# Semi device-independent security of one-way QKD

Nicolas Brunner & Marcin Pawlowski

PRA 84, 010302(R) (2011)

University of BRISTOL

EPSRC
Engineering and Physical Sciences Research Council

# Device-Independent (DI) QKD

Acin, Barrett, NB, Colbeck, Ekert, Gisin, Hanggi, Hardy, Kent, Masanes, Massar, Pironio, Renner, Scarani, Wolf...

Fundamental & practical interest

Based on nonlocality (Bell violation)

$\Rightarrow$ Entanglement

Implementation is very challenging: **loophole-free Bell test**
(Gisin, Pironio, Sangouard, PRL 2010)

# Device-Independent (DI) QKD

Acin, Barrett, NB, Colbeck, Ekert, Gisin, Hanggi, Hardy, Kent, Masanes, Massar, Pironio, Renner, Scarani, Wolf...

Fundamental & practical interest

Based on nonlocality (Bell violation)

⇒ Entanglement

Implementation is very challenging: **loophole-free Bell test**
(Gisin, Pironio, Sangouard, PRL 2010)

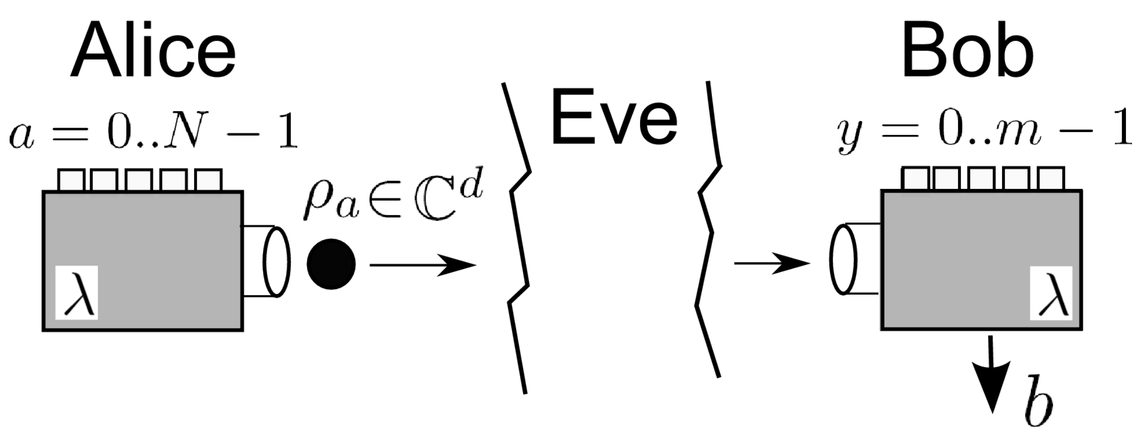
⇒ **Can we think of something simpler?**

