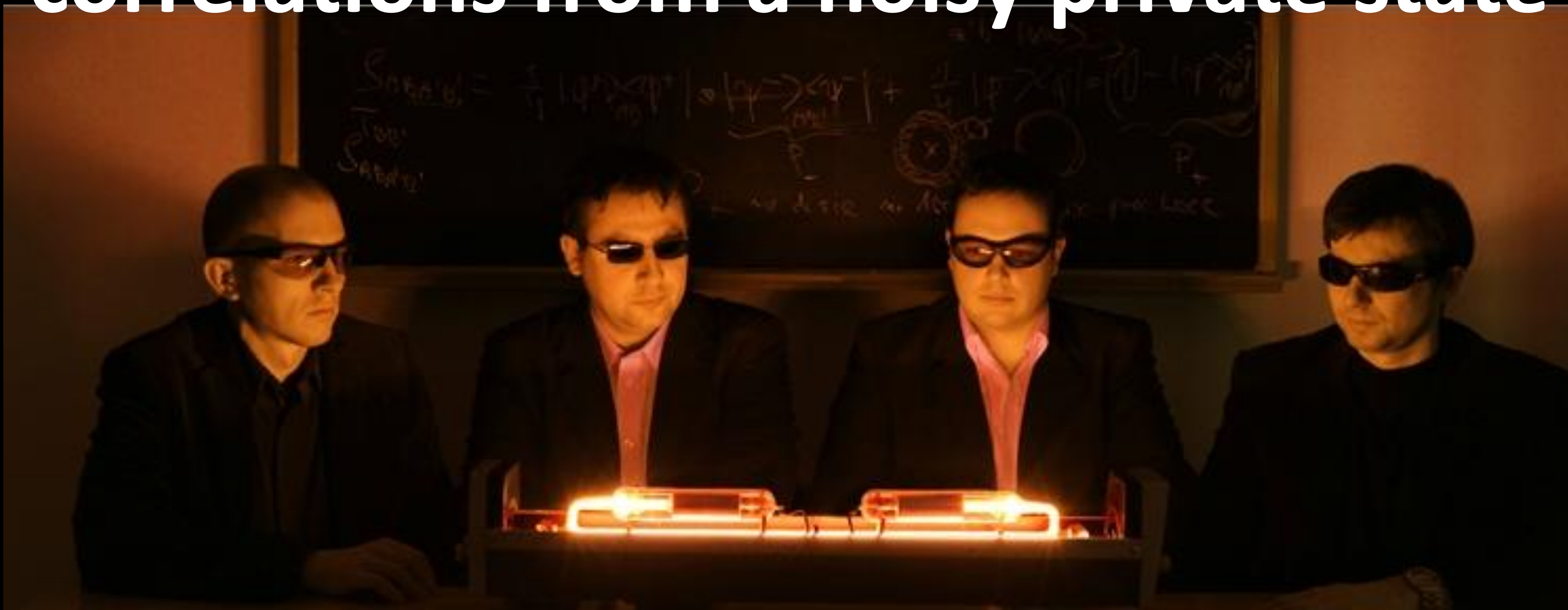
Experimental extraction of secure correlations from a noisy private state



K. Banaszek[1, 2]   P. Horodecki[3]   K. Dobek[2]   M. Karpiński[1]   R. Demkowicz-Dobrzański[1]

[1]*Faculty of Physics, University of Warsaw, Poland*

[2]*Institute of Physics, Nicolaus Copernicus University, Toruń, Poland*

[3]*Faculty of Applied Physics and Mathematics, Technical University of Gdansk, Poland*

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

UNIVERSITAS VARSOVIENSIS

FAMO

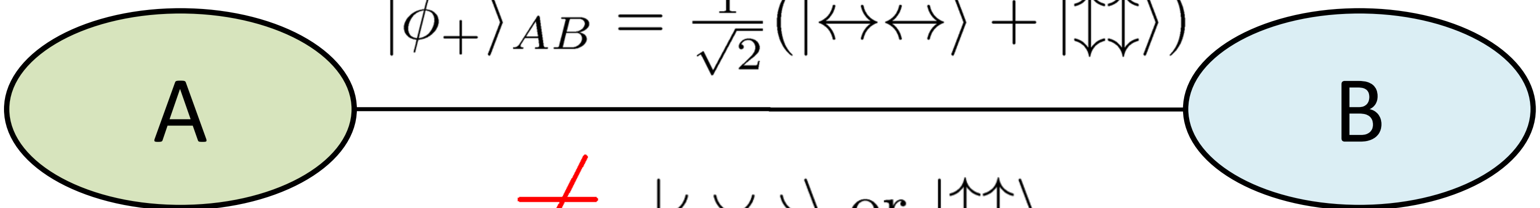
QESSENCE

FNP Foundation for Polish Science TEAM Programme

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

Entangled states

$$|\phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle\right)$$



$$\neq \quad |\leftrightarrow\leftrightarrow\rangle \text{ or } |\updownarrow\updownarrow\rangle$$

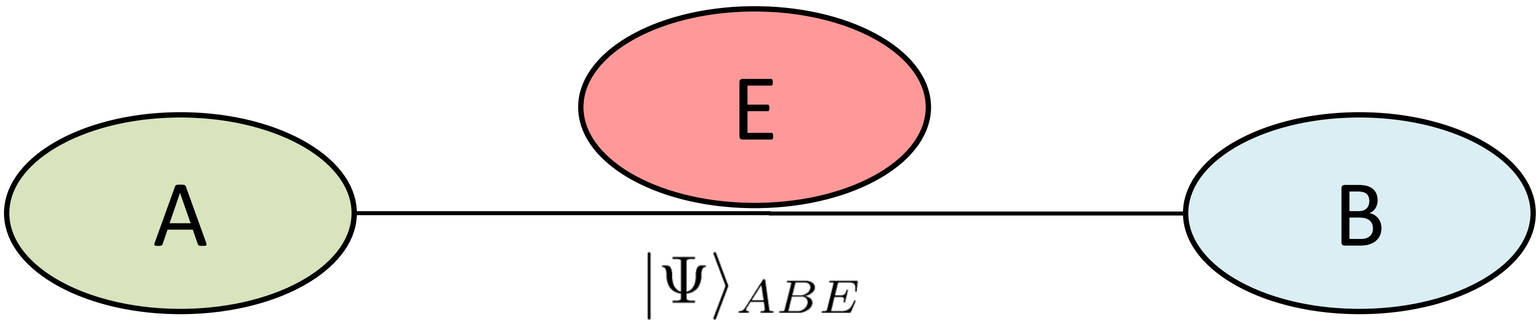
$$\frac{1}{\sqrt{2}}\left(|\swarrow\!\!\!\!\!\nearrow\swarrow\!\!\!\!\!\nearrow\rangle + |\nwarrow\!\!\!\!\!\searrow\nwarrow\!\!\!\!\!\searrow\rangle\right) \quad = \quad \frac{1}{\sqrt{2}}\left(|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle\right)$$

$$|\swarrow\!\!\!\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + |\updownarrow\rangle\right)$$

$$|\nwarrow\!\!\!\!\!\searrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle - |\updownarrow\rangle\right)$$

