Experimental security analysis of a four-photon private state

Konrad Banaszek
Rafał Demkowicz-Dobrzański
Michał Karpiński
Wydział Fizyki
Uniwersytet Warszawski

Krzysztof Dobek
Wydział Fizyki, Uniwersytet Adama Mickiewicza w Poznaniu

Paweł Horodecki
Wydział Fizyki Technicznej i Matematyki Stosowanej, Politechnika Gdańska

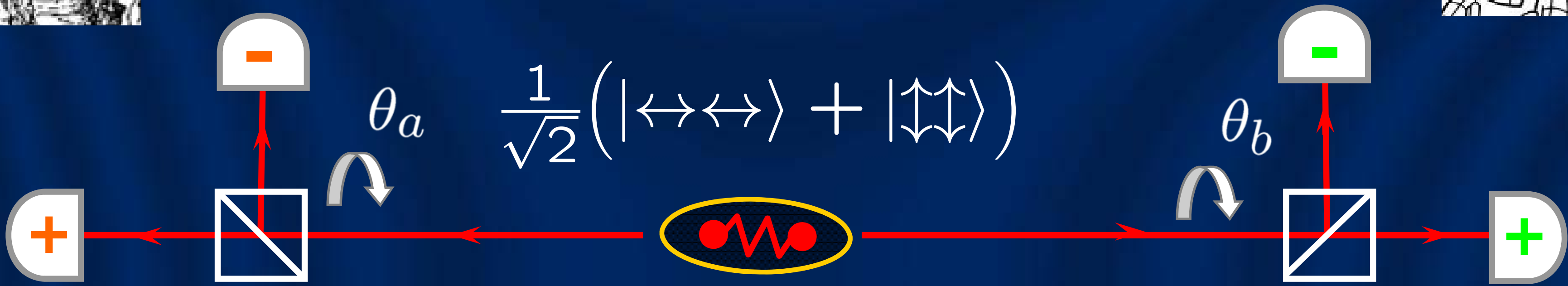
Karol Horodecki
Instytut Informatyki, Uniwersytet Gdański

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

FNP
Foundation for Polish Science

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

Bell's inequalities



A: $\theta_a = 45^o$

A': $\theta_a = 0^o$

B: $\theta_b = 22.5^o$

B': $\theta_b = 67.5^o$

Clauser-Horne-Shimony-Holt inequality is violated!

$$\langle AB\rangle + \langle A'B\rangle + \langle AB'\rangle - \langle A'B'\rangle = 2\sqrt{2}$$

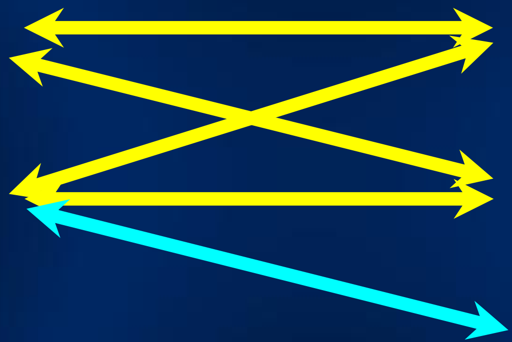
Quantum cryptography

A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)

For each photon pair Alice and Bob select randomly measurement bases…

A_1: $\theta_a = 45^o$

A_2: $\theta_a = 0^o$



B_1: $\theta_b = 22.5^o$

B_2: $\theta_b = 67.5^o$

B_3: $\theta_b = 0^o$

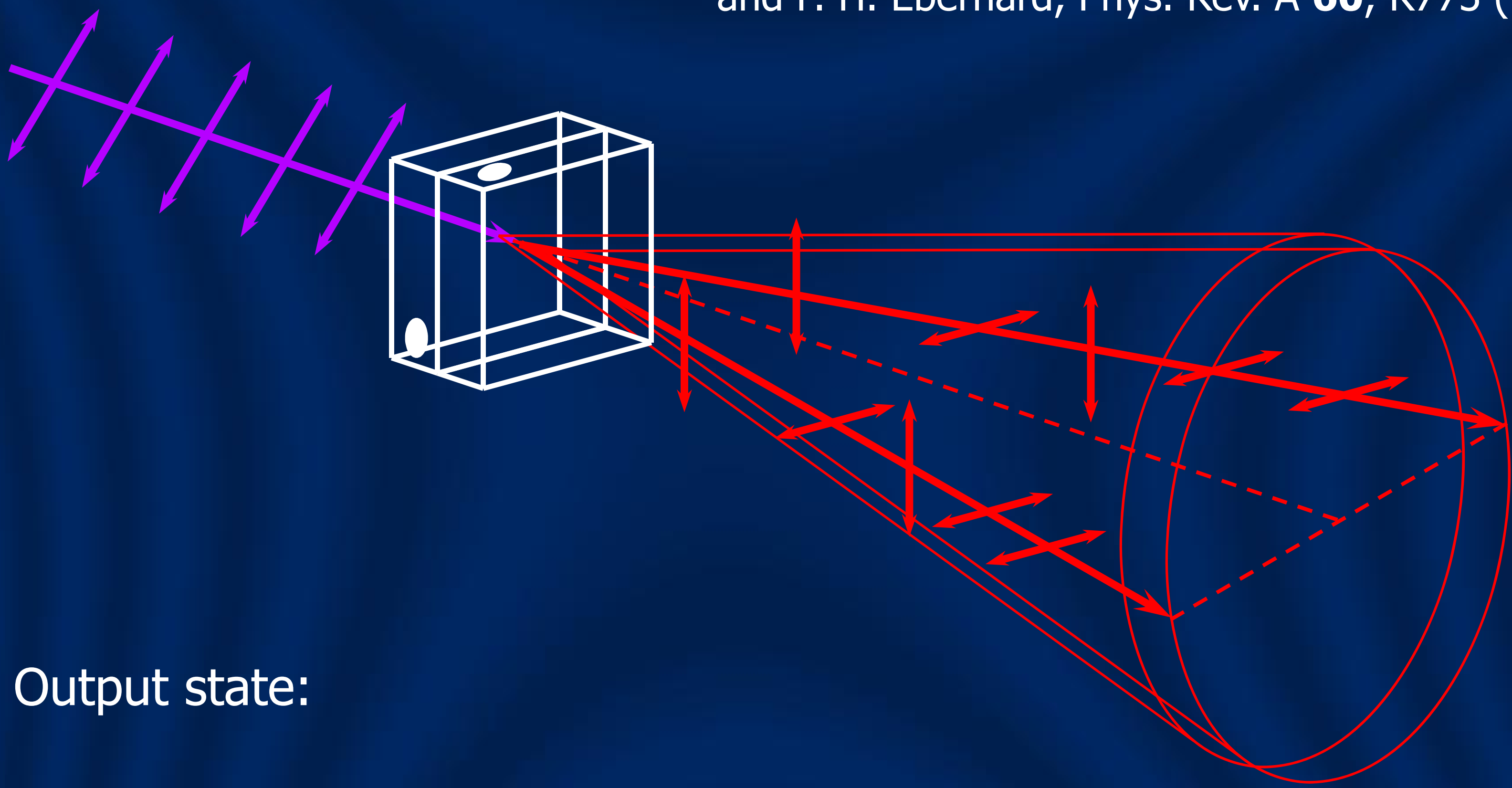
…and compare measurements over a public channel afterwards.

