$$

Born's rule	POVM condition	
$p(j\|i) \geq 0 \quad \forall i,j$	$M_i \geq 0 \quad \forall i \in \{0,\cdots,n\}$	Positivity
$p(j\|i) \in \mathbb{R} \quad \forall i,j$	$M_i = M_i^\dagger \quad \forall i \in \{0,\cdots,n\}$	Hermitian
$\sum_j p(j\|i) = 1 \quad \forall i$	$M_0 + M_1 + \cdots + M_n = I$	Completeness
$p(j\|i) = 0 \quad \forall i \neq j$	$\mathrm{Tr}\rho_i M_j = \delta_{ij}\mathrm{Tr}\rho_i M_i \qquad \forall i \neq j$	Unambiguous discrimination

Constructing optimization problem

POVM for unambiguous discrimination

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\mathrm{Tr}\rho_i M_j = \delta_{ij} \mathrm{Tr}\rho_i M_i \qquad \forall i \neq j$

Theorem 1. [T. Rudolph *et al.*] If $supp(\rho_i)$ satisfies $supp(\rho_i) \notin \cup_{j\neq i} supp(\rho_j)$ for all $\rho_i \in S_n$, then there exists POVM that performs unambiguous discrimination on S_n.

T. Rudolph, R. W. Spekkens, and P. S. Turner, Unambiguous discrimination of mixed states, Phys. Rev. A **68**, 010301R (2003).
A. Chefles, Unambiguous discrimination between linearly independent quantum states, Phys. Lett. A **239**, 339 (1998).

Constructing optimization problem

POVM for unambiguous discrimination

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\mathrm{Tr}\rho_i M_j = \delta_{ij} \mathrm{Tr}\rho_i M_i \quad \forall i \neq j$

Theorem 1. [T. Rudolph *et al.*] If $supp(\rho_i)$ satisfies $supp(\rho_i) \notin \cup_{j\neq i} supp(\rho_j)$ for all $\rho_i \in S_n$, then there exists POVM that performs unambiguous discrimination on S_n.

However, exploiting Theorem 1 is quite difficult.

⇩

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle\psi_i|M_j|\psi_i\rangle = \delta_{ij}\langle\psi_i|M_i|\psi_i\rangle \quad \forall i \neq j$

Theorem 2. [A. Chefles] If $\bar{S}_n$ is a set of linearly independent pure states, then there exists POVM that performs unambiguous discrimination on $\bar{S}_n$.

T. Rudolph, R. W. Spekkens, and P. S. Turner, Unambiguous discrimination of mixed states, Phys. Rev. A **68**, 010301R (2003).
A. Chefles, Unambiguous discrimination between linearly independent quantum states, Phys. Lett. A **239**, 339 (1998).

Constructing optimization problem

POVM for unambiguous discrimination

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\mathrm{Tr}\rho_i M_j = \delta_{ij} \mathrm{Tr}\rho_i M_i \quad \forall i \neq j$

Theorem 1. [T. Rudolph *et al.*] If $supp(\rho_i)$ satisfies $supp(\rho_i) \notin \bigcup_{j\neq i} supp(\rho_j)$ for all $\rho_i \in S_n$, then there exists POVM that performs unambiguous discrimination on S_n.

However, exploiting Theorem 1 is quite difficult.

$\Downarrow$

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle\psi_i|M_j|\psi_i\rangle = \delta_{ij}\langle\psi_i|M_i|\psi_i\rangle \quad \forall i \neq j$

Theorem 2. [A. Chefles] If $\bar{S}_n$ is a set of linearly independent pure states, then there exists POVM that performs unambiguous discrimination on $\bar{S}_n$.

Simplified Proof. **[D. Ha and Y. Kwon]**

$$M_i = \alpha_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| \; (i = 1, \cdots, n), \quad \alpha_i \geq 0 \;\wedge\; \alpha_i \in \mathbb{R}$$

$$|\tilde{\psi}_i\rangle = \sum_{j=1}^{n} G_{ji}^{-1}|\psi_j\rangle, \; G = \{\langle\psi_i|\psi_j\rangle\}_{i,j=1}^{n}\text{: Gram matrix}$$

$$M_0 = I - M_1 - M_2 - \cdots - M_n$$

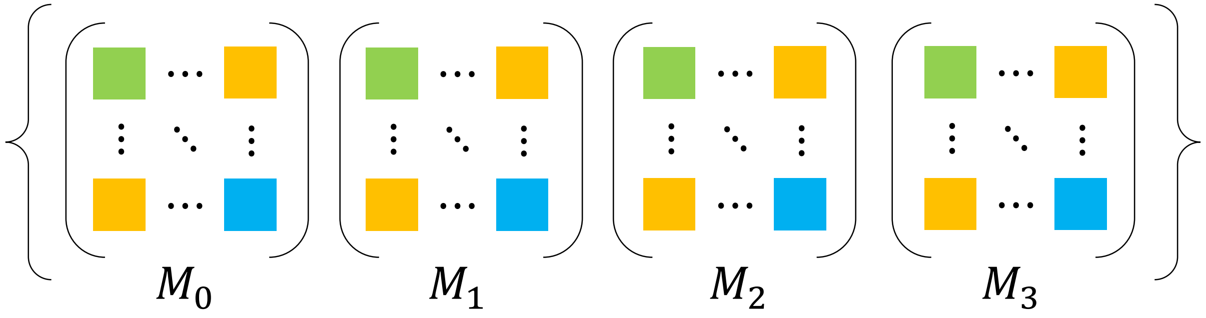
D. Ha and Y. Kwon, Analysis of optimal unambiguous discrimination of three pure quantum states, Phys. Rev. A **91**, 062312 (2015).

Constructing optimization problem

POVM for unambiguous discrimination

Power of Theorem 2.

POVM



such that

I. $M_i \geq 0, M_i = M_i^{\dagger} \quad \forall i \in \{0, \cdots, n\}$

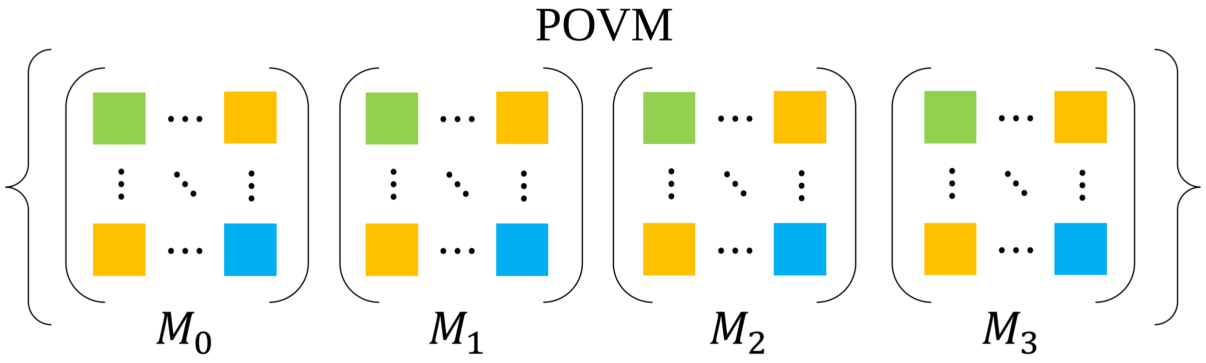
II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$

Constructing optimization problem

POVM for unambiguous discrimination

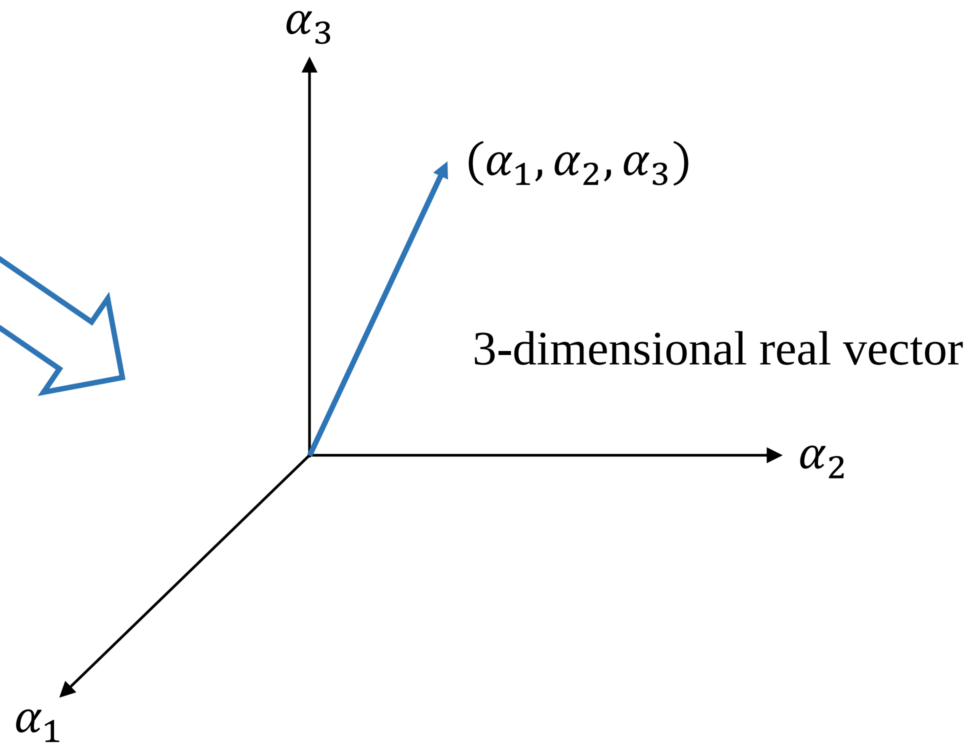
Power of Theorem 2.



$$M_i = \alpha_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| \ (i = 1, \cdots, n), \quad \alpha_i \geq 0 \ \wedge \ \alpha_i \in \mathbb{R}$$

$$|\tilde{\psi}_i\rangle = \sum_{j=1}^{n} G_{ji}^{-1} |\psi_j\rangle, \qquad G = \{\langle\psi_i|\psi_j\rangle\}_{i,j=1}^{n}\text{: Gram matrix}$$

$$M_0 = I - M_1 - M_2 - \cdots - M_n$$



Constructing optimization problem

POVM for unambiguous discrimination

Theorem 3. **[D. Ha and Y. Kwon]** Let define Hermitian matrix $\bar{M} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^{n}$ and all $m \times m$ $(m < n)$ principal submatrices $\bar{M}_m$. M_0 is positive-semidefinite if and only if every $\bar{M}$ and $\forall \bar{M}_m$ is positive-semidefinite.

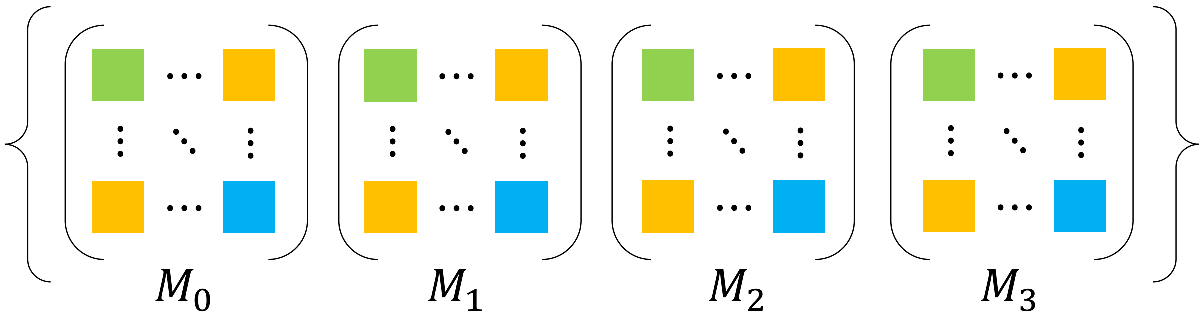
D. Ha and Y. Kwon, Analysis of optimal unambiguous discrimination of three pure quantum states, Phys. Rev. A **91**, 062312 (2015).
R. Bhatia, *Positive Definite Matrices* (Princeton University Press, 2006).

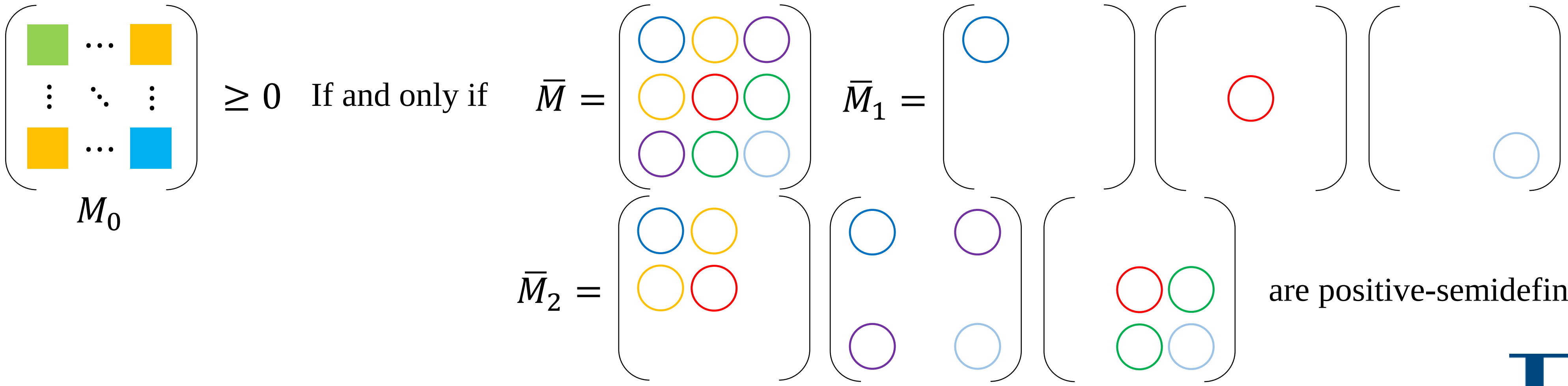
Constructing optimization problem

POVM for unambiguous discrimination

Theorem 3. **[D. Ha and Y. Kwon]** Let define Hermitian matrix $\bar{M} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^{n}$ and all $m \times m$ $(m < n)$ principal submatrices $\bar{M}_m$.
M_0 is positive-semidefinite if and only if every $\bar{M}$ and $\forall \bar{M}_m$ is positive-semidefinite.

Example. Let consider POVM





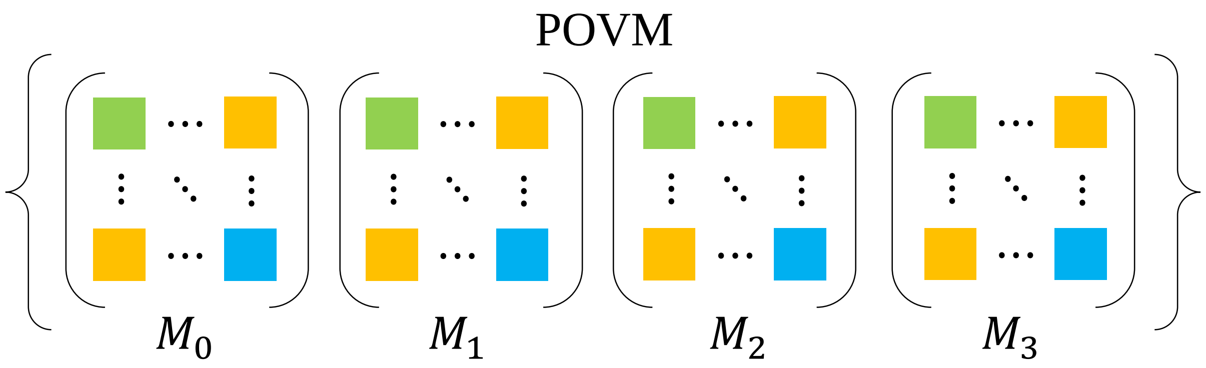
are positive-semidefinite.

HYU 한양대학교 HANYANG UNIVERSITY

Constructing optimization problem

POVM for unambiguous discrimination

Power of Theorem 3.

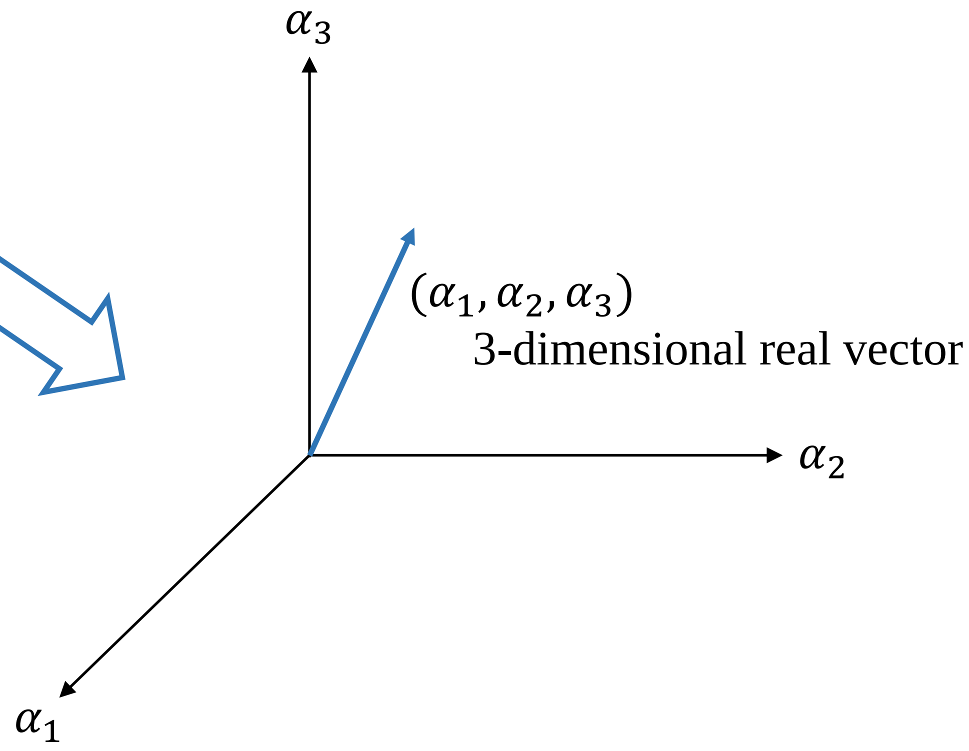


Constraint

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$

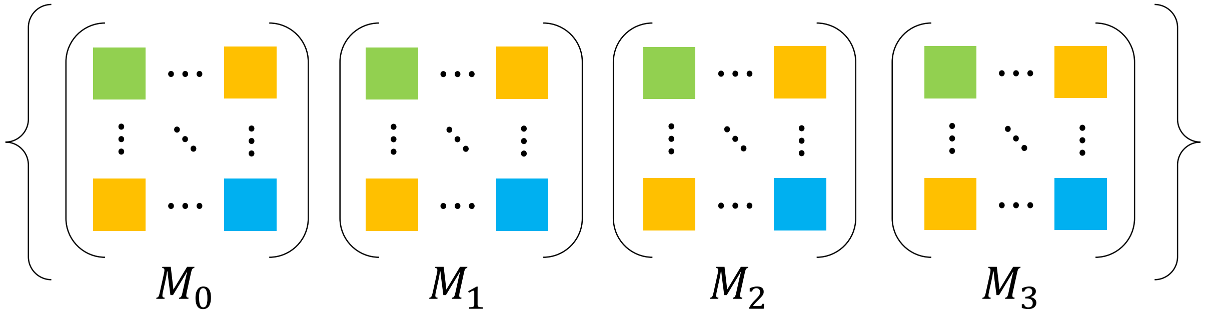


Constructing optimization problem

POVM for unambiguous discrimination

Power of Theorem 3.

POVM

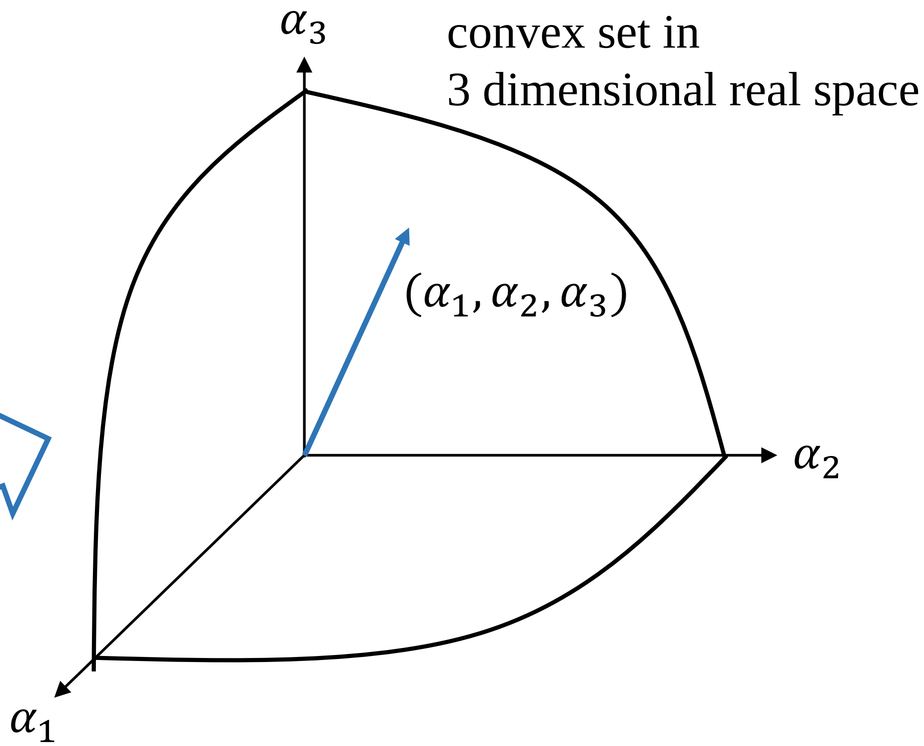


Constraint

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$



Constructing optimization problem

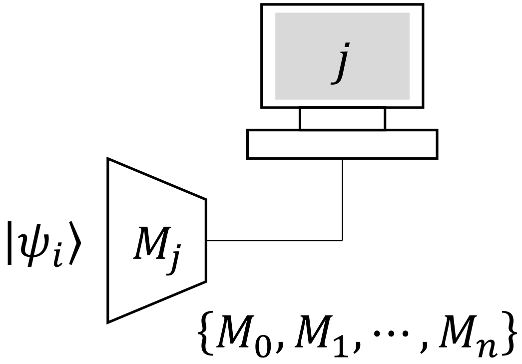
POVM for unambiguous discrimination

POVM

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$



Constructing optimization problem

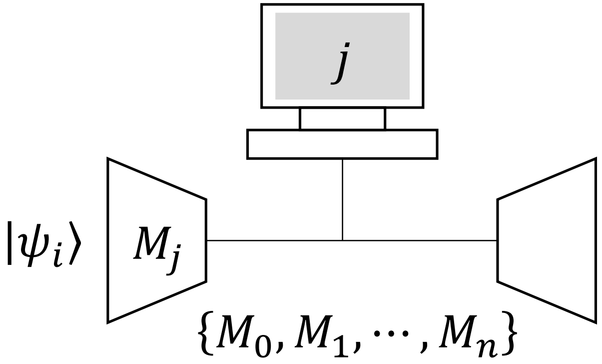
Constructing Kraus operator

POVM

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$



$$|\phi_i\rangle = \frac{K_i |\phi_i\rangle}{\sqrt{\langle \phi_i | K_i^\dagger K_i | \phi_i \rangle}}$$