There is no equivalent model in which photons had fixed polarization states before our measurements (Bell inequalities)

Secure key thanks to entanglement



If A and B make sure that their state is of the form

$$|\phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle)$$

then

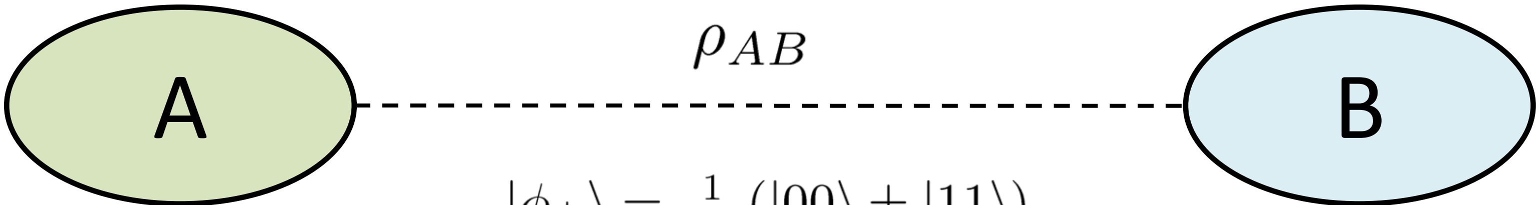
$$|\Phi\rangle_{ABE} = |\phi_+\rangle_{AB} \otimes |\varphi\rangle_E$$

E has no information on their measurement results

$$|0\rangle := |\leftrightarrow\rangle \qquad |1\rangle := |\updownarrow\rangle$$

A and B share one secret bit

Noisy entanglement



$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

Statistical mixture

$$\rho_{AB} = \frac{1}{2}|\phi_+\rangle\langle\phi_+| + \frac{1}{2}|\phi_-\rangle\langle\phi_-| = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$$

Correlations are no longer secure

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \qquad \rho_{AB} = \mathrm{Tr}_E(|\Phi\rangle\langle\Phi|)$$

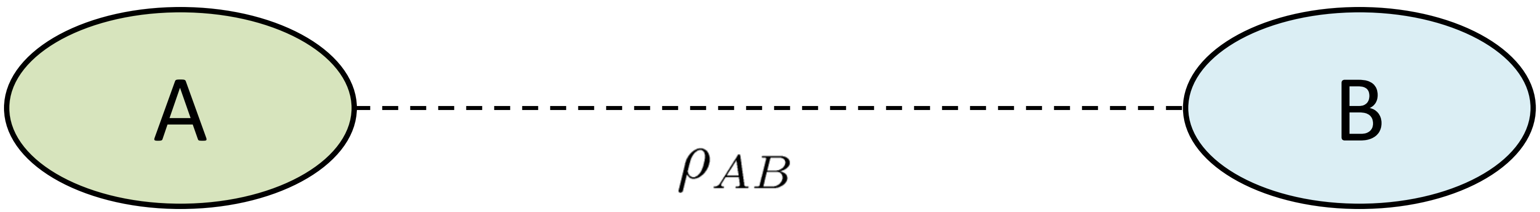
$$|\phi_+\rangle\langle\phi_+| = \frac{1}{2}\begin{pmatrix} \boxed{1} & \cdot & \cdot & \boxed{1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \boxed{1} & \cdot & \cdot & \boxed{1} \end{pmatrix} \longrightarrow \rho_{AB} = \frac{1}{2}\begin{pmatrix} \boxed{1} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \boxed{1} \end{pmatrix}$$