Perfect correlations → one-time pad

Security test

Entangled photon pairs

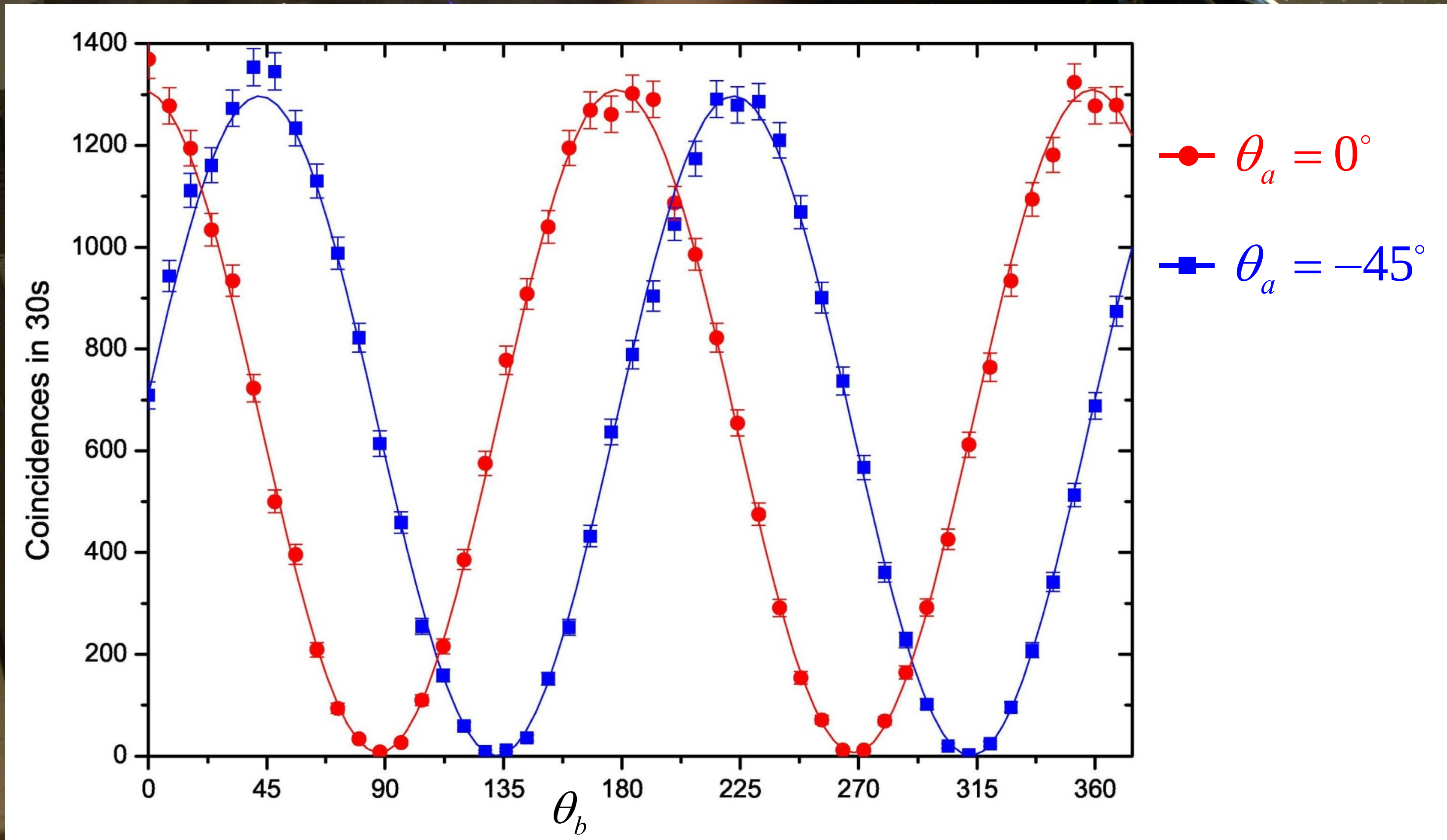
P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999)



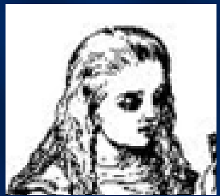
Output state:

$$|\Phi_+\rangle \propto |\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle$$

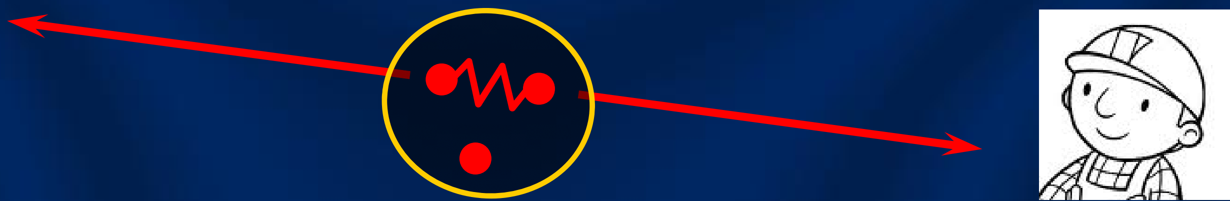
Correlation measurements



Entanglement monogamy



$$|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big)$$



- Even when the pair has been prepared by Eve…

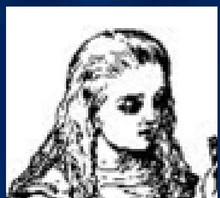
- …if Alice and Bob verify that the systems arrived in a maximally entangled pure state…

- …measurement results will be known *only* to Alice and Bob.

Statistical mixture

Define: $$|\Phi_\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB})$$

Equally weighted mixture:
$$\begin{aligned} &\tfrac{1}{2}|\Phi_+\rangle_{AB}\langle\Phi_+| + \tfrac{1}{2}|\Phi_-\rangle_{AB}\langle\Phi_-| \\ &= \tfrac{1}{2}\Big(|00\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\Big) \\ &= \mathrm{Tr}_E\Big(|\Psi\rangle_{ABE}\langle\Psi|\Big) \end{aligned}$$



Alice

Eve

Bob

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|000\rangle_{ABE} + |111\rangle_{ABE}\Big)$$

Density matrix

Maximally entangled state	Statistical mixture
$\vert\Phi_+\rangle_{AB}\langle\Phi_+\vert$	$\frac{1}{2}\Big(\vert\Phi_+\rangle_{AB}\langle\Phi_+\vert + \vert\Phi_-\rangle_{AB}\langle\Phi_-\vert\Big)$

$$\begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} \qquad \begin{pmatrix} \frac{1}{2} & \cdot & \cdot & \frac{1}{2} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \frac{1}{2} & \cdot & \cdot & \frac{1}{2} \end{pmatrix} \qquad\qquad \begin{pmatrix} \frac{1}{2} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \frac{1}{2} \end{pmatrix}$$

- Correlations between measurement outcomes in the key basis
- Security tested by the violation of Bell's inequalities
  (If trusting quantum theory, could be also tested by measurements in the $(|0\rangle \pm |1\rangle)/\sqrt{2}$ basis.)