Kraus operator

I. $M_i = K_i^\dagger K_i$

II. $K_i |\psi_i\rangle \propto |\phi_i\rangle$ where

$\{|\phi_1\rangle, \cdots, |\phi_n\rangle\}$: linearly independent

Constructing optimization problem

Constructing Kraus operator

POVM

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$

II. $M_0 + M_1 + \cdots + M_n = I$

III. $\langle \psi_i | M_j | \psi_i \rangle = \delta_{ij} \langle \psi_i | M_i | \psi_i \rangle \quad \forall i \neq j$

$i \neq 0$

K_i can be obtained using singular value decomposition:

$$K_i = U_i \sqrt{M_i}$$

$\Downarrow$

Kraus operator

I. $M_i = K_i^\dagger K_i$

II. $K_i |\psi_i\rangle \propto |\phi_i\rangle$ where

$\{|\phi_1\rangle, \cdots, |\phi_n\rangle\}$: linearly independent

Constructing optimization problem

Constructing Kraus operator

POVM

I. $M_i \geq 0, M_i = M_i^\dagger \quad \forall i \in \{0, \cdots, n\}$
II. $M_0 + M_1 + \cdots + M_n = I$
III. $\langle\psi_i|M_j|\psi_i\rangle = \delta_{ij}\langle\psi_i|M_i|\psi_i\rangle \quad \forall i \neq j$

Kraus operator

I. $M_i = K_i^\dagger K_i$
II. $K_i|\psi_i\rangle \propto |\phi_i\rangle$ where
$\{|\phi_1\rangle, \cdots, |\phi_n\rangle\}$: linearly independent

$i = 0$

K_i can be obtained using following lemma:

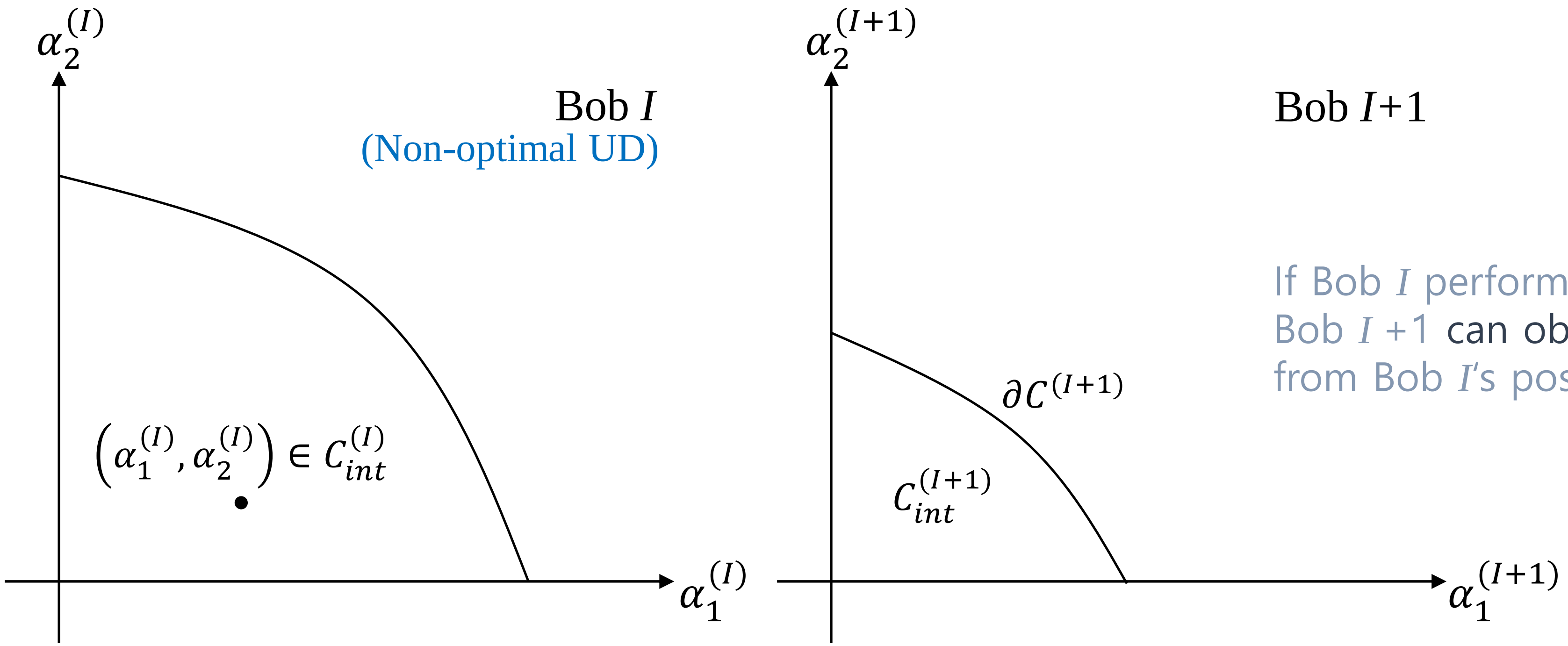
Lemma. [M. Namkung and Y. Kwon]

$M_0 = K_0^\dagger K_0$ if and only if $\langle\psi_i|M_0|\psi_j\rangle = \langle\psi_i|K_0^\dagger K_0|\psi_j\rangle$.

M. Namkung and Y. Kwon, Analysis of Sequential State Discrimination for Linearly Independent Pure Quantum States, Scientific Reports, **8**, 6515 (2018).

Constructing optimization problem

Property of Kraus operator



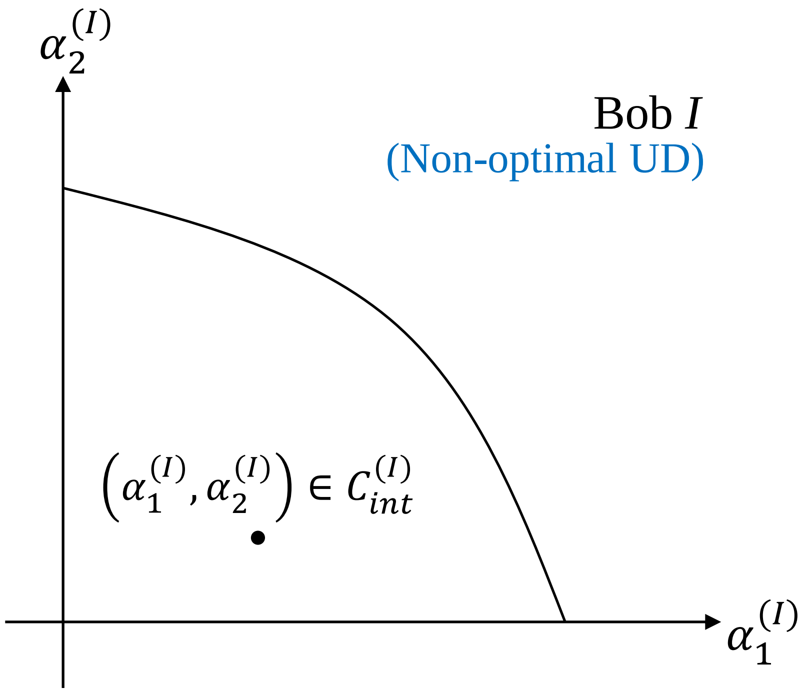
If Bob I performs non-optimal UD,
Bob $I+1$ can obtain partial information
from Bob I's post-measurement state.

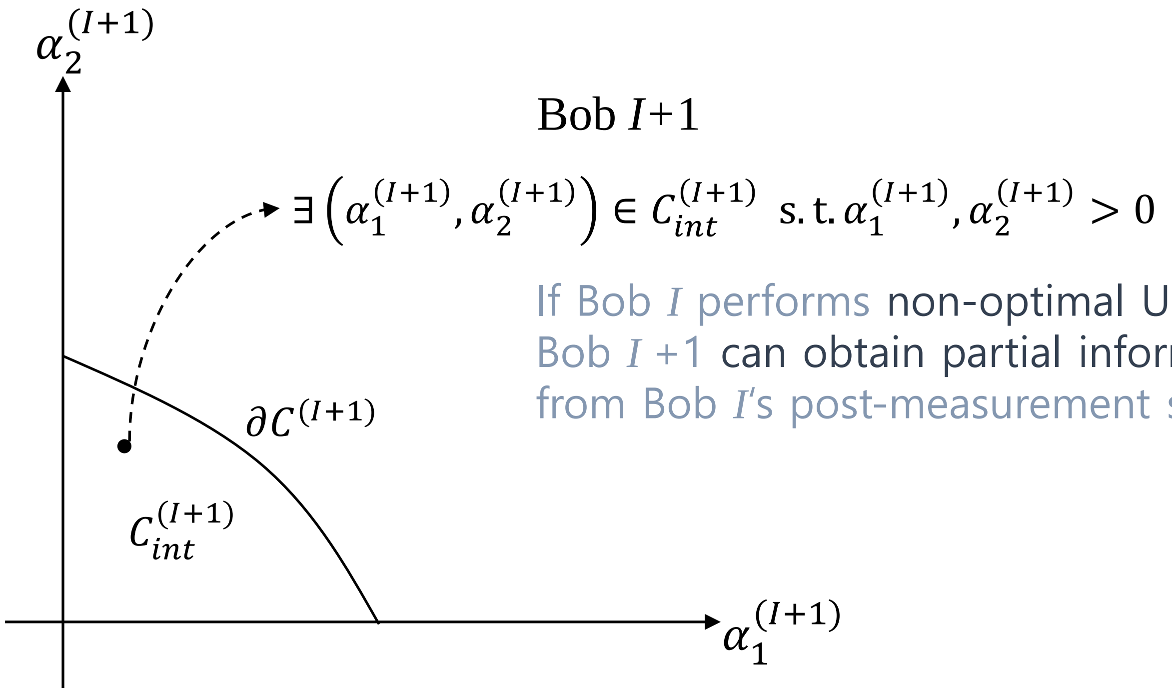
M. Namkung and Y. Kwon, Analysis of Sequential State Discrimination for Linearly Independent Pure Quantum States, Scientific Reports, **8**, 6515 (2018).

HYU 한양대학교 HANYANG UNIVERSITY

Constructing optimization problem

Property of Kraus operator



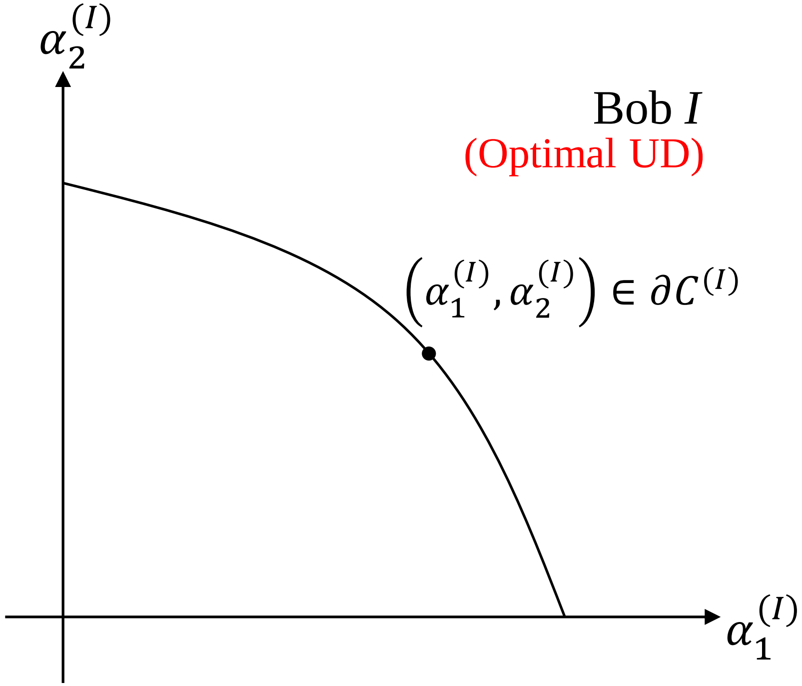


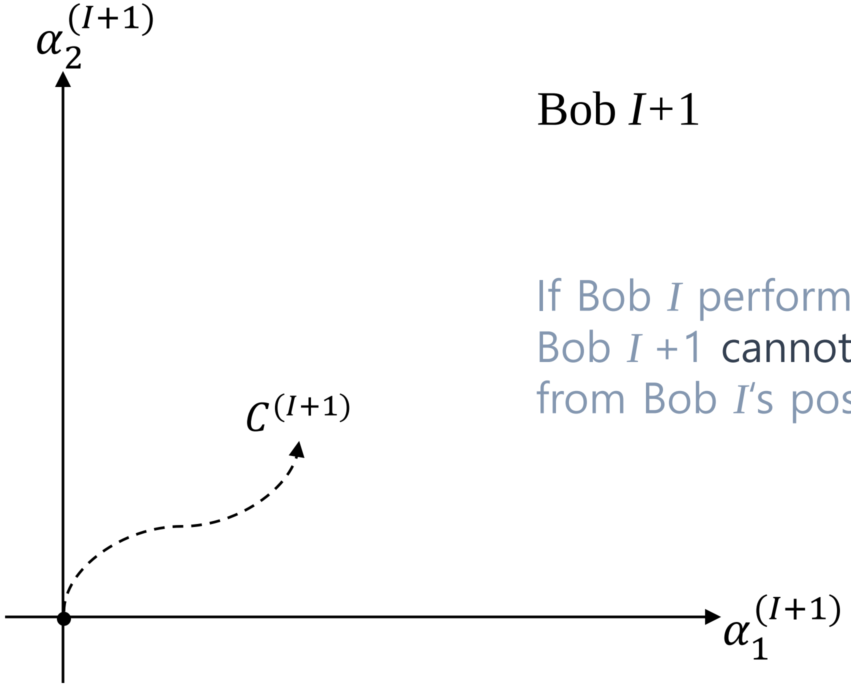
If Bob I performs non-optimal UD,
Bob $I+1$ can obtain partial information
from Bob I's post-measurement state.

M. Namkung and Y. Kwon, Analysis of Sequential State Discrimination for Linearly Independent Pure Quantum States, Scientific Reports, **8**, 6515 (2018).

Constructing optimization problem

Property of Kraus operator





Bob I+1

If Bob I performs optimal UD,
Bob I +1 cannot obtain partial information
from Bob I's post-measurement state.

M. Namkung and Y. Kwon, Analysis of Sequential State Discrimination for Linearly Independent Pure Quantum States, Scientific Reports, **8**, 6515 (2018).

Constructing optimization problem

Optimization problem (result)

$$\begin{aligned}
&\text{maximize} \quad P_s^{(B_1,\cdots,B_N)} = \sum_{i=1}^{n} q_i \alpha_i^{(1)} \alpha_i^{(2)} \alpha_i^{(3)} \times \cdots \times \alpha_i^{(N)} \\
&\text{subject to} \quad \left(\alpha_1^{(I)}, \cdots, \alpha_n^{(I)}\right) \in C_{int}^{(I)} \qquad \forall I \leq N-1 \\
&\qquad\qquad\quad\;\; \left(\alpha_1^{(I)}, \cdots, \alpha_n^{(I)}\right) \in \partial C^{(N)}
\end{aligned}$$

Remark: $\alpha_i^{(I)}$ is probability that Bob I obtains outcome i, given that Alice prepares $|\psi_i\rangle$.

Constructing optimization problem

Optimization problem (two pure states, three receivers)

maximize $P_S^{(B_1,B_2,B_3)} = q_1\alpha_1\beta_1\gamma_1 + q_2\alpha_2\beta_2\gamma_2$

subject to $(1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2$

$$(1-\beta_1)(1-\beta_2) > \left|\left\langle\phi_1^{(B_1)}\middle|\phi_2^{(B_1)}\right\rangle\right|^2$$

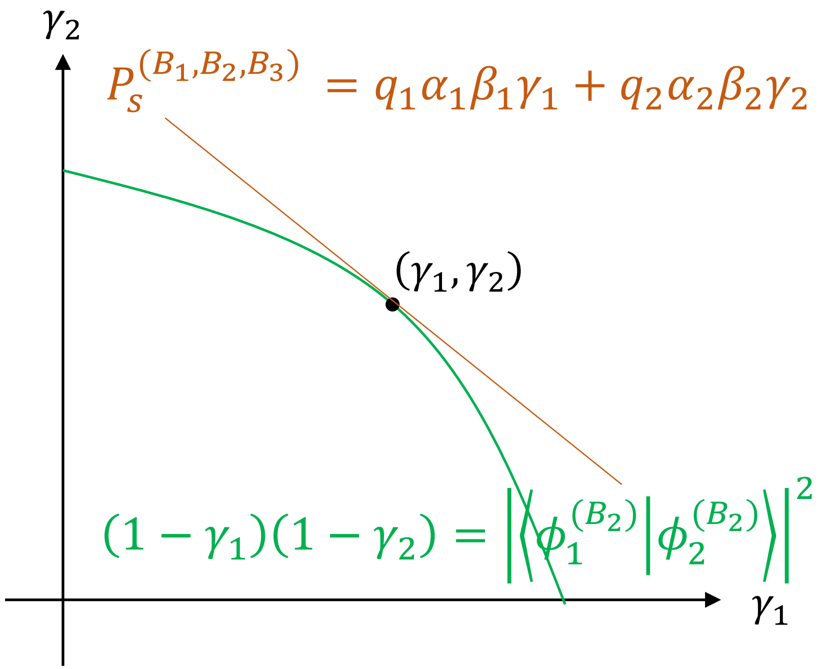
$$(1-\gamma_1)(1-\gamma_2) = \left|\left\langle\phi_1^{(B_2)}\middle|\phi_2^{(B_2)}\right\rangle\right|^2$$

Constructing optimization problem

Optimization problem (two pure states, three receivers)

maximize $P_s^{(B_1,B_2,B_3)} = q_1\alpha_1\beta_1\gamma_1 + q_2\alpha_2\beta_2\gamma_2$

subject to
$$(1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2$$
$$(1-\beta_1)(1-\beta_2) > \left|\left\langle\phi_1^{(B_1)}\middle|\phi_2^{(B_1)}\right\rangle\right|^2$$
$$(1-\gamma_1)(1-\gamma_2) = \left|\left\langle\phi_1^{(B_2)}\middle|\phi_2^{(B_2)}\right\rangle\right|^2$$



Remark: (γ_1,γ_2) is obtained by finding a tangential point between a plane $P_s^{(B_1,B_2,B_3)} = q_1\alpha_1\beta_1\gamma_1 + q_2\alpha_2\beta_2\gamma_2$ and a surface $(1-\gamma_1)(1-\gamma_2) = \left|\left\langle\phi_1^{(B_1)}\middle|\phi_2^{(B_2)}\right\rangle\right|^2$.

Constructing optimization problem

Optimization problem (two pure states, three receivers)

$$\text{maximize} \quad P_s^{(B_1,B_2,B_3)} = q_1\alpha_1\beta_1 + q_2\alpha_2\beta_2 - 2|\langle\psi_1|\psi_2\rangle|\sqrt{\frac{q_1 q_2 \alpha_1\alpha_2\beta_1\beta_2}{(1-\alpha_1)(1-\alpha_2)(1-\beta_1)(1-\beta_2)}}$$

$$\text{subject to} \quad (1-\alpha_1)(1-\alpha_2) > |\langle\psi_1|\psi_2\rangle|^2$$

$$\beta_2 \le \frac{\beta_1(1-\beta_1)}{\beta_1(1-\beta_1)+X(\alpha_1,\alpha_2)}, \quad X(\alpha_1,\alpha_2) = \frac{q_2\alpha_2}{q_1\alpha_1}\frac{|\langle\psi_1|\psi_2\rangle|^2}{(1-\alpha_1)(1-\alpha_2)}$$

$$\beta_1 \le \frac{\beta_2(1-\beta_2)}{\beta_2(1-\beta_2)+Y(\alpha_1,\alpha_2)}, \quad Y(\alpha_1,\alpha_2) = \frac{q_1\alpha_1}{q_2\alpha_2}\frac{|\langle\psi_1|\psi_2\rangle|^2}{(1-\alpha_1)(1-\alpha_2)}$$

Remark: In general, this optimization problem can be solved by using nonlinear programming, including random search method, sequential linear programming, and penalty function method.

S. S. Rao, *Engineering optimization: theory and practice* (Wiley, 2009).

Constructing optimization problem

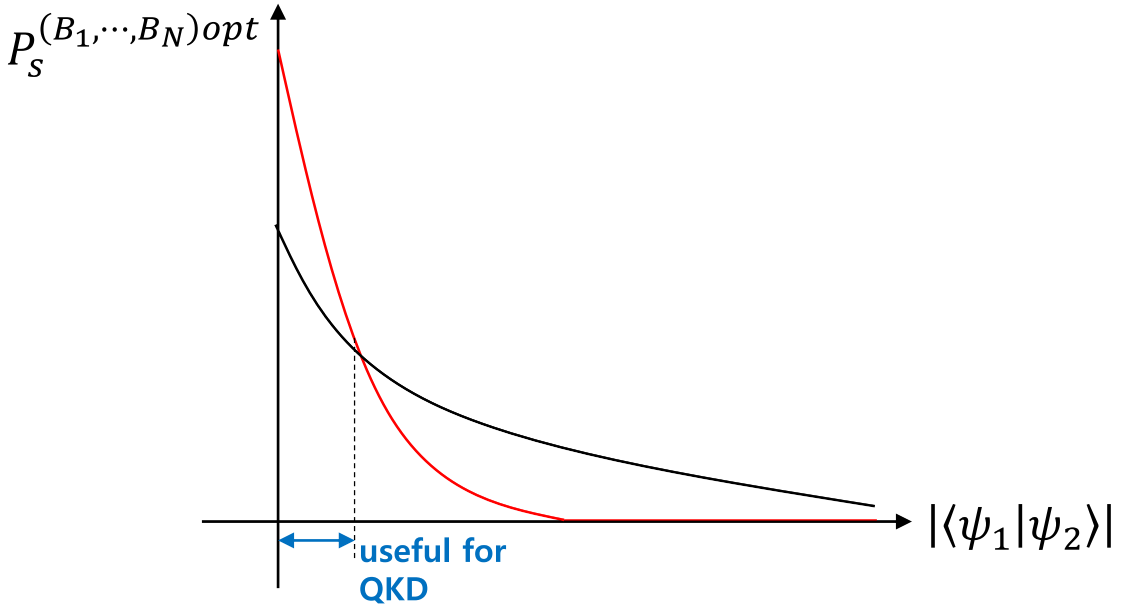
Optimal success probability (two pure states with equal prior probabilities, N receivers)

Discriminating two states: $P_S^{(B_1,\cdots,B_N)opt} = \left(1 - |\langle\psi_1|\psi_2\rangle|^{1/N}\right)^N$ $\quad |\langle\psi_1|\psi_2\rangle| < \left(2^{1/N} - 1\right)^N$

Discriminating one out of two states: $P_S^{(B_1,\cdots,B_N)opt} = \frac{1}{2}\left(1 - |\langle\psi_1|\psi_2\rangle|^{2/N}\right)^N$ $\quad |\langle\psi_1|\psi_2\rangle| \geq \left(2^{1/N} - 1\right)^N$

Remark 1: Optimal success probability satisfies the result of [J. A. Bergou *et al.*], and [C.-Q. Pang *et al*].