Security

Correlations

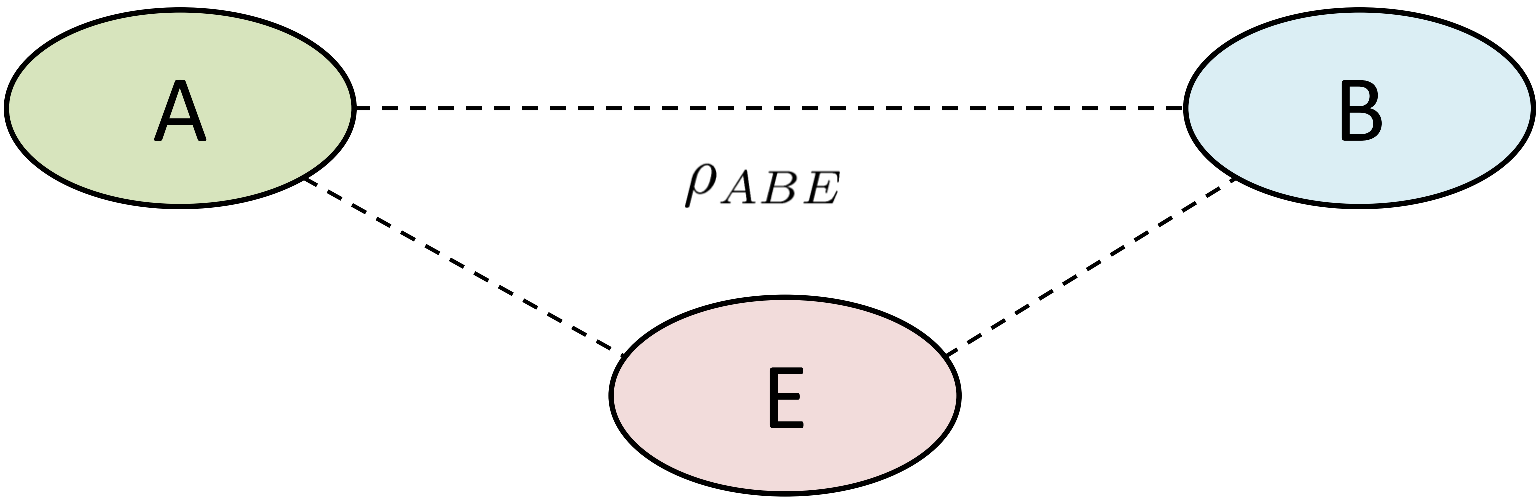
Entanglement distillation

Usually we deal we noisy entangled states

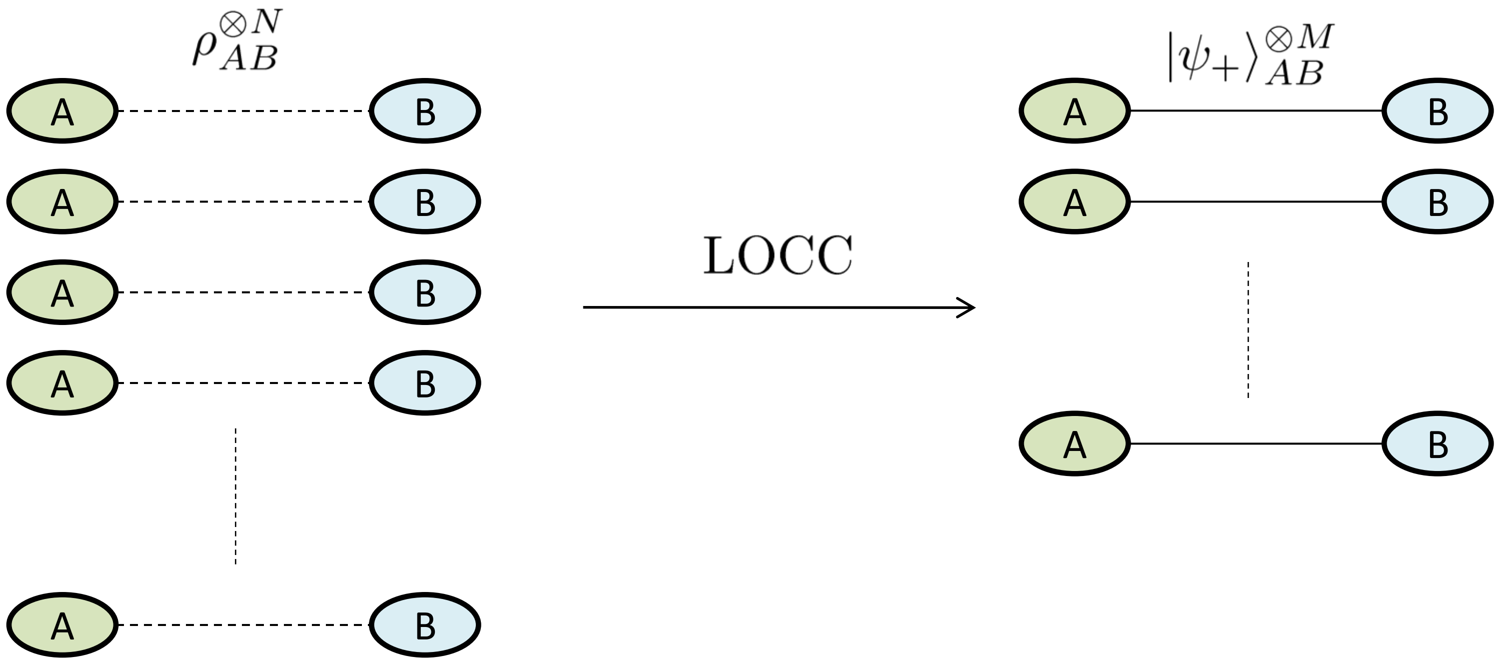


Entanglement distillation

Usually we deal we noisy entangled states



Entanglement distillation



Distillable entanglement $$E_D = \lim_{N\to\infty}\left(\frac{M(N)}{N}\right)$$

Secure key length $$K \geq E_D$$

D. Deutsch et al. PRL 77, 2318 (1996)

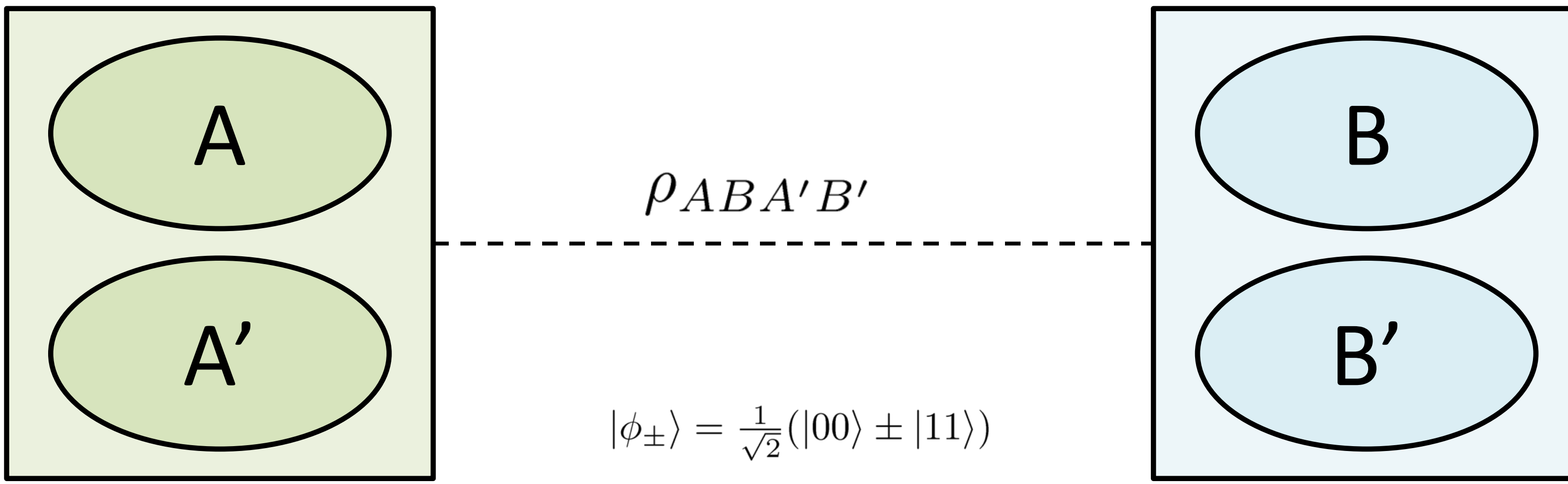
$$K \gneq E_D?$$

Key distillation ≠ Entanglement distillation

e.g. There exist bound entangled states (E_D=0) with K>0

K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim PRL 94, 160502 (2005)

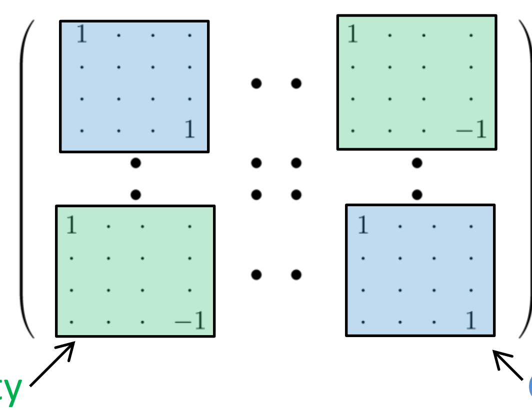
4 qubit state with $K = E_D$



$$\rho_{ABA'B'} = \frac{1}{2}\left(|\phi_+\rangle\langle\phi_+| \otimes |00\rangle\langle 00| + |\phi_-\rangle\langle\phi_-| \otimes |11\rangle\langle 11|\right)$$