Noisy entanglement

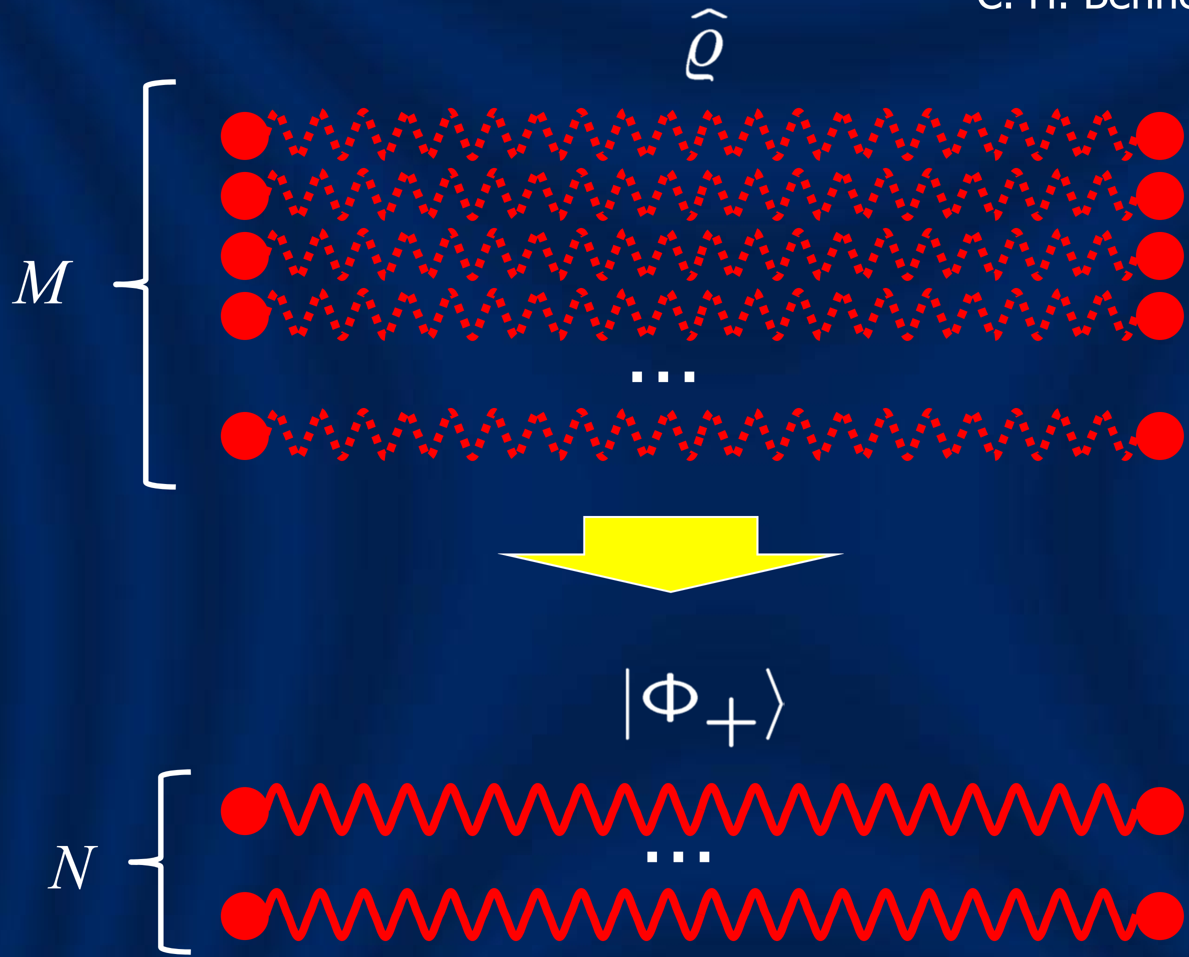
$$\tfrac{1}{4}|\Phi_+\rangle_{AB}\langle\Phi_+| + \tfrac{3}{4}|\Phi_-\rangle_{AB}\langle\Phi_-|$$

$$\begin{pmatrix} \frac{1}{2} & \cdot & \cdot & \frac{1}{4} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \frac{1}{4} & \cdot & \cdot & \frac{1}{2} \end{pmatrix}$$

How much secure key can be extracted from a noisy state?

Distillation

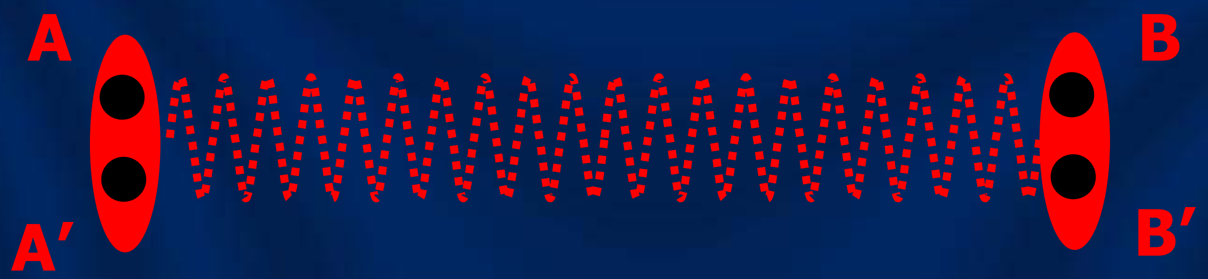
C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996)



Distillable entanglement: $E_D(\hat{\varrho}) = \lim_{M\to\infty} \frac{N}{M}$

Example I

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



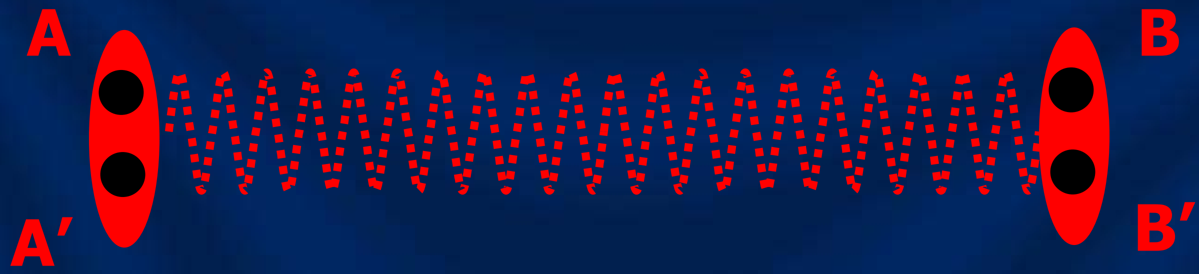
$$\hat{\varrho}_{AA'BB'} \;=\; \frac{3}{4}|\Phi_+\rangle_{AB}\langle\Phi_+| \otimes \hat{\varrho}^{(+)}_{A'B'} + \frac{1}{4}|\Phi_-\rangle_{AB}\langle\Phi_-| \otimes \hat{\varrho}^{(-)}_{A'B'}$$

Shield states:

$$\hat{\varrho}^{(+)}_{A'B'} = |00\rangle_{A'B'}\langle 00|, \qquad \hat{\varrho}^{(-)}_{A'B'} = |11\rangle_{A'B'}\langle 11|$$

enable Alice and Bob to distinguish locally $|\Phi_\pm\rangle_{AB}$ and generate the key using the standard strategy. Hence $E_D = 1$

Example II



What if

$$\hat{\varrho}^{(+)}_{A'B'} = \frac{1}{3}(\hat{\mathbb{1}} - |\Psi_-\rangle_{A'B'}\langle\Psi_-|)$$

$$\hat{\varrho}^{(-)}_{A'B'} = |\Psi_-\rangle_{A'B'}\langle\Psi_-| \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

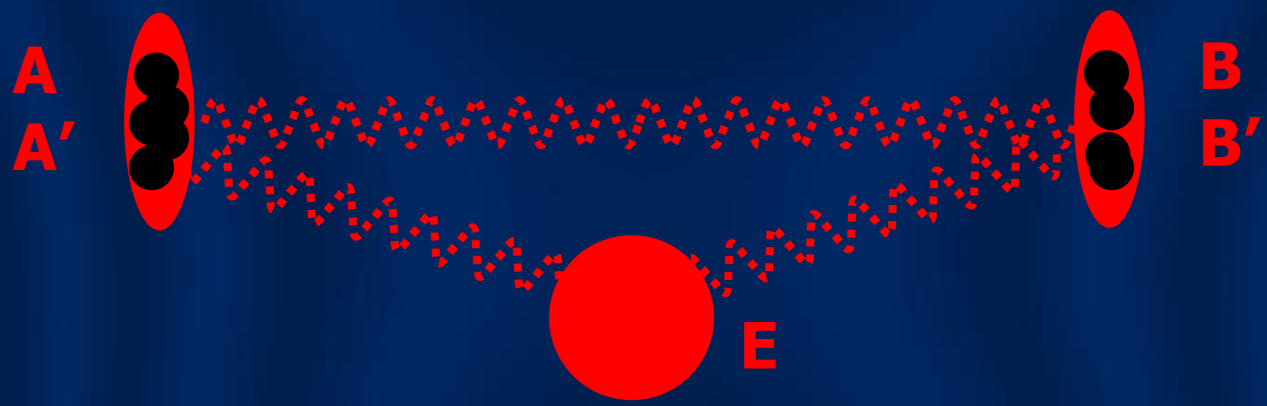
- States $\hat{\varrho}^{(+)}_{A'B'}$ and $\hat{\varrho}^{(-)}_{A'B'}$ cannot be discriminated unambiguously using local operations and classical communication.