# Semi DI QKD

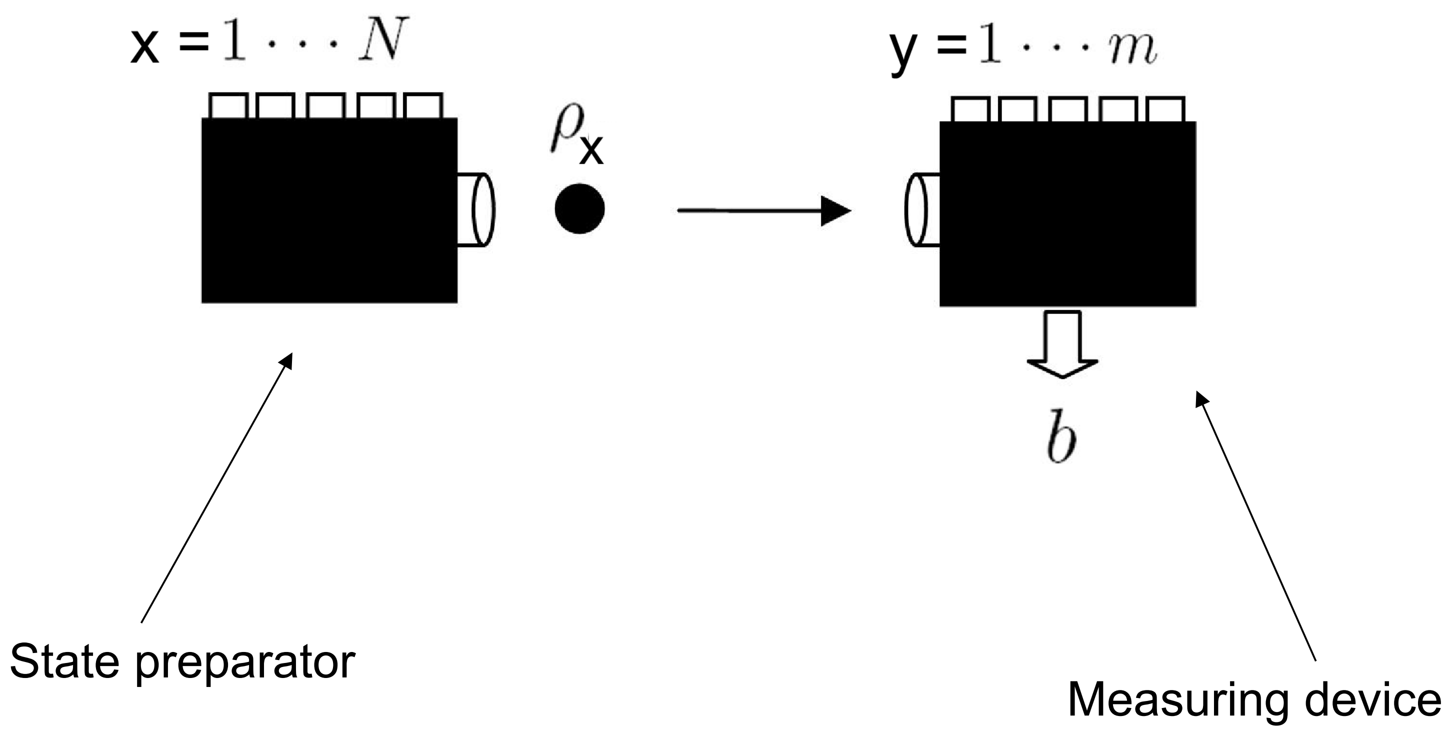
**Semi DI scenario:**
**Uncharacterized devices but bounded Hilbert space dimension**