Remark 2: Sequential state discrimination of two pure states is suitable for multiparty QKD, when the number of receivers is not too many.



J. A. Bergou et al., Extracting information from a qubit by multiple observers: Towards a theory of sequential state discrimination, Phys. Rev. Lett. 111, 100503 (2013).
C.-Q. Pang et al., Sequential state discrimination and requirement of quantum dissonance, Phys. Rev. A **88**, 052331 (2013).

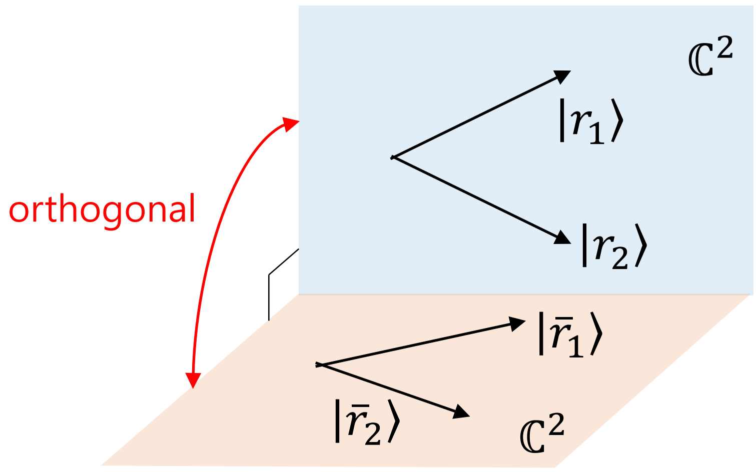
HYU 한양대학교 HANYANG UNIVERSITY

Constructing optimization problem

Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of POVM)



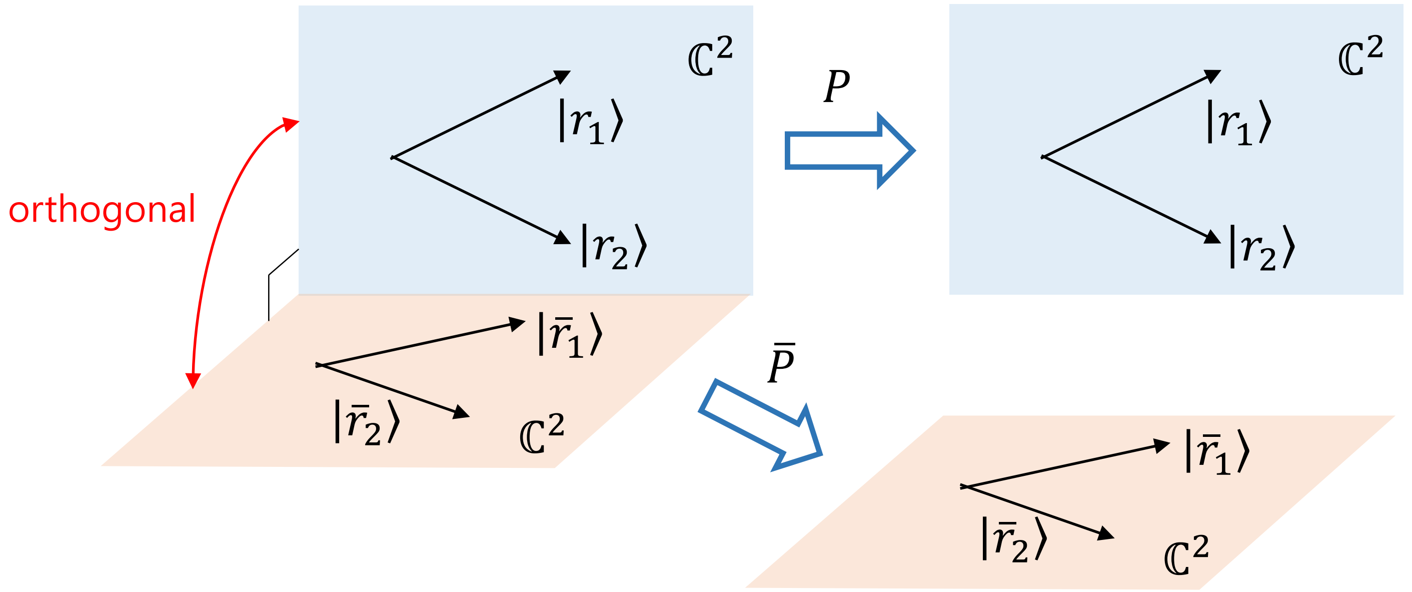
U. Herzog, Optimum unambiguous discrimination of two mixed states and application to a class of similar states, Phys. Rev. A **75**, 052309 (2007).

Constructing optimization problem

Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of POVM)



U. Herzog, Optimum unambiguous discrimination of two mixed states and application to a class of similar states, Phys. Rev. A **75**, 052309 (2007).

HYU 한양대학교 HANYANG UNIVERSITY

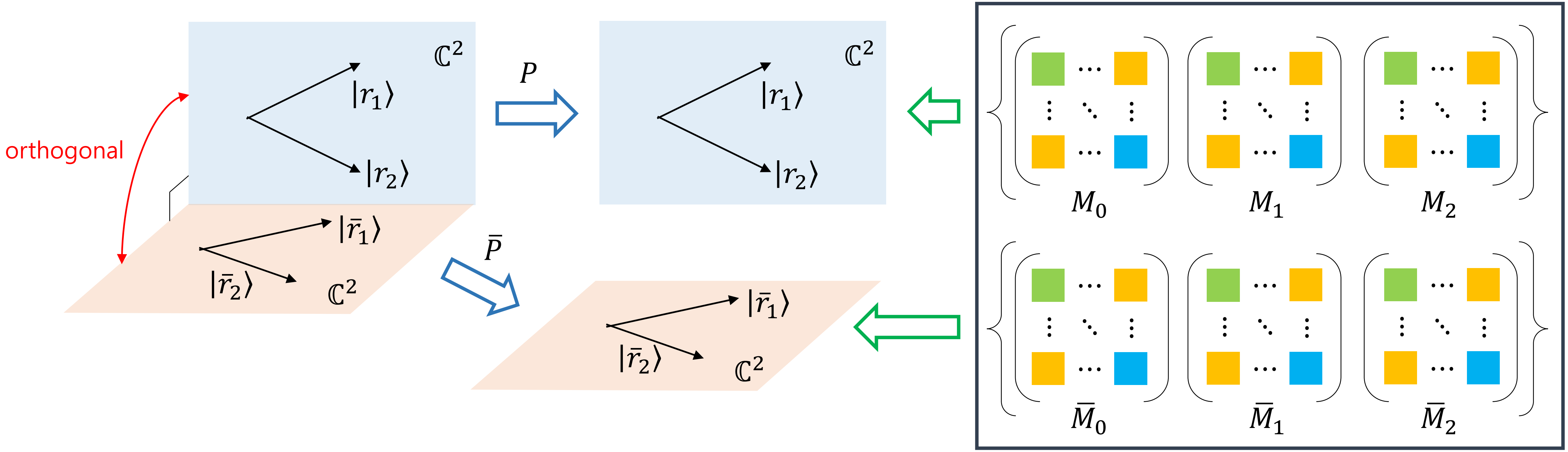
Constructing optimization problem

Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of POVM)

$\{M_i \oplus \bar{M}_j\}_{i,j=0}^{2}$

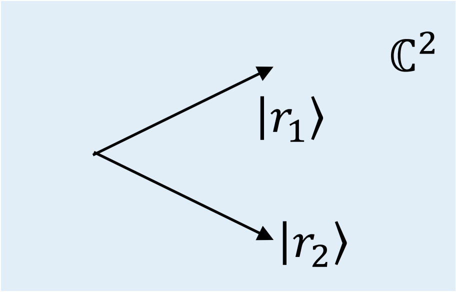


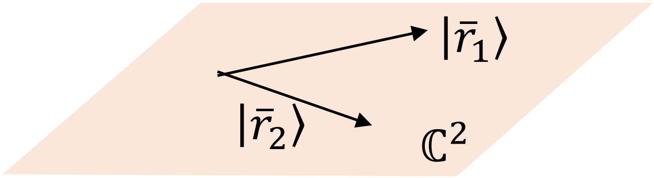
U. Herzog, Optimum unambiguous discrimination of two mixed states and application to a class of similar states, Phys. Rev. A **75**, 052309 (2007).

Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of Kraus operator)





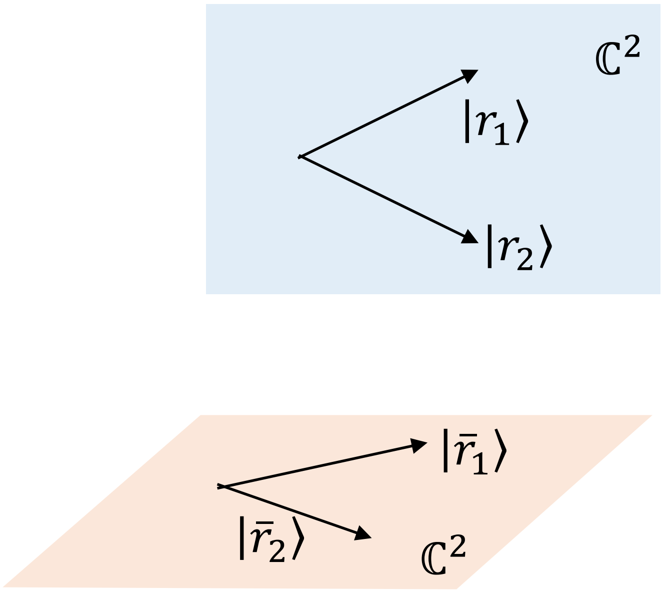
M. Namkung and Y. Kwon, Optimal sequential state discrimination between two mixed quantum states, Phys. Rev. A **96**, 022318 (2017).

Constructing optimization problem

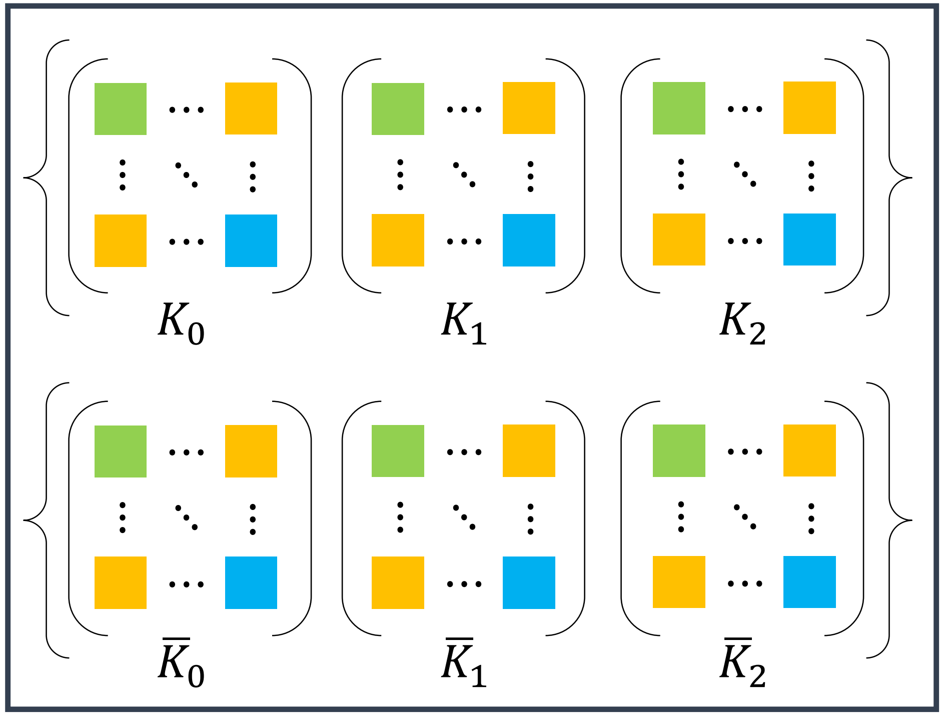
Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of Kraus operator)



$\{K_i \oplus \bar{K}_j\}_{i,j=0}^{2}$



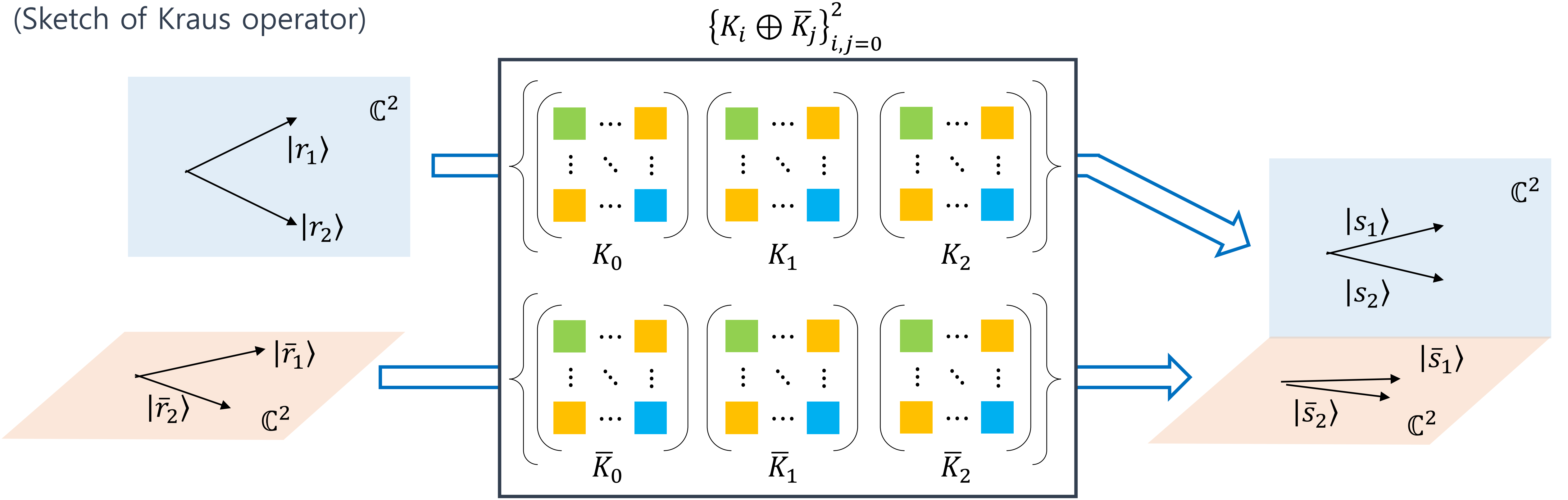
M. Namkung and Y. Kwon, Optimal sequential state discrimination between two mixed quantum states, Phys. Rev. A **96**, 022318 (2017).

Constructing optimization problem

Extending problem to mixed states case

$$\rho_1 = r_1|r_1\rangle\langle r_1| + \bar{r}_1|\bar{r}_1\rangle\langle\bar{r}_1|$$
$$\rho_2 = r_2|r_2\rangle\langle r_2| + \bar{r}_2|\bar{r}_2\rangle\langle\bar{r}_2|$$

(Sketch of Kraus operator)



M. Namkung and Y. Kwon, Optimal sequential state discrimination between two mixed quantum states, Phys. Rev. A **96**, 022318 (2017).

HYU 한양대학교 HANYANG UNIVERSITY

Extending problem to mixed states case (result)

$$\text{maximize} \quad P_S^{(B_1,\cdots,B_N)} = q_1\left(r_1\prod_{l=1}^{N}\alpha_1^{(l)} + r_1\prod_{l=1}^{N}\bar{\alpha}_1^{(l)}\right) + q_2\left(r_2\prod_{l=1}^{N}\alpha_2^{(l)} + r_2\prod_{l=1}^{N}\bar{\alpha}_2^{(l)}\right)$$

$$\text{subject to} \quad \left(1-\alpha_1^{(1)}\right)\left(1-\alpha_2^{(1)}\right) > |\langle r_1|r_2\rangle|^2 \qquad \left(1-\bar{\alpha}_1^{(1)}\right)\left(1-\bar{\alpha}_2^{(1)}\right) > |\langle \bar{r}_1|\bar{r}_2\rangle|^2$$

$$\left(1-\alpha_1^{(I)}\right)\left(1-\alpha_2^{(I)}\right) > \left|\left\langle s_1^{(I-1)}\middle|s_2^{(I-1)}\right\rangle\right|^2 \qquad \left(1-\bar{\alpha}_1^{(I)}\right)\left(1-\bar{\alpha}_2^{(I)}\right) > \left|\left\langle \bar{s}_1^{(I-1)}\middle|\bar{s}_2^{(I-1)}\right\rangle\right|^2$$

$$\left(1-\alpha_1^{(N)}\right)\left(1-\alpha_2^{(N)}\right) = \left|\left\langle s_1^{(N-1)}\middle|s_2^{(N-1)}\right\rangle\right|^2 \qquad \left(1-\bar{\alpha}_1^{(N)}\right)\left(1-\bar{\alpha}_2^{(N)}\right) = \left|\left\langle \bar{s}_1^{(N-1)}\middle|\bar{s}_2^{(N-1)}\right\rangle\right|^2$$

M. Namkung and Y. Kwon, Optimal sequential state discrimination between two mixed quantum states, Phys. Rev. A **96**, 022318 (2017).

Constructing optimization problem

Extending problem to mixed states case (result)

maximize $p_s^{(B_1,\cdots,B_N)} = q_1 r_1 \prod_{l=1}^{N} \alpha_1^{(l)} + q_2 r_2 \prod_{l=1}^{N} \alpha_2^{(l)}$

subject to
$$\left(1-\alpha_1^{(1)}\right)\left(1-\alpha_2^{(1)}\right) > |\langle r_1|r_2\rangle|^2$$
$$\left(1-\alpha_1^{(I)}\right)\left(1-\alpha_2^{(I)}\right) > \left|\left\langle s_1^{(I-1)}\middle|s_2^{(I-1)}\right\rangle\right|^2$$
$$\left(1-\alpha_1^{(N)}\right)\left(1-\alpha_2^{(N)}\right) = \left|\left\langle s_1^{(N-1)}\middle|s_2^{(N-1)}\right\rangle\right|^2$$

sub-optimization problem 1

maximize $\bar{p}_s^{(B_1,\cdots,B_N)} = q_1 \bar{r}_1 \prod_{l=1}^{N} \bar{\alpha}_1^{(l)} + q_2 \bar{r}_2 \prod_{l=1}^{N} \bar{\alpha}_2^{(l)}$

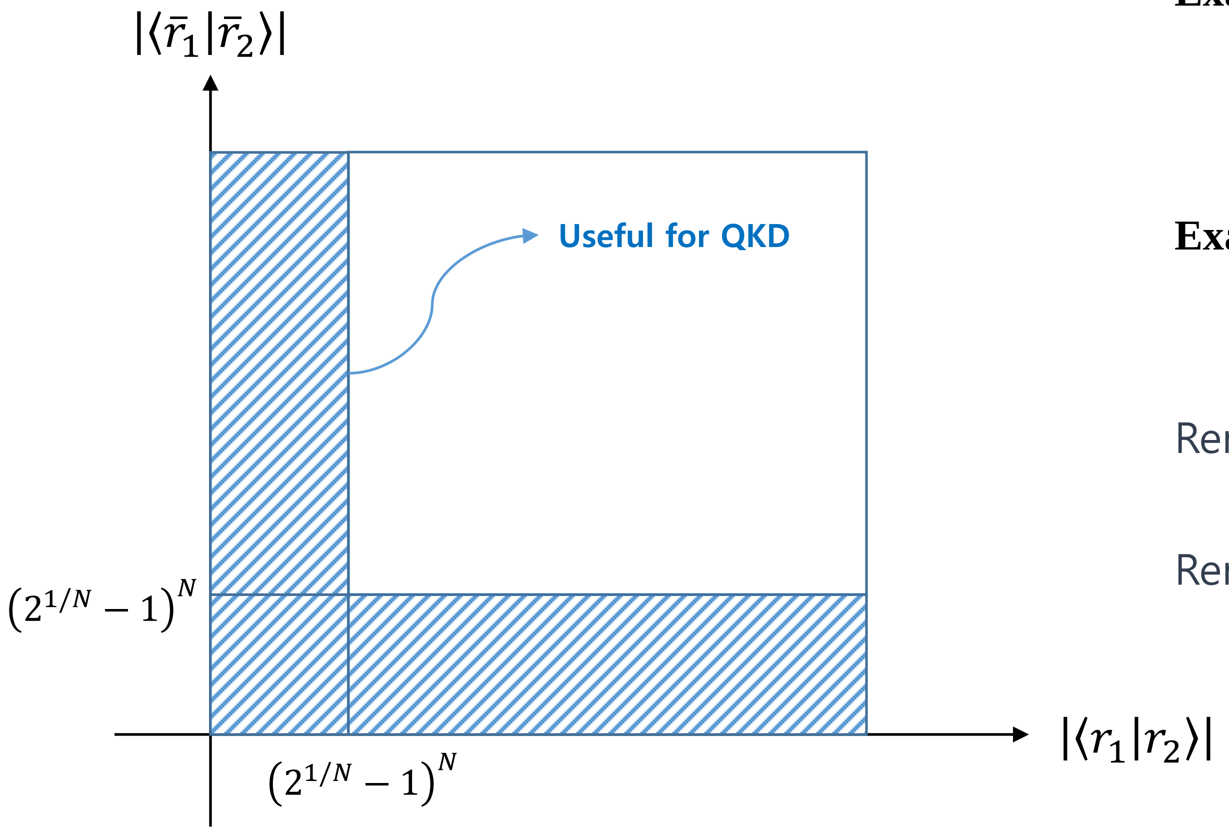
subject to
$$\left(1-\bar{\alpha}_1^{(1)}\right)\left(1-\bar{\alpha}_2^{(1)}\right) > |\langle \bar{r}_1|\bar{r}_2\rangle|^2$$
$$\left(1-\bar{\alpha}_1^{(I)}\right)\left(1-\bar{\alpha}_2^{(I)}\right) > \left|\left\langle \bar{s}_1^{(I-1)}\middle|\bar{s}_2^{(I-1)}\right\rangle\right|^2$$
$$\left(1-\bar{\alpha}_1^{(N)}\right)\left(1-\bar{\alpha}_2^{(N)}\right) = \left|\left\langle \bar{s}_1^{(N-1)}\middle|\bar{s}_2^{(N-1)}\right\rangle\right|^2$$

sub-optimization problem 2

M. Namkung and Y. Kwon, Optimal sequential state discrimination between two mixed quantum states, Phys. Rev. A **96**, 022318 (2017).

