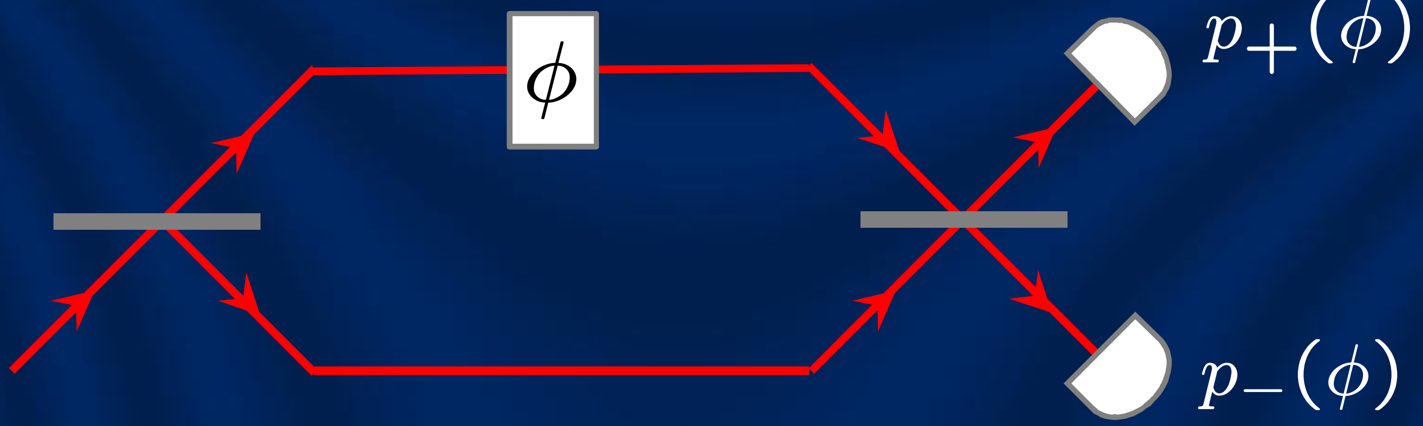
Which-way experiment with an internal degree of freedom

Konrad Banaszek
Michał Karpiński
Czesław Radzewicz
University of Warsaw

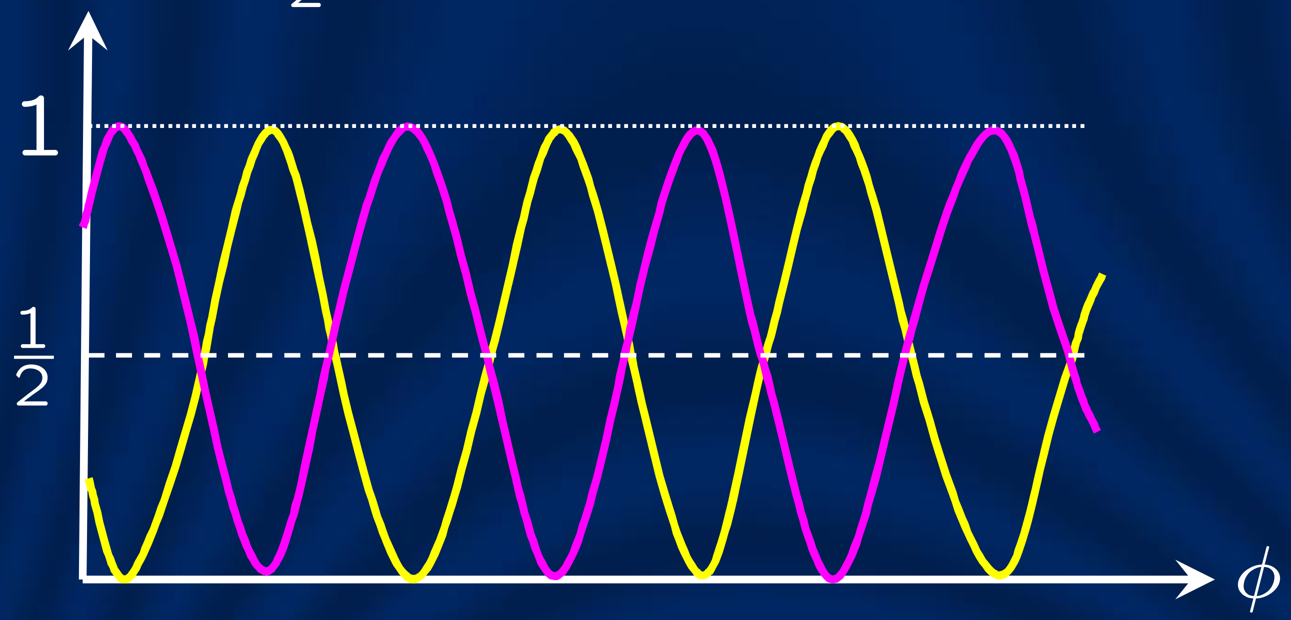
Paweł Horodecki
Technical University of Gdańsk
National Quantum Information Centre in Gdańsk

SEVENTH FRAMEWORK PROGRAMME
INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI
FNP
Fundacja na rzecz Nauki Polskiej
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Mach-Zehnder interferometer

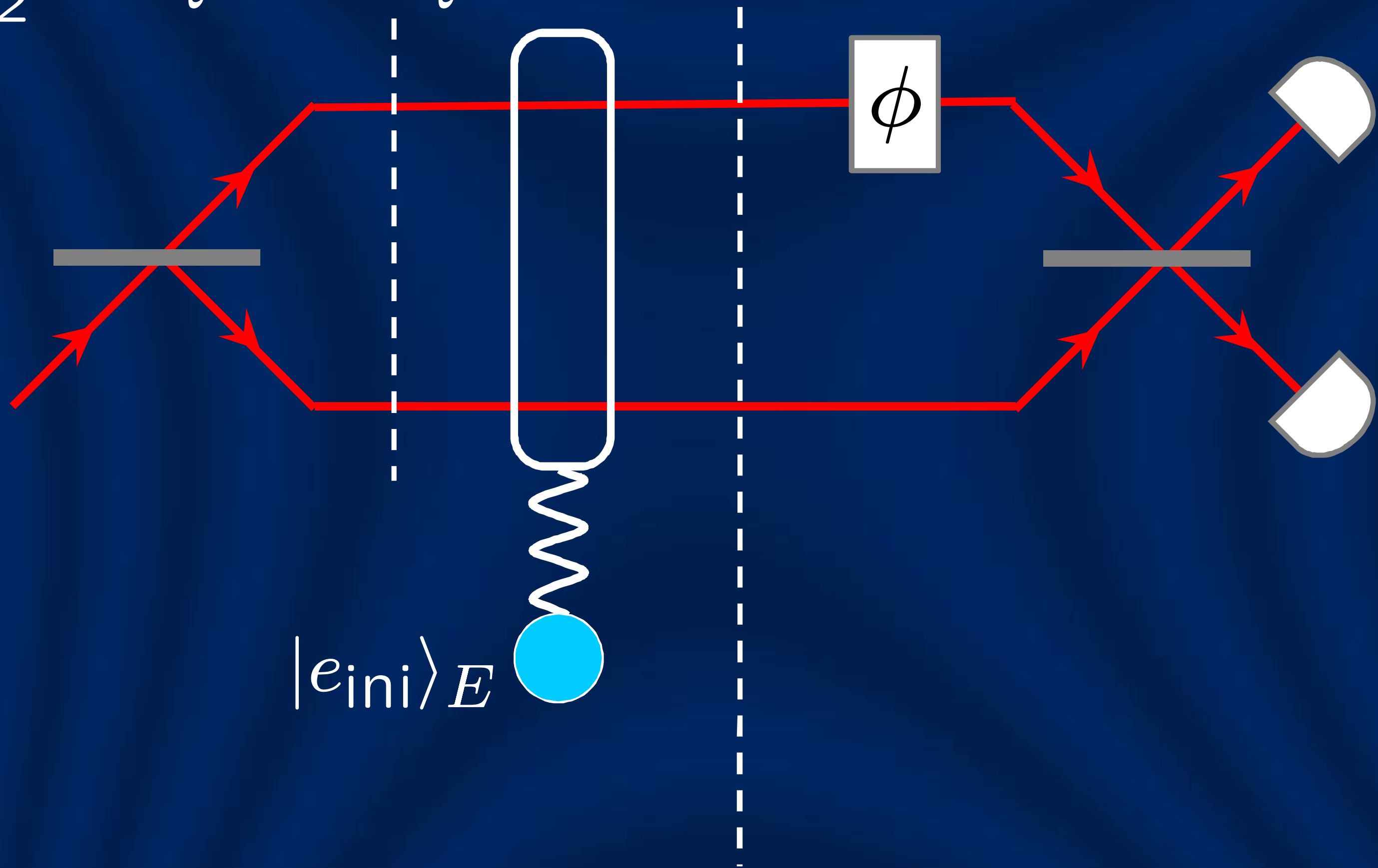


$$p_\pm(\phi) = \tfrac{1}{2}(1 \pm \cos\phi)$$



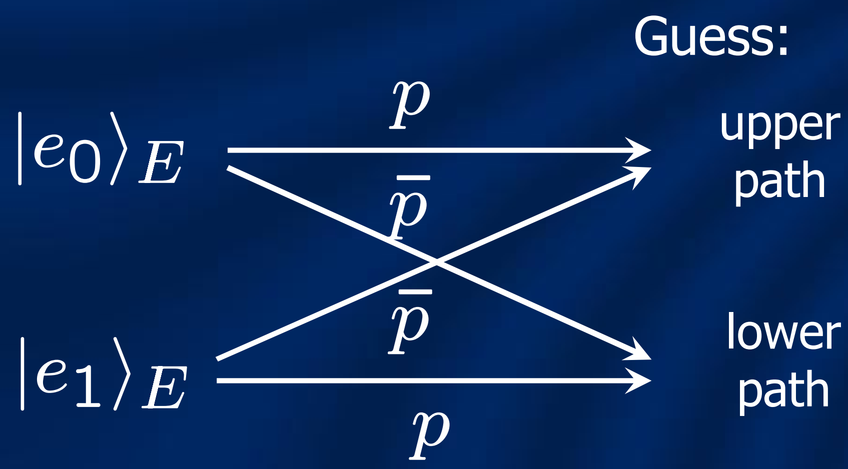
Which way?