Local measurement on A’, B’ distinguishes between two entagled states in A and B

$$\rho_{ABA'B'} = \frac{1}{4}$$

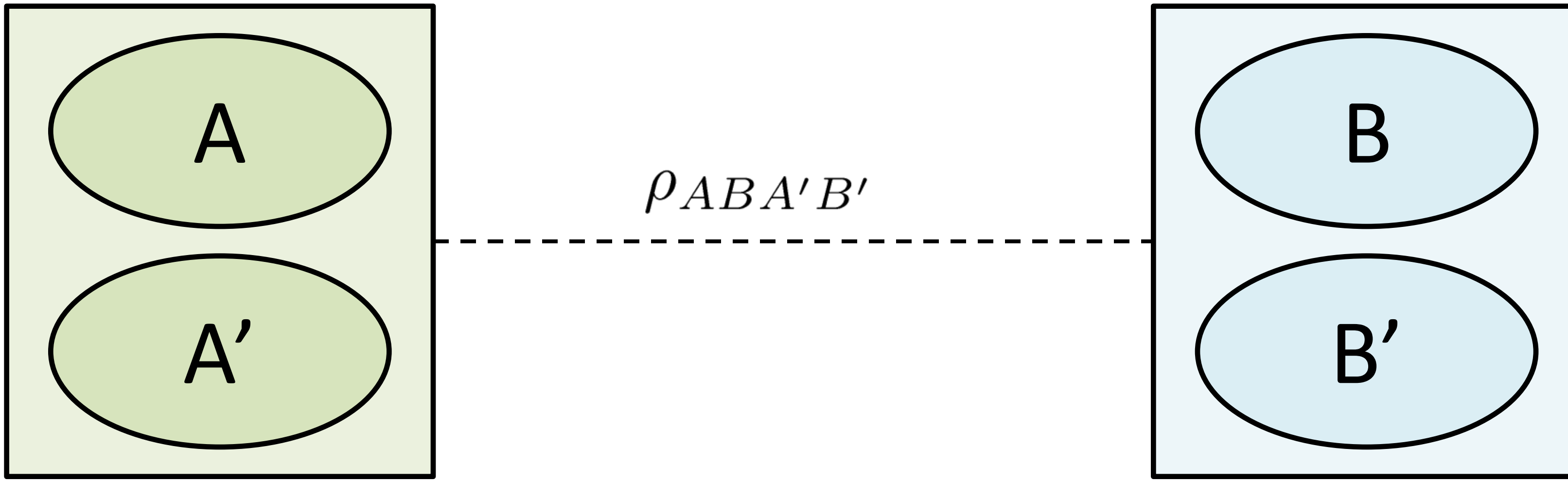


$$E_D = 1$$

$$\frac{1}{4}\left\| \begin{matrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 \end{matrix} \right\|_1 = \frac{1}{2}$$

$$K = 1$$

4 qubit state with $K > E_D$



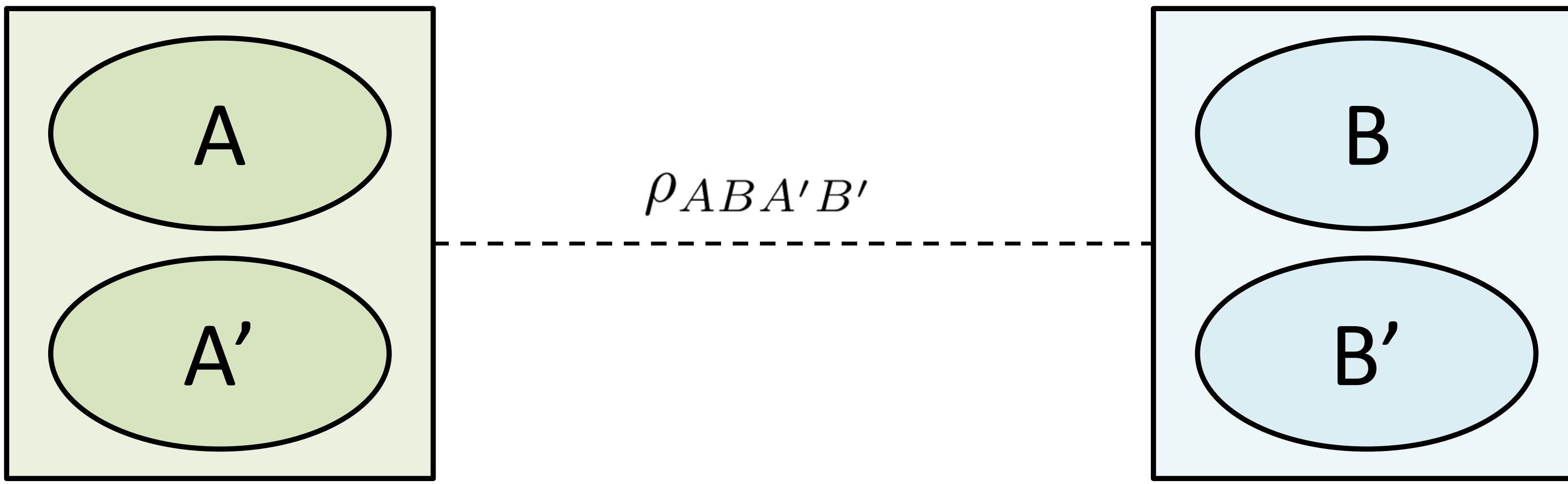
$$\rho_{ABA'B'} = \frac{1}{4}\left(|\phi_+\rangle\langle\phi_+| \otimes P_+ + |\phi_-\rangle\langle\phi_-| \otimes |\psi_-\rangle\langle\psi_-|\right)$$

$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ $P_+ = |\phi_+\rangle\langle\phi_+| + |\phi_-\rangle\langle\phi_-| + |\psi_+\rangle\langle\psi_+|$

No local measurement distinguishing between P_+ and $|\psi_-\rangle\langle\psi_-|$

$E_D < 1$ $E_D \leq \log_2 \mathrm{Tr}|\rho^{T_{BB'}}| \approx 0.585$

4 qubit state with $K > E_D$



$$\rho_{ABA'B'} = \frac{1}{4}\left(|\phi_+\rangle\langle\phi_+| \otimes P_+ + |\phi_-\rangle\langle\phi_-| \otimes |\psi_-\rangle\langle\psi_-|\right)$$

$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ $\quad |\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ $\quad P_+ = |\phi_+\rangle\langle\phi_+| + |\phi_-\rangle\langle\phi_-| + |\psi_+\rangle\langle\psi_+|$

$$\rho_{ABA'B'} = \frac{1}{8}\begin{pmatrix} \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} & \cdots & \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \\ \vdots & \vdots\vdots & \vdots \\ \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} & \cdots & \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \end{pmatrix}$$