Constructing optimization problem

Extending problem to mixed states case (in case of $q_1 = q_2,\ r_1 = r_2 = r,\ \bar{r}_1 = \bar{r}_2 = \bar{r}$)



Example 1. $r = 0.6, \bar{r} = 0.4, s = 0.7, \bar{s} = 0.0001, N = 3$

$$P_s^{(B_1,\cdots,B_N)opt} = 0.294443356418367$$

Example 2. $r = 0.6, \bar{r} = 0.4, s = 0.7, \bar{s} = 0.0001, N = 4$

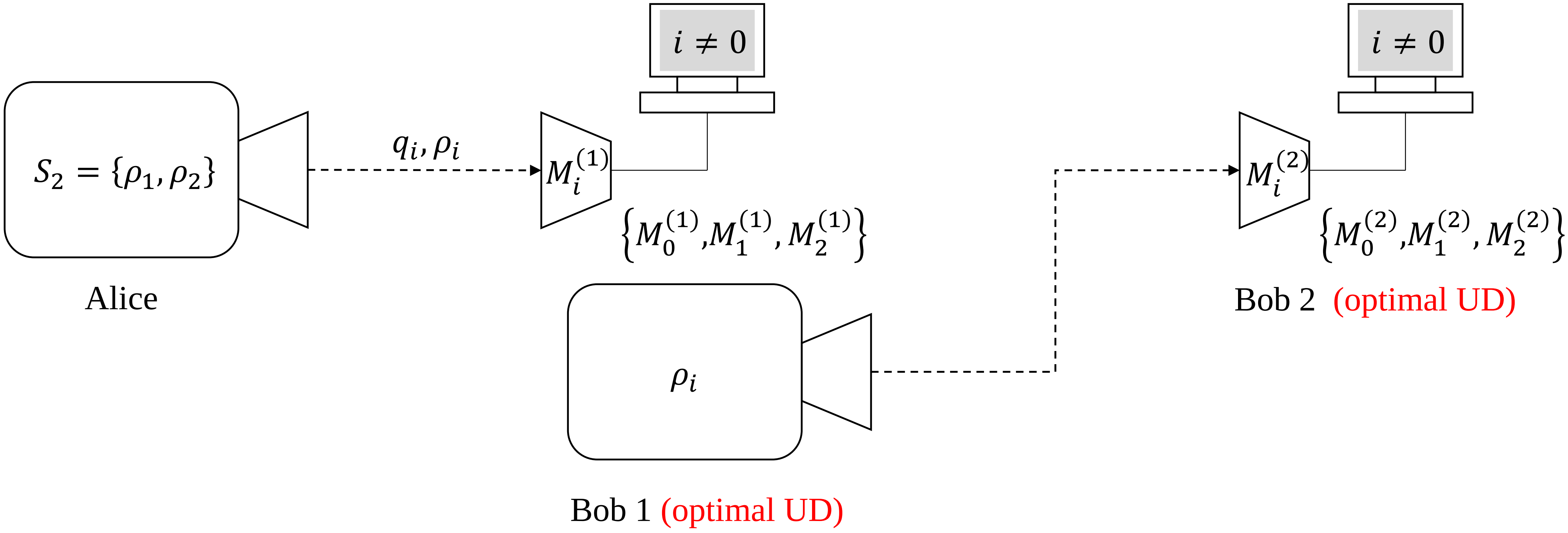
$$P_s^{(B_1,\cdots,B_N)opt} = 0.182986042905254$$

Remark 1: Sequential state discrimination of two mixed states can be performed with large success probability.

Remark 2: Sequential state discrimination can applied to multiparty QKD, even if the number of receivers is too many.

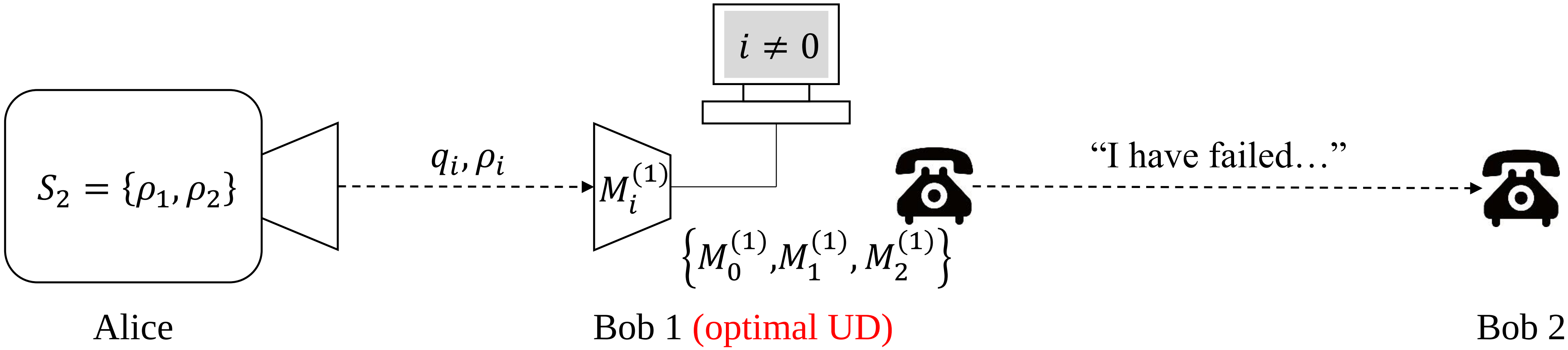
Comparison with other scenarios

Quantum reproducing



Comparison with other scenarios

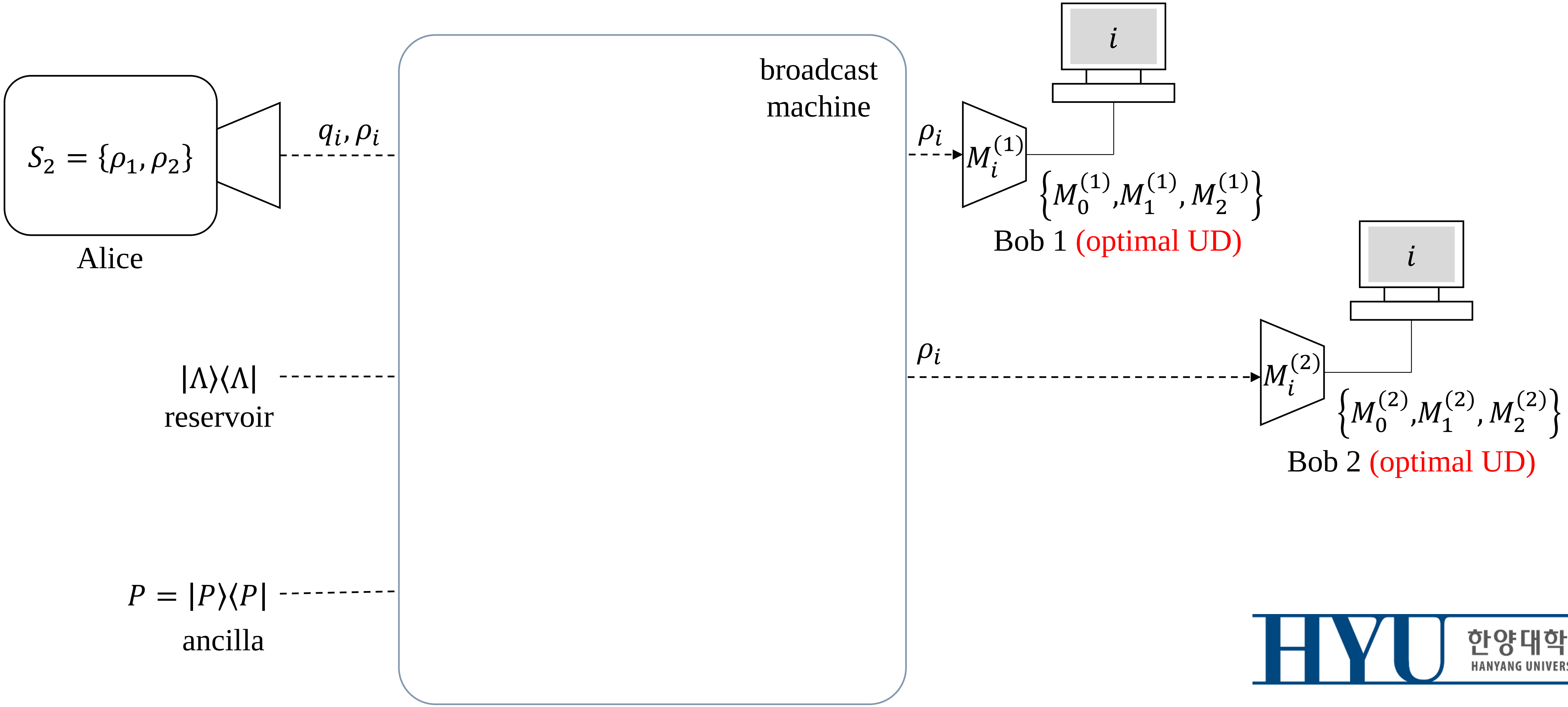
Quantum reproducing



Comparison with other scenarios

Probabilistic Quantum Broadcasting

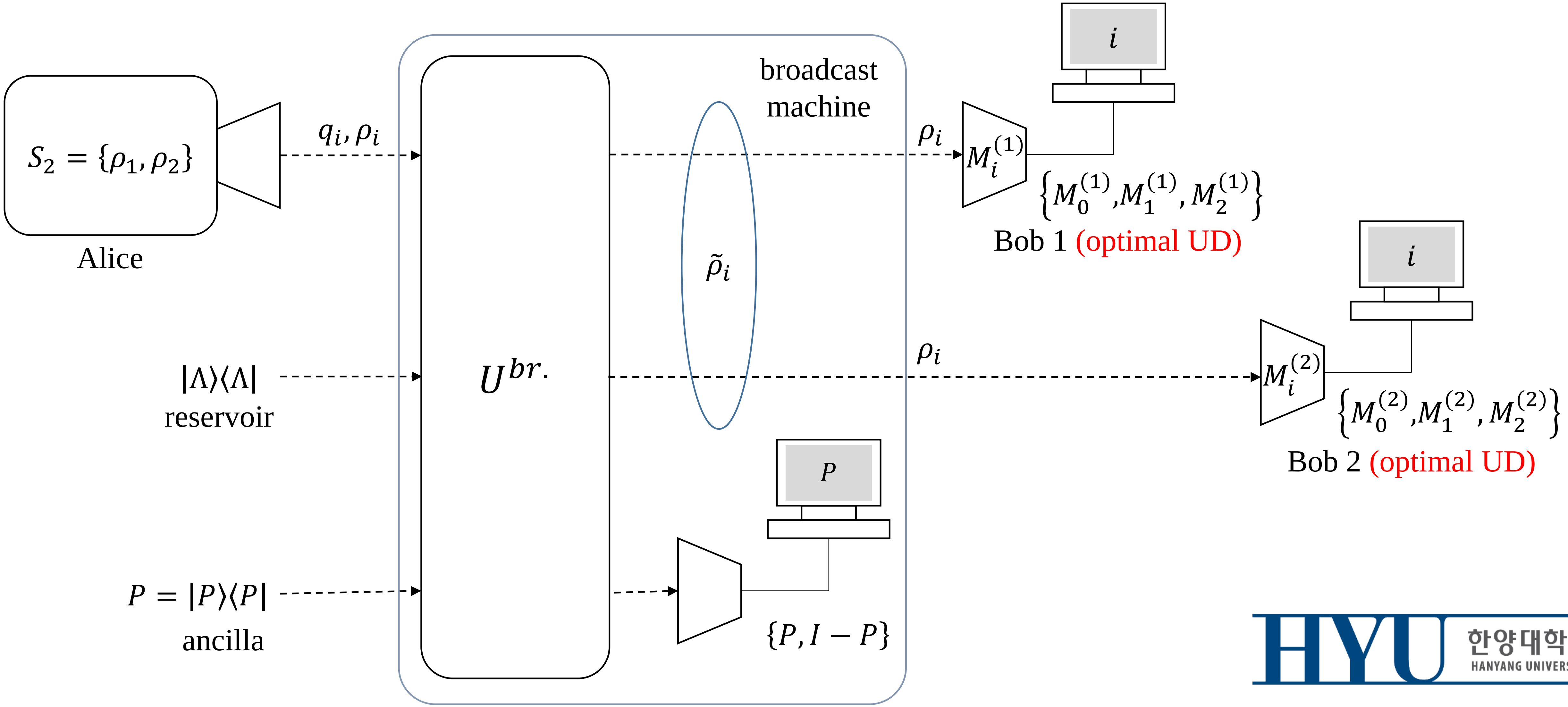
L. Li et al., Probabilistic broadcasting of mixed states, J. Phys. A: Math. Theor. 42, 175302 (2009).



Comparison with other scenarios

Probabilistic Quantum Broadcasting

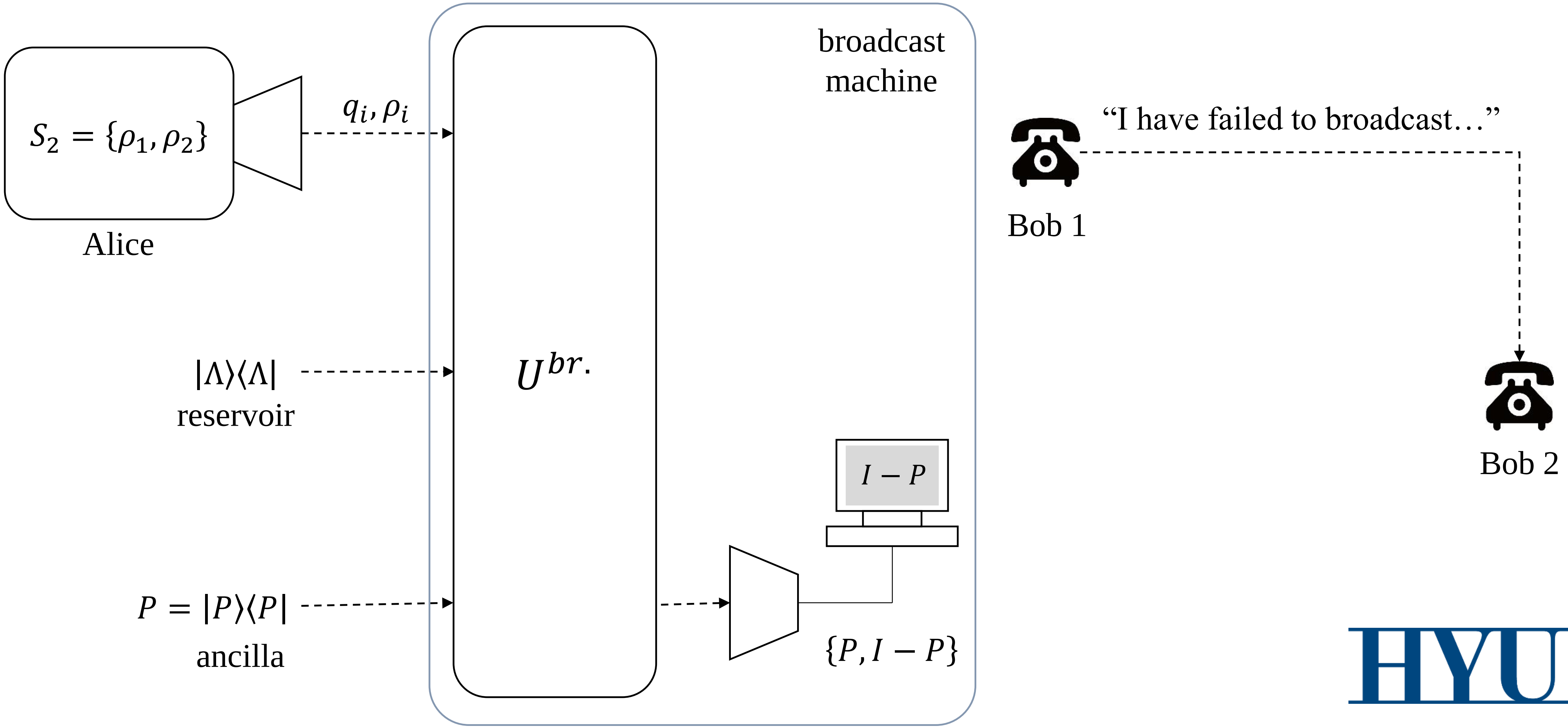
L. Li et al., Probabilistic broadcasting of mixed states, J. Phys. A: Math. Theor. 42, 175302 (2009).



Comparison with other scenarios

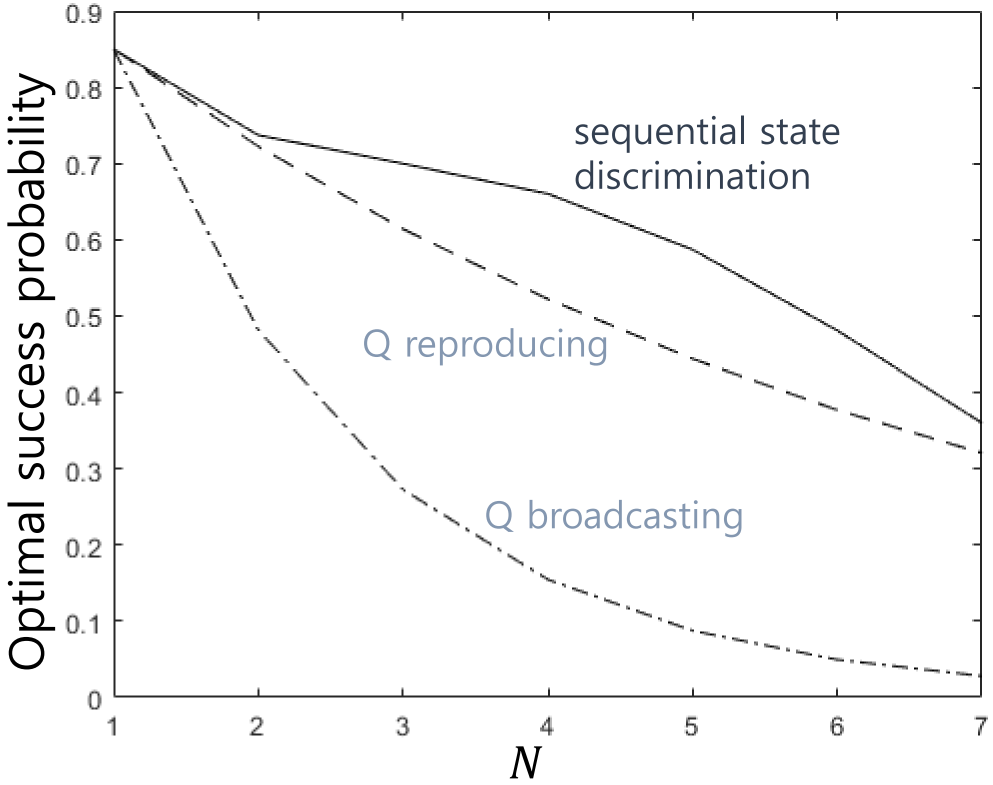
Probabilistic Quantum Broadcasting

L. Li et al., Probabilistic broadcasting of mixed states, J. Phys. A: Math. Theor. 42, 175302 (2009).



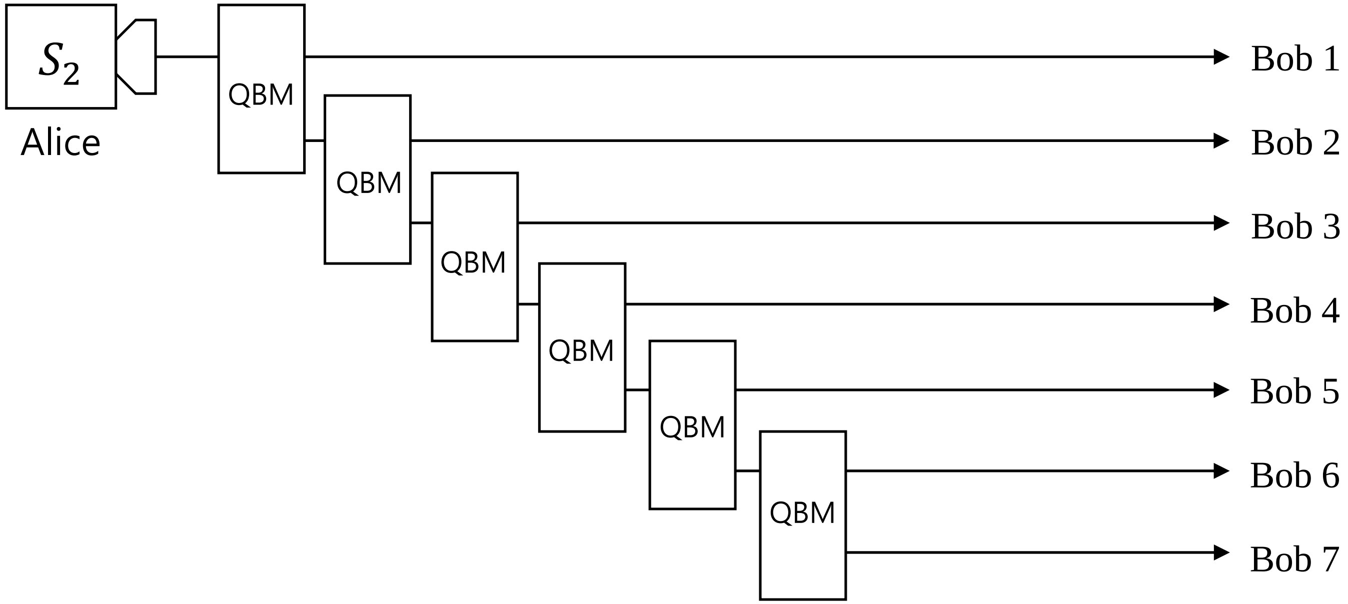
Comparison with other scenarios

Optimal success probabilities



Example. $r = 0.3,\ \bar{r} = 0.7,\ s = 0.5,\ \bar{s} = 5 \times 10^{-8},\ N \in \{1, \cdots, 7\}$

(probabilistic quantum broadcasting)

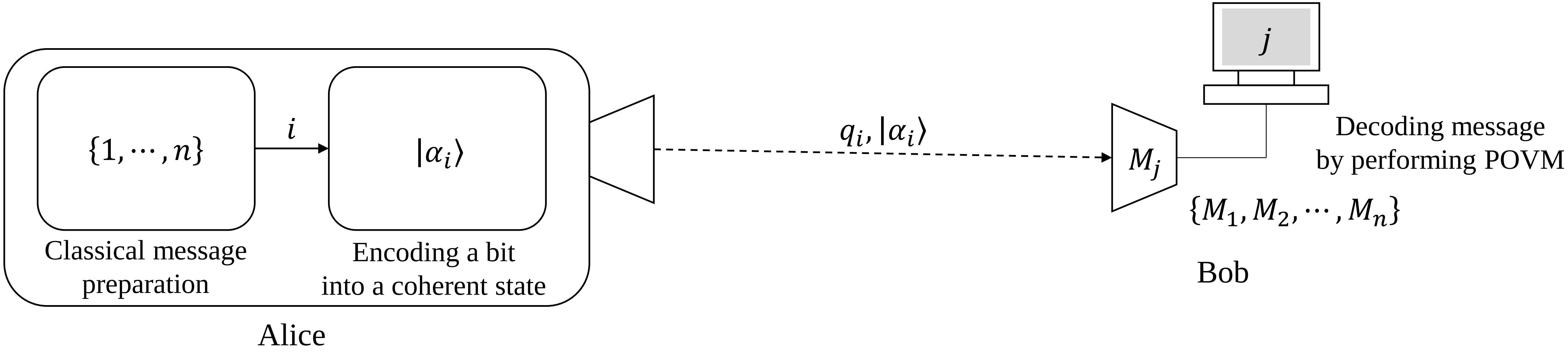


Remark : Sequential state discrimination outperform quantum reproducing and quantum broadcasting strategies.

Part II

Application

Realistic QKD based on coherent states



Realistic quantum key distribution

Realistic quantum key distribution can be expressed as *quantum state discrimination of coherent states*. For example, B92 protocol can be expressed as *unambiguous discrimination of coherent states*.