$$\frac{1}{\sqrt{2}}(|0\rangle_Q + |1\rangle_Q)$$



$$\frac{1}{\sqrt{2}}(|0\rangle_Q|e_0\rangle_E + |1\rangle_Q|e_1\rangle_E)$$

Minimum-error measurement



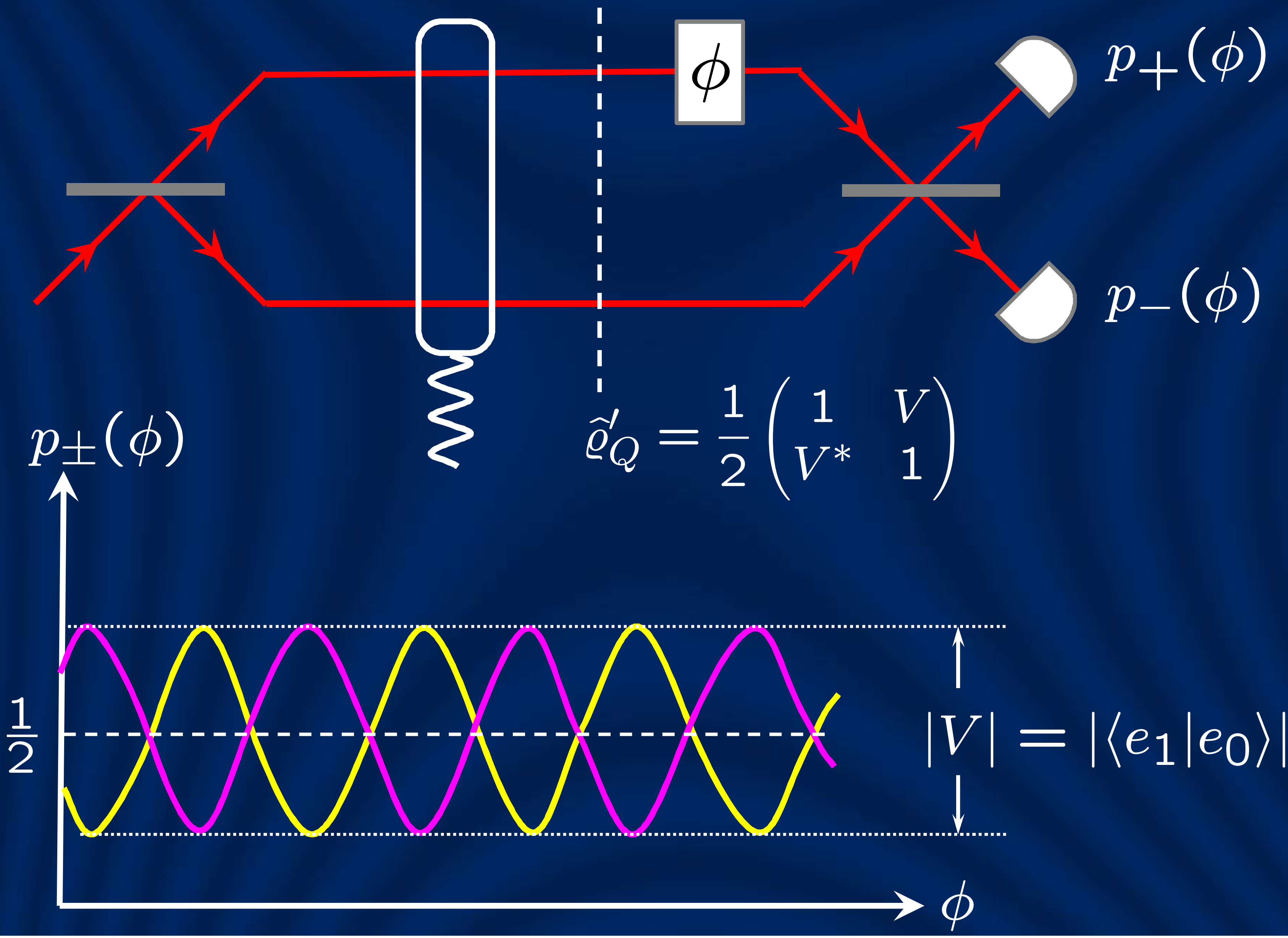
$$p + \bar{p} = 1$$

Maximum *distinguishability* for

- Equiprobable input states
- Symmetric errors

$$p - \bar{p} \leq D = \sqrt{1 - |\langle e_0 | e_1 \rangle|^2}$$

Visibility



ϕ
$p_+(\phi)$
$p_-(\phi)$
$\hat{\varrho}'_Q = \frac{1}{2}\begin{pmatrix} 1 & V \\ V^* & 1 \end{pmatrix}$
$p_\pm(\phi)$
$\frac{1}{2}$
$|V| = |\langle e_1|e_0\rangle|$
ϕ

Trade-off

B.-G. Englert, Phys. Rev. Lett. **77**, 2154 (1996)