**Security proof for 1-way (prepare & measure) configuration**

**Proof based on dimension witnesses and random-access-codes**
**Not on entanglement**

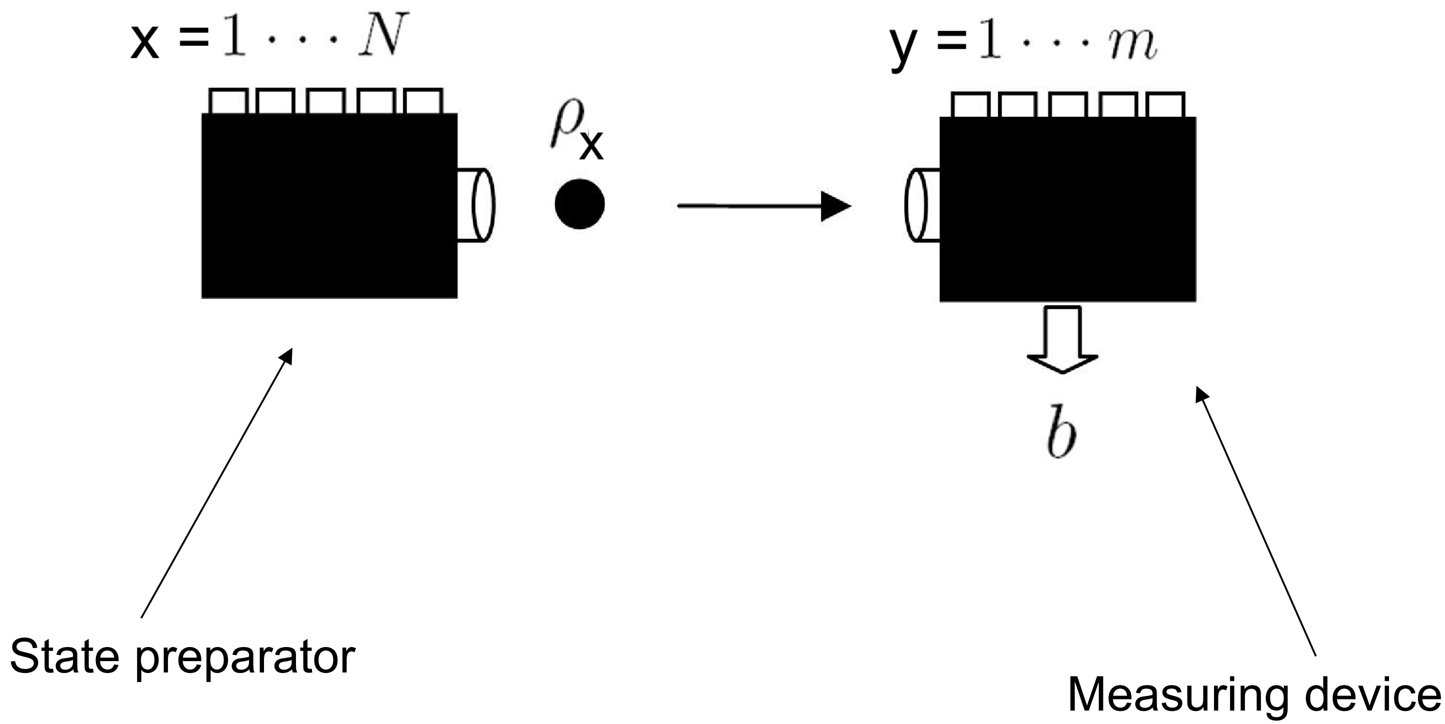


# Setup



x = $1 \cdots N$
$\rho_x$
y = $1 \cdots m$
$b$
State preparator
Measuring device

# Setup




$P(b|x,y)$

Can we make a device-independent (DI) statement about the dimensionality of $\rho_x$?

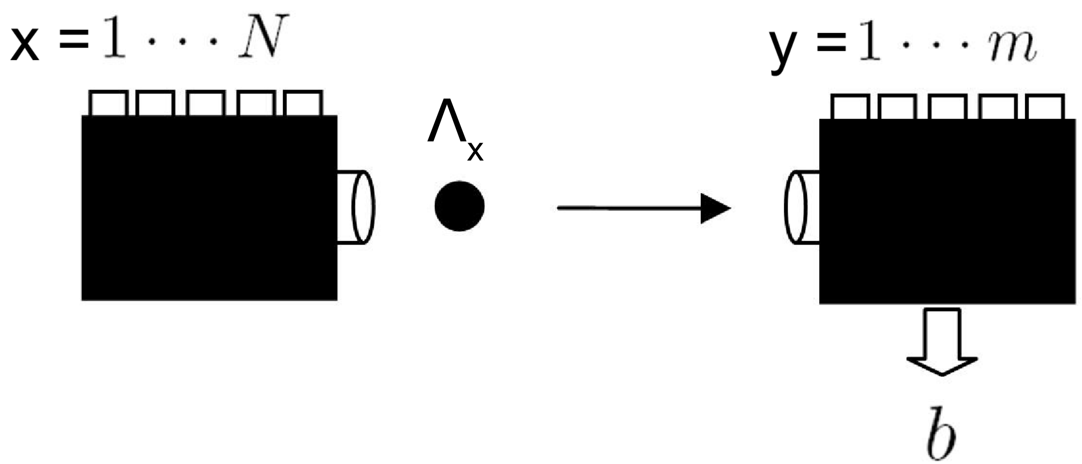
# Data Table

<table>
<tr><th></th><th colspan="2">m1</th><th colspan="2">m2</th><th></th></tr>
<tr><th></th><th>+1</th><th>-1</th><th>+1</th><th>-1</th><th>...</th></tr>
<tr><td>P1</td><td>P(+1|1,1)</td><td>P(-1|1,1)</td><td>P(+1|1,2)</td><td>P(-1|1,2)</td><td></td></tr>
<tr><td>P2</td><td>P(+1|2,1)</td><td>P(-1|2,1)</td><td>P(+1¦2,2)</td><td>P(-1¦2,2)</td><td></td></tr>
<tr><td>...</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Given a data table, can we find useful bounds on the classical and quantum dimensions?