G. Cariolaro, *Quantum Communications* (Springer, 2015).

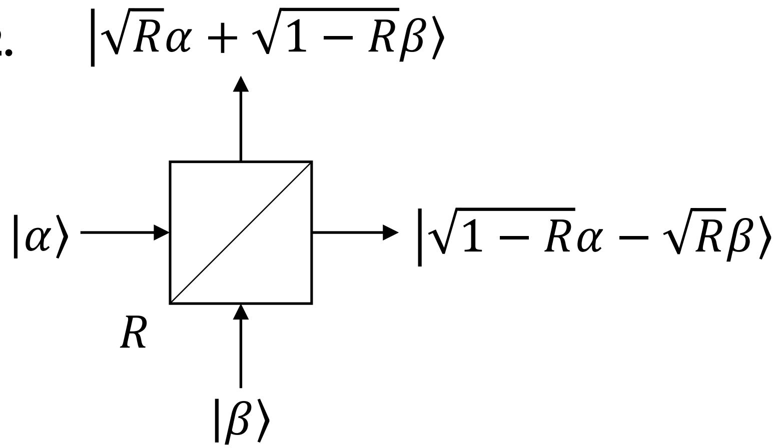
Introduction: coherent state and operations

Definition. [R. J. Glauber]

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \ , \qquad n : \text{number of photons}$$

Lemma 1. $\hat{D}(\gamma)|\alpha\rangle = e^{\gamma \hat{a} - \gamma^* \hat{a}^\dagger}|\alpha\rangle \simeq |\alpha + \gamma\rangle$

Lemma 2.



R. J. Glauber, Coherent and Incoherent States of the Radiation Field, Phys. Rev. **131**, 2766 (1963).

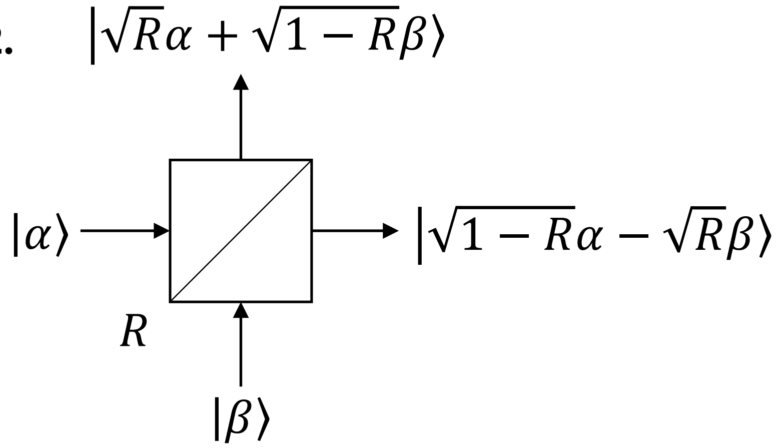
Introduction: coherent state and operations

Definition. [R. J. Glauber]

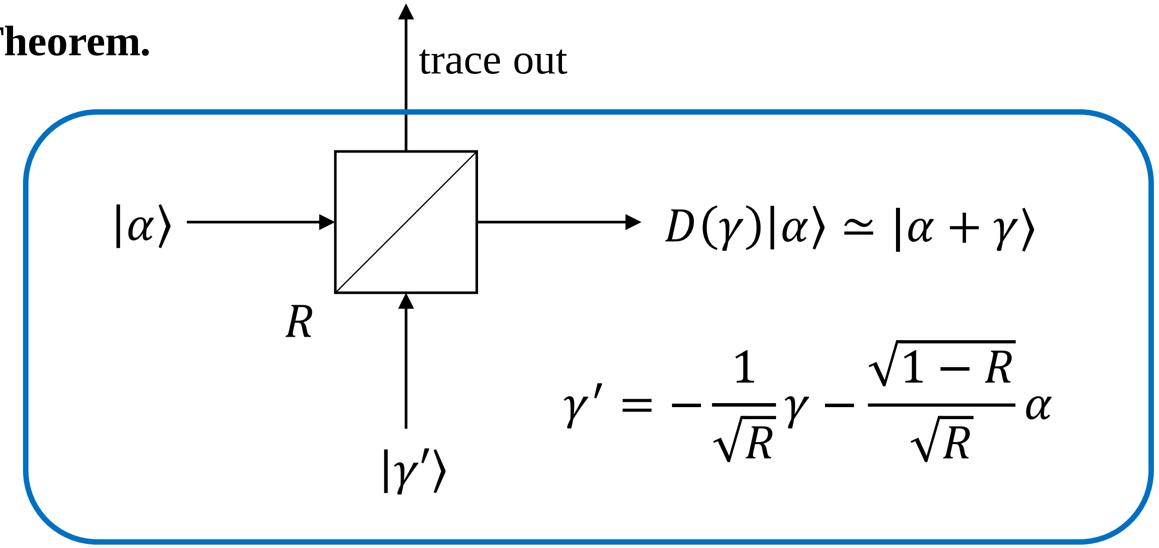
$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle\ ,\qquad n : \text{number of photons}$$

Lemma 1. $\hat{D}(\gamma)|\alpha\rangle = e^{\gamma\hat{a}-\gamma^*\hat{a}^\dagger}|\alpha\rangle \simeq |\alpha+\gamma\rangle$

Lemma 2.



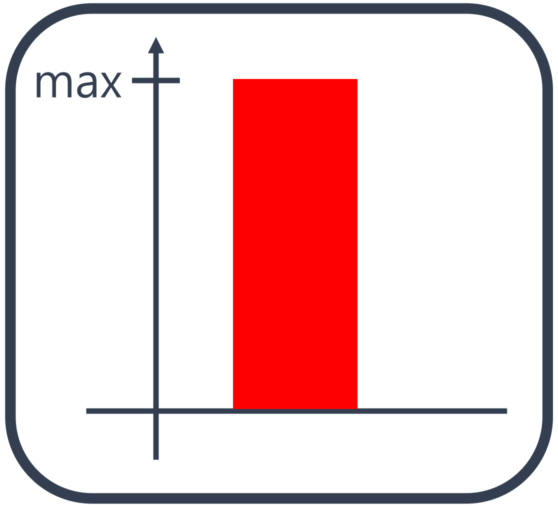
Theorem.



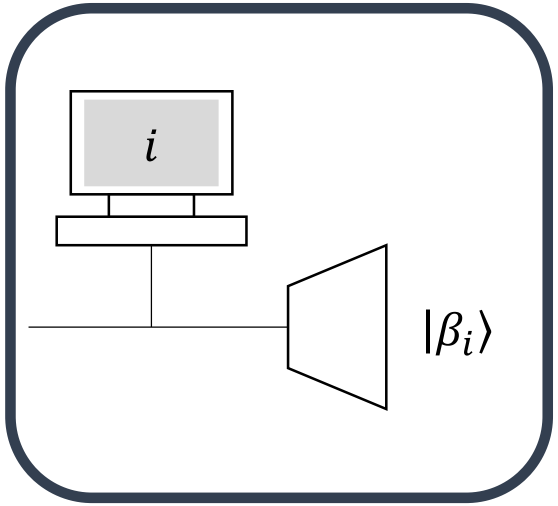
R. J. Glauber, Coherent and Incoherent States of the Radiation Field, Phys. Rev. **131**, 2766 (1963).

Implementing sequential state discrimination

Requirement for implementing sequential state discrimination



- Optical design should implement optimal unambiguous discrimination

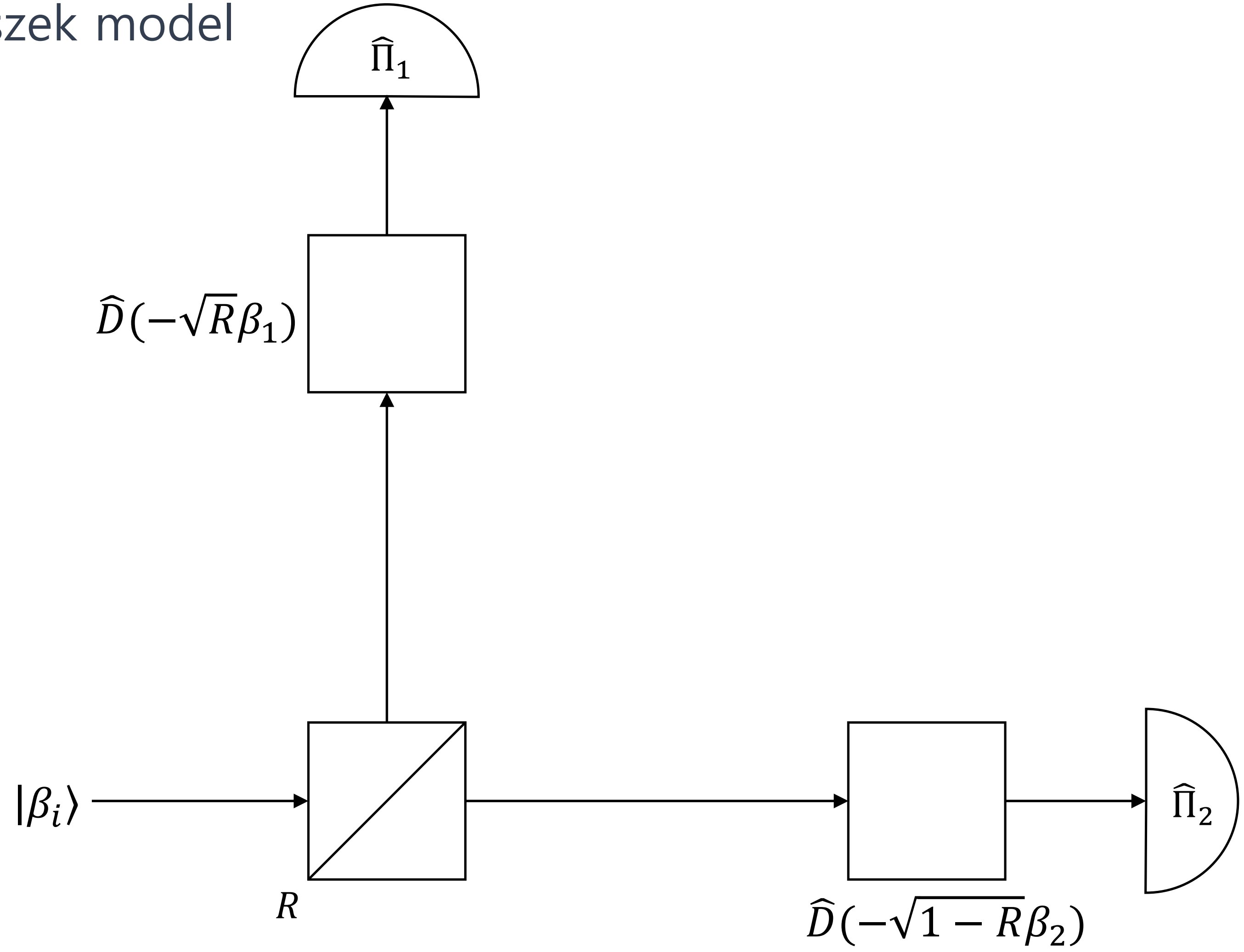


- Optical design should produce non-orthogonal post-measurement states

M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

Implementing sequential state discrimination

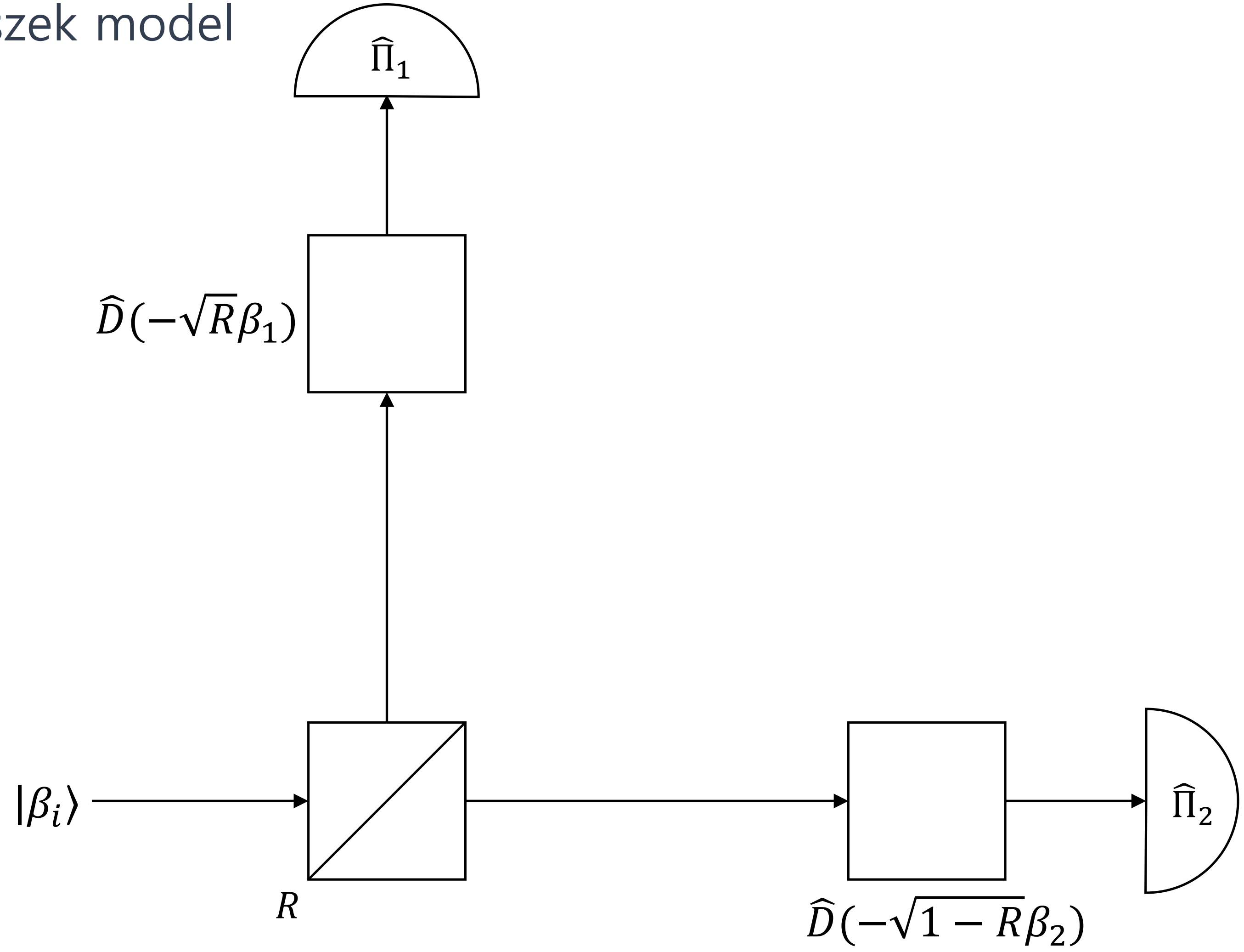
Banaszek model



K. Banaszek, Optimal receiver for quantum cryptography with two coherent states, Phys. Lett. A **253**, 12 (1999).

Implementing sequential state discrimination

Banaszek model



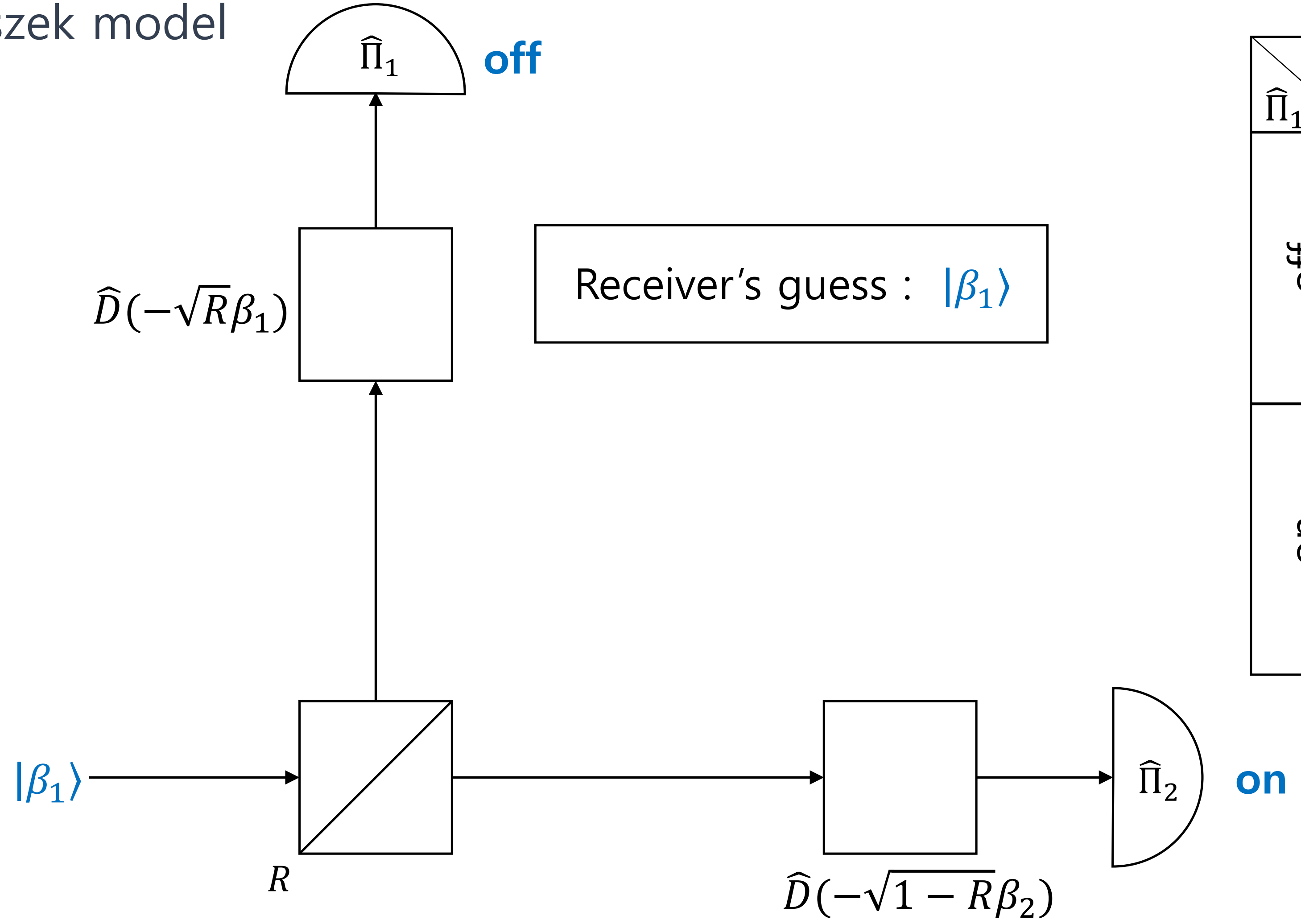
$\hat{\Pi}_1$ \ $\hat{\Pi}_2$	off	on
off	inconclusive	correct
on	error (forbidden)	(forbidden)

K. Banaszek, Optimal receiver for quantum cryptography with two coherent states, Phys. Lett. A **253**, 12 (1999).

HYU 한양대학교 HANYANG UNIVERSITY

Implementing sequential state discrimination

Banaszek model



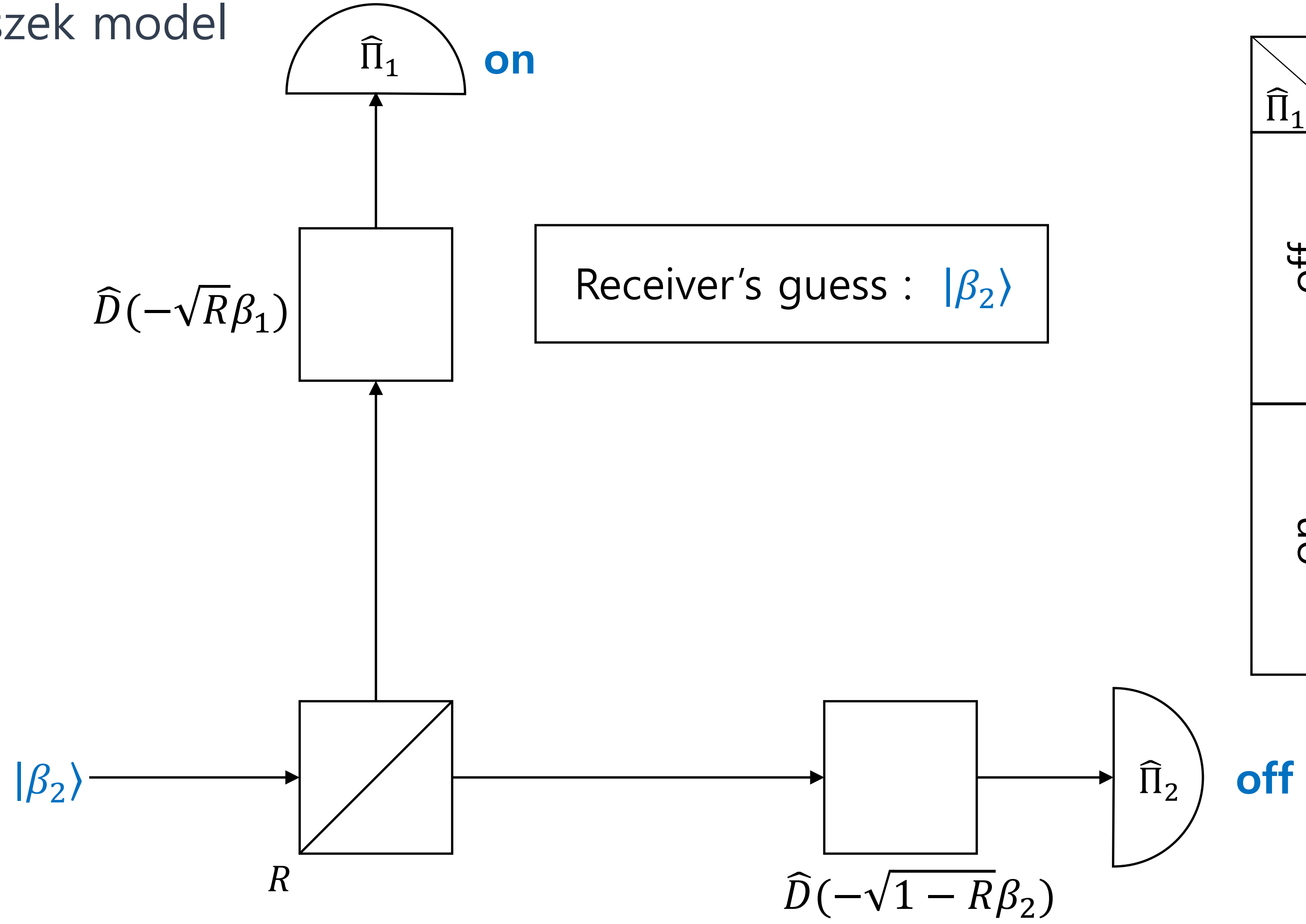
$\hat{\Pi}_1$ \ $\hat{\Pi}_2$	off	on
off	inconclusive	**correct**
on	error (forbidden)	(forbidden)