Security Correlations

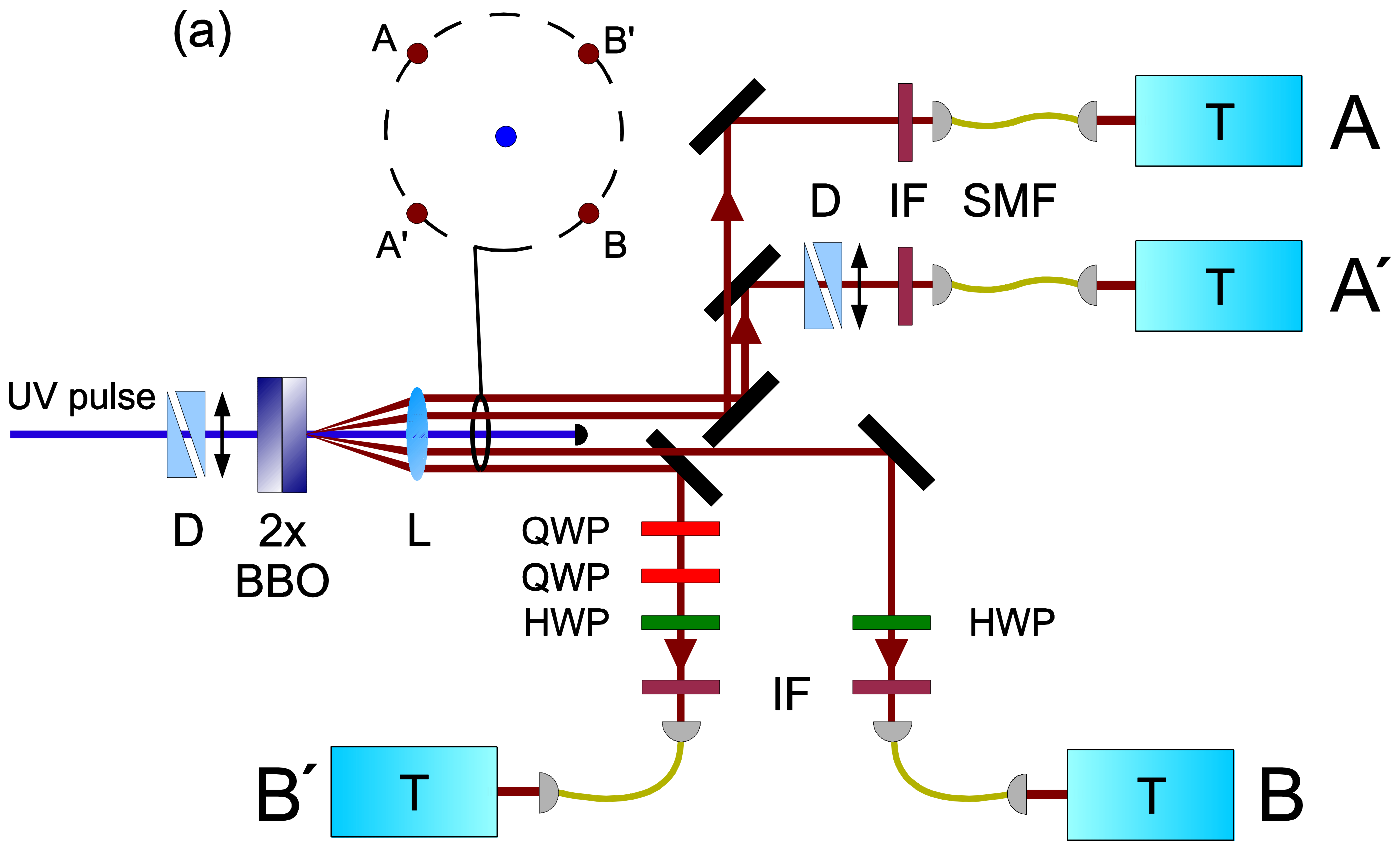
$$E_D \leq 0.585$$

$$\frac{1}{8}\left\| \begin{matrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{matrix} \right\| = \frac{1}{2}$$

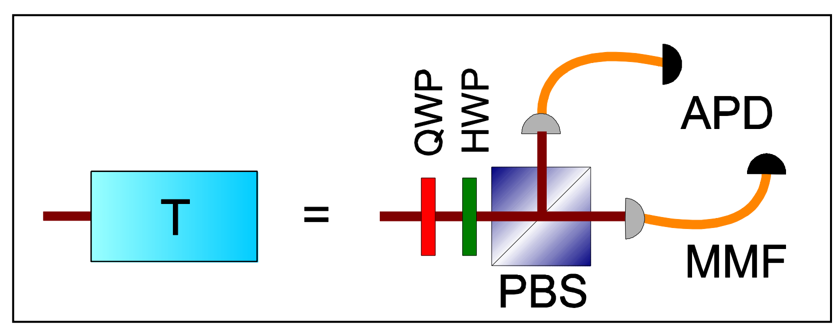
$$K = 1$$

Experimental setup

(more in the next talk by K. Dobek...)



4 photon coincidences 2/s



State reconstruction

3 x 3 x 3 x 3 = 81 different measurement basis $\sigma_i \otimes \sigma_j \otimes \sigma_k \otimes \sigma_l$

In each basis 16 different coincidence patterns

$\sim 5 \cdot 10^5$ **events grouped in 81 x 16 =1296 types**

$n_{b,m} \quad (b = 1 \ldots 81, m = 1 \ldots 16) \qquad N = \sum_{b,m} n_{b,m} = 5 \cdot 10^5$

$$\Pi_{b,m} \Big\downarrow \quad p_{b,m} = \mathrm{Tr}(\rho \Pi_{b,m})$$

$$\rho \pm \delta\rho$$

$$K \pm \delta K > E_D \pm \delta E_D$$

Total uncertainty = state preparation uncertainty + mesurement implementation uncertainty + reconstruction uncertainty

Max likelihood with positive semi-definiteness condition

$\rho = T^\dagger T \qquad T = $ ◥ $\qquad t_k \quad k = 1 \ldots d^2$

$p(i|\rho) = Tr(\Pi_i \rho) \qquad n_i$ - number of events

$\mathcal{L} = \prod_i p(i|\rho)^{n_i}$ - likelihood function

$$\boxed{\max_T \log \mathcal{L}(T^\dagger T) \qquad \Sigma_{ij}^{-1} = \left(\frac{\partial^2}{\partial t_i \partial t_j} \mathcal{L} \right)}$$

Pros: - positive semi-definiteness guaranteed

Cons: - unpractical for large number of qubits (>6)
- uncertainty may be underestimated for small samples
- for small samples tendency to return purer states

K. Banaszek, G. M. D'Ariano, M. Paris, M. Sacchi , PRA 61, 010304 (1999)

Bayesian approach

$p(\rho)$ - apriori distribution $\quad p(i|\rho) = Tr(\Pi_i \rho)$

$$p(\rho|\{i_1, \ldots, i_N\}) \propto p(\{i_1, \ldots, i_N\}|\rho)p(\rho)$$

$$\boxed{\tilde{\rho} = \int d\rho \; \rho p(\rho|\{i_1, \ldots, i_N\})}$$

Pros: - clear statistical interpretation
- uncertainty of reconstruction appearing naturally
- no need for numerical optimization