Which-way information

$$D = \sqrt{1 - |\langle e_0 | e_1 \rangle|^2}$$

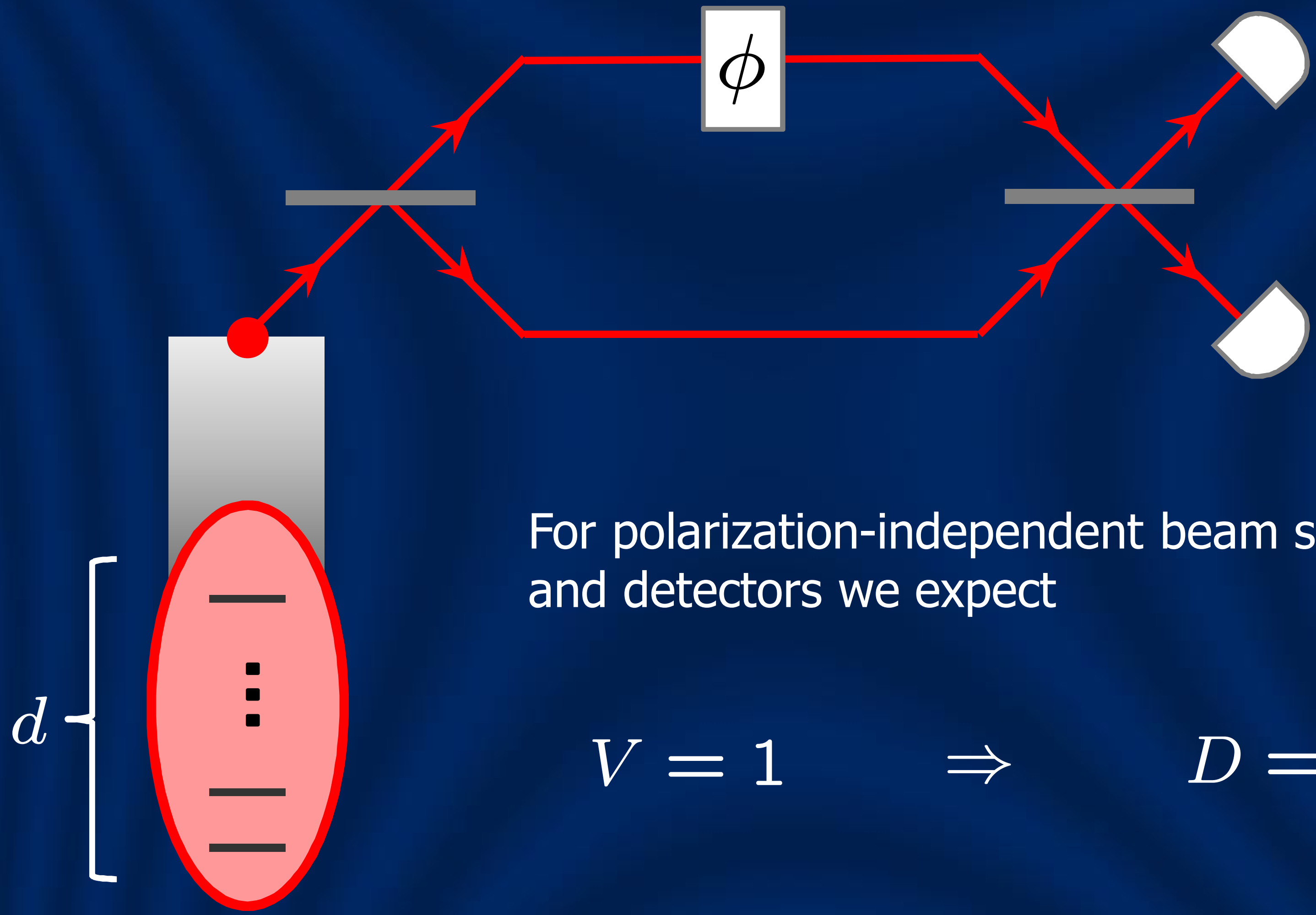
Interference visibility

$$|V| = |\langle e_1 | e_0 \rangle|$$

Bound

$$D^2 + |V|^2 \leq 1$$

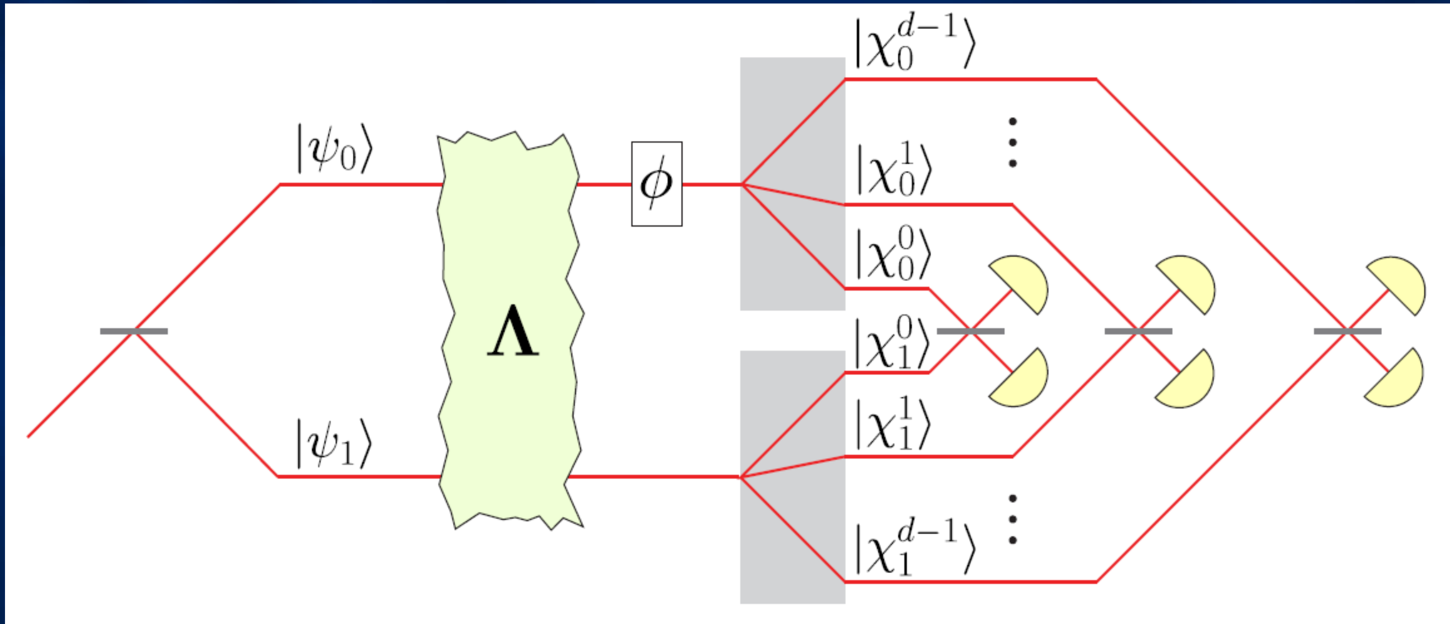
Spin



For polarization-independent beam splitters and detectors we expect

$$V = 1 \quad \Rightarrow \quad D = 0$$

Projective spin filtering



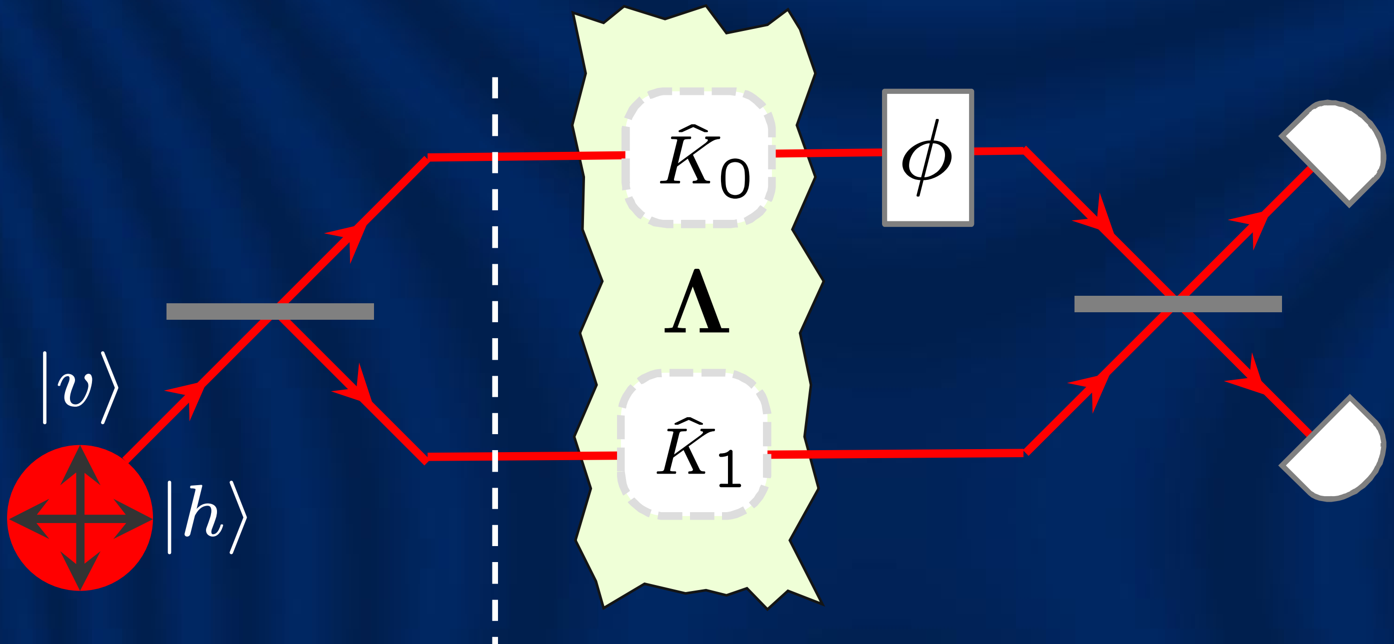
Fractional visibility V^ν at the ν th pair of output ports:

$$p_\pm^\nu(\phi) = \frac{1}{2}[p^\nu \pm \mathrm{Re}(\mathrm{e}^{\mathrm{i}\phi} V^\nu)]$$

Conjecture:

$$D^2 + \left(\sum_{\nu=0}^{d-1} |V^\nu| \right)^2 \leq 1$$

Example



$\hat{K}_0$	$\hat{K}_1$
$\hat{I}$	$\hat{I}$
$\hat{X}$	$\hat{X}$
$\hat{Y}$	$-\hat{Y}$
$\hat{Z}$	$\hat{Z}$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_Q + |1\rangle_Q) \otimes |\psi\rangle_S$$

$$\boldsymbol{\Lambda}\Big(|\Psi\rangle\langle\Psi|\Big) = \tfrac{1}{2}\Big(|0\rangle_Q\langle 0| \otimes \tfrac{1}{2}\hat{I}_S + |1\rangle_Q\langle 1| \otimes \tfrac{1}{2}\hat{I}_S$$
$$+ (|0\rangle_Q\langle 1| + |1\rangle_Q\langle 0|) \otimes \tfrac{1}{2}(|\psi\rangle_S\langle\psi|)^T\Big)$$

Channel properties

For any choice of projective filters,

$$\sum_\nu |V^\nu| \leq \frac{1}{2} \quad \Rightarrow$$

No stringent bound on distinguishability

Alternative realization of the channel:

$$\frac{1}{\sqrt{2}}\Big(|0\rangle_Q + |1\rangle_Q\Big)\Big(\psi_h|h\rangle_S + \psi_v|v\rangle_S\Big)|e_{\text{ini}}\rangle_E$$

$$\rightarrow |\Psi'\rangle_{QSE} = \frac{1}{2}\Big[|0\rangle_Q\Big(\psi_h|h\rangle_S|e_1\rangle_E + \psi_h|v\rangle_S|e_2\rangle_E$$
$$+\psi_v|h\rangle_S|e_3\rangle_E + \psi_v|v\rangle_S|e_4\rangle_E\Big)$$
$$+|1\rangle_Q\Big(\psi_h|h\rangle_S|e_1\rangle_E + \psi_v|h\rangle_S|e_2\rangle_E$$
$$+\psi_h|v\rangle_S|e_3\rangle_E + \psi_v|v\rangle_S|e_4\rangle_E\Big)\Big]$$

Environment states

$$\widetilde{\varrho}_E'^{(i)} = 2\mathrm{Tr}_S\Big({}_Q\langle i|\Psi'\rangle_{QSE}\langle\Psi'|i\rangle_Q\Big) \qquad i = 0, 1$$

Input polarisation	$\widetilde{\varrho}_E'^{(0)}$	$\widetilde{\varrho}_E'^{(1)}$
$\|h\rangle_S\langle h\|$	$\frac{1}{2}\Big(\|e_1\rangle_E\langle e_1\| + \|e_2\rangle_E\langle e_2\|\Big)$	$\frac{1}{2}\Big(\|e_1\rangle_E\langle e_1\| + \|e_3\rangle_E\langle e_3\|\Big)$
$\|v\rangle_S\langle v\|$	$\frac{1}{2}\Big(\|e_3\rangle_E\langle e_3\| + \|e_4\rangle_E\langle e_4\|\Big)$	$\frac{1}{2}\Big(\|e_2\rangle_E\langle e_2\| + \|e_4\rangle_E\langle e_4\|\Big)$
$\frac{1}{2}\Big(\|h\rangle_S\langle h\| + \|v\rangle_S\langle v\|\Big)$	$\frac{1}{4}\sum_{i=1}^{4}\|e_i\rangle_E\langle e_i\|$	$\frac{1}{4}\sum_{i=1}^{4}\|e_i\rangle_E\langle e_i\|$

Channel

As the interaction with the environment does not transfer the particle between the arms of the interferometer:

$$\mathbf{\Lambda}\Big(|i\rangle_Q\langle j| \otimes \hat{\sigma}_S\Big) = |i\rangle_Q\langle j| \otimes \mathbf{\Lambda}_{ij}(\hat{\sigma}_S), \quad i,j = 0,1$$

$\mathbf{\Lambda}_{00}, \mathbf{\Lambda}_{11}$ – spin channels for individual arms

$\mathbf{\Lambda}_{01}$ – characterizes coherence between arms (not necessarily a positive map!)