K. Banaszek, Optimal receiver for quantum cryptography with two coherent states, Phys. Lett. A **253**, 12 (1999).

HYU 한양대학교 HANYANG UNIVERSITY

Implementing sequential state discrimination

Banaszek model

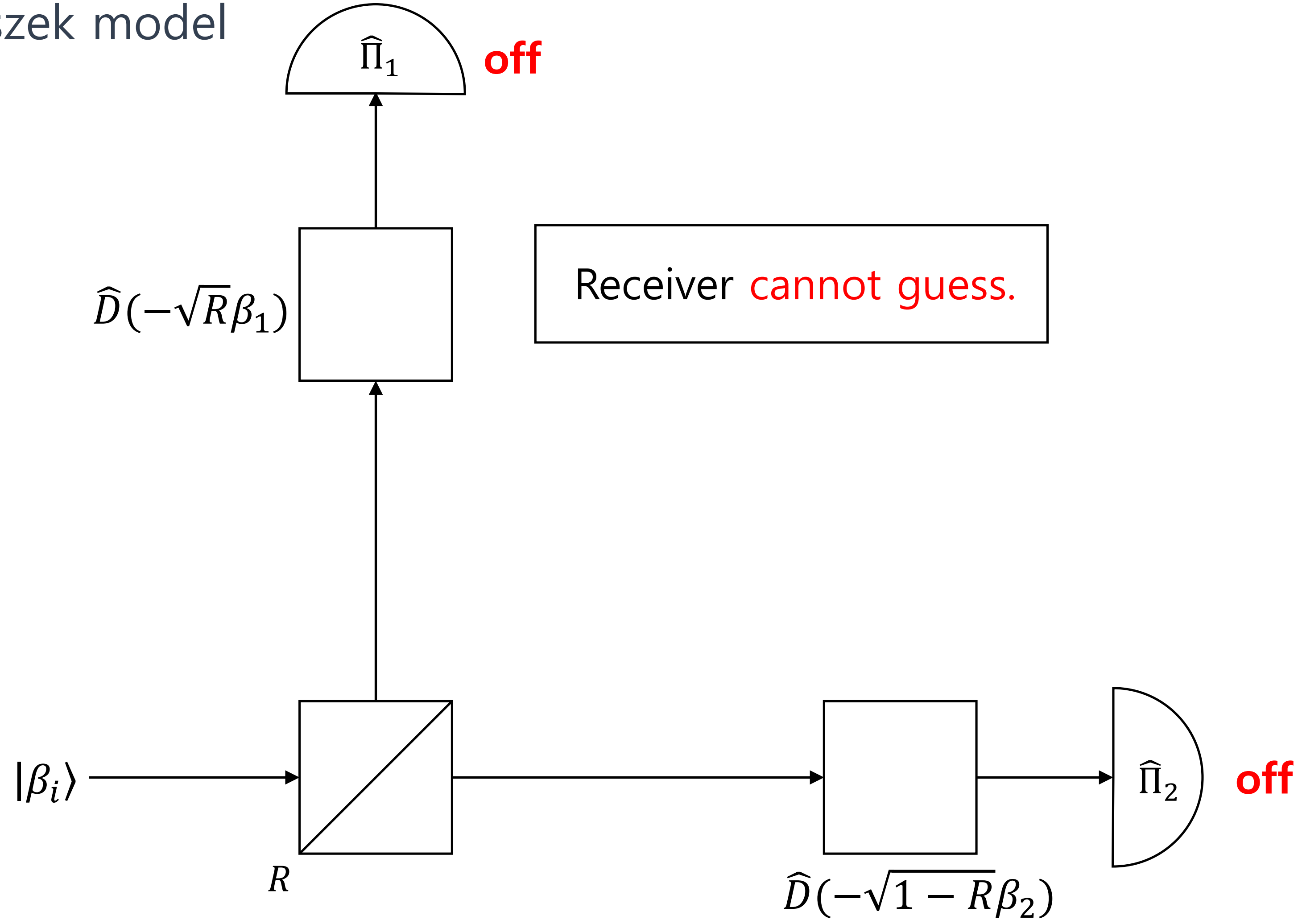


$\hat{\Pi}_1$ \ $\hat{\Pi}_2$	off	on
off	inconclusive	error (forbidden)
on	**correct**	(forbidden)