Cons: - difficult numerically due to the need for normalization of aposteriori sitribution
- choice of the apriori distribution

Bayesian approach + gaussian approximation

$\rho = \sum_k x_k \sigma_k$ $\qquad \sigma_k$ - hermitian basis $\qquad k = 1 \dots d^2$

a priori distribution $p(\vec{x}) \propto \exp\left[-\frac{1}{2}(\vec{x}-\vec{x}_0)^T \Sigma^{-1} (\vec{x}-\vec{x}_0)\right]$

$$p(i|\vec{x}) = \mathrm{Tr}(\rho \Pi_i) = \mathrm{Tr}(\textstyle\sum_k x_k \sigma_k \Pi_i) = (A\vec{x})_i \qquad A_{ik} = \mathrm{Tr}\sigma_k \Pi_i$$

$$\begin{tikzcd} \boxed{\vec{x}} \arrow[r, shift left, "\vec{p} = A\vec{x}"] & \boxed{\vec{p}} \arrow[l, shift left, red] \arrow[r, shift left, "\mathrm{Mtn}(N,\vec{p})"] & \boxed{\vec{n}} \arrow[l, shift left, red] \end{tikzcd}$$

$$p_{\mathrm{Mtn}(N,\vec{p})}(\vec{n}) = \frac{N!}{n_1! \dots n_m} p_1^{n_1} \cdot \dots \cdot p_m^{n_m}$$

K. Audenaert, S. Scheel, New J. Phys. 11, 023028 (2009)

$$\begin{tikzcd}
\boxed{\vec{x}} \arrow[r, shift left, "\vec{p} = A\vec{x}"] & \boxed{\vec{p}} \arrow[l, shift left] \arrow[r, shift left, "\mathrm{Mtn}(N,\vec{p})"] & \boxed{\vec{n}} \arrow[l, shift left, "\mathrm{D}(N,\vec{n})"]
\end{tikzcd}$$

Gaussian approximation

$$p(\vec{x}|\vec{n}) \propto \exp\left[-\tfrac{1}{2}(A\vec{x} - \langle\vec{p}\rangle)^T \Sigma^{(D)-1}(A\vec{x} - \langle\vec{p}\rangle)\right] \exp\left[-\tfrac{1}{2}(\vec{x} - \vec{x}_0)^T \Sigma^{-1}(\vec{x} - \vec{x}_0)\right]$$

A posteriori mean and covariance matrix

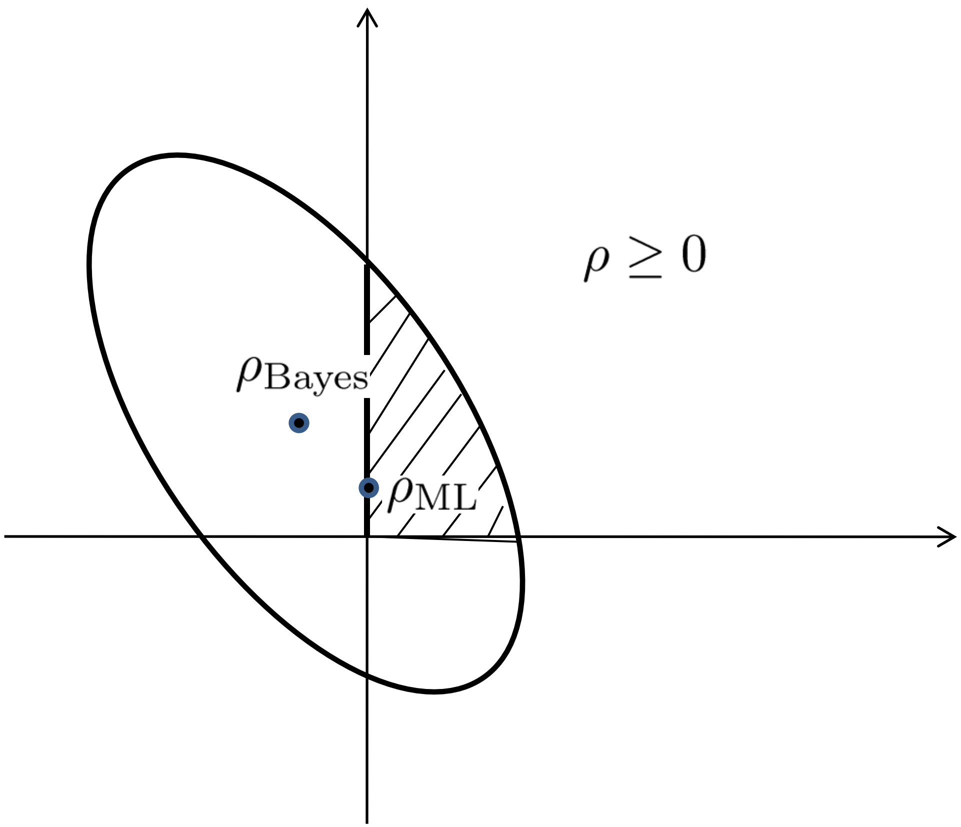
$$\boxed{\Sigma'^{-1} = A^{-1}\Sigma^{(D)-1}A + \Sigma^{-1} \qquad \vec{x}' = A^{-1}\langle\vec{p}\,\rangle - \Sigma'\Sigma^{-1}(\vec{x}_0 - A^{-1}\langle\vec{p}\rangle)}$$

Pros:
- easily obtained uncertainties of reconstruction
- much faster than Max-Likelihood(20s instead of 30min)

Cons:
- no guarantee for positive semi-defniniteness
- choice of a priori distribution

What about positivity?

We need positivity, otherwise we cannot calculate *E_D* nor *K*



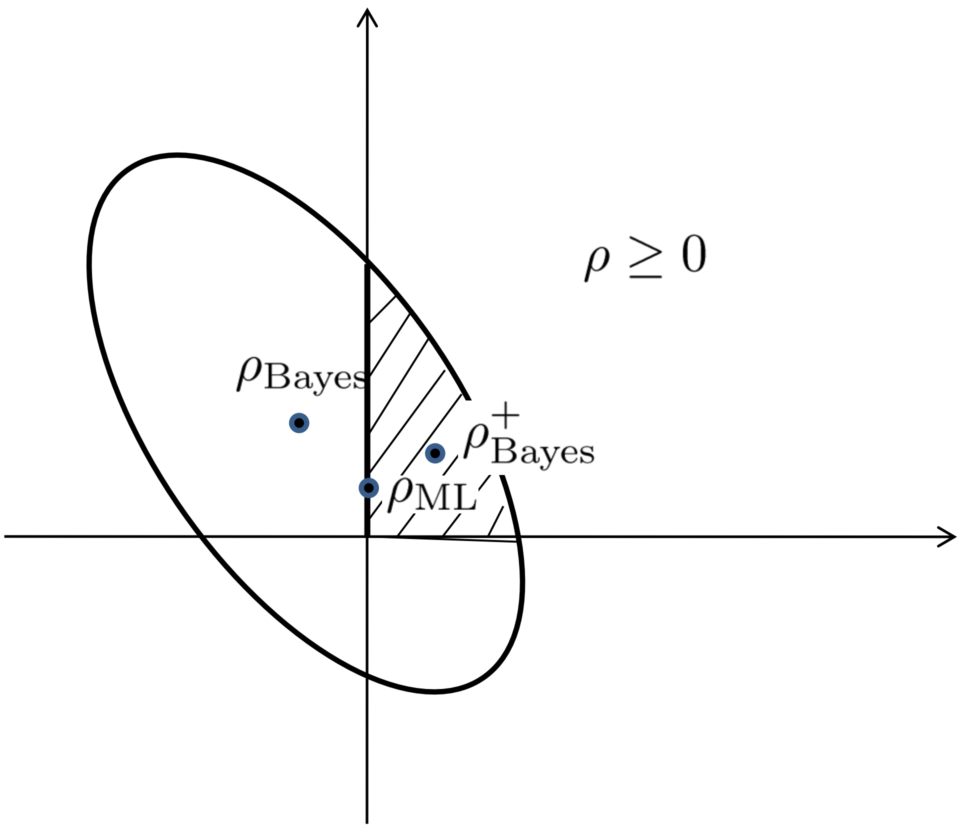
$$p_{\mathrm{trunc}}(\rho) = \begin{cases} p_{\mathrm{Bayes}}(\rho), & \rho \geq 0 \\ 0 & \end{cases}$$

Slice sampling (in d^2 dimensions)

Check whether ρ_{ML} is within the e.g. 95% confidence interval

What about positivity?

We need positivity, otherwise we cannot calculate E_D nor K



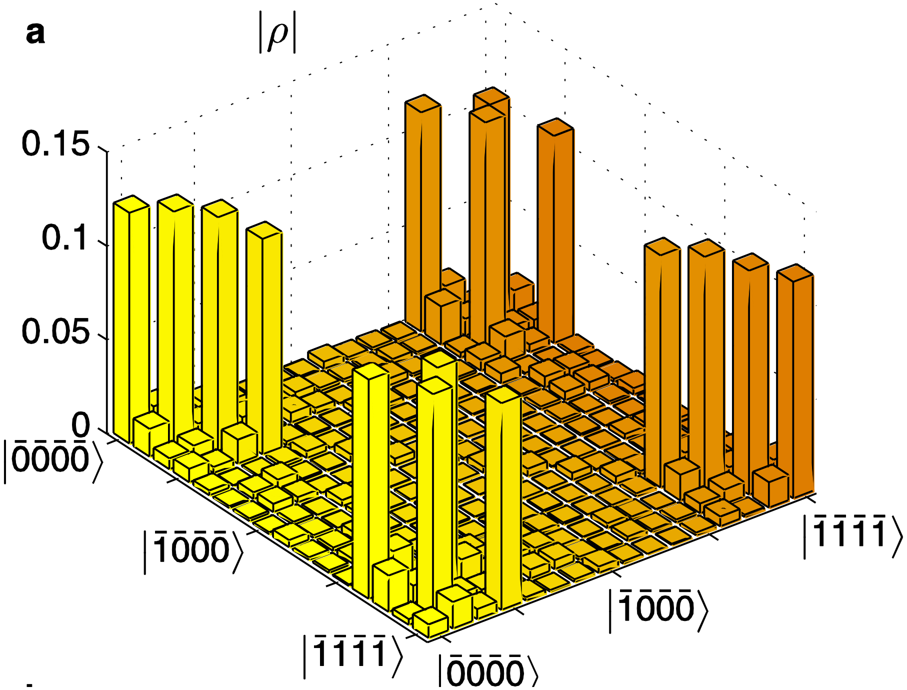
$$p_{\mathrm{trunc}}(\rho) = \begin{cases} p_{\mathrm{Bayes}}(\rho), & \rho \geq 0 \\ 0 \end{cases}$$

Slice sampling (in d^2 dimensions)

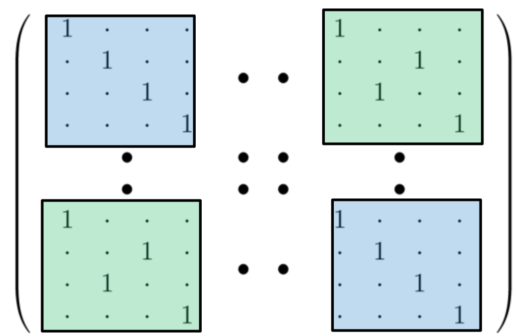
We get a representative sample of density matrices

Check whether ρ_{ML} is within the e.g. 95% confidence interval)