- Distillable entanglement bounded by log-negativity:

$$E_D \leq \log_2 3 - 1 \approx 0.585$$

Eavesdropping

K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim,
Phys. Rev. Lett. **94**, 160502 (2005)



The worst case scenario: all the noise is controlled by Eve

$$\hat{\varrho}_{AA'BB'} = \mathrm{Tr}_E\big(|\Psi\rangle_{AA'BB'E}\langle\Psi|\big)$$

Alice → Eve channel

Alice measures an outcome a with a probability

$$p_a = \mathrm{Tr}_{A'BB'E}\Big({}_A\langle a|\Psi\rangle\langle\Psi|a\rangle_A\Big)$$

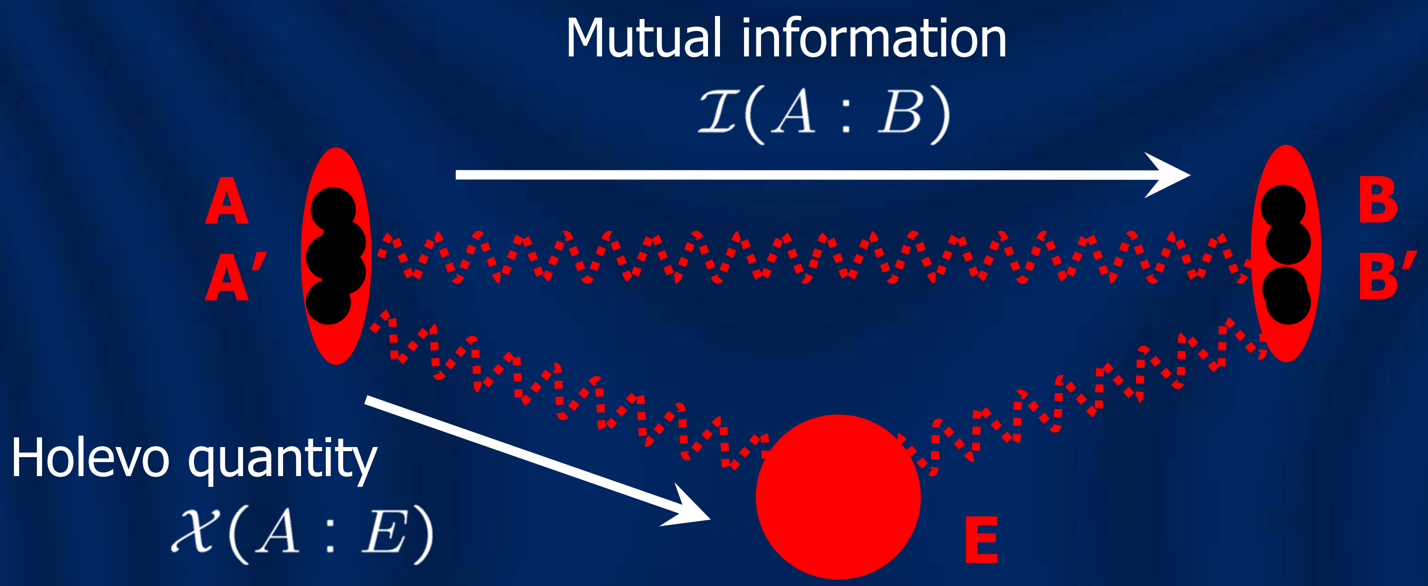
Eve infers a from the conditional state of her subsystem E:

$$\hat{\varrho}_E^{(a)} = \frac{1}{p_a}\mathrm{Tr}_{AA'BB'}[|\Psi\rangle\langle\Psi|(|a\rangle_A\langle a| \otimes \hat{I}_{A'BB'})]$$

Holevo quantity:

$$\mathcal{X}(A:E) = S\left(\sum_a p_a \hat{\varrho}_E^{(a)}\right) - \sum_a p_a S\left(\hat{\varrho}_E^{(a)}\right)$$

Key rate



Key rate $K_D \geq \mathcal{I}(A:B) - \mathcal{X}(A:E)$

For Example II, Eve's subsystem contains no information about outcomes of Alice's measurement on her qubit, hence $K_D = 1$.

Shield

Without the shield:

$$\mathrm{Tr}_{A'B'}\left(\hat{\varrho}_{AA'BB'}\right) = \begin{pmatrix} \frac{1}{2} & \cdot & \cdot & \frac{1}{4} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \frac{1}{4} & \cdot & \cdot & \frac{1}{2} \end{pmatrix}$$

■ key ■ security

The complete

$$\begin{pmatrix} \frac{1}{8} & \cdot & \cdot & \cdot \\ \cdot & \frac{1}{8} & \cdot & \cdot \\ \cdot & \cdot & \frac{1}{8} & \cdot \\ \cdot & \cdot & \cdot & \frac{1}{8} \end{pmatrix} \qquad \begin{pmatrix} \frac{1}{8} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \frac{1}{8} & \cdot \\ \cdot & \frac{1}{8} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \frac{1}{8} \end{pmatrix}$$