K. Banaszek, Optimal receiver for quantum cryptography with two coherent states, Phys. Lett. A **253**, 12 (1999).

Implementing sequential state discrimination

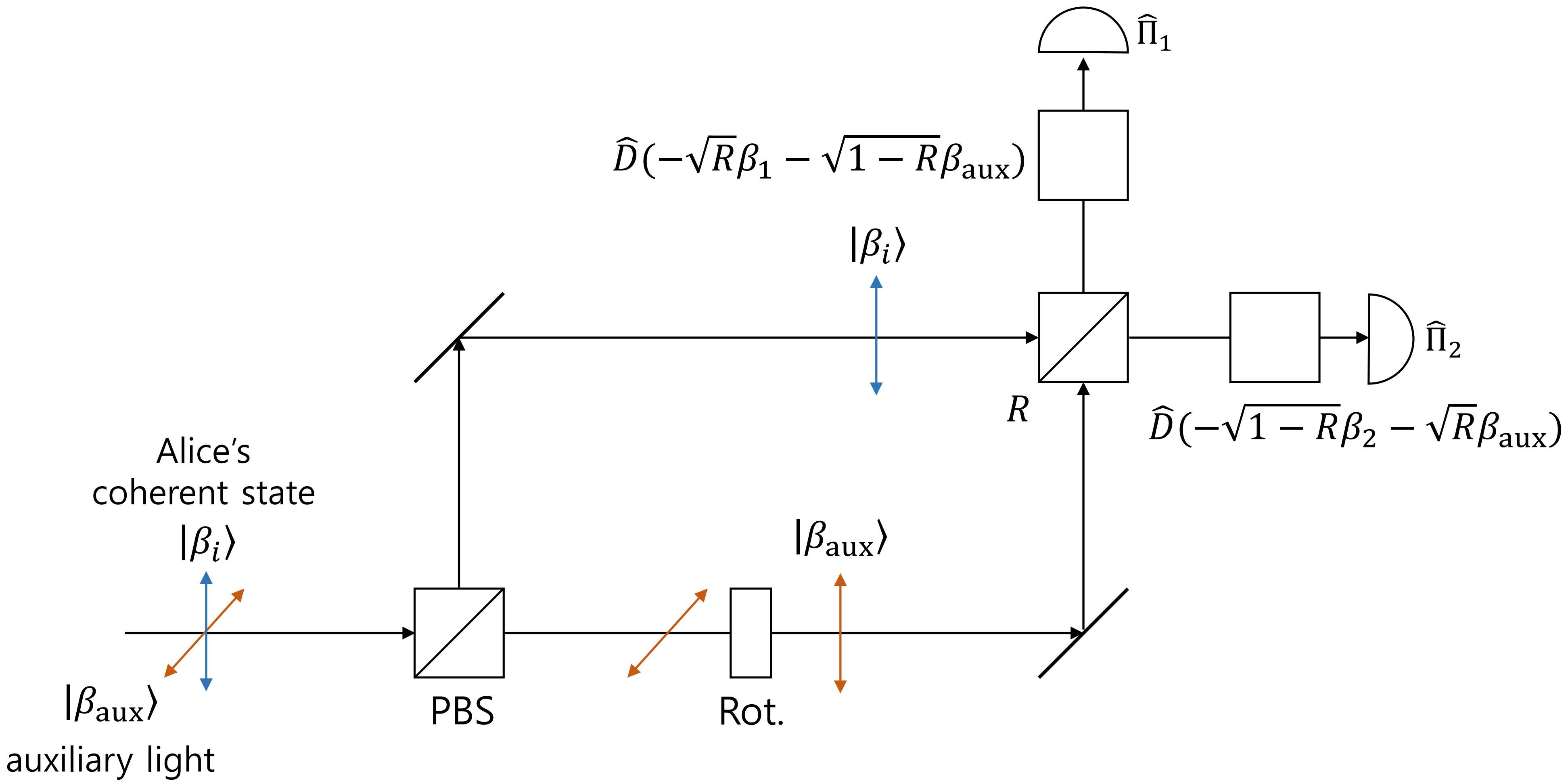
Banaszek model



K. Banaszek, Optimal receiver for quantum cryptography with two coherent states, Phys. Lett. A **253**, 12 (1999).

Implementing sequential state discrimination

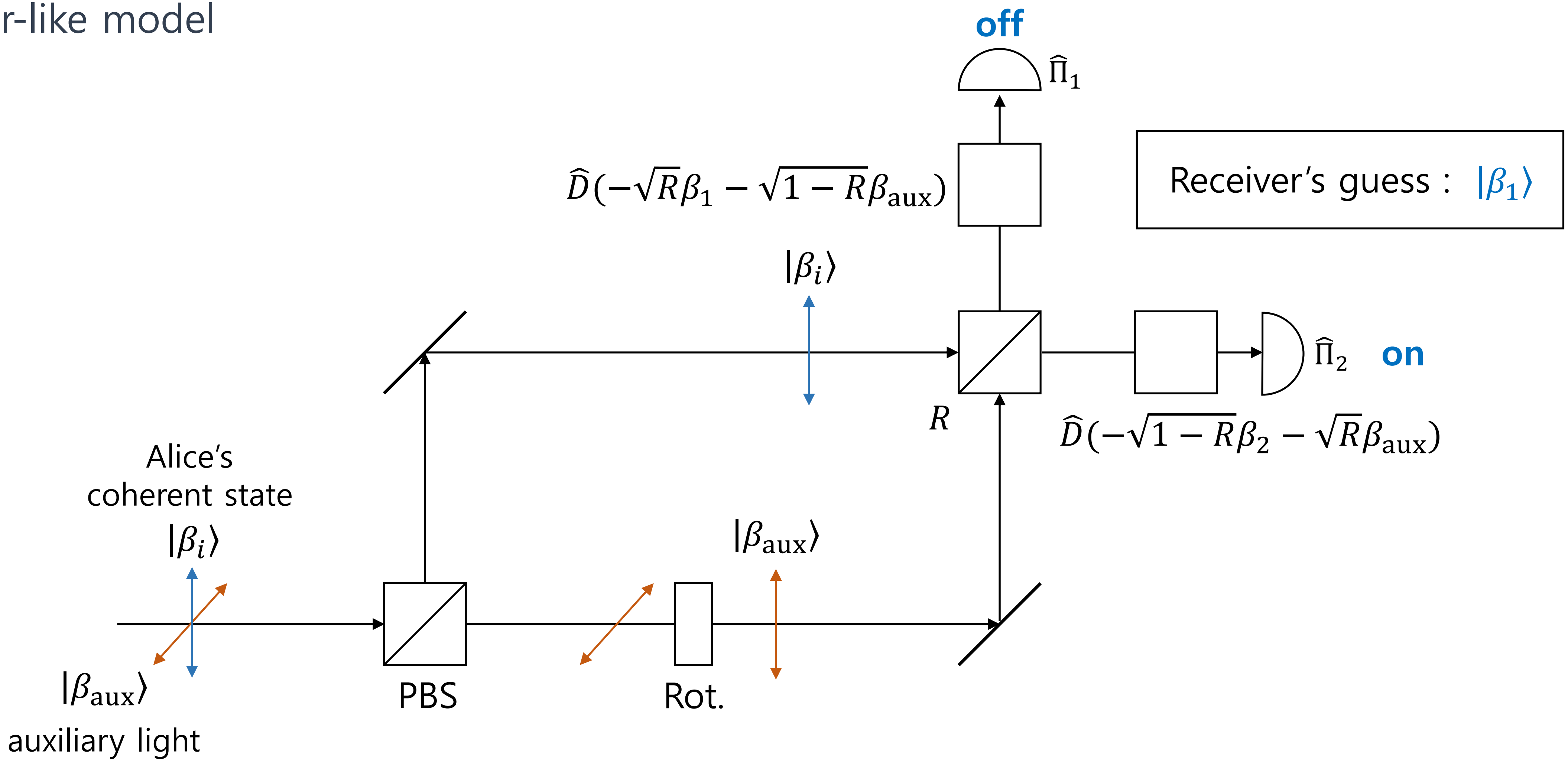
Huttner-like model



B. Huttner et al., Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

Implementing sequential state discrimination

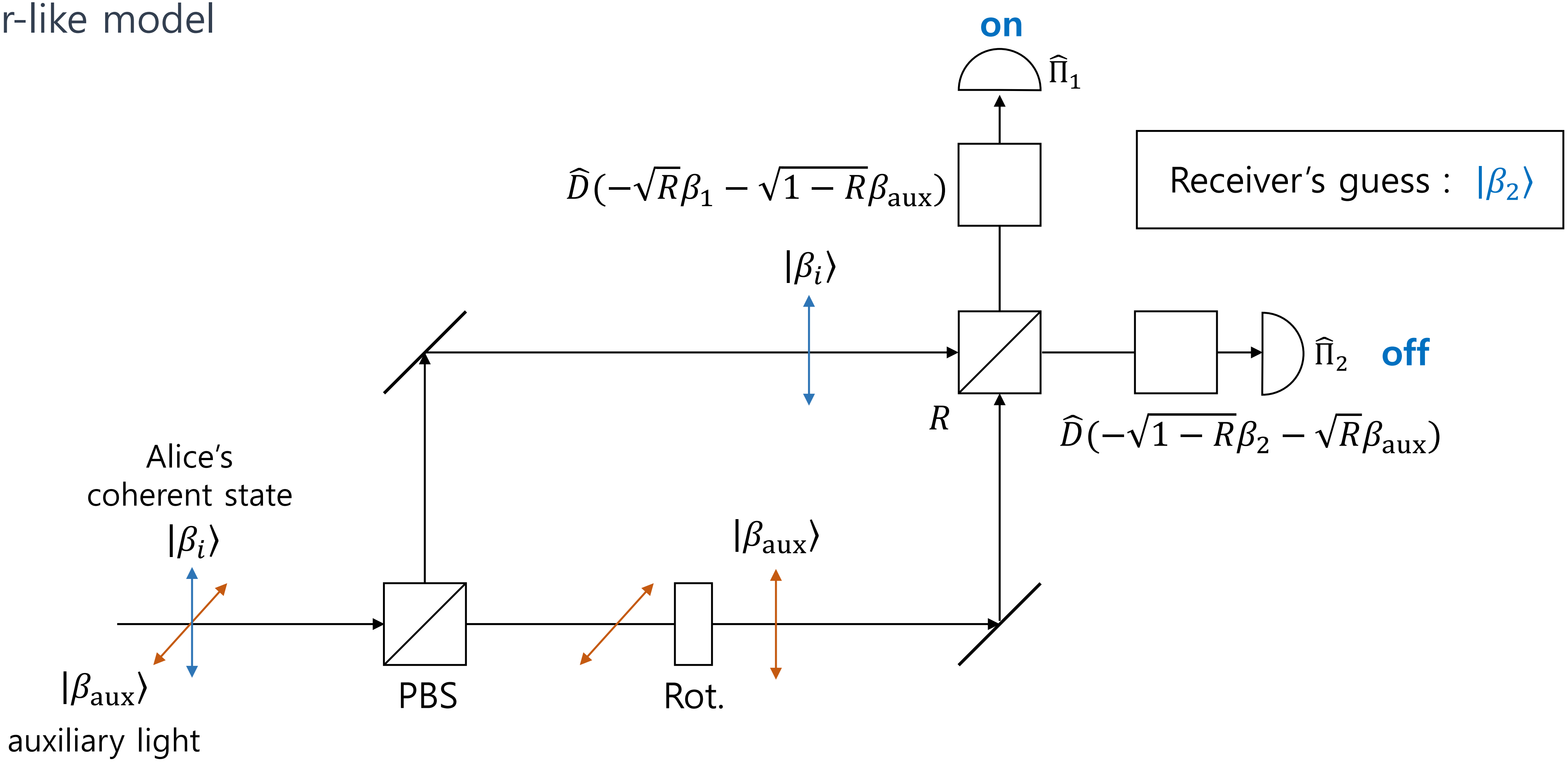
Huttner-like model



B. Huttner et al., Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

Implementing sequential state discrimination

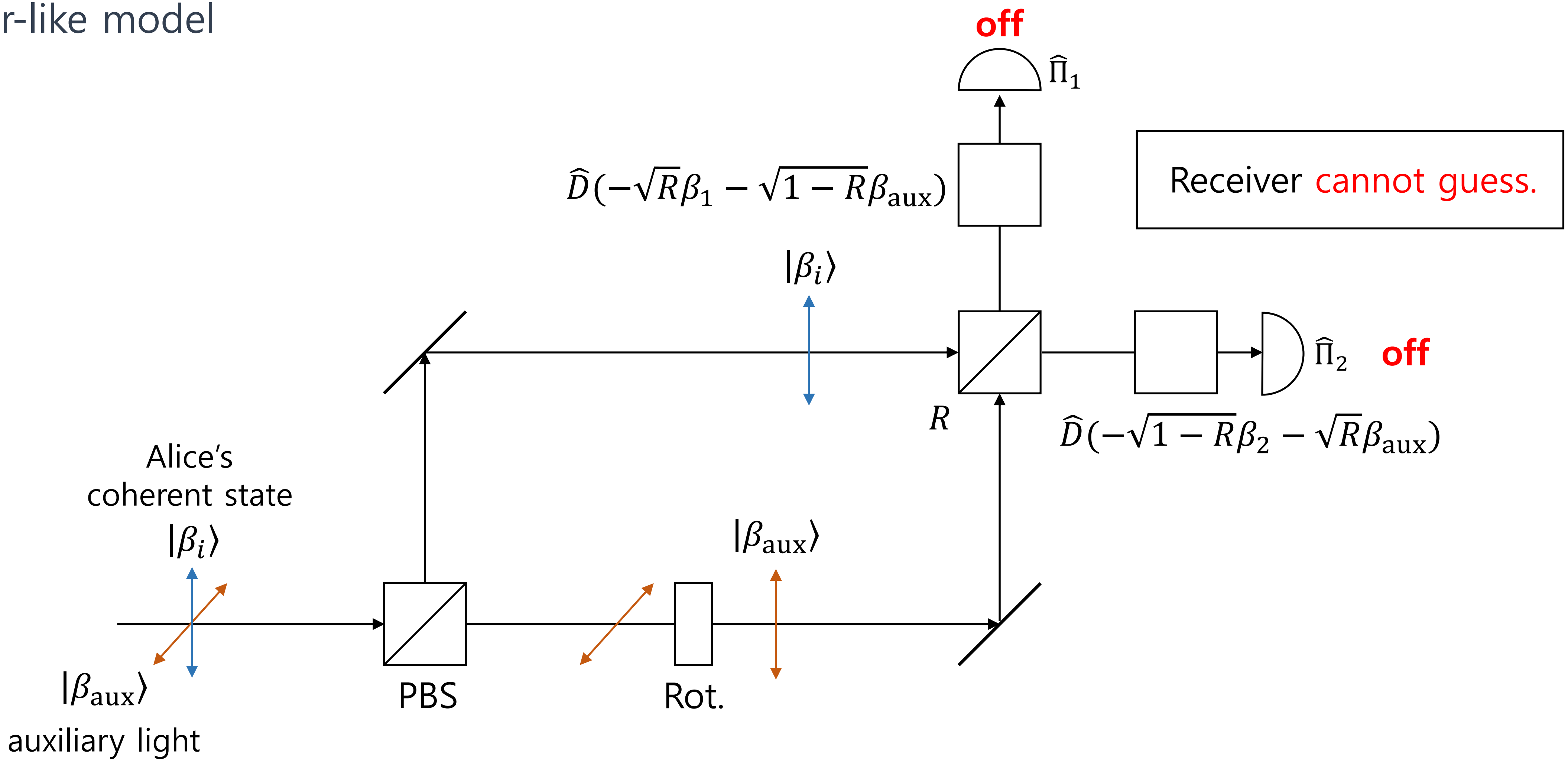
Huttner-like model



B. Huttner et al., Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

Implementing sequential state discrimination

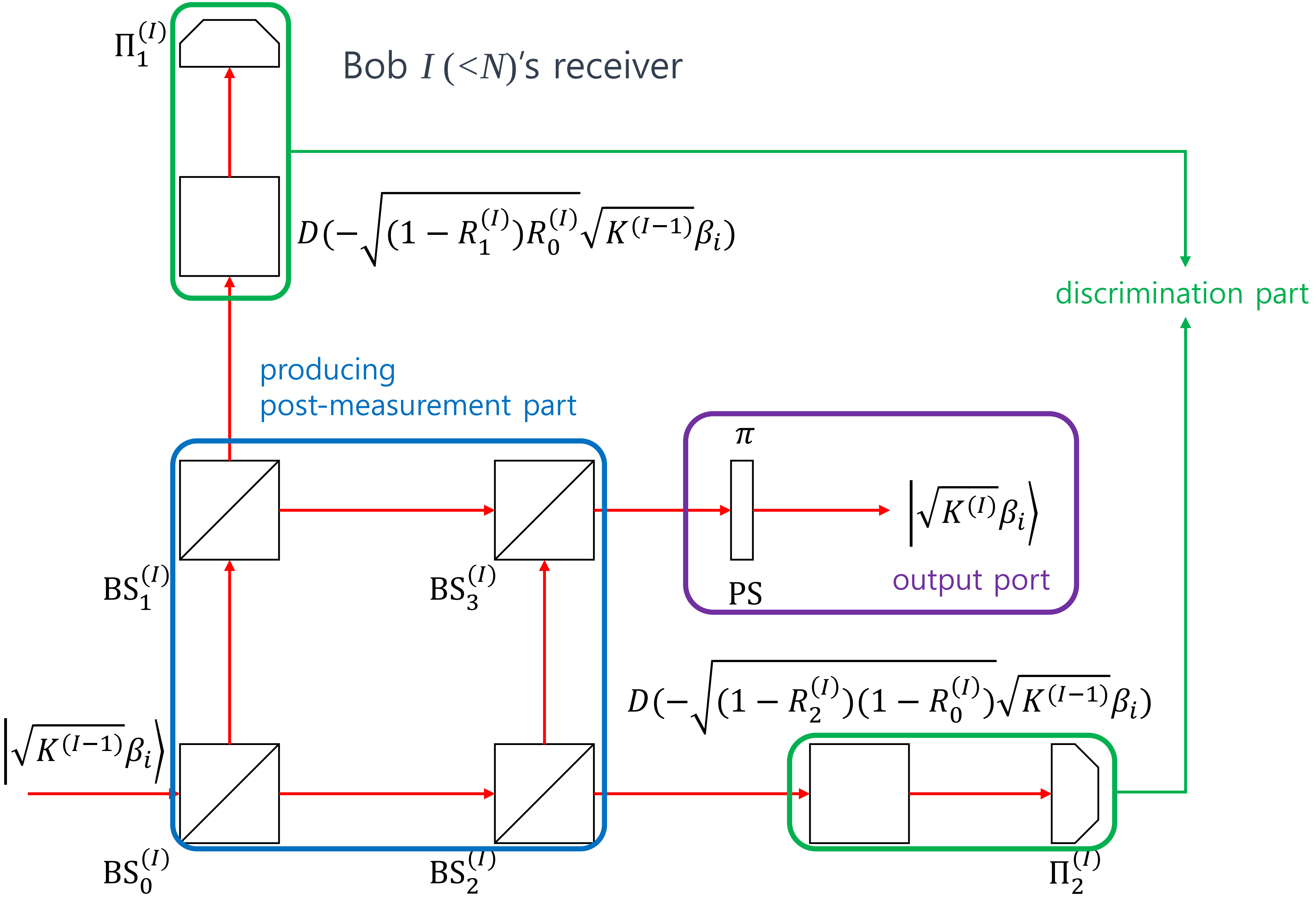
Huttner-like model



B. Huttner et al., Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

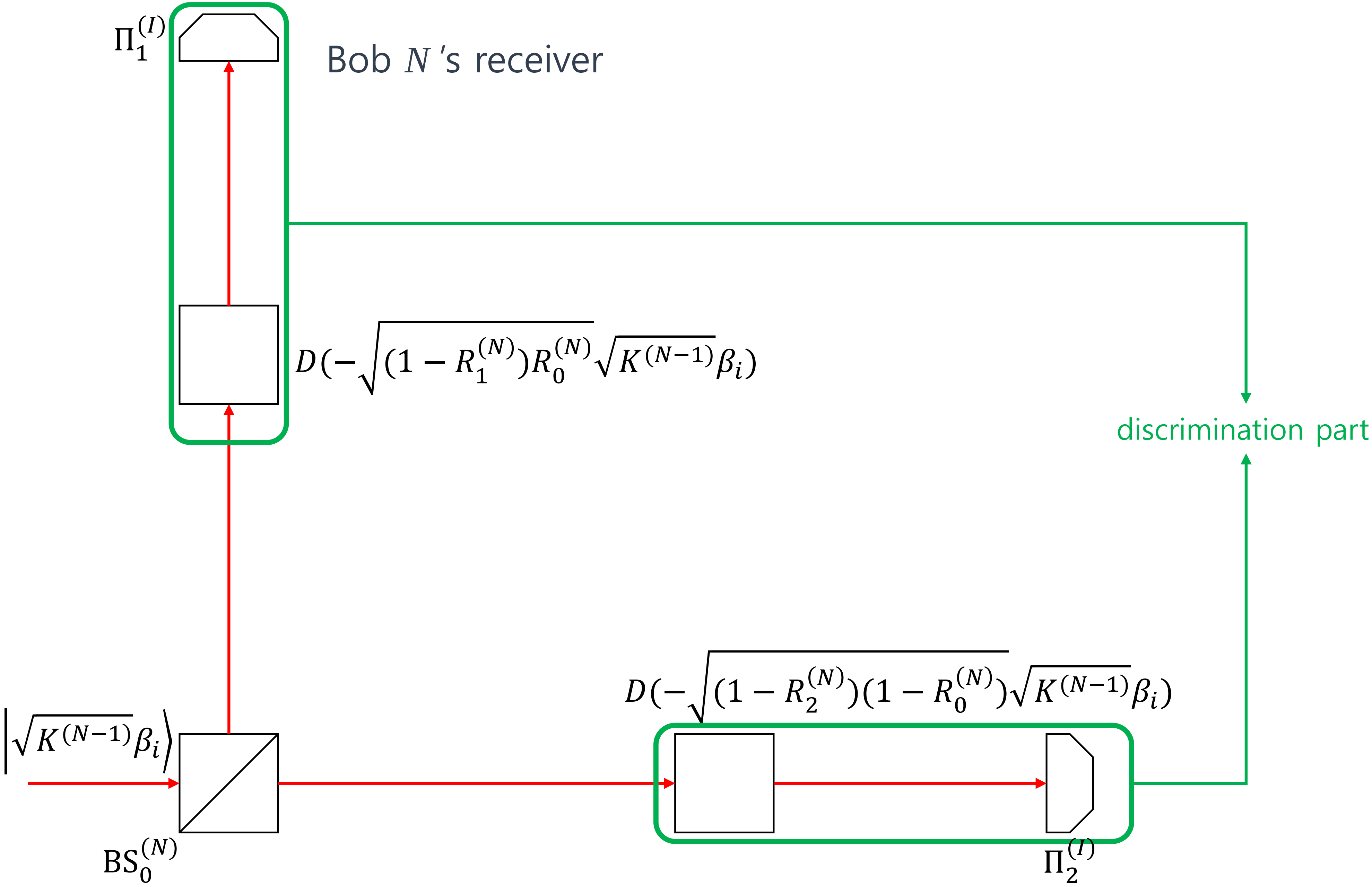
Implementing sequential state discrimination

M. Namkung and Y. Kwon,
Sequential state discrimination
of coherent states,
Scientific Reports **8**, 16915 (2018).



Implementing sequential state discrimination

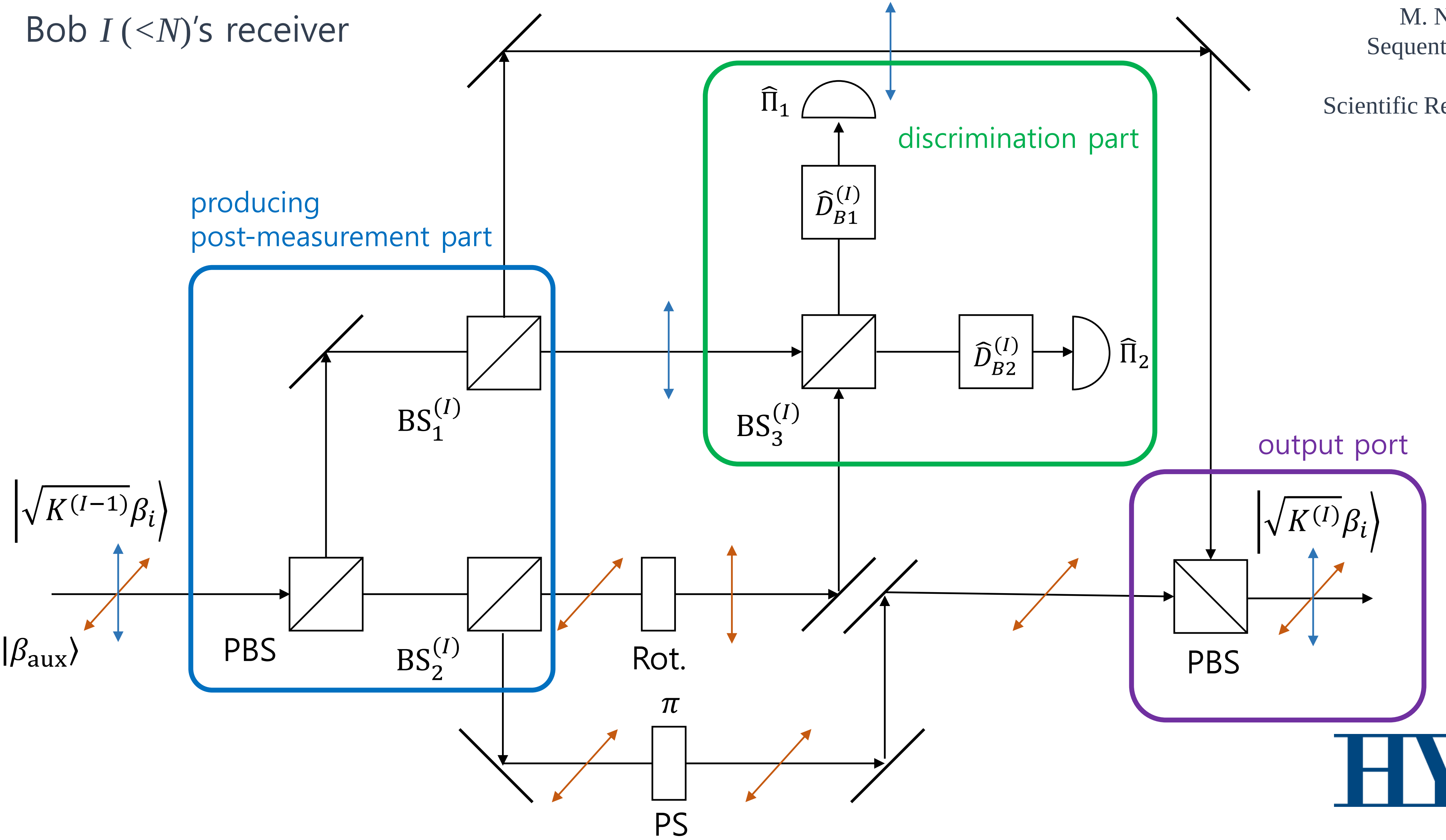
M. Namkung and Y. Kwon,
Sequential state discrimination
of coherent states,
Scientific Reports **8**, 16915 (2018).



Implementing sequential state discrimination

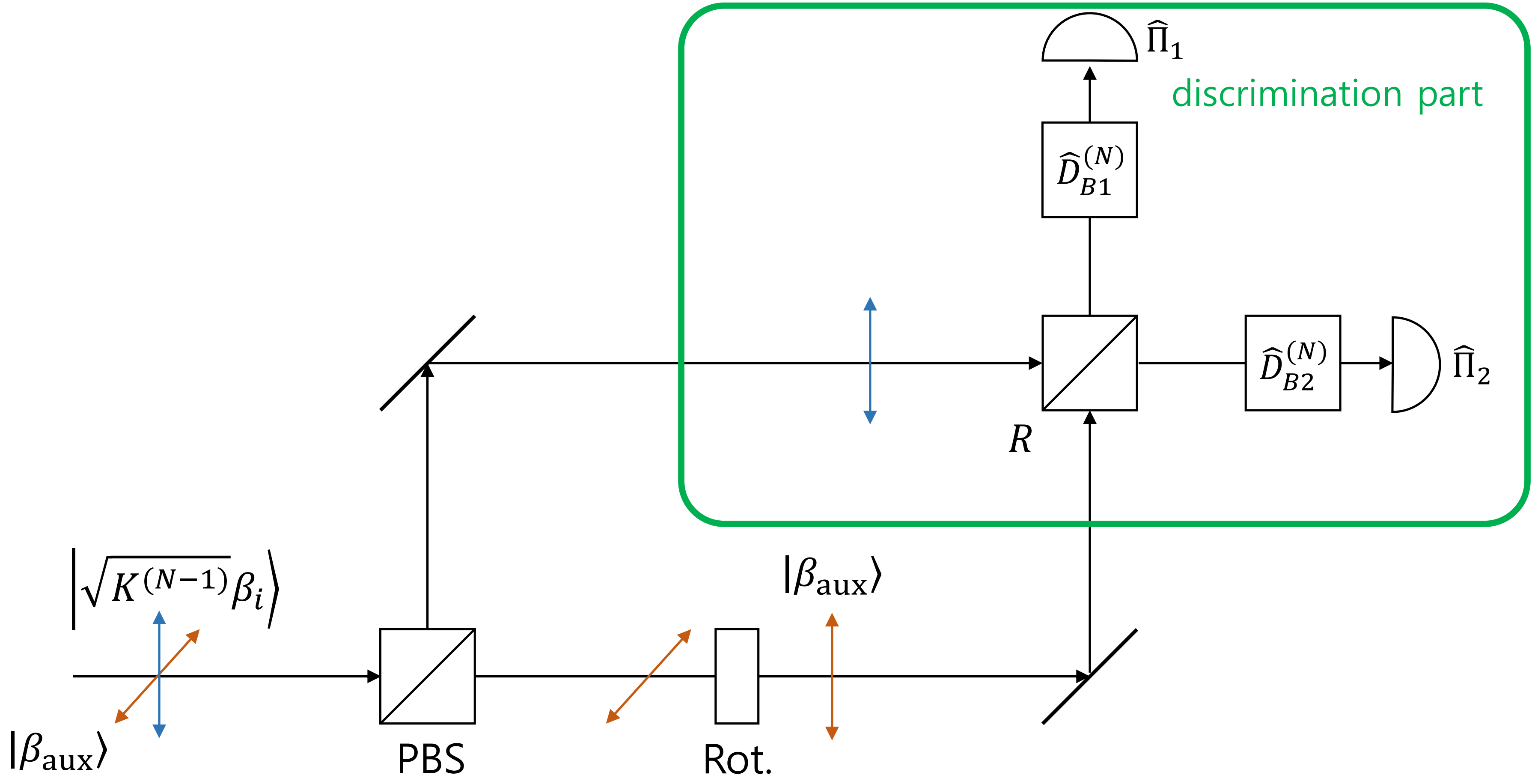
Bob $I\,(<N)$'s receiver

M. Namkung and Y. Kwon,
Sequential state discrimination
of coherent states,
Scientific Reports **8**, 16915 (2018).



Implementing sequential state discrimination

Bob N's receiver

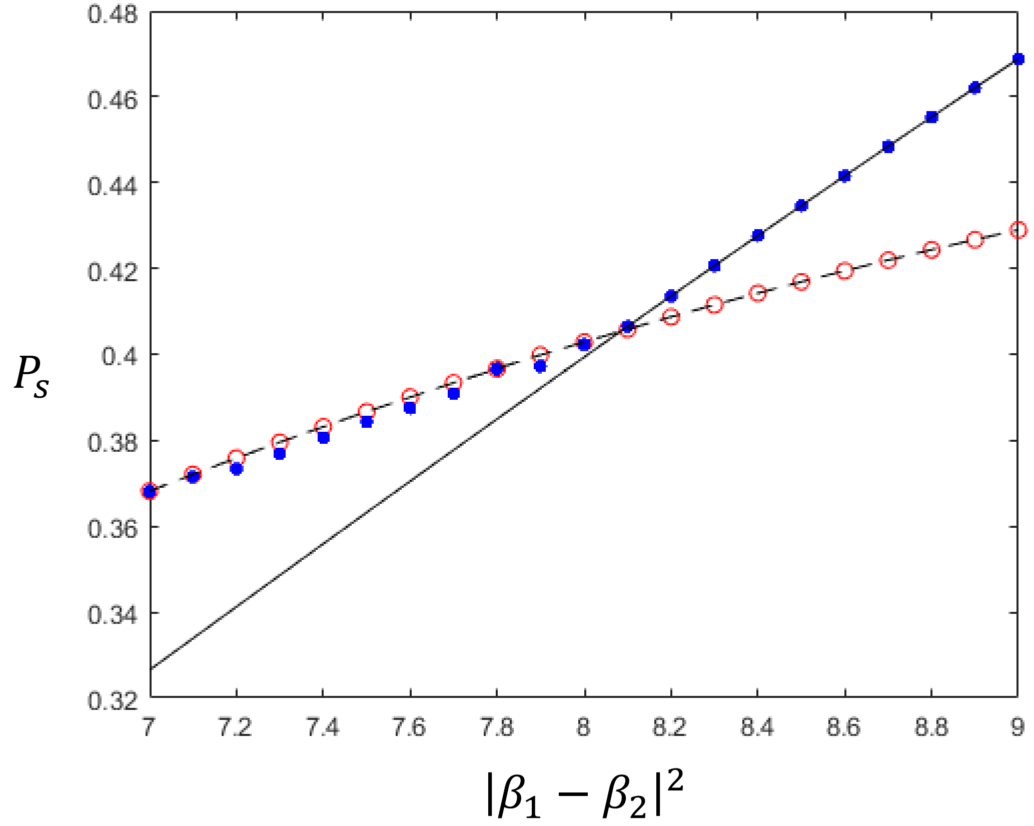


M. Namkung and Y. Kwon,
Sequential state discrimination
of coherent states,
Scientific Reports **8**, 16915 (2018).

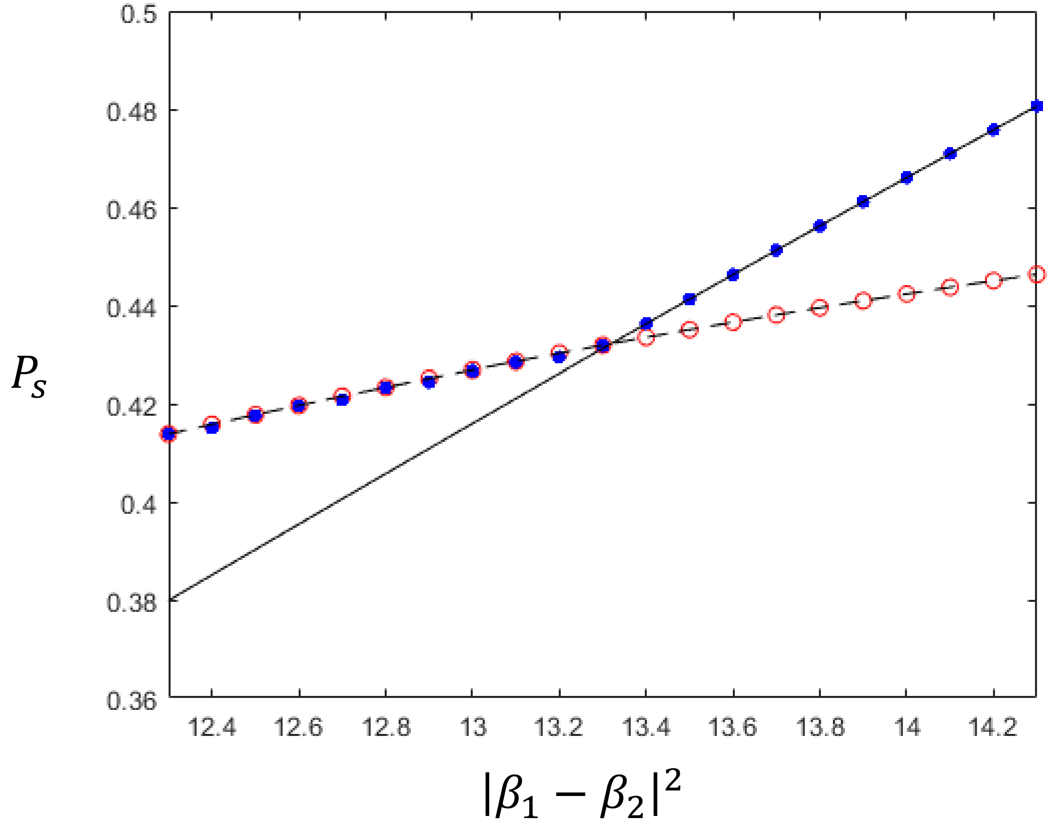
Implementing sequential state discrimination

Optimal success probability

(three receivers)

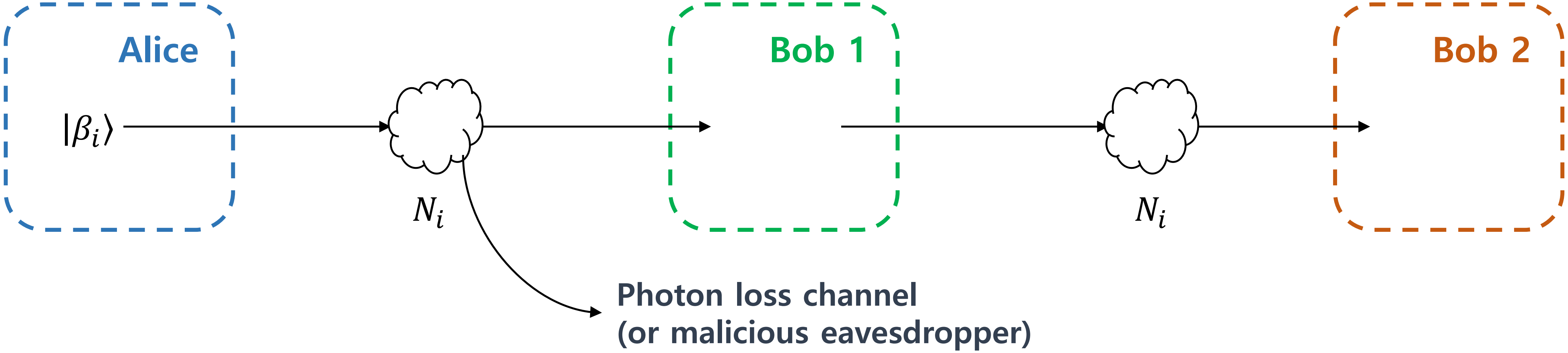


(four receivers)



Sequential state discrimination in noisy channel

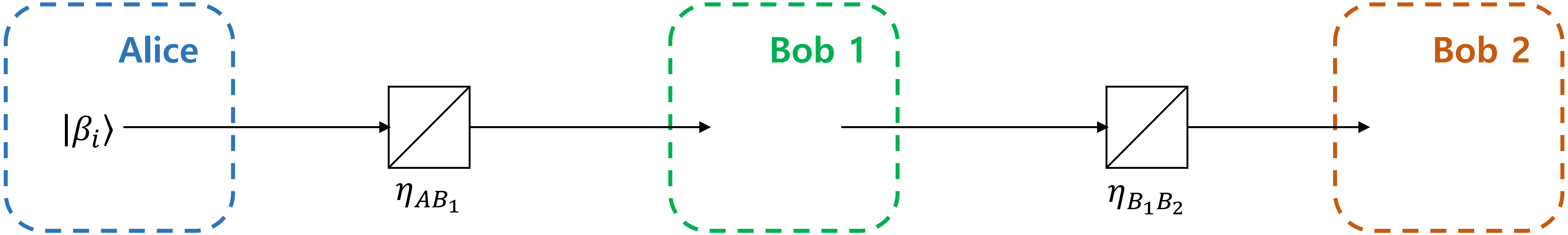
Noisy channel in Banaszek model



R. A. Campos et al., Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statics, Phys. Rev. A **40**, 1371 (1989).
S. J. D. Phoenix, Wave-packet evolution in the damped oscillator, Phys. Rev. A **41**, 5132 (1990).

Sequential state discrimination in noisy channel

Noisy channel in Banaszek model



R. A. Campos et al., Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statics, Phys. Rev. A **40**, 1371 (1989).
S. J. D. Phoenix, Wave-packet evolution in the damped oscillator, Phys. Rev. A **41**, 5132 (1990).