N. Harrigan, T. Rudolph, and S. Aaronson, arXiv:0709.1149

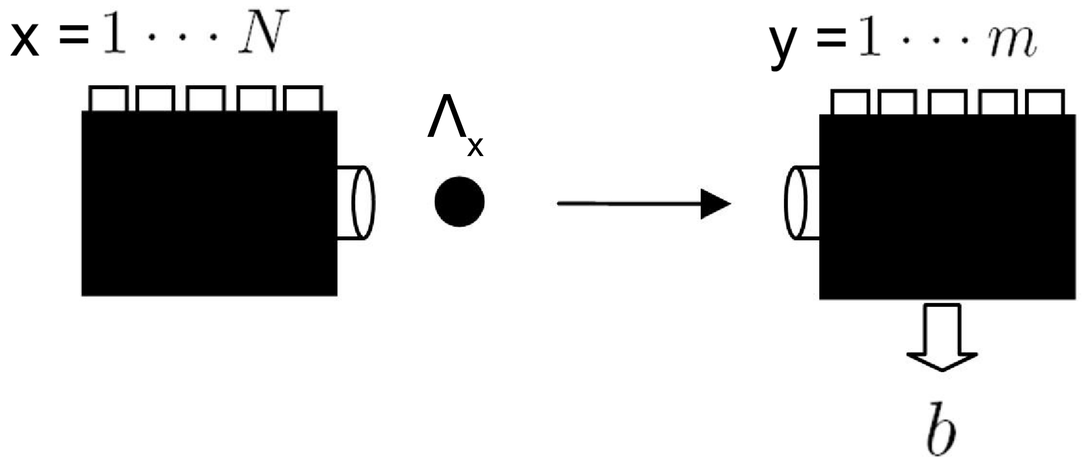
# Testing classical systems




$\Lambda_x$ is a classical state of dimension d, ie a probability distribution over dits

Experiment = set $\vec{E}$ of correlators $E_{xy} = P(b = +1|x, y) - P(b = -1|x, y)$

# Testing classical systems




$\Lambda_x$ is a classical state of dimension d, ie a probability distribution over dits

Experiment = set $\vec{E}$ of correlators $E_{xy} = P(b=+1|x,y) - P(b=-1|x,y)$

**Dimension witness** $$\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$$

(~Bell inequality for data tables)

R. Gallego, NB, C. Hadley, A. Acin, PRL 2010

# Dimension witnesses

**Simple observation:** if $N \le d$ then all experiments can be reproduced classically

$\Rightarrow$ $N > d$ (more preparations than tested dimension)

# Dimension witnesses

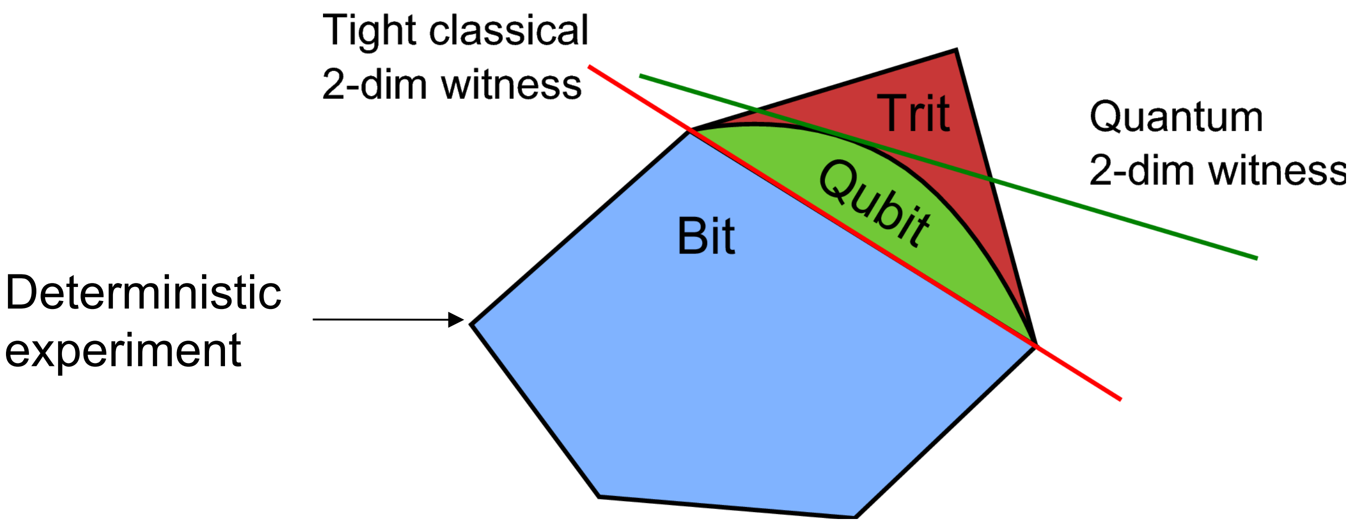
**Simple observation:** if N<=d then all experiments can be reproduced classically

⇒ $N > d$ (more preparations than tested dimension)

**How to find dimension witnesses?**

⇒ **Geometrical approach**

# Geometry




Set of experiments possible with classical systems of dim d is a polytope

⟹ Facets = Tight classical dim-witness

$$\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$$

$$\leq Q_d$$ Q dimension witness

# Example

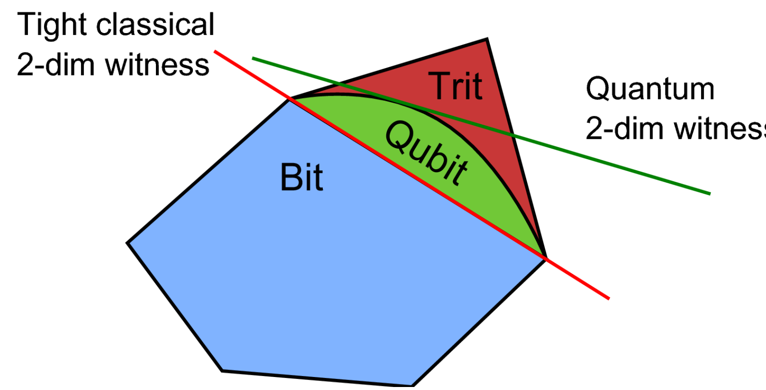
Simplest case: 3 preparations and 2 measurements

$$I_3 \equiv |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \leq 3.$$

| | M1 | M2 |
|---|---|---|
| P1 | + | + |
| P2 | + | - |
| P3 | - | 0 |

$\leq$ 3 (bit)

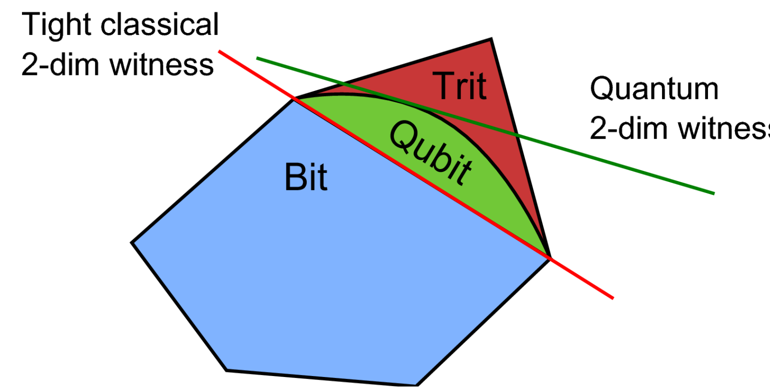
$\leq$ 5 (trit)



# Example

Simplest case: 3 preparations and 2 measurements

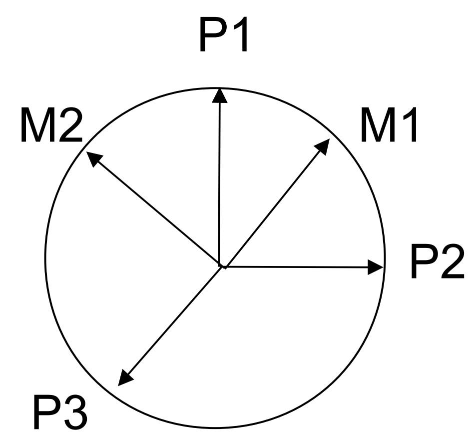
$$I_3 \equiv |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \leq 3.$$




| | M1 | M2 |
|---|---|---|
| P1 | + | + |
| P2 | + | - |
| P3 | - | 0 |

$\leq$ 3 (bit)

$\leq$ 5 (trit)




With qubits: $I_3 \leq 1 + 2\sqrt{2} \approx 3.8284$

Importance of 3rd preparation: CHSH is not a witness (Leggett-Garg not DI)

# What can we do with this quantum advantage ?

- No-go theorem for ontological models