B

0

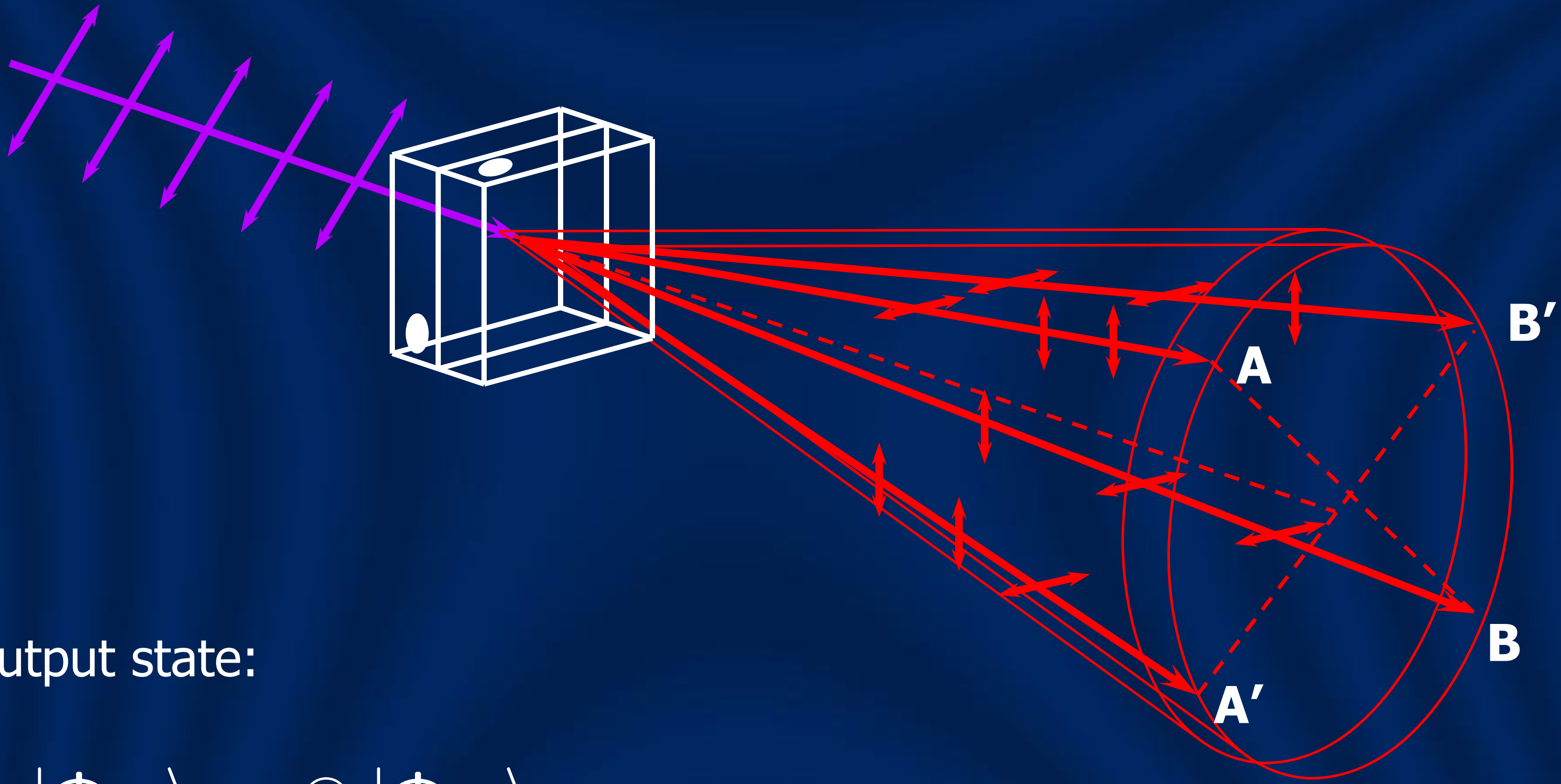
1

$$\hat{\varrho}_{AA'BB'} = \begin{pmatrix} \cdots & & & \\ \bullet & \bullet & \bullet & \bullet \\ \begin{smallmatrix} \frac{1}{8} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \frac{1}{8} & \cdot \\ \cdot & \frac{1}{8} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \frac{1}{8} \end{smallmatrix} & \bullet & \bullet & \begin{smallmatrix} \frac{1}{8} & \cdot & \cdot & \cdot \\ \cdot & \frac{1}{8} & \cdot & \cdot \\ \cdot & \cdot & \frac{1}{8} & \cdot \\ \cdot & \cdot & \cdot & \frac{1}{8} \end{smallmatrix} \end{pmatrix}$$

10

11

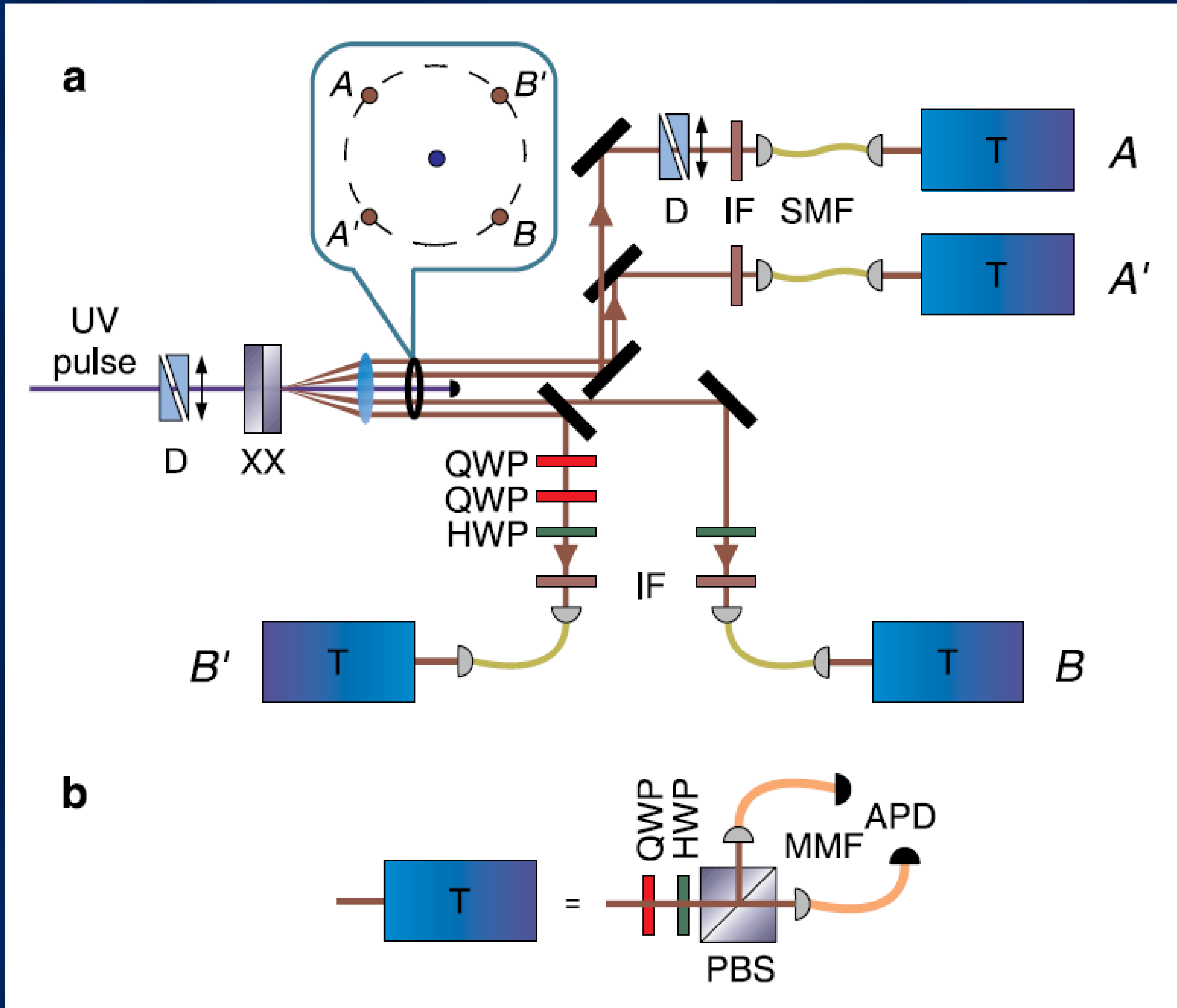
Double photon pairs



Output state:

$$|\Phi_+\rangle_{AB} \otimes |\Phi_+\rangle_{A'B'}$$

Experimental setup



Quantum state tomography

Projective qubit measurements: $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$

Four-qubit POVM:

$$\hat{M}_i = |\pm_{i_A}\rangle \otimes |\pm_{i_{A'}}\rangle \otimes |\pm_{i_B}\rangle \otimes |\pm_{i_{B'}}\rangle$$

$3^4 = 81$ measurement bases

$3^4 \times 2^4 = 1296$ event types

Probability of an outcome i:

$$p(i|\hat{\varrho}) = Tr(\hat{M}_i \hat{\varrho})$$

n_i: number of events i

$$\sum_i n_i \approx 5 \times 10^5$$

Density matrix estimate $\hat{\varrho}$

Maximum likelihood reconstruction

Probability of an outcome i:

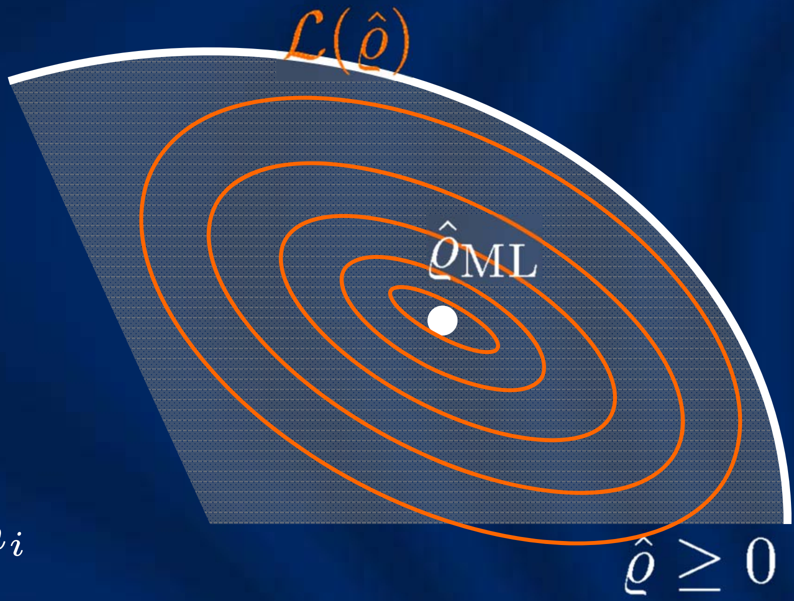
$$p(i|\hat{\varrho}) = Tr(\hat{M}_i \hat{\varrho})$$

n_i– number of events i

Likelihood function:

$$\mathcal{L}(\hat{\varrho}) = p(\{n_i\}|\hat{\varrho}) = \prod_i [p(i|\hat{\varrho})]^{n_i}$$

Maximum-likelihood estimate $\hat{\varrho}_{\mathrm{ML}}$
maximizes $\mathcal{L}(\hat{\varrho})$



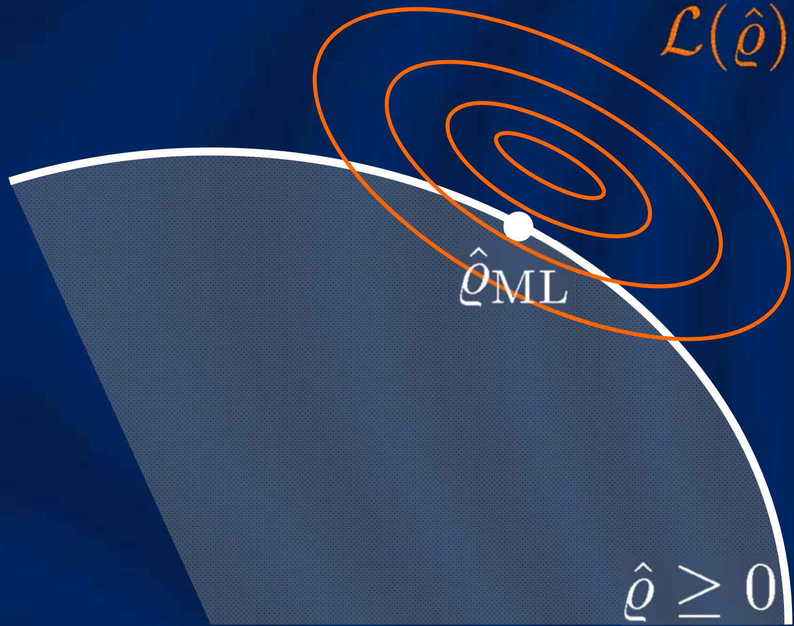
ML: Parametrisation

K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi,
Phys. Rev. A **61**, 010304(R) (1999)

Ensuring positivity: $\hat{\varrho} = \hat{T}^\dagger \hat{T}, \quad \hat{T} =$ ◥

Task: maximize $\log \mathcal{L}(T^\dagger T)$

with a constraint $\mathrm{Tr}(T^\dagger T) = 1$



PRO: - Guaranteed positivity

CON: - Impractical in higher dimensions (>6 qubits)
- Underestimates errors, difficult to include uncertainty of the measuring device (Monte Carlo simulations)
- Biased towards low-rank matrices for undersampled data

Bayesian approach

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

A priori distribution $p(\hat{\varrho})$

A posteriori: $p(\hat{\varrho}|\{n_i\}) \propto p(\{n_i\}|\hat{\varrho})p(\hat{\varrho})$

Estimate: $\hat{\varrho}_{\text{Bayes}} = \int d\varrho\; \hat{\varrho}\, p(\hat{\varrho}|\{n_i\})$

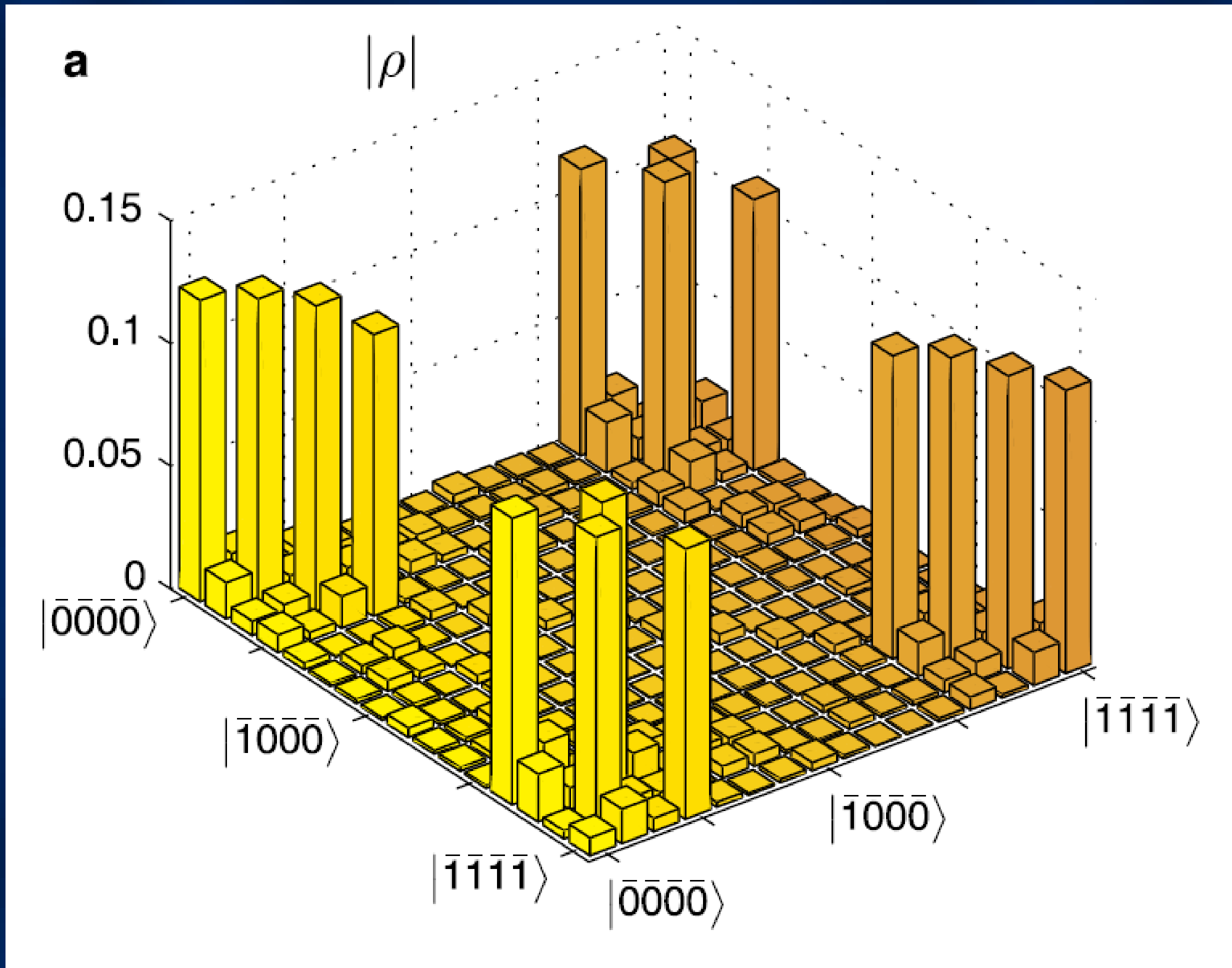
- Gaussian approximation
- Truncated to positive definite density operators

PRO: - Clear statistical interpretation
- Provides uncertainty
- No numerical optimisation

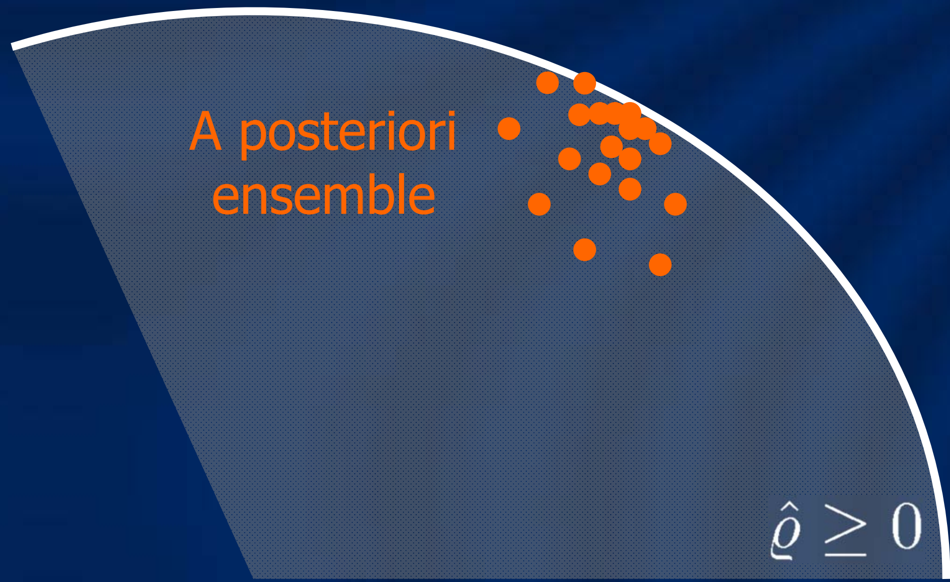
CON: - Difficult to normalise probability distribution
- A priori distribution not well defined

State reconstruction

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



Privacy characterisation



Warning:

$$\langle f(\hat{\varrho}) \rangle \neq f(\langle \hat{\varrho} \rangle)$$

More conservative

Distillable entanglement: $E_D \leq 0.581(4)$

Key (cqq scenario): $K \geq 0.690(7)$

Distillation protocol

$$\hat{\varrho}_{AA'BB'} = \tfrac{1}{4}|\Phi_+\rangle_{AB}\langle\Phi_+| \otimes \left(\hat{\mathbb{1}}_{A'B'} - |\Psi_-\rangle_{A'B'}\langle\Psi_-|\right)$$
$$+\tfrac{1}{4}|\Phi_-\rangle_{AB}\langle\Phi_-| \otimes |\Psi_-\rangle_{A'B'}\langle\Psi_-|$$

Measure qubits $A'B'$ in the same basis.

50% → Identical outcomes

$$\hat{\varrho}_{AB} = |\Phi_+\rangle\langle\Phi_+|$$

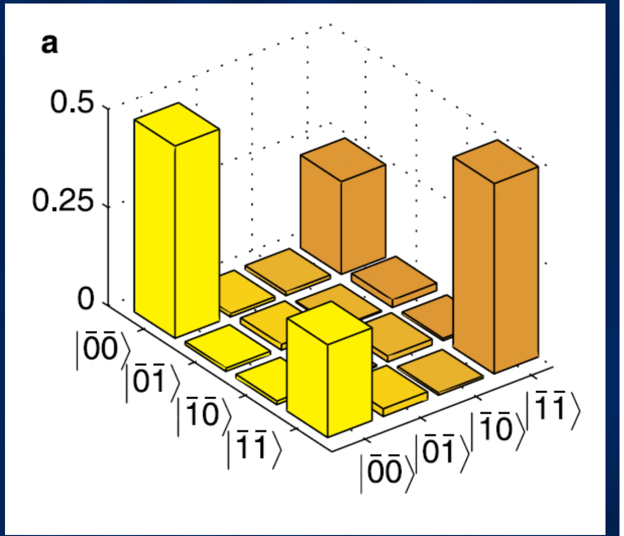
50% → Opposite outcomes

$$\hat{\varrho}_{AB} = \tfrac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)$$

Single-copy distillation

Reduced density matrix $\hat{\varrho}_{AB}$

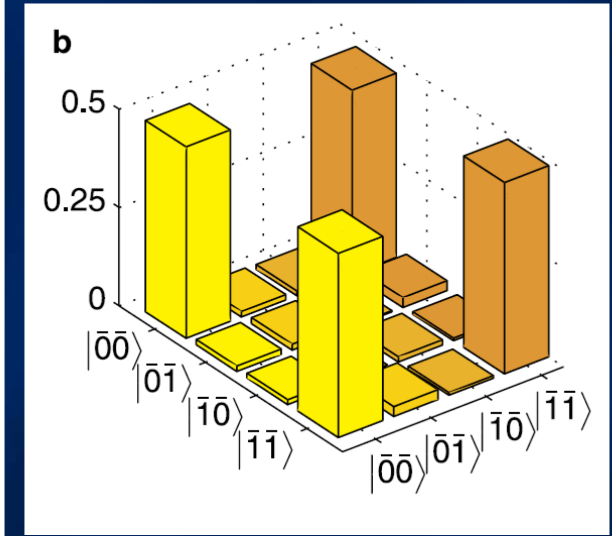
average



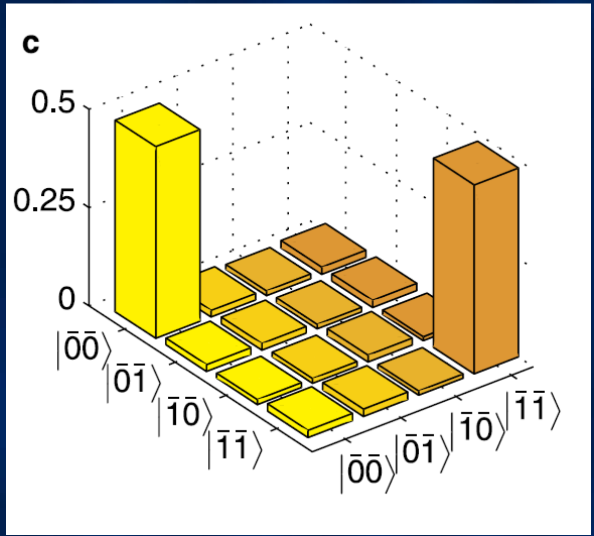
$K = 0$

conditional

identical outcomes $A'B'$



opposite outcomes $A'B'$



$K = 0.354(5)$

Cryptographic key

Optimal strategy		Distillation-based approach
Raw key: 3716 bits		Raw key: 1859 bits
↓	Error correction	↓
2726 bits		$\approx$ 1300 bits
↓	Privacy amplification	↓
Secure key: 2164 bits		Secure key: $<$ 650 bits

Witnessing privacy

$$\hat{\varrho}_{AA'BB'} = \begin{pmatrix} \hat{A}_{00,00} & \hat{A}_{00,01} & \hat{A}_{00,10} & \hat{A}_{00,11} \\ \hat{A}_{01,00} & \hat{A}_{01,01} & \hat{A}_{01,10} & \hat{A}_{01,11} \\ \hat{A}_{10,00} & \hat{A}_{10,01} & \hat{A}_{10,10} & \hat{A}_{10,11} \\ \hat{A}_{11,00} & \hat{A}_{11,01} & \hat{A}_{11,10} & \hat{A}_{11,11} \end{pmatrix}$$

$$K\left(\hat{\varrho}_{AA'BB'}\right) \geq K\left(\hat{\sigma}_{AB}\right)$$

where

$$\hat{\sigma}_{AB} = \frac{1}{2} \begin{pmatrix} p_+ & \cdot & \cdot & c_+ \\ \cdot & p_- & c_- & \cdot \\ \cdot & c_- & p_- & \cdot \\ c_+ & \cdot & \cdot & p_+ \end{pmatrix} \qquad \begin{aligned} p_+ &= ||\hat{A}_{00,00} + \hat{A}_{11,11}|| \\ c_+ &= ||\hat{A}_{00,11} + \hat{A}_{11,00}|| \end{aligned}$$

Single witness

K. Banaszek, K. Horodecki, and P. Horodecki,
Phys. Rev. A **85**, 012330 (2012)

Suppose we have measured

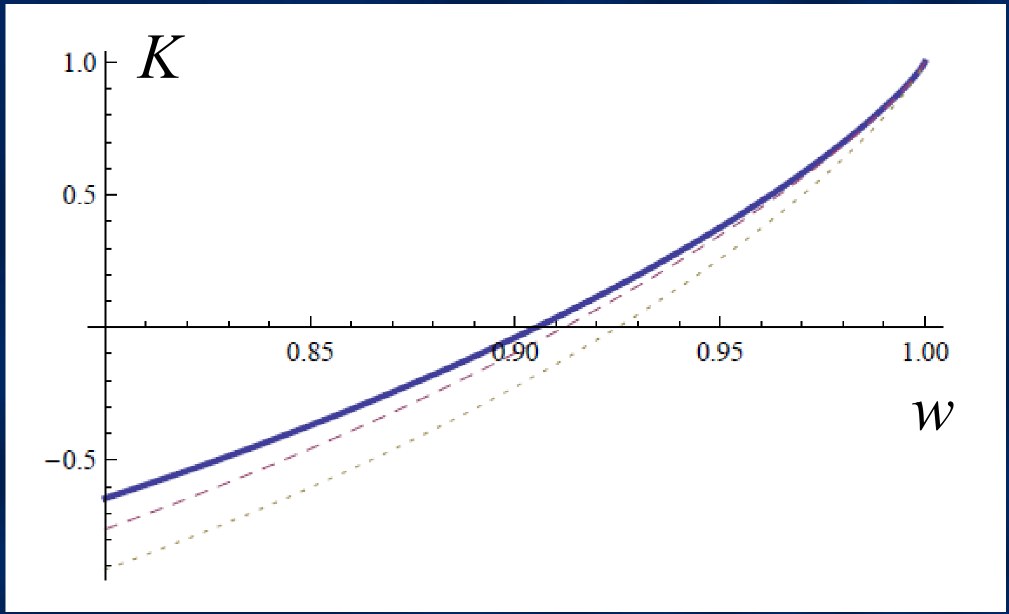
$$w = \left| \left\langle (\sigma_A^x \otimes \sigma_B^x - \sigma_A^y \otimes \sigma_B^y) \otimes \hat{U}_{A'B'} \right\rangle \right|$$

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

We have:

$$p_+ \geq c_+ \geq w$$

Take the worst-case scenario for p_-, c_-



Two observables

K. Banaszek, K. Horodecki, and P. Horodecki,
Phys. Rev. A **85**, 012330 (2012)

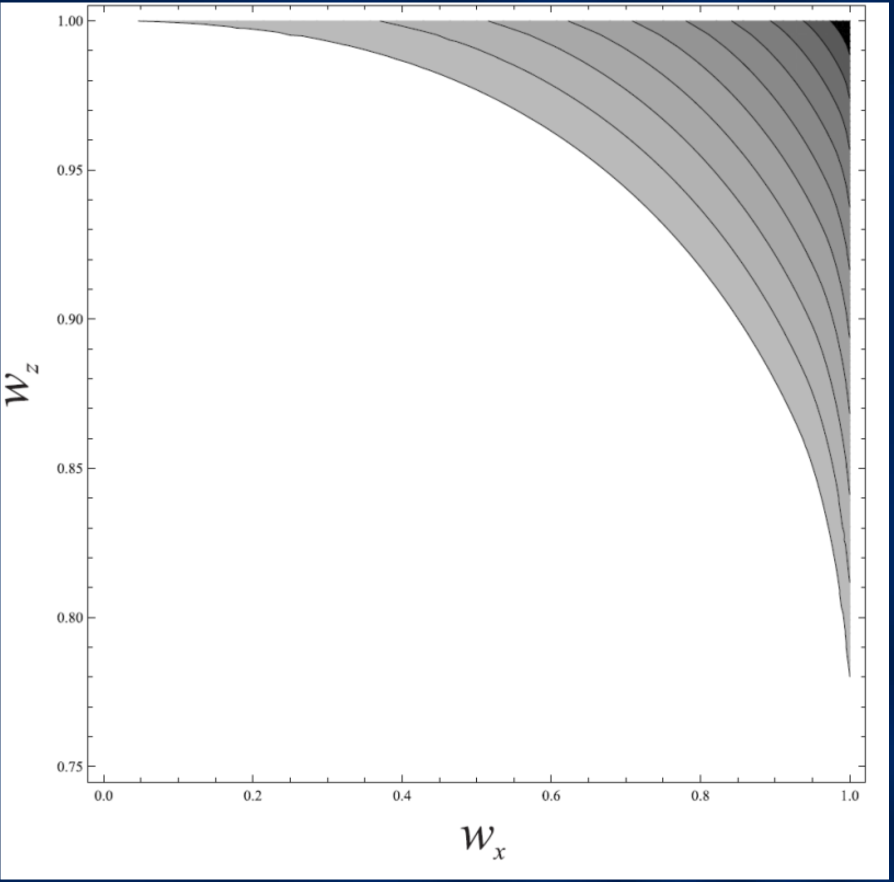
$$w_x = \left| \left\langle \sigma_A^x \otimes \sigma_B^x \otimes \hat{U}_{A'B'} \right\rangle \right| \qquad w_z = \left| \left\langle \sigma_A^z \otimes \sigma_B^z \otimes \hat{I}_{A'B'} \right\rangle \right|$$

We have:

$$c_+ + c_- \geq w_x$$

$$p_\pm = \frac{1}{2}(1 \pm w_z)$$

$$c_- \leq p_-$$



Conclusions

- Experimental demonstration of the separation between distillable entanglement and cryptographic key contents
- Practical comparison of quantum state reconstruction methods for a noisy multiqubit state
- Full privacy analysis based on the reconstructed state
- Evaluation of highly non-linear information theoretic quantities
- Implementation of a simple entanglement distillation protocol
- Witnessing privacy with few observables
- Multiple degrees of freedom?