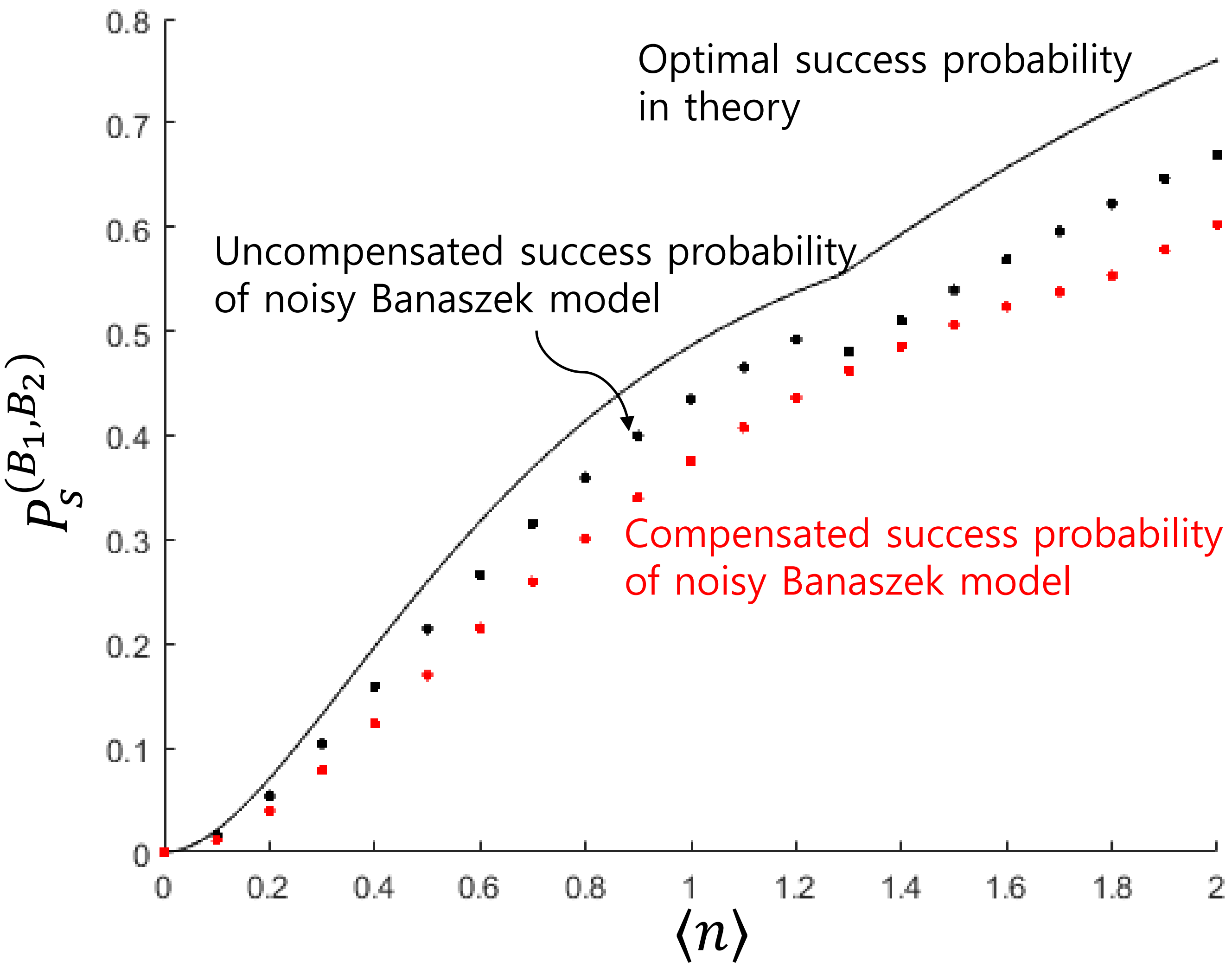
Sequential state discrimination in noisy channel

Noisy channel in Banaszek model

Example. $|\beta_1\rangle = |\alpha\rangle,\ |\beta_2\rangle = |-\alpha\rangle$

In view of noisy channel:
Photon loss noise can be compensated,
but success probability decreases.

In view of eavesdropping:
Eavesdropping decreases success probability.

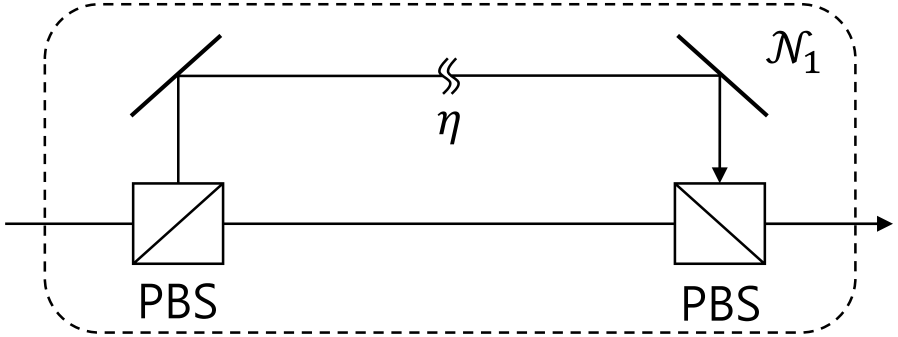


M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

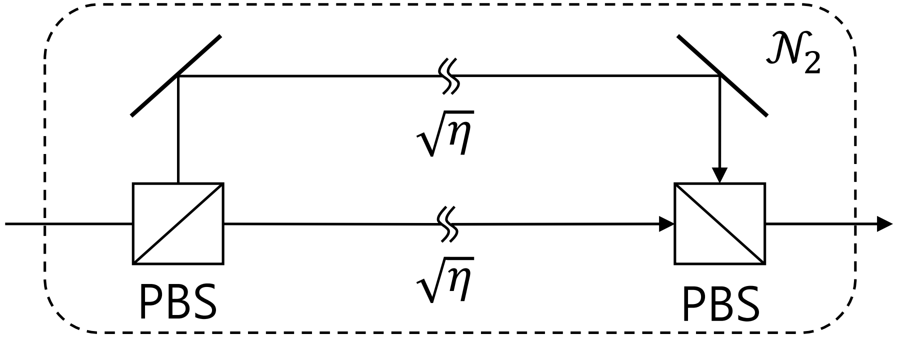
Sequential state discrimination in noisy channel

Noisy channel in Huttner-like model

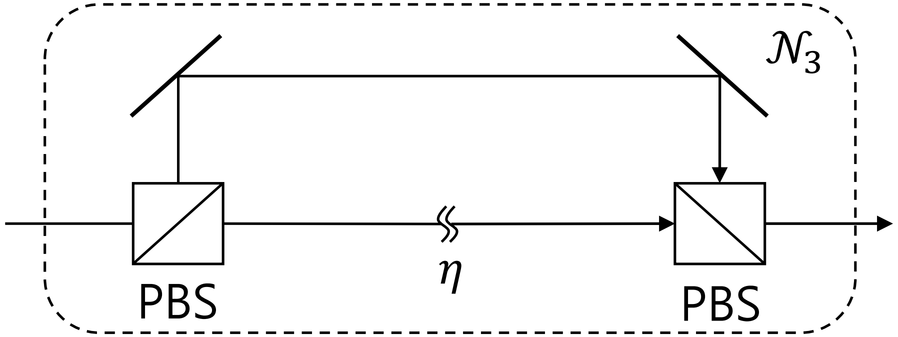
Photon loss(eavesdropping)
on Alice's coherent state only



Photon loss(eavesdropping)
on Alice's coherent state
and auxiliary light



Photon loss(eavesdropping)
on auxiliary light only

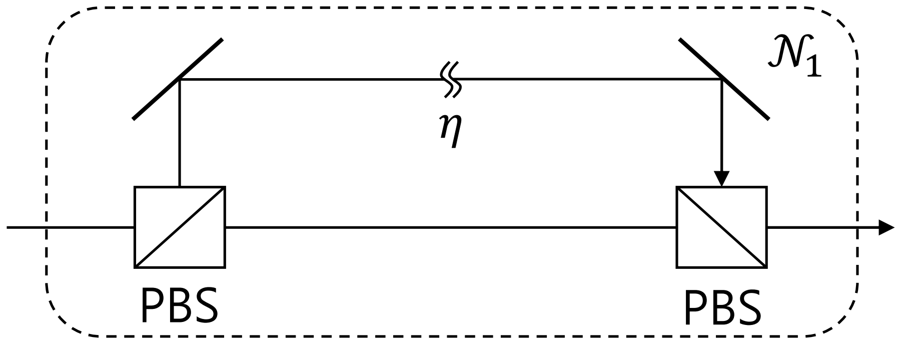


M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

Sequential state discrimination in noisy channel

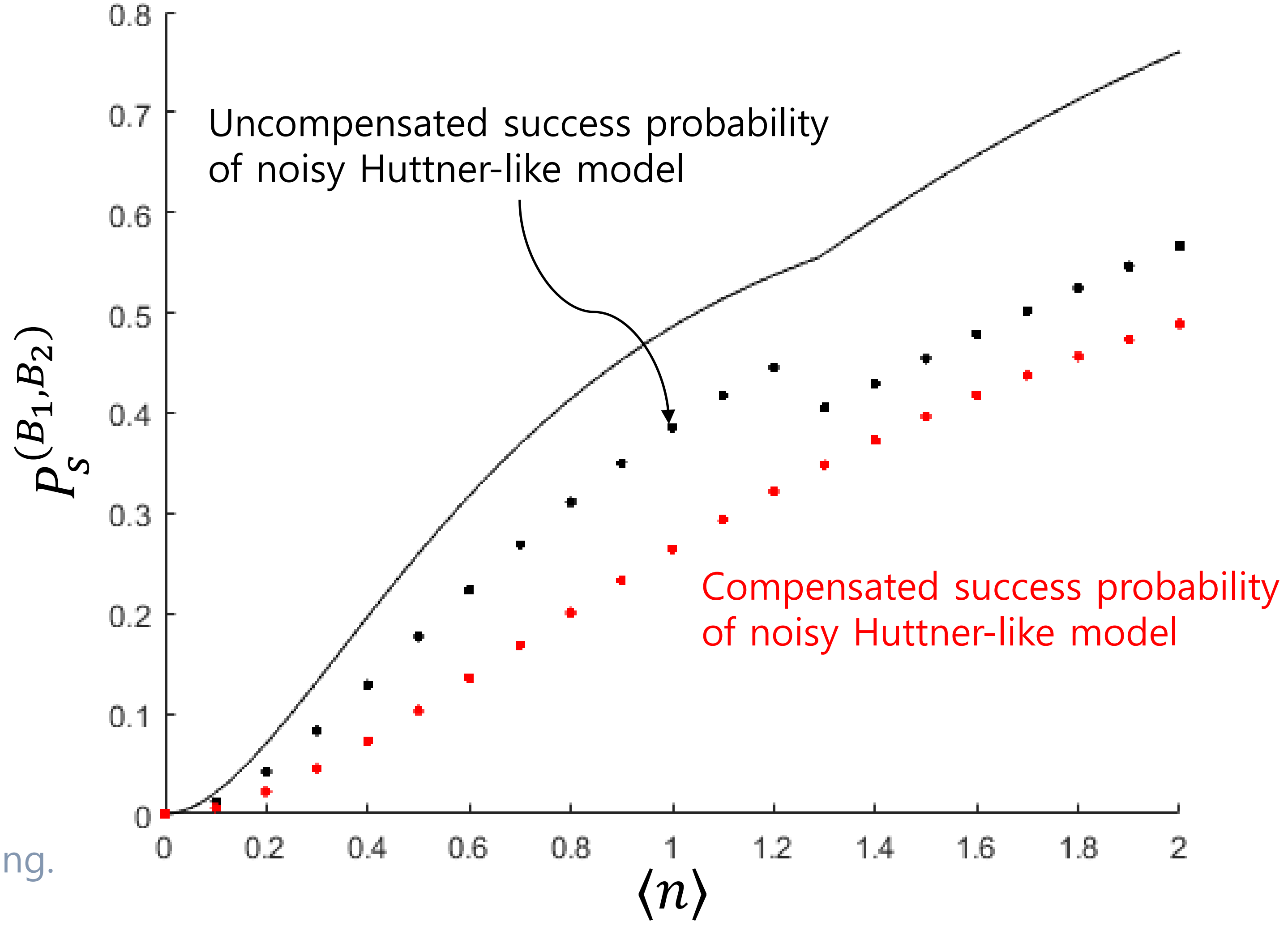
Noisy channel in Huttner-like model

Photon loss(eavesdropping)
on Alice's coherent state only



In view of noisy channel:
Compensation decreases large amount of success probability.

In view of eavesdropping:
Because of decreasing, receivers notice eavesdropping.

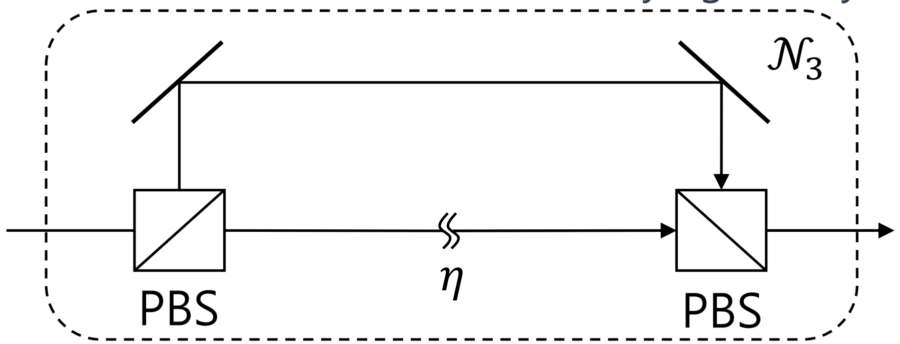


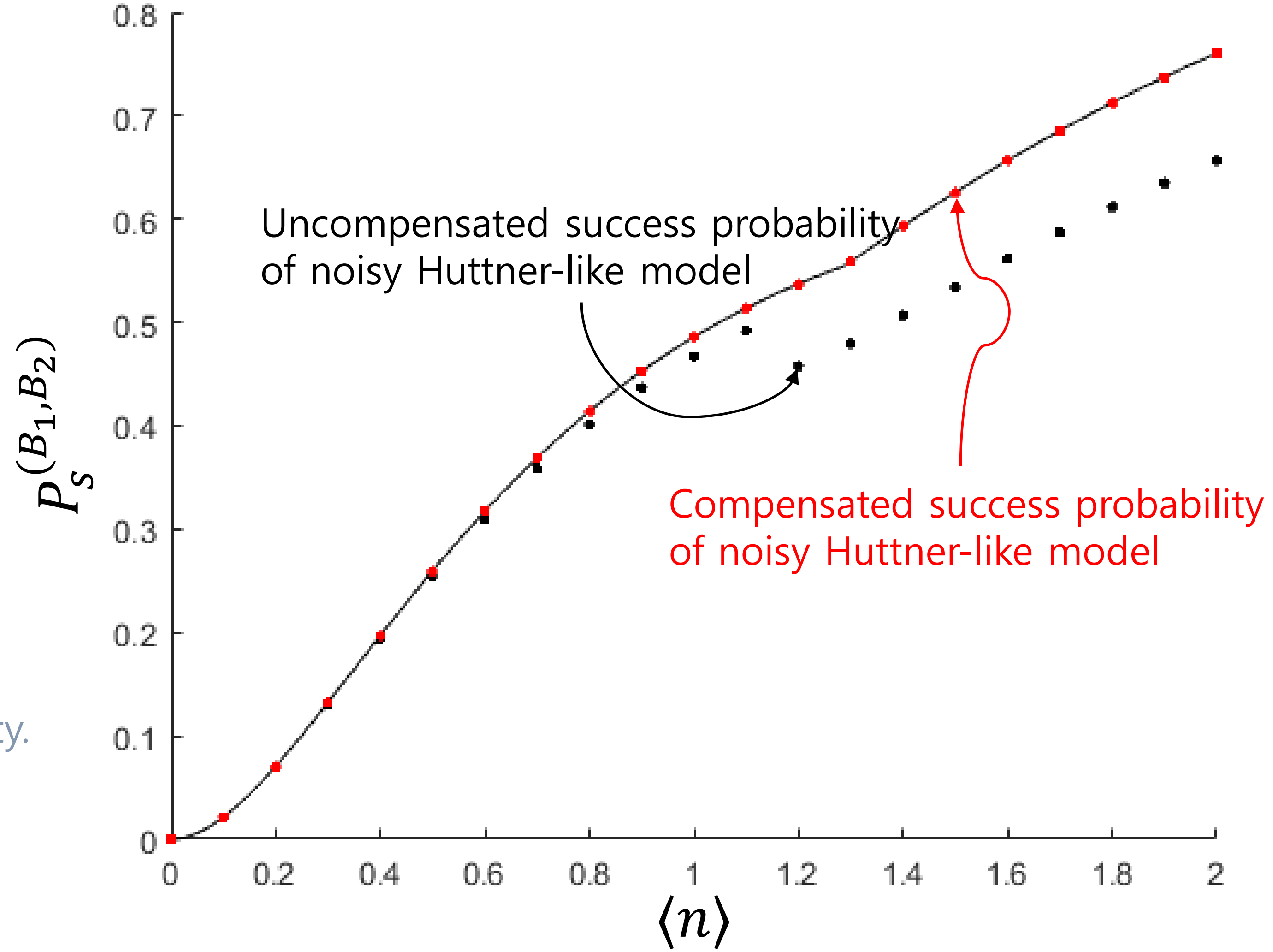
M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

Sequential state discrimination in noisy channel

Noisy channel in Huttner-like model

Photon loss(eavesdropping)
on auxiliary light only



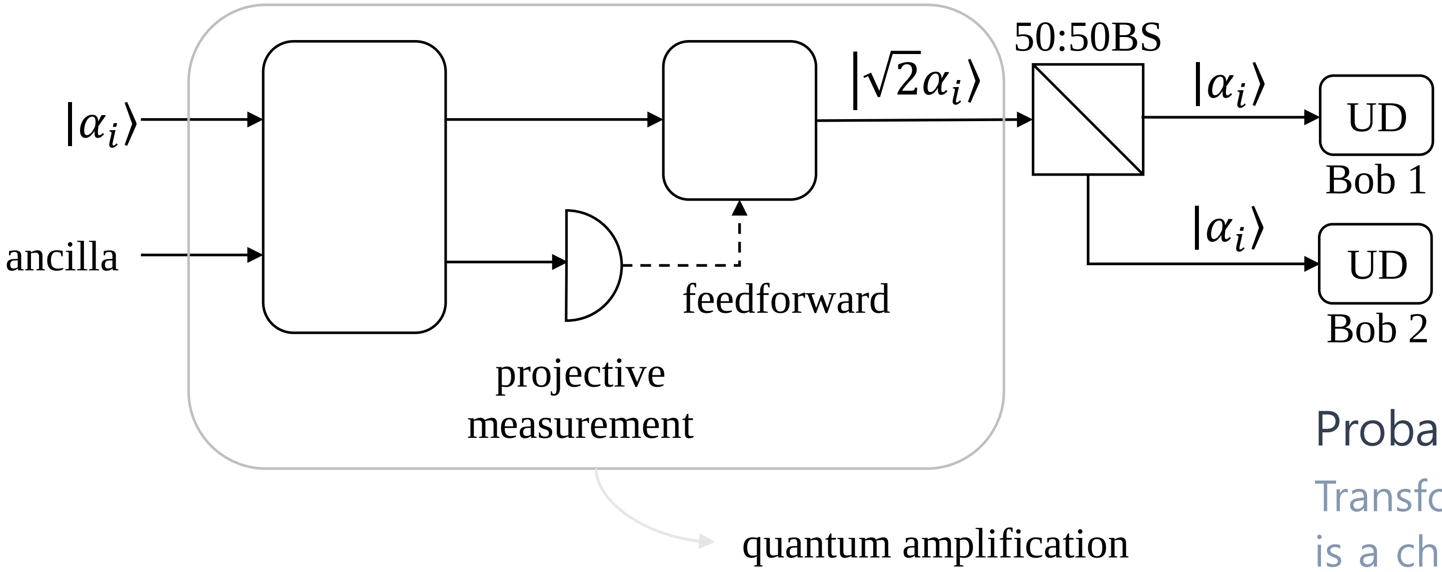


In view of noisy channel:
Compensation does not decrease success probability.

In view of eavesdropping:
Eavesdropper cannot obtain any information.

M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

Comparison with probabilistic cloning strategy



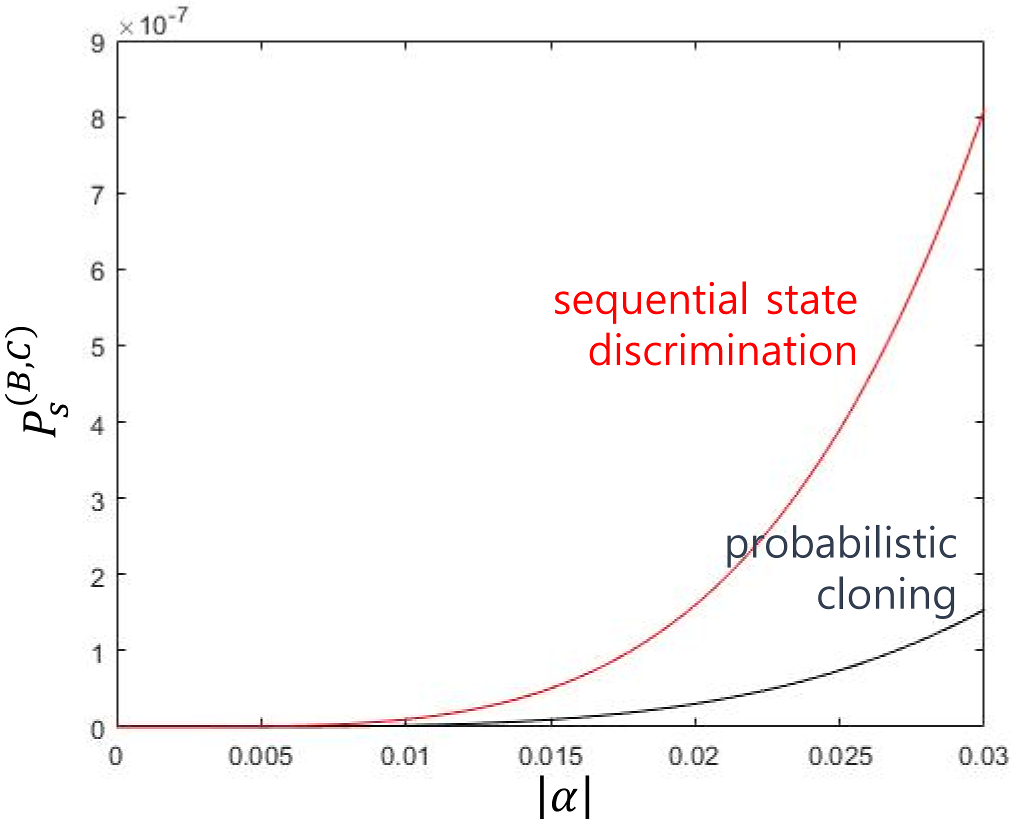
Probabilistic cloning using linear optics

Transforming an unknown coherent state $|\alpha\rangle$ into $|\sqrt{2}\alpha\rangle$ is a challenging task.

J. Ho et al., Experimental noiseless linear amplification using weak measurements, New J. Phys. **18**, 093026 (2016).

Comparison with probabilistic cloning strategy

Optimal success probabilities



According to this graph, sequential state discrimination outperforms quantum probabilistic cloning strategy

M. Namkung and Y. Kwon, Sequential state discrimination of coherent states, Scientific Reports **8**, 16915 (2018).

Conclusion

Part I : Theory

- We express sequential state discrimination for N receivers in mathematical optimization problem.
- Sequential state discrimination of two pure states can be applied to multiparty QKD, when the number of receivers is not too many.
- Sequential state discrimination of two mixed states can be applied to multiparty QKD, even if the number of receivers is too many.
- Optimal success probability of mixed states sequential state discrimination excesses that of quantum reproducing and quantum probabilistic broadcasting strategy. This means that sequential state discrimination is more suitable for multiparty QKD than other two strategies.

Conclusion

Part II : Application

- We propose the method to implement sequential state discrimination of two coherent states using linear optics.
- Probabilistic cloning cannot be performed using linear optics except for weak coherent states. Therefore, this strategy is difficult to be implemented technically.
- Optimal success probability of sequential state discrimination excesses that of probabilistic cloning strategy.
- These two facts mean that sequential state discrimination of coherent states is more suitable for realistic multiparty QKD than probabilistic cloning strategy. Especially, Huttner-like model confirms security in realistic situation.

Future work and further information

This talk is based on following works and recent results prepared in submission:

- M. Namkung and Y. Kwon, Phys. Rev. A **96**, 022318 (2017).
- M. Namkung and Y. Kwon, Scientific Reports **8**, 6515 (2018).
- M. Namkung and Y. Kwon, Scientific Reports **8**, 16915 (2018).

We plan to investigate sequential state discrimination of N quantum states. In case of three pure states, we may exploit following reference:

- D. Ha and Y. Kwon, Phys. Rev. A **91**, 062312 (2015).

Thank you for attention!

감사합니다!