Example:

$$\mathbf{\Lambda}_{00}(\hat{\sigma}) = \mathbf{\Lambda}_{11}(\hat{\sigma}) = \tfrac{1}{d}\hat{I}\,\mathrm{Tr}\hat{\sigma}$$

$$\mathbf{\Lambda}_{01}(\hat{\sigma}) = \mathbf{\Lambda}_{10}(\hat{\sigma}) = \tfrac{1}{d}\hat{\sigma}^T$$

Result

K. Banaszek, P. Horodecki, M. Karpiński, and C. Radzewicz,
Nature Commun. **4**, 2594 (2013)

Trade-off:

$$D^2 + V_G^2 \leq 1$$

where *generalized visibility* is defined as:

$$V_G = d\left\|(\mathbf{I}\otimes\mathbf{\Lambda}_{01})\Big((\hat{I}\otimes\sqrt{\hat{\varrho}_0})|\Phi_+\rangle\langle\Phi_+|(\hat{I}\otimes\sqrt{\hat{\varrho}_1})\Big)\right\|$$

$\hat{\varrho}_0, \hat{\varrho}_1$ – conditional input spin states in individual arms

$|\Phi_+\rangle$ – normalized maximally entangled $d \otimes d$ state

$||\cdot||$ – trace norm

Examples

1) No noise: $\mathbf{\Lambda}_{01} = \mathbf{I}$

Independently of spin preparation, $V_G = \sqrt{\text{Tr}\hat{\varrho}_0 \text{Tr}\hat{\varrho}_1} = 1$

2) $\mathbf{\Lambda}_{01}(\hat{\sigma}) = (\text{Tr}\hat{\sigma})\hat{\sigma}_0,$ where $\text{Tr}\hat{\sigma}_0 = 1.$

The generalized visibility is given by fidelity:

$$V_G = ||\sqrt{\hat{\varrho}_0}\sqrt{\hat{\varrho}_1}|| = \text{Tr}\sqrt{\sqrt{\hat{\varrho}_0}\hat{\varrho}_1\sqrt{\hat{\varrho}_0}}$$

and reaches one iff $\hat{\varrho}_0 = \hat{\varrho}_1$

3) $\mathbf{\Lambda}_{01}(\hat{\sigma}) = \hat{\sigma}^T/d$

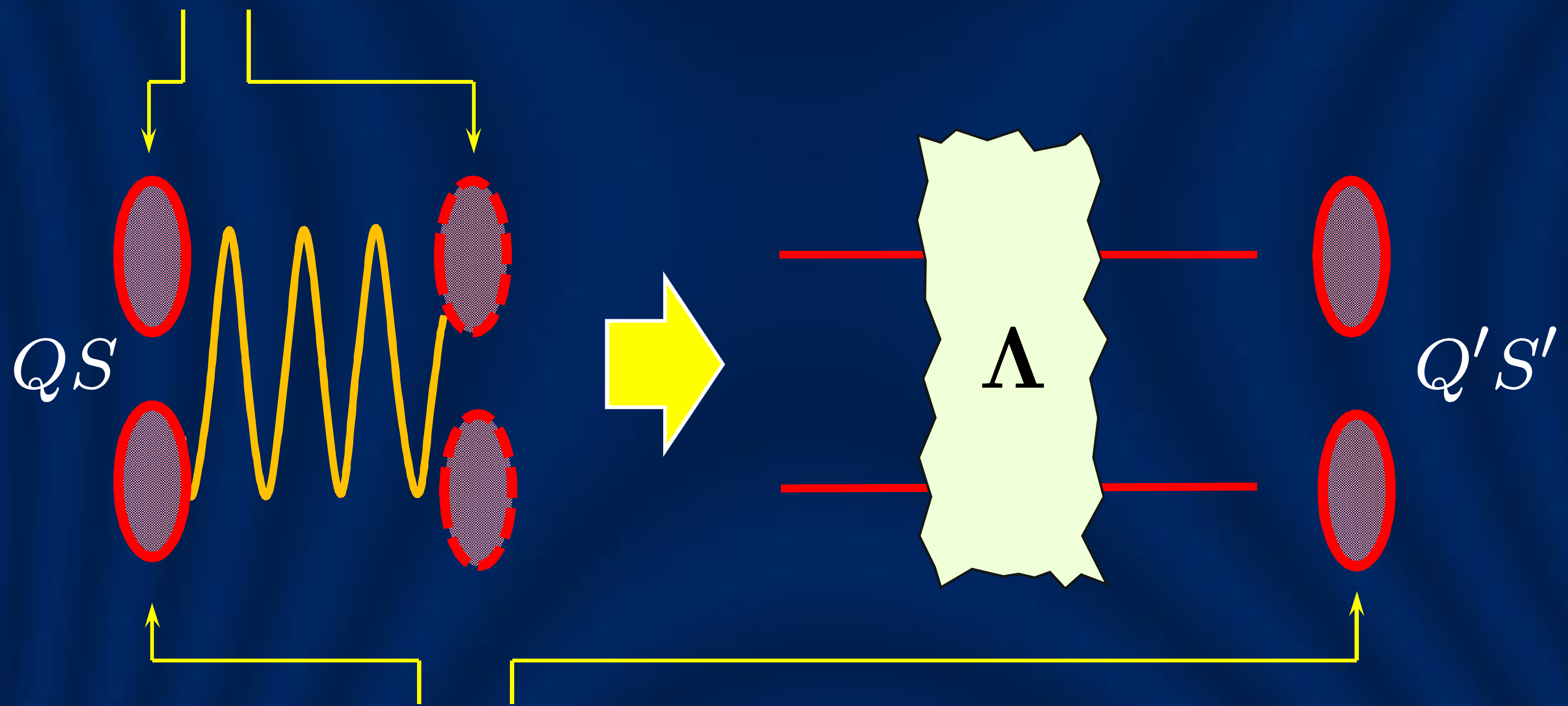
$$V_G = \frac{1}{d}||\sqrt{\hat{\varrho}_0}||\,||\sqrt{\hat{\varrho}_1}|| \leq \sqrt{\text{Tr}\hat{\varrho}_0 \text{Tr}\hat{\varrho}_1} = 1$$

For a pure preparation $V_G = \frac{1}{d}$. Equality holds iff $\hat{\varrho}_0 = \hat{\varrho}_1 = \frac{1}{d}\hat{I}$

Choi-Jamiołkowski isomorphism

Maximally entangled state of two replicas of the system:

$$|\Phi_+\rangle_{QSQ'S'}$$



$$\widehat{\Lambda}_{QSQ'S'} = (\mathbf{I} \otimes \mathbf{\Lambda})\Big(|\Phi_+\rangle_{QS'QS'}\langle\Phi_+|\Big)$$

Purification

Purification:

$$\hat{\Lambda}_{QSQ'S'} = \mathrm{Tr}_E\Big(|\Lambda\rangle_{QSQS'E}\langle\Lambda|\Big)$$

Because the particle is not transferred between paths:

$$|\Lambda\rangle_{QSQ'S'E} = \frac{1}{\sqrt{2}}\Big(|00\rangle_{QQ'}|\Lambda_0\rangle_{SS'E} + |11\rangle_{QQ'}|\Lambda_1\rangle_{SS'E}\Big)$$

Equivalent channel representation:

$$\boldsymbol{\Lambda}(\hat{\varrho})_{Q'S'} = 2d\,\mathrm{Tr}_{QSE}\Big(|\Lambda\rangle_{QSQ'S'E}\langle\Lambda|\hat{\varrho}^T_{QS}\Big)$$

Environment states

$$\widetilde{\hat{\varrho}}'^{(i)}_E = d\,\mathrm{Tr}_{SS'}\Big((\hat{\varrho}_i)^T_S |\Lambda_i\rangle_{SS'E}\langle\Lambda_i| \Big), \qquad i = 0, 1$$

Environment states can be purified

$$\widetilde{\hat{\varrho}}'^{(i)}_E = \mathrm{Tr}_{SS'}\Big(|\mathcal{E}^{(i)}\rangle_{SS'E}\langle\mathcal{E}^{(i)}| \Big)$$

using

$$|\mathcal{E}_i\rangle_{SS'E} = \hat{U}^{(i)}_{SS'}\sqrt{d(\hat{\varrho}_i)^T_S}\,|\Lambda_i\rangle_{SS'E},$$

where $\hat{U}^{(i)}_{SS'}$ are arbitrary unitaries.

Distiguishability bound

Because adding subsystems can only increase distinguishability,

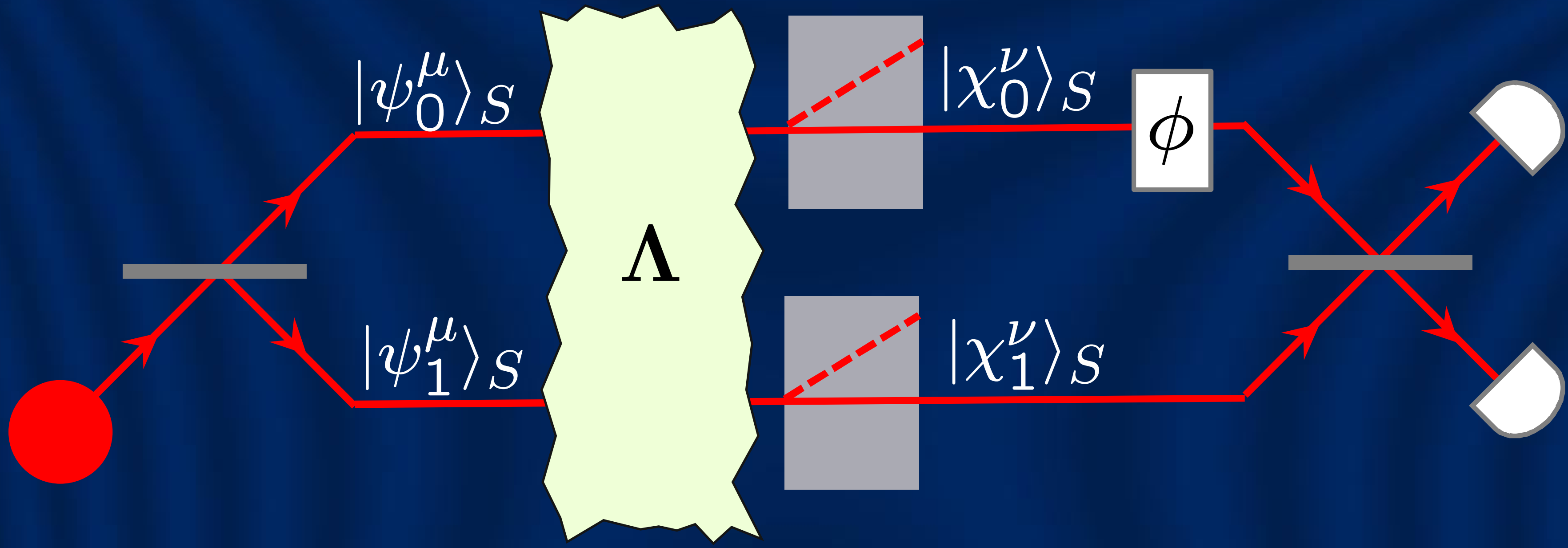
$$D = \frac{1}{2}||\widetilde{\varrho}_E'^{(0)} - \widetilde{\varrho}_E'^{(1)}|| \leq \sqrt{1 - |\langle \mathcal{E}_0 | \mathcal{E}_1 \rangle|^2}$$

The strongest bound is obtained by maximizing over scalar products

$$V_G = \max_{\widehat{U}_{SS'}^{(0)}, \widehat{U}_{SS'}^{(1)}} |\langle \mathcal{E}_0 | \mathcal{E}_1 \rangle|$$

$$= d \Big|\Big| (\mathbf{I} \otimes \mathbf{\Lambda}_{01}) \Big((\hat{I} \otimes \sqrt{\widehat{\varrho}_0}) |\Phi_+\rangle \langle \Phi_+| (\hat{I} \otimes \sqrt{\widehat{\varrho}_1}) \Big) \Big|\Big|$$

Fractional visibility measurement



$$p_\pm^{\mu\nu}(\phi) = \frac{1}{2}[p^{\mu\nu} + \mathrm{Re}(V^{\mu\nu}\mathrm{e}^{\mathrm{i}\phi})]$$

Fractional visibility for preparation μ and filter ν

$$V^{\mu\nu} = \langle\chi_0^\nu|\mathbf{\Lambda}_{01}\left(|\psi_0^\mu\rangle\langle\psi_1^\mu|\right)|\chi_1^\nu\rangle$$

Estimating generalized visibility

For any $\hat{U}^\dagger\hat{U} \leq \hat{I}$ we have $||\hat{A}|| \geq \left|\mathrm{Tr}(\hat{U}\hat{A})\right|$. Consequently,

$$V_G \geq d\left|\mathrm{Tr}\left\{\left[(\sqrt{\hat{\varrho}_1^T}\otimes\hat{I})\hat{U}(\sqrt{\hat{\varrho}_0^T}\otimes\hat{I})\right](\mathbf{I}\otimes\mathbf{\Lambda}_{01})\Big(|\Phi_+\rangle\langle\Phi_+|\Big)\right\}\right|$$

Fractional visibilities can be written as:

$$V^{\mu\nu} = d\mathrm{Tr}\left\{\left[\Big(|\psi_0^\mu\rangle\langle\psi_1^\mu|\Big)^T\otimes|\chi_1^\nu\rangle\langle\chi_0^\nu|\right](\mathbf{I}\otimes\mathbf{\Lambda}_{01})\Big(|\Phi_+\rangle\langle\Phi_+|\Big)\right\}$$

Take a set of complex $\alpha_{\mu\nu}$ satisfying

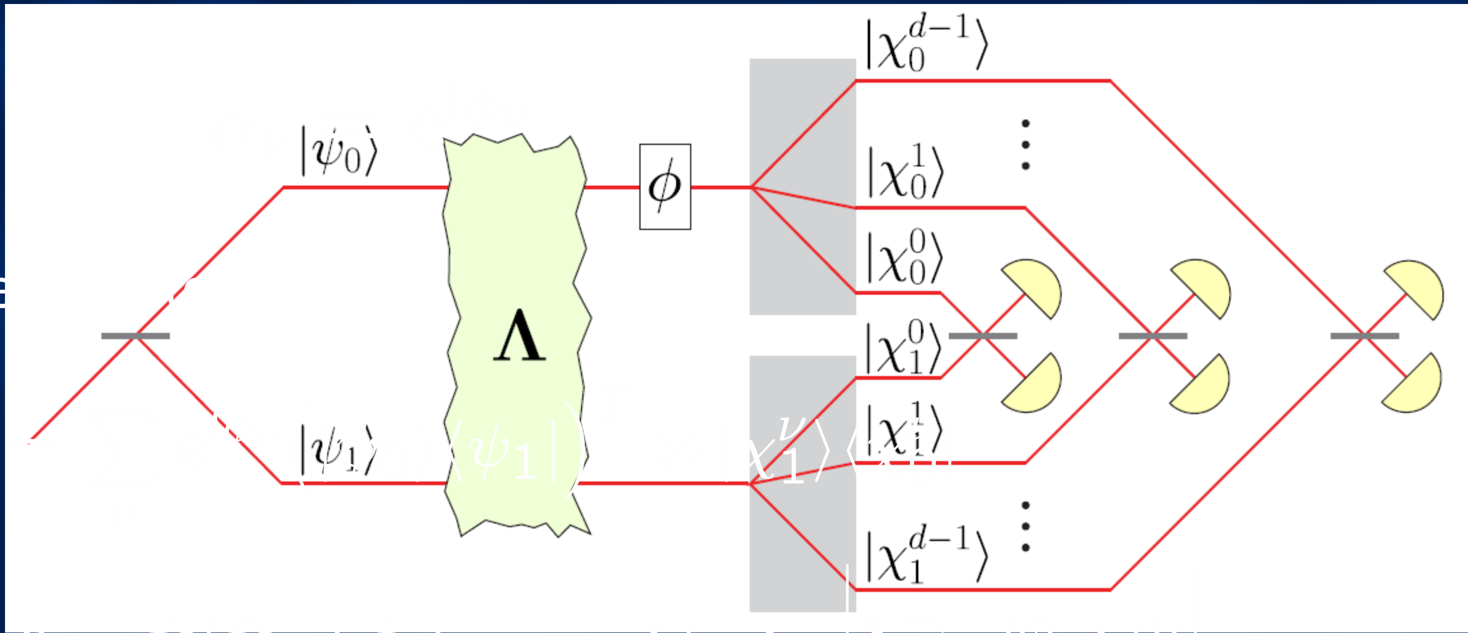
$$\sum_{\mu\nu}\alpha_{\mu\nu}\Big(|\psi_0^\mu\rangle\langle\psi_1^\mu|\Big)^T\otimes|\chi_1^\nu\rangle\langle\chi_0^\nu| = (\sqrt{\hat{\varrho}_1^T}\otimes\hat{I})\hat{U}(\sqrt{\hat{\varrho}_0^T}\otimes\hat{I}),$$

$$\hat{U}^\dagger\hat{U} \leq \hat{I}$$

$$\Longrightarrow \quad V_G \geq \left|\sum_{\mu\nu}\alpha_{\mu\nu}V^{\mu\nu}\right|$$

Projective filtering

Let



The

$\hat{U}$

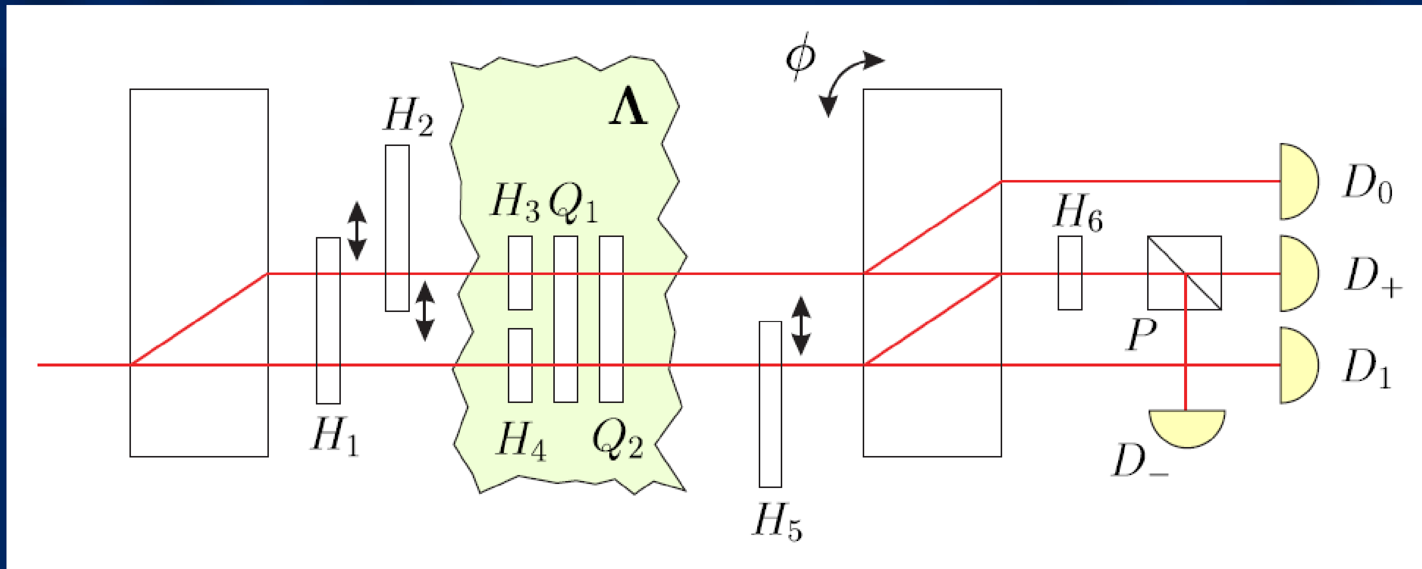
satisfies $\hat{U}^\dagger \hat{U} \leq \hat{I}$, hence $V_G \geq \left| \sum_\nu e^{i\phi_\nu} V^\nu \right|$

Maximization over arbitrary phases ϕ_ν yields

$$V_G \geq \sum_\nu |V^\nu|$$

Experiment

K. Banaszek, P. Horodecki, M. Karpiński, and C. Radzewicz,
Nature Commun. **4**, 2594 (2013)



Preparations $\mu = hh, hv, vh, vv$

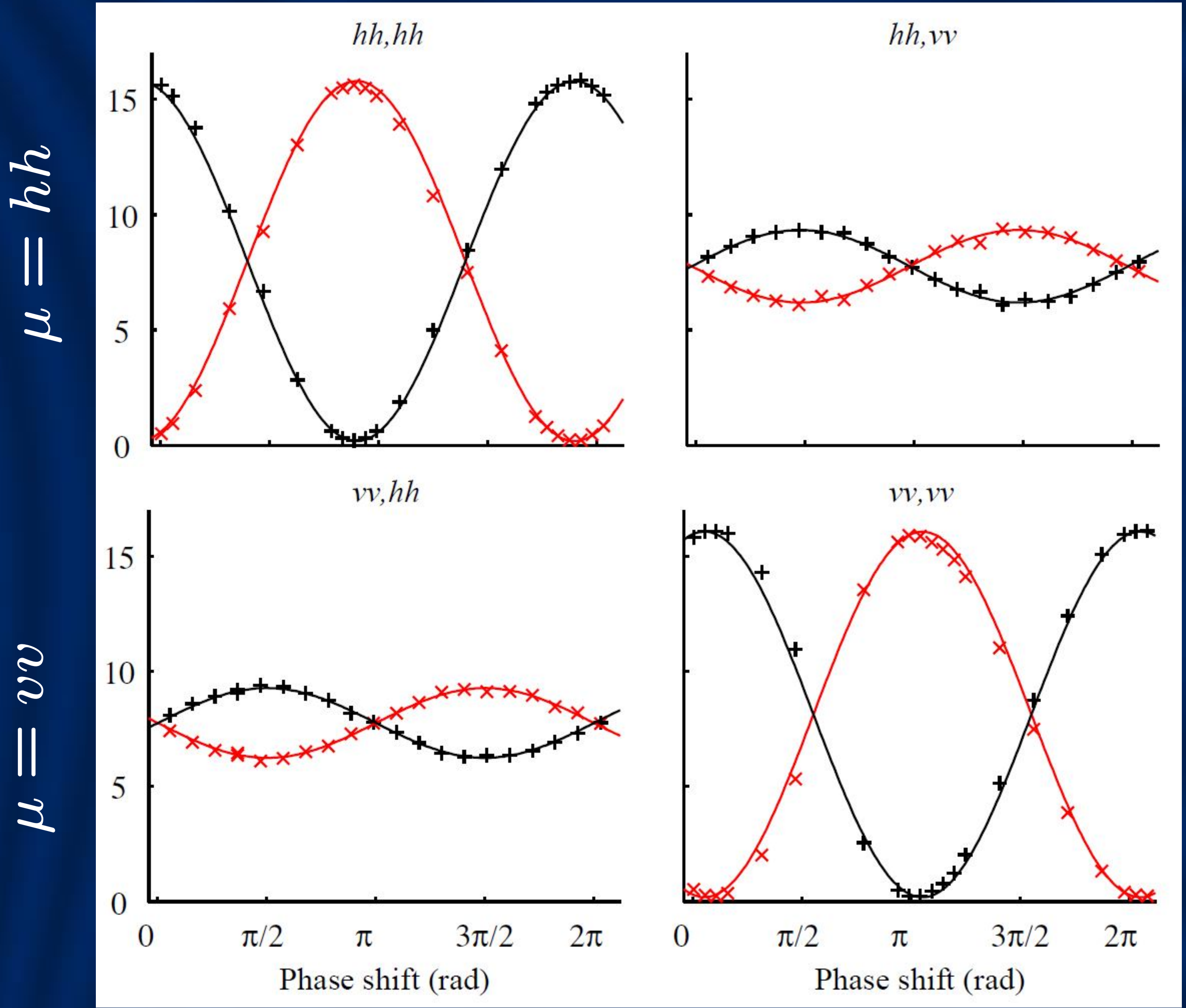
Filters $\nu = hh, hv, vh, vv$

Theoretical detection probability $p^{\mu\nu} = \frac{1}{2}$

$V^{\mu\nu}$

$\mu \backslash \nu$	hh	hv	vh	vv
hh	$\frac{1}{2}$	0	0	0
hv	0	0	$\frac{1}{2}$	0
vh	0	$\frac{1}{2}$	0	0
vv	0	0	0	$\frac{1}{2}$

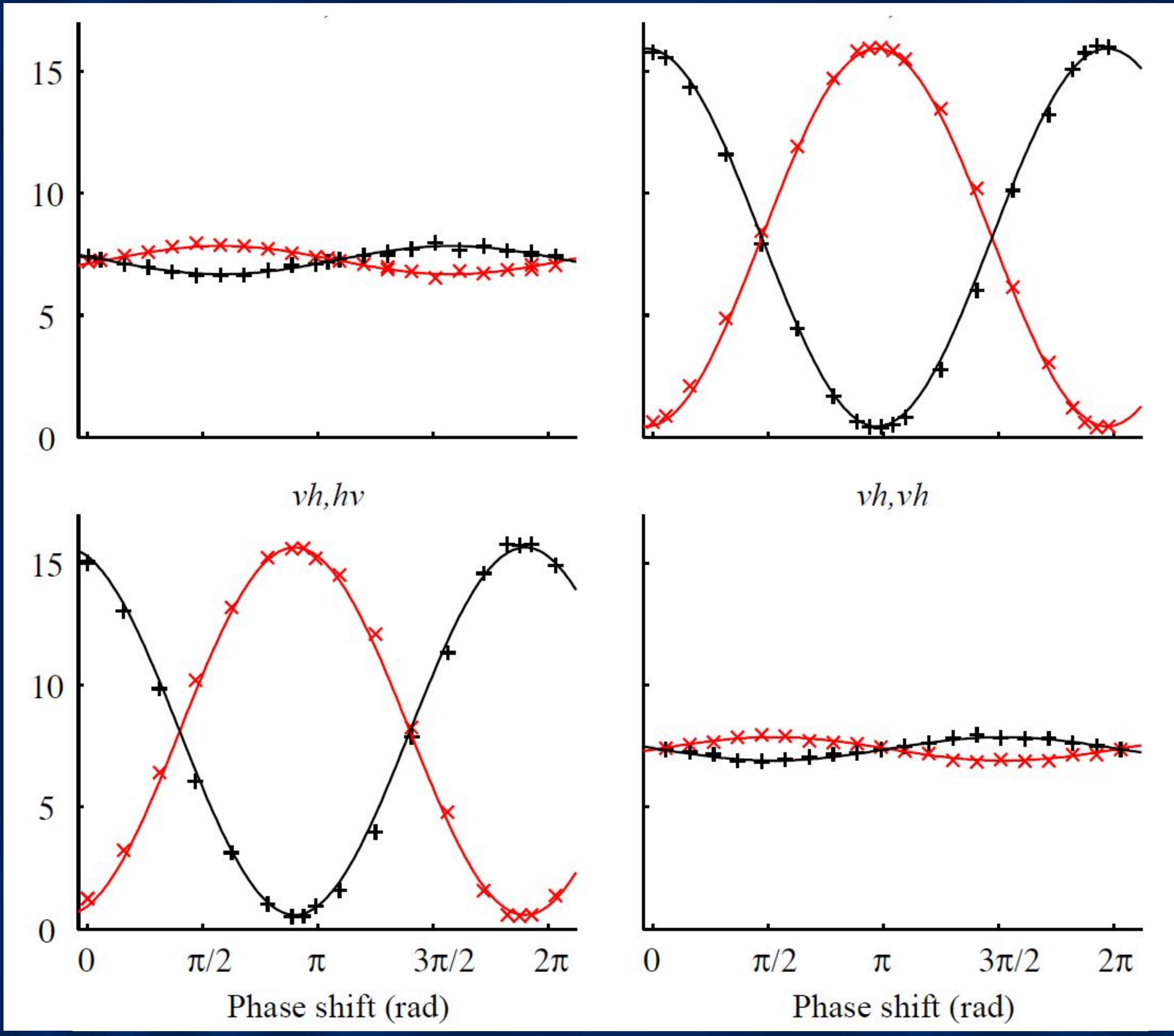
Fractional visibilities



Fractional visibilities cont'd

$\mu = hv$

$\mu = vh$



Mixed input polarization

$$\sum_{\mu\nu} \alpha_{\mu\nu} \Big(|\psi_0^\mu\rangle\langle\psi_1^\mu| \Big)^T \otimes |\chi_1^\nu\rangle\langle\chi_0^\nu| = (\sqrt{\hat{\varrho}_1^T} \otimes \hat{I}) \hat{U} (\sqrt{\hat{\varrho}_0^T} \otimes \hat{I})$$

$$\hat{\varrho}_0 = \hat{\varrho}_1 = \tfrac{1}{2}\hat{I}$$

Take

$$\alpha_{hh,hh} = \tfrac{1}{2} e^{i\theta_1}$$

$$\alpha_{hv,vh} = \tfrac{1}{2} e^{i\theta_2}$$

$$\alpha_{vh,hv} = \tfrac{1}{2} e^{i\theta_3}$$

$$\alpha_{vv,vv} = \tfrac{1}{2} e^{i\theta_4}$$

and zero otherwise

$$V_G \geq \tfrac{1}{2} \Big| e^{i\theta_1} V^{hh,hh} + e^{i\theta_2} V^{hv,vh} + e^{i\theta_3} V^{vh,hv} + e^{i\theta_4} V^{vv,vv} \Big|$$

Maximization over phases yields

$$V_G \geq \tfrac{1}{2} \Big(|V^{hh,hh}| + |V^{hv,vh}| + |V^{vh,hv}| + |V^{vv,vv}| \Big)$$

Experimental data

$\mu\nu$	$p^{\mu\nu}$	$V^{\mu\nu}$	$\mu\nu$	$p^{\mu\nu}$	$V^{\mu\nu}$
hh, hh	0.489	0.476	hh, vv	0.512	0.104
hv, vh	0.513	0.488	hv, hv	0.490	0.039
vh, hv	0.511	0.479	vh, vh	0.490	0.032
vv, vv	0.489	0.478	vv, hh	0.512	0.100

Uncertainty ≤ 0.003

Pure preparation: $V_G \geq 0.580(6)$ at most.

Completely mixed preparation:

$$V_G \geq \frac{1}{2}\Big(|V^{hh,hh}| + |V^{hv,vh}| + |V^{vh,hv}| + |V^{vv,vv}|\Big)$$
$$= 0.960(6)$$

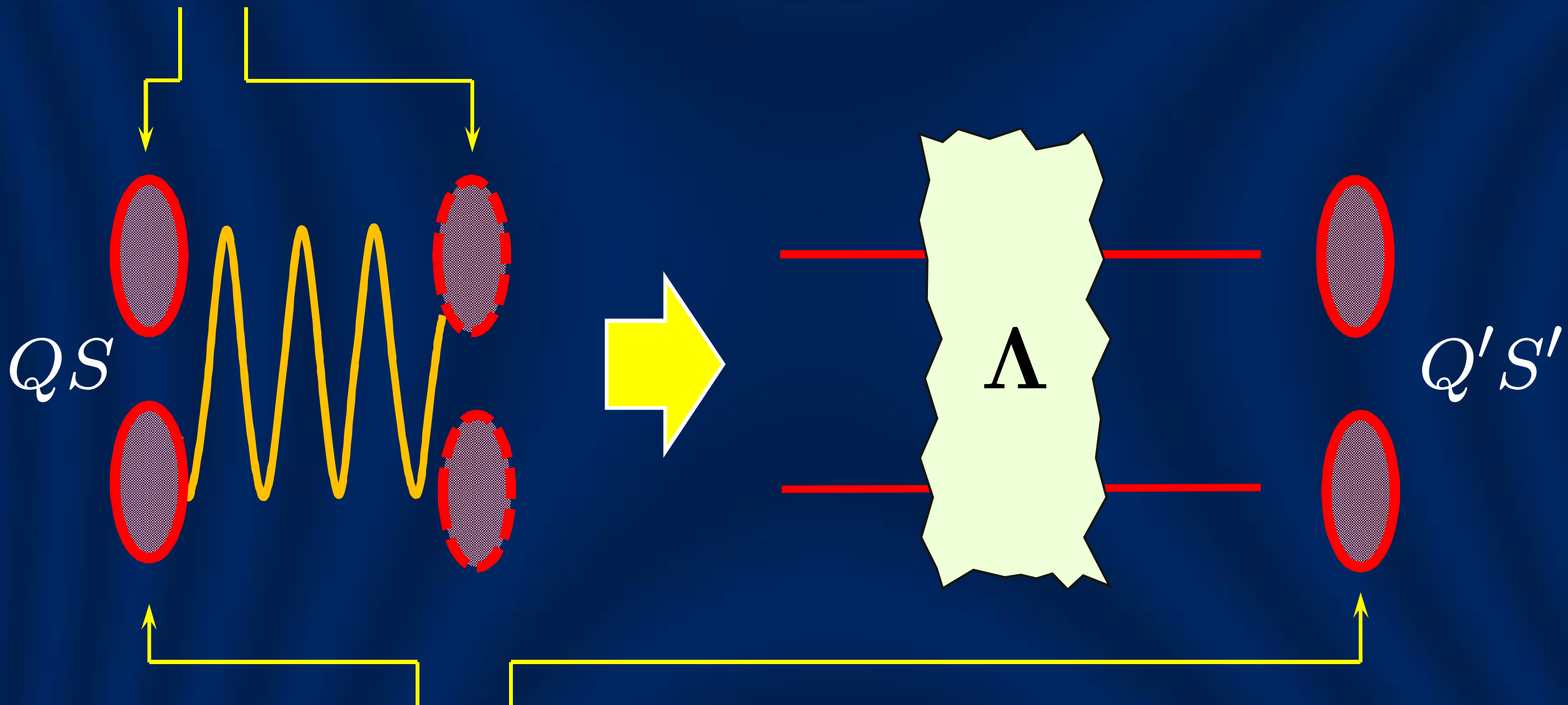
from just four measurements of fractional visibilities!

Conclusions

- Which-way information can be protected by introducing noise in the internal degree of freedom
- Stringent bounds on the amount of which-way information can be obtained from *few* visibility measurements
- Prepare-and-measure quantum cryptography with composite quantum systems: noise may be needed to ensure security
- A non-trivial set of preparations and measurements may be required to verify security

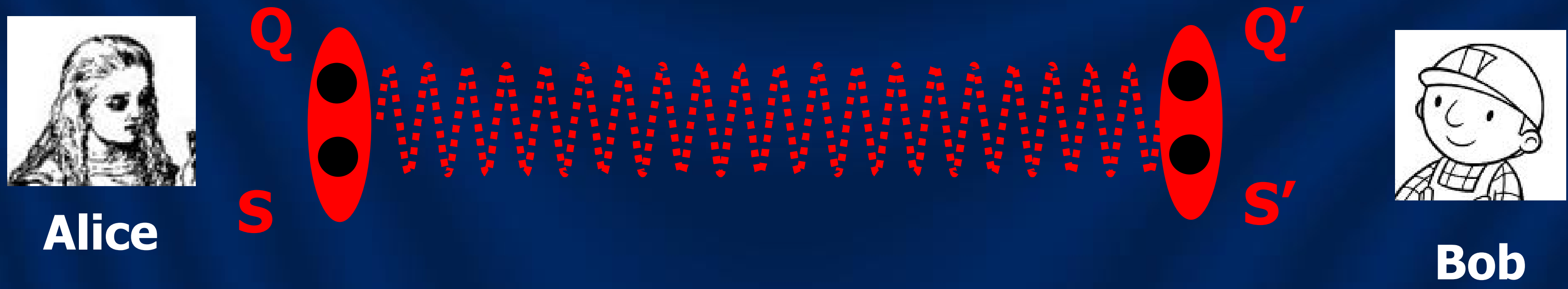
Choi-Jamiołkowski isomorphism

$$|\Phi_+\rangle_{QSQ'S'}$$



$$\hat{\Lambda}_{QSQ'S'} = (\mathbf{I} \otimes \Lambda)\Big(|\Phi_+\rangle_{QS'QS'}\langle\Phi_+|\Big)$$

Bipartite state



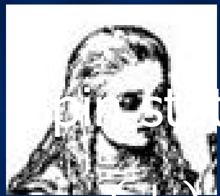
$$\hat{\Lambda}_{QSQ'S'} \;=\; \frac{3}{4}|\Phi_+\rangle_{QQ'}\langle\Phi_+| \otimes \hat{\varrho}^{(+)}_{SS'} + \frac{1}{4}|\Phi_-\rangle_{QQ'}\langle\Phi_-| \otimes \hat{\varrho}^{(-)}_{SS'}$$

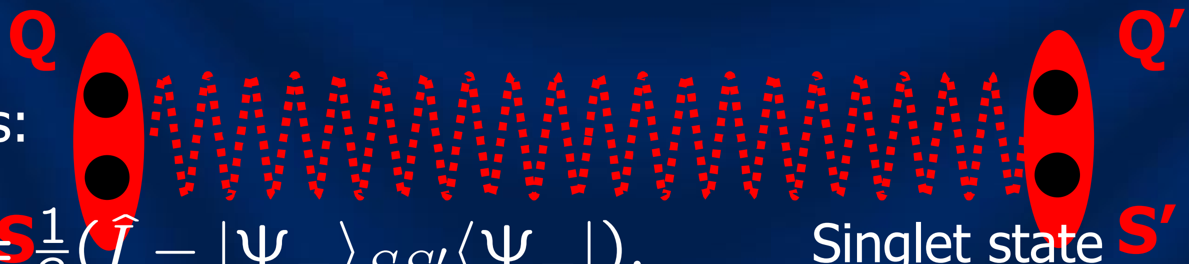
Path (qubit) states:

$$|\Phi_\pm\rangle_{QQ'} = \frac{1}{\sqrt{2}}(|00\rangle_{QQ'} \pm |11\rangle_{QQ'})$$

Measurements in the 0/1 basis
are random and perfectly correlated $\Longrightarrow$ Cryptographic key?

Spin states





$$\hat{\varrho}^{(+)}_{SS'} = \frac{1}{3}(\hat{I} - |\Psi_-\rangle_{SS'}\langle\Psi_-|),$$

$$\hat{\varrho}^{(-)}_{SS'} = |\Psi_-\rangle_{SS'}\langle\Psi_-|$$

Singlet state

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$\hat{\Lambda}_{QSQ'S'} = \frac{3}{4}|\Phi_+\rangle_{QQ'}\langle\Phi_+| \otimes \hat{\varrho}^{(+)}_{SS'} + \frac{1}{4}|\Phi_-\rangle_{QQ'}\langle\Phi_-| \otimes \hat{\varrho}^{(-)}_{SS'}$$

- States $\hat{\varrho}^{(+)}_{SS'}$ and $\hat{\varrho}^{(-)}_{SS'}$ are orthogonal… $\Rightarrow$ Key obtained from qubits QQ' is secure
- …but they cannot be distinguished unambiguously by local operations and classical communication $\Rightarrow$ Distillable entanglement, bounded by log-negativity

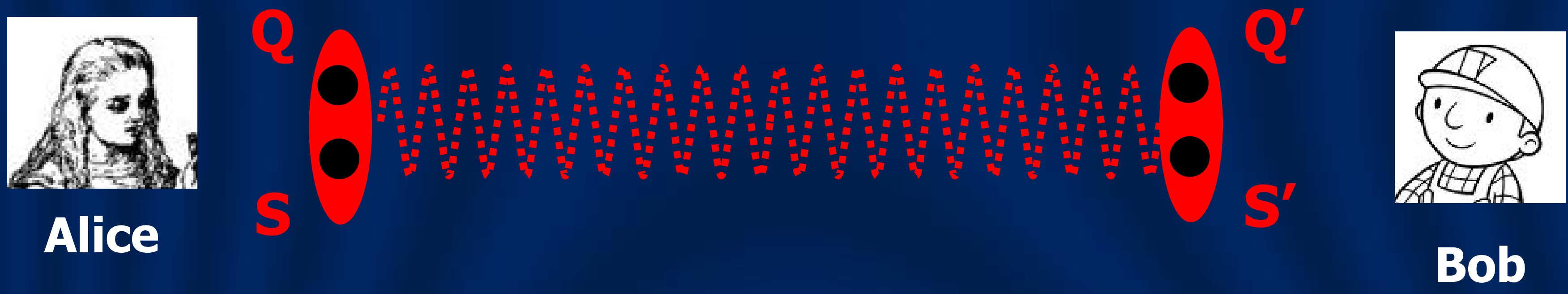
$$E_D \leq \log_2 3 - 1$$

is *strictly* less than the key rate!

Private states

General theory:

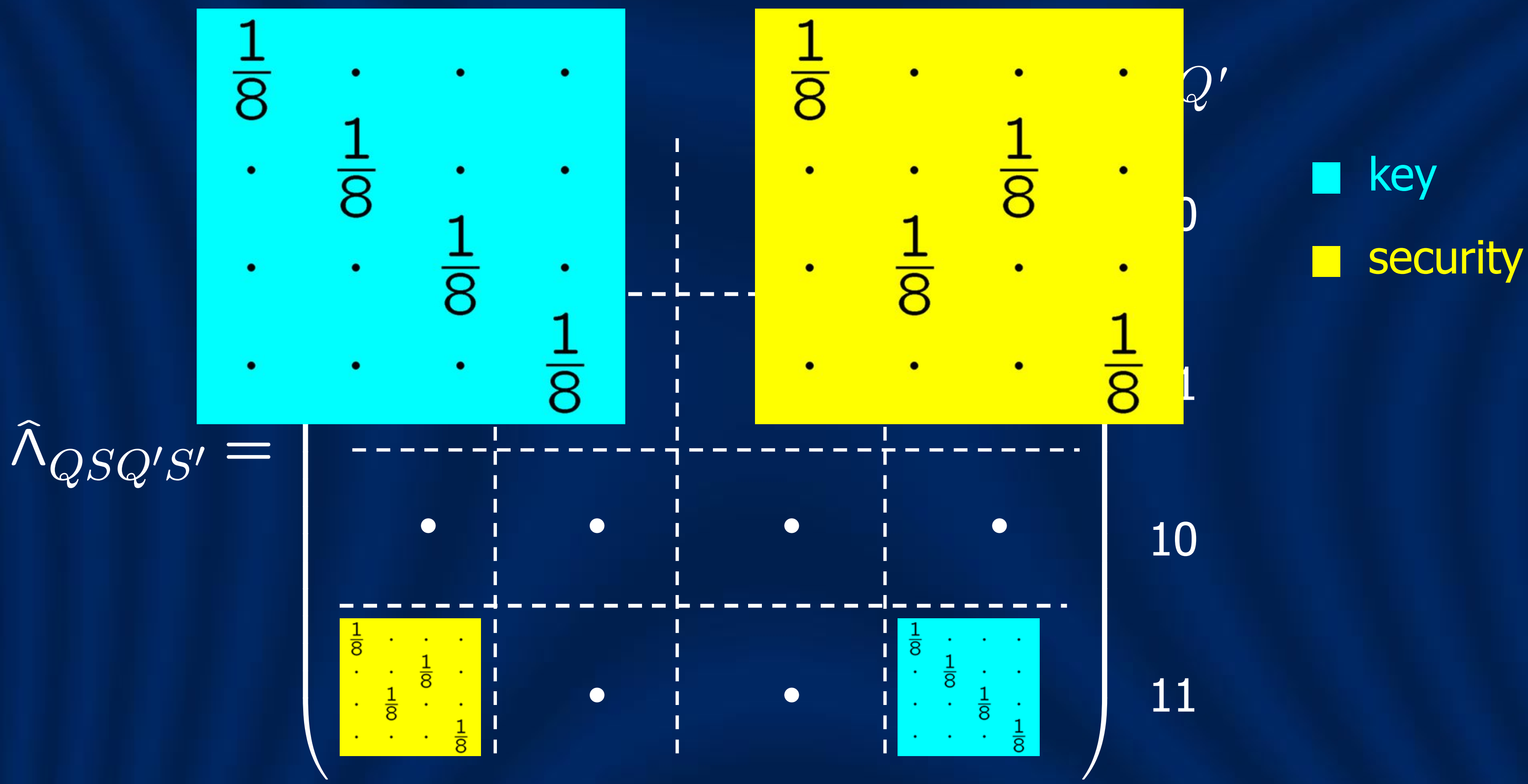
K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim,
Phys. Rev. Lett. **94**, 160502 (2005);
IEEE Trans. Inf. Theory **55**, 1898 (2009)



QQ' - *key* subsystem

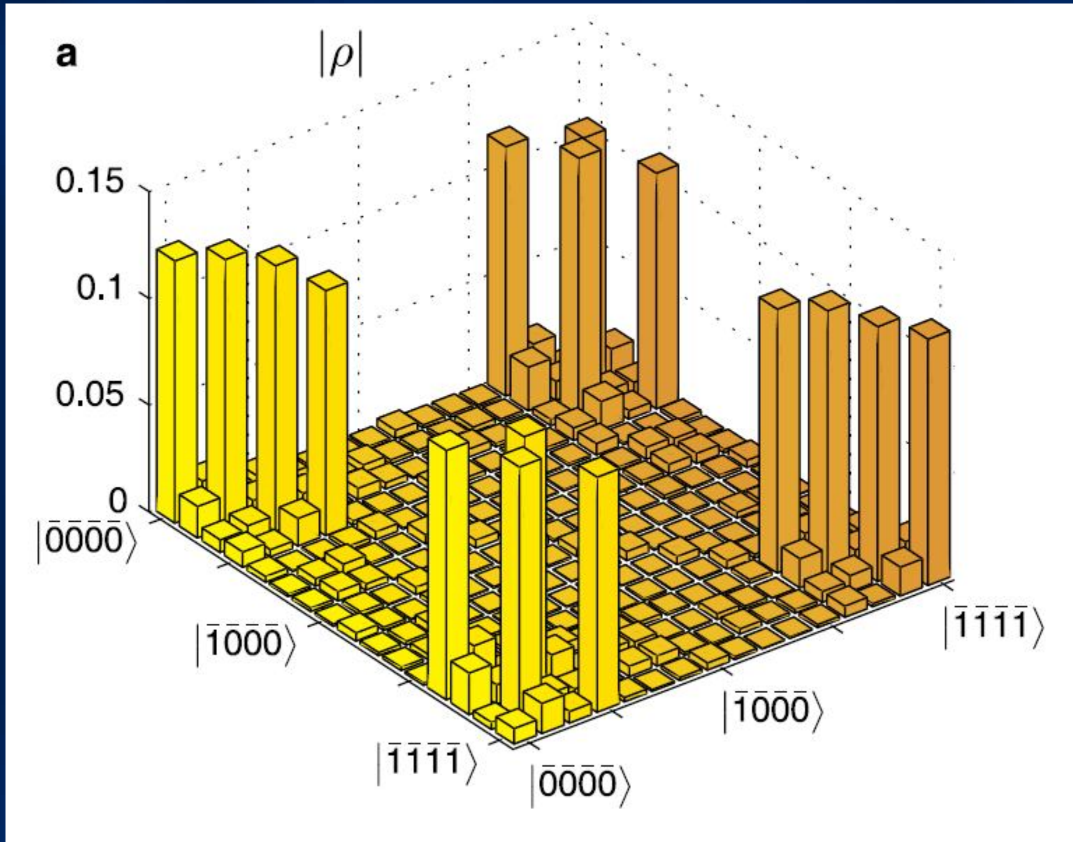
SS' - *shield* subsystem

Density matrix



State reconstruction

K. Dobek. M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, and P. Horodecki, Phys. Rev. Lett. **106**, 030501 (2011)



Distillable entanglement

$$E_D \leq 0.581(4)$$

Key rate (cqq scenario)

$$K \geq 0.690(7)$$