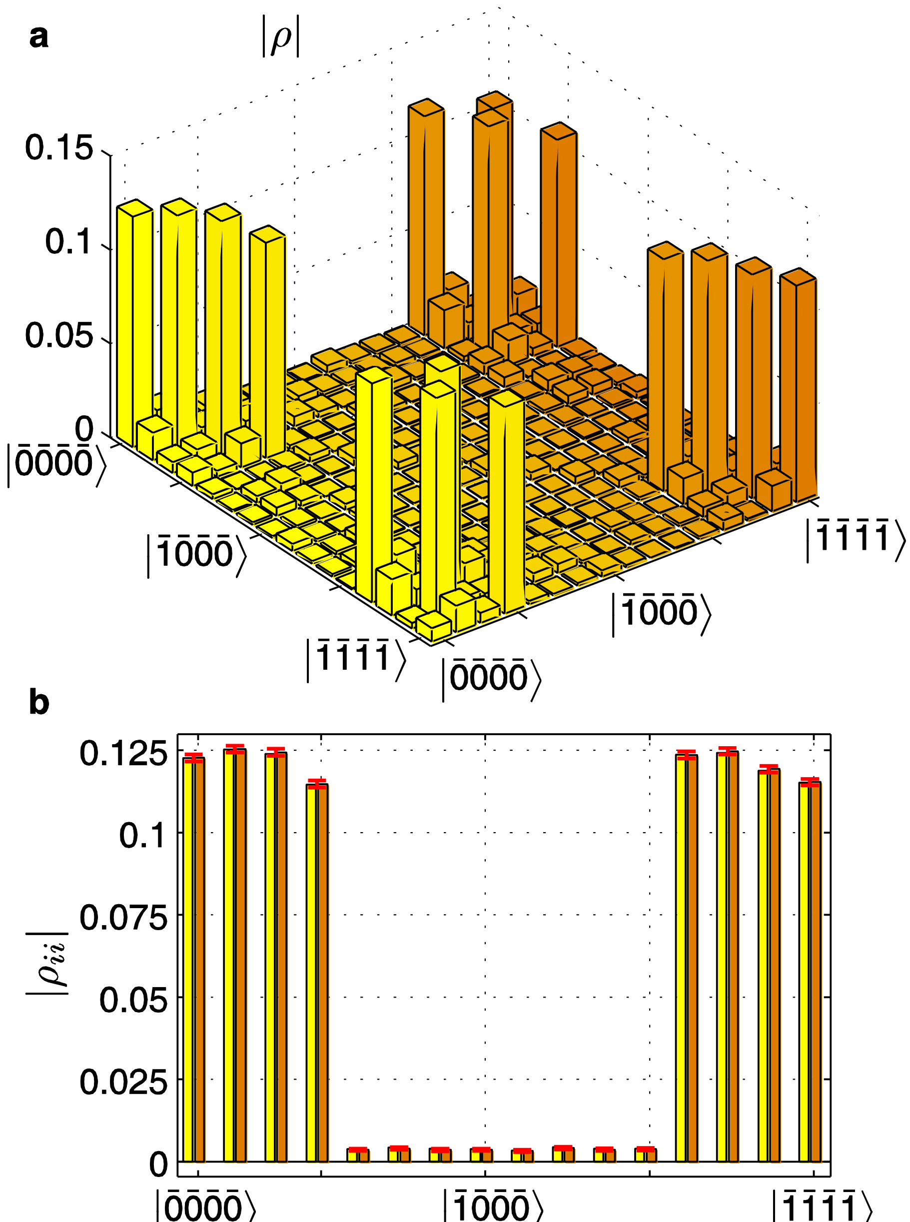
Recnostruction



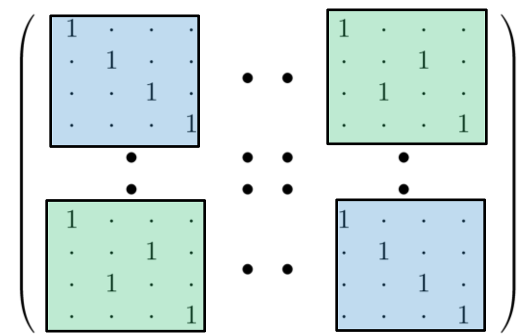
$$F = 0.9724(7)$$



Reconstruction



$$F = 0.9724(7)$$



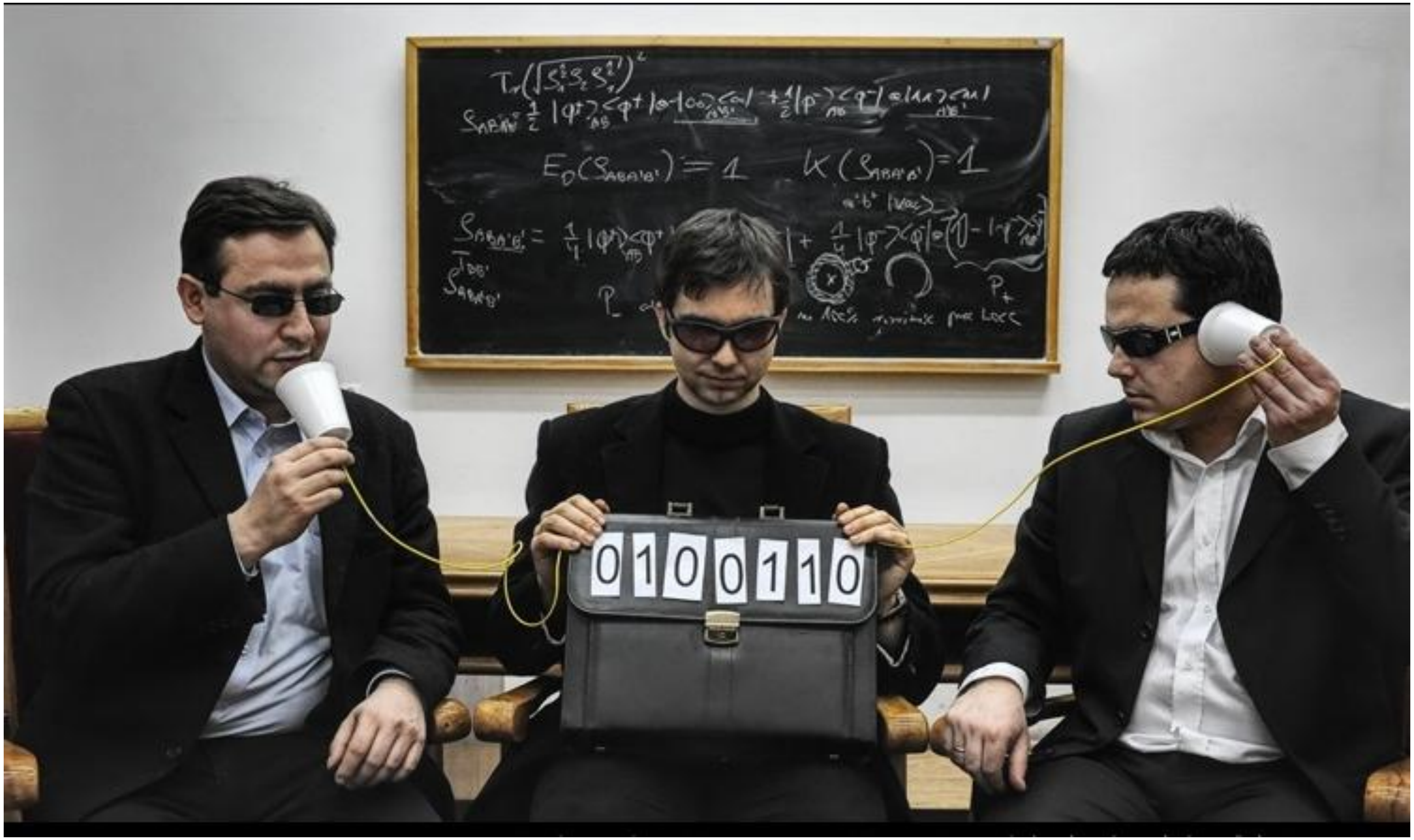
$$E_D^{\text{Bayes}} \leq 0.581(4)$$

$$K^{\text{Bayes}} = 0.690(7)$$

$$E_D^{\text{ML}} \leq 0.578(4) \quad K^{\text{ML}} = 0.704(7)$$

Summary

We have extracted secure cryptographic key from noisy entangled states with low distillable entanglement



K. Dobek, M. Karpiński, RDD, K. Banaszek, P. Horodecki, Phys. Rev. Lett. **106**, 030501 (2011)

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

UNIVERSITAS VARSOVIENSIS

FAMO

QESSENCE

FNP TEAM Programme
Foundation for Polish Science

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND