Minimal tomography and its applications

J. Rehacek, Z. Hradil
Department of Optics, Palacky University
Olomouc, Czech Republic

B.-G. Englert and D. Kaszlikowski
Department of Physics, NUS, Singapore

Outline

- Minimal tomography
  - What is minimal (symmetric) tomography?
  - Possible realizations
  - Performance
- Applications
  - Cryptography
  - Vortex beams

Tomography

- Complete characterization of a quantum source in dimension *d*

density matrix: d^2-1 independent parameters

measurement: d^2-1 independent probabilities

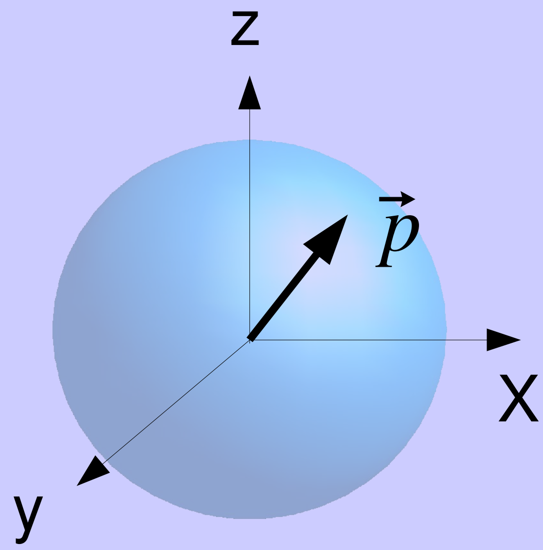
- Example:

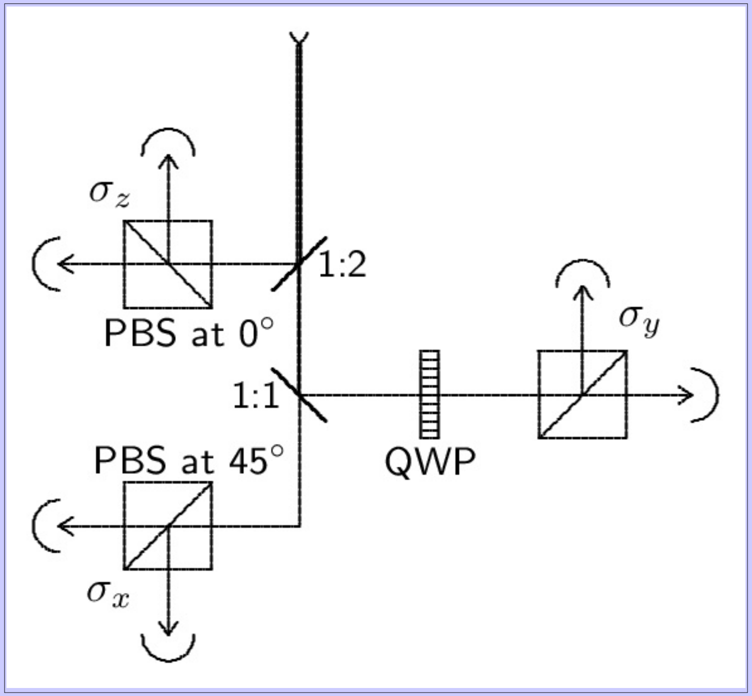
state of a qubit is determined by three independent probabilities

Ellipsometry

- Spin ½ particle, polarization ...

$$\rho = \frac{1}{2}\hat{I} + \frac{1}{2}\vec{s}\cdot\vec{\hat{\sigma}}$$





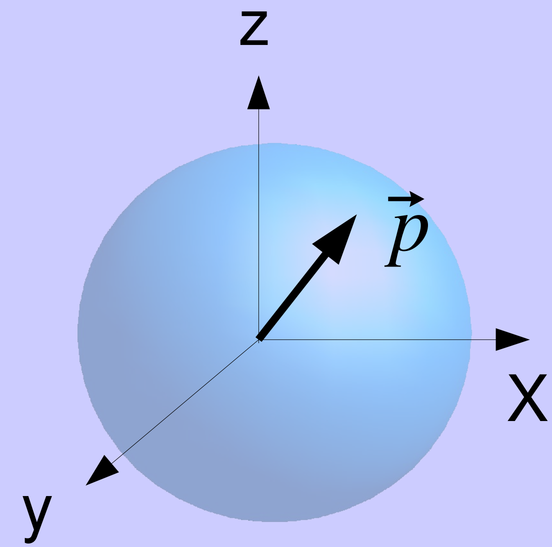
Standard ellipsometry setup

Ellipsometry ...

- Reconstruction

$$\Pi_{x\uparrow} = 1/6(1+\sigma_x)$$
$$\Pi_{x\downarrow} = 1/6(1-\sigma_x)$$
$$\Pi_{y\uparrow, y\downarrow, z\uparrow, z\downarrow} = \ \ldots$$

$$\rho = \frac{1}{2}\hat{I} + \frac{1}{2}\vec{s}\cdot\vec{\hat{\sigma}}$$



$$s_x = 3\langle \Pi_{x\uparrow}\rangle - 3\langle \Pi_{x\downarrow}\rangle, \ \ldots$$

- This is a six-element POVM $\rightarrow$ overdetermined problem

Minimal tomography

- Minimal

  d^2 channels in dimension d (this is 4 channels for qubits)

- Symmetric

  $$\mathrm{Tr}\{\Pi_i \Pi_j\} = \mathrm{const}, \forall i \neq j$$

- Noiseless

  POVM elements are subnormalized projectors

  $$\Pi_j = \frac{1}{d} |\phi_j\rangle\langle\phi_j|, \quad |\langle\phi_j|\phi_j\rangle|^2 = \frac{1}{d+1}$$

Construction

- Minimal POVM provides a global minimum of the functional

$$S=\sum_{j,k} |\langle \phi_j | \phi_k \rangle|^4 \geq \frac{2d^3}{d+1}$$

- Minimization is done over d^2 vectors $|\phi_j\rangle$
- Alternatively, POVMs can be obtained from a vector $|\phi\rangle$ via

$$|\phi_{dj+k}\rangle = D_{jk}|\phi\rangle, \quad D_{jk}=\sum_{m=0}^{d-1} e^{\frac{2\pi i}{d} j(m+k/2)} |(k+m) \bmod d\rangle\langle m|$$

J.M. Renes et al. Phys. Rev. A

Qubits

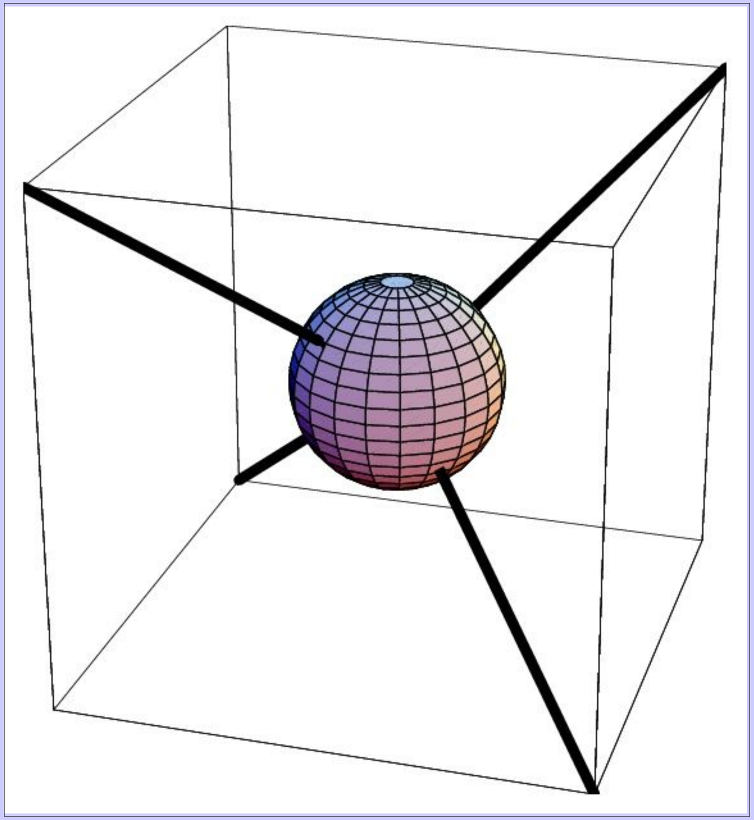
- Dimension $d=2$

$$\Pi_1=\frac{1}{4}+\frac{1}{4\sqrt{3}}(\sigma_x+\sigma_y+\sigma_z)$$

$$\Pi_2=\frac{1}{4}+\frac{1}{4\sqrt{3}}(\sigma_x-\sigma_y-\sigma_z)$$

$$\Pi_3=\frac{1}{4}+\frac{1}{4\sqrt{3}}(-\sigma_x+\sigma_y-\sigma_z)$$

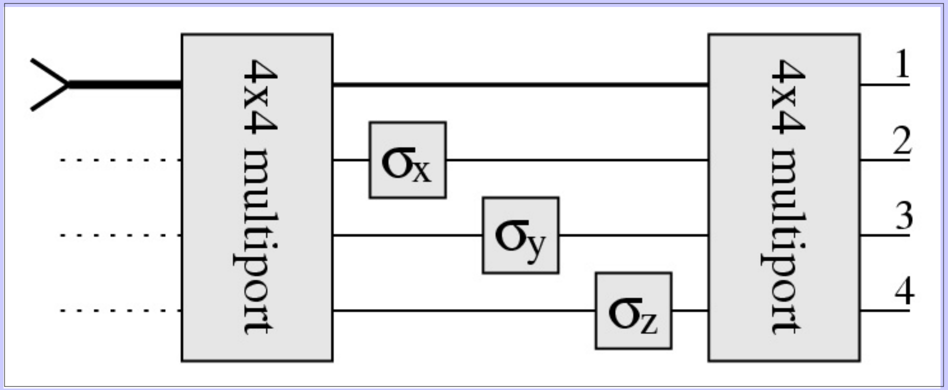
$$\Pi_4=\frac{1}{4}+\frac{1}{4\sqrt{3}}(-\sigma_x-\sigma_y+\sigma_z)$$

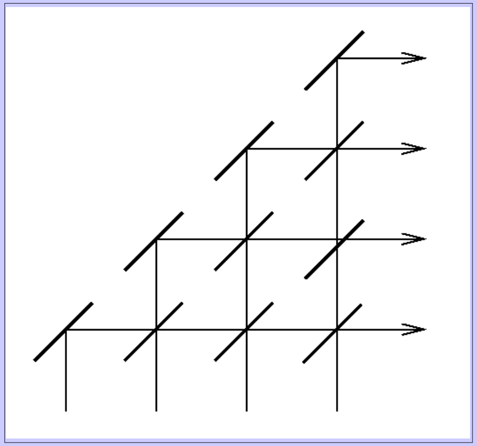


- Tetrahedron geometry

Optical implementation

- Multiport



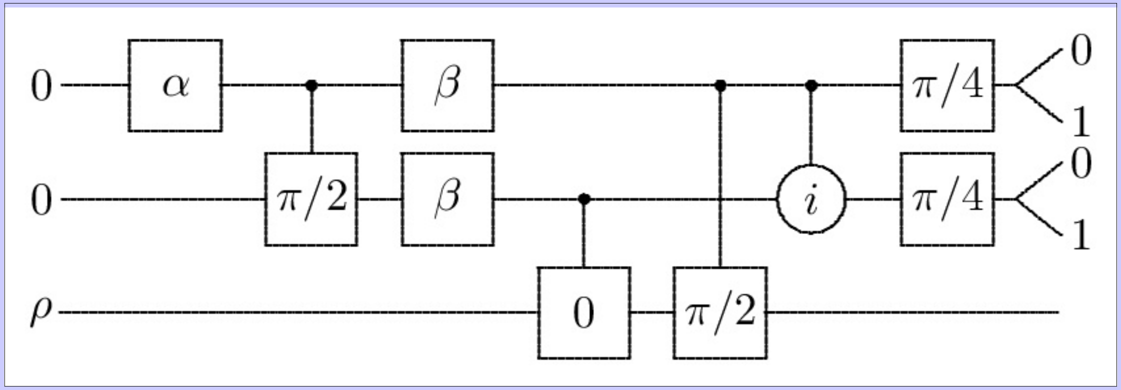


$$\Pi_1 = \frac{1}{4} + \frac{1}{4\sqrt{3}}(\hat{\sigma}_x + \hat{\sigma}_y + \hat{\sigma}_z), \ \ldots$$

- ½ of intensity goes through the upper arm; the rest is equally distribute among σ_x, σ_y and σ_z channels

Optical implementation...

- Equivalent computation network



$$00 \rightarrow \Pi_1, \quad 01 \rightarrow \Pi_2, \ldots$$

$$\sin(2\alpha) = (\sqrt{3} - 1)/3, \quad \tan(2\beta) = \sqrt{3} + 1$$

- some other schemes

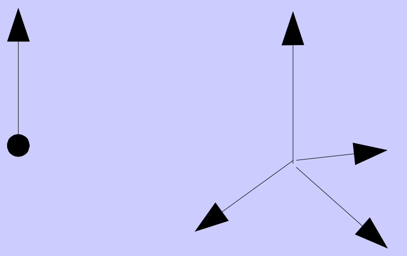
Clarke et al., PRA 64, 012303 (2001)
Decker, Janzing, and Beth , Int J. Quantum Inf. 2, 353 (2004)
Rehacek, Englert, and Kaszlikowski, PRA 70, 052321 (2004)

Performance

- Assymptotic efficiency (pure states)
  - parallel strategy

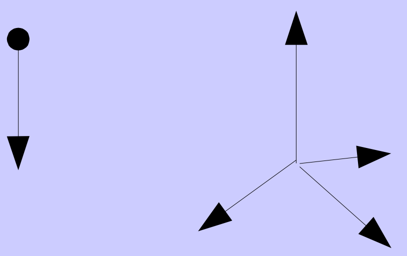
qubit POVM

$$1-\langle F \rangle \approx \frac{1}{N}$$



  - antiparallel strategy

$$1-\langle F \rangle \approx \frac{1}{2N}$$



Simple self-learning protocol

- Step 1

$N/2$ particles are measured $\longrightarrow$ $\rho(N/2)$

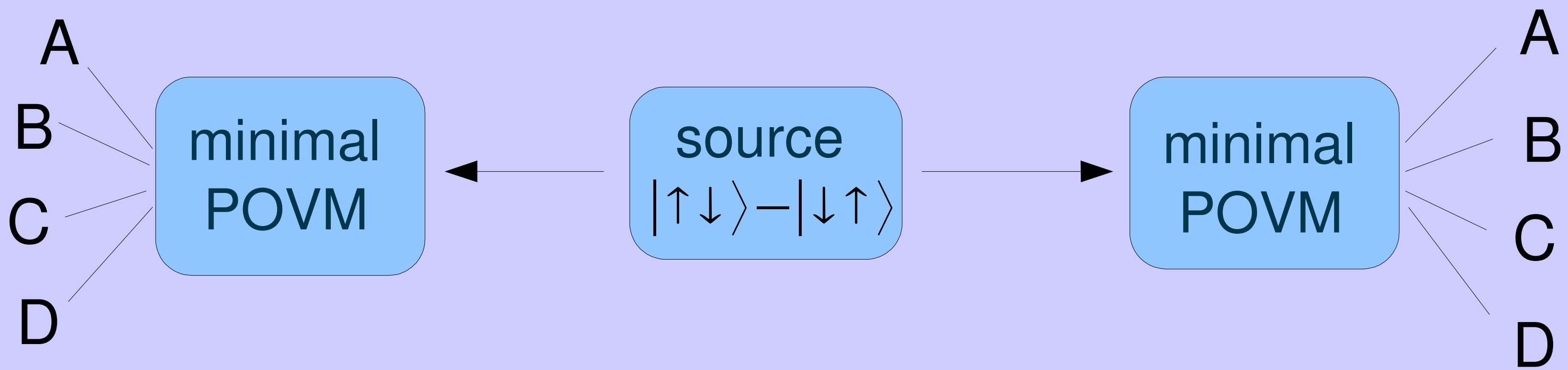
- Step 2

second half of the ensemble is used for reconstructing the state [antiparallel strategy with respect to $\rho(N/2)$]

$$\boxed{1-\langle F\rangle \approx \frac{2}{N} \approx 2\left(1-\frac{N+2}{N+3}\right)}$$

Quantum cryptography

- Minimal POVM on singlet states yields strong correlations



$$I_{AB} = \log_2(16/12)\,\text{bits} \approx 0.415\,\text{bits}$$

- Alice and Bob can fully characterize the source $\longrightarrow$ tomographic QKD protocol

Singapore protocol

- two-way (public) communication

	1	2	3	4	5	6	7	8	9
Alice:	A	C	A	D	D	B	A	B	A
Bob:	B	A	D	A	B	D	D	C	D

Alice → Bob: 1,3

Bob → Alice: (B,D)=1; (A,C)=0 (at random)

shared secret bit “0” is generated

Alice → Bob: 7,9

Bob → Alice: sorry...

A and D are recorded as parts of new sequences

Efficiency

- 1^{st} iteration:

probability of Bob's success: 2/3

letters used: 2, i.e. **1/3bits** generated per qubit

- 2^{nd} iteration:

probability of Bob's failure: 1/3

probability of Bob's success, next round: 2/3

letters used: 4, i.e. **1/18bits** generated per qubit

- n^{th} iteration:

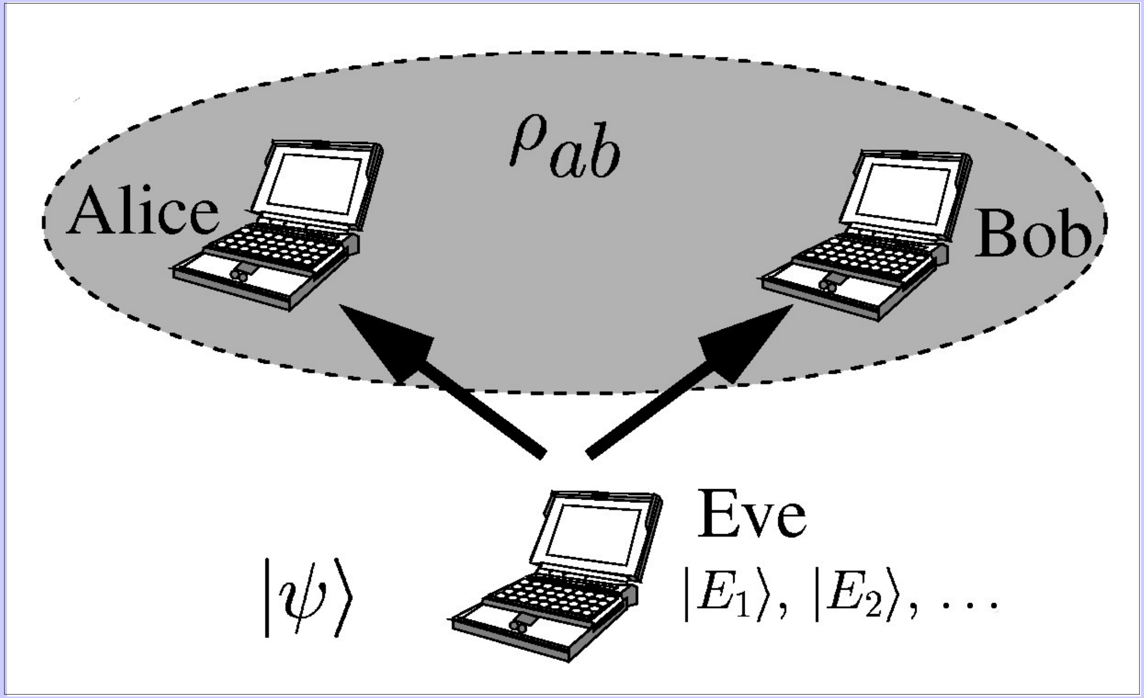
$$\frac{2}{3}\left(1-\frac{2}{3}\right)^{n-1}\left(\frac{1}{2}\right)^{n}=\frac{1}{3}\frac{1}{6^{n-1}}$$

asymptotical limit= 0.4

first three iterations: $(1/3+1/18+1/108)\approx 0.398$

Security analysis

- Eve is given the control of the source:



Eve's ancilla states are determined by ρ_{ab} .
Which Eve's measurement maximizes I_{AE} ?

Security analysis ...

- white noise: $\rho_{ab} = (1-\epsilon)|\Psi_{\rm sing}\rangle\langle\Psi_{\rm sing}| + \frac{\epsilon}{4}\hat{1}$
- best thing Eve can do: $|\Psi\rangle = \sum_{ij} |E_{ij}\rangle_e |i\rangle_a |j\rangle_b$
- tomography: $\mathrm{Tr}_e\{|\Psi\rangle\langle\Psi|\} = \rho_{ab}$

$$\Rightarrow \quad |E_{ij}\rangle = \sum_k c_k^{ij} |k\rangle_e, \quad C = \sqrt{\rho_{ab}}$$

- conditioned states:

$$\rho_e^j = \mathrm{Tr}_{ab}\{|\Psi\rangle\langle\Psi|\Pi_a^j\}$$

- Minimal POVM $\longrightarrow$ pyramidal Eve's states

Optimization

- Optimal Eve's measurement maximizes

$$I_{AE}(p_{ij}) = \sum_{ij} p_{ij} \log \frac{p_{ij}}{p_i p_j}, \quad p_{ij} = \mathrm{Tr}\{\rho_e^j \Pi_e^i\}$$

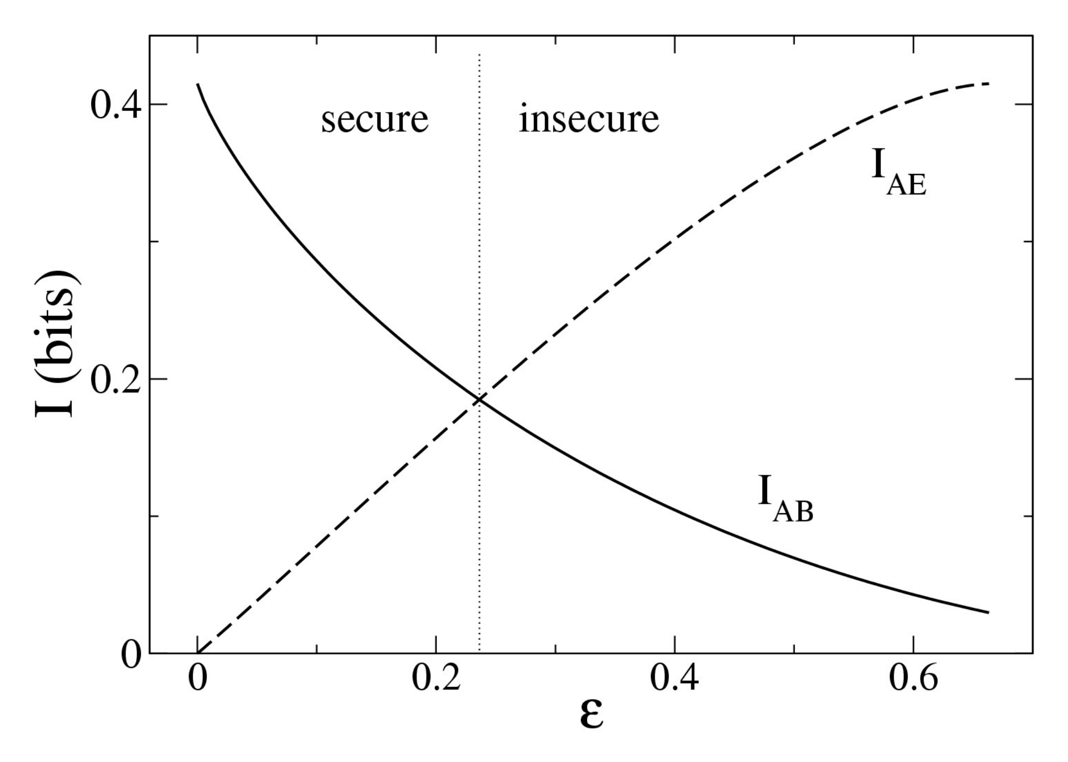
  - concave functional with respect to Eve's measurement
  - all maxima lie at the boundary of the convex set of all POVMs
  - numerical search

Rehacek, Englert, and Kaszlikowski, PRA 71, 054303 (2005)

Results ...

- security diagram

$$\epsilon_{\text{thr}} \approx 0.2363$$



Englert et al., quant-ph/0412075

Results ...

- weak noise limit $\epsilon \to 0$:

  a von Neuman measurement is optimal

- strong noise limit $\epsilon \to 1$:

  optimal measurement has five channels

- efficiency (bit rate) of QKD with minimal tomography is significantly larger compared to the six-state BB84 protocol for all $\epsilon < \epsilon_{\mathrm{thr}}$

Englert et al., quant-ph/0412075

Outlook: vortex beams

- superposition of vortex beams with complex coefficients $\longrightarrow$ quantum state

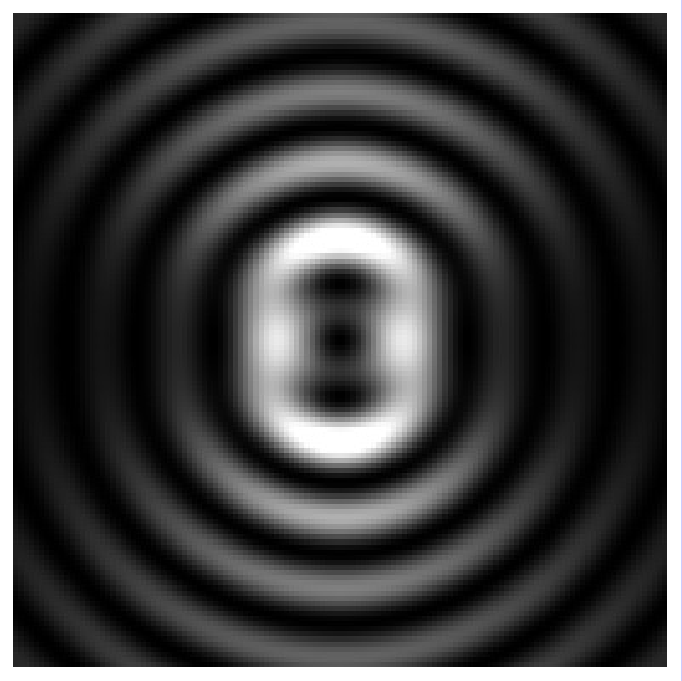
$$\boxed{\mathrm{POVM}: \ \rho \ \rightarrow \ \mathrm{transformation} \ \rightarrow \ \mathrm{intensity\,scan}}$$

- spatial light modulators: effective implementation of quantum operations
- recontruction: minimal state tomography

Bessel beams

- Generation: periodical azimuthal modulation

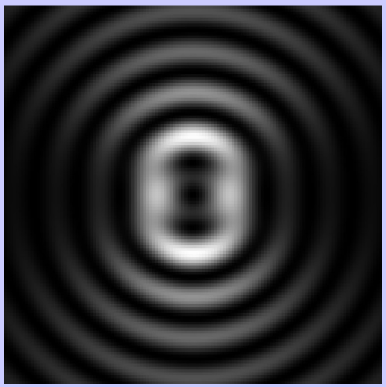
$$A(\varphi) = A_0\, e^{im\varphi}$$

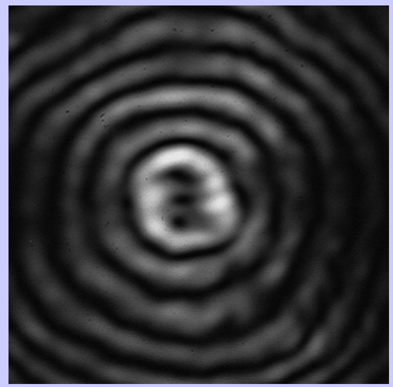


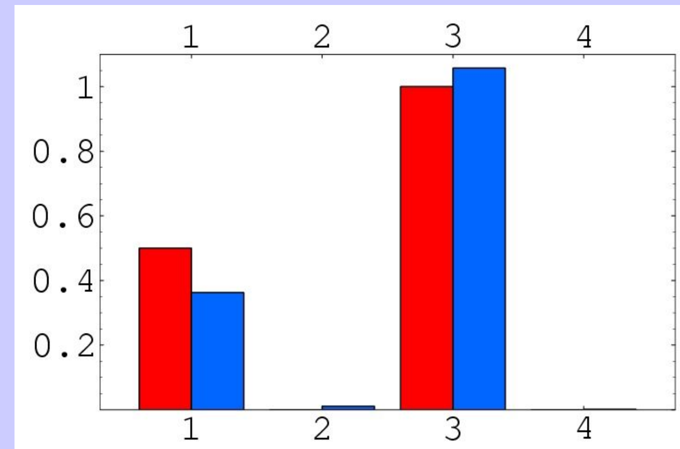
- Interesting properties:
  - non-diffracting character
  - robust (self-reconstruction)
  - carry orbital momentum

Experiment

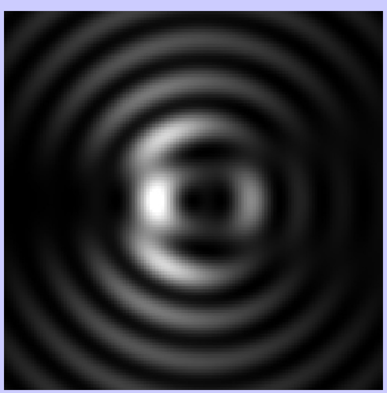
- Superposition of four vortices

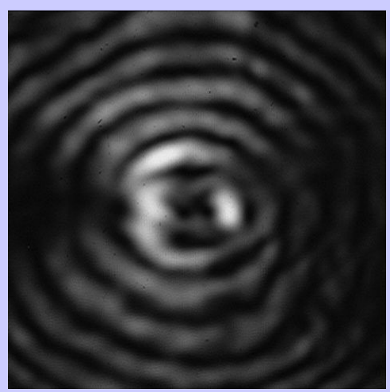


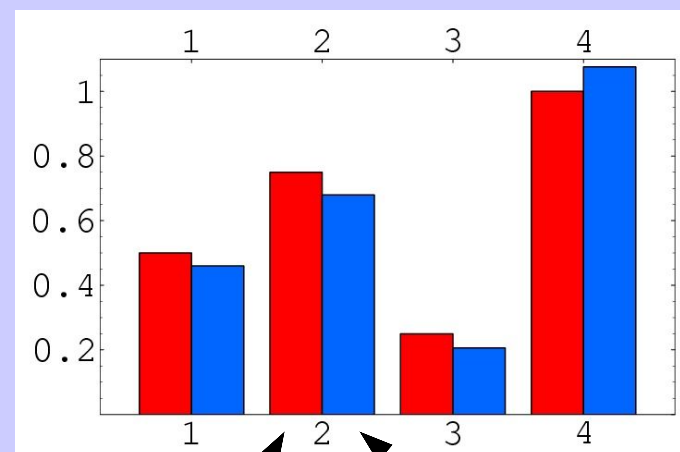




$F > 0.98$







$F > 0.99$

Theoretical transversal distribution of intensity

Actually measured intensity distribution

Used weights

Reconstructed weights

Conclusions

- Minimal symmetric tomography was introduced
- Its properties were discussed
- Its optical implementations were shown
- Its applications in QKD were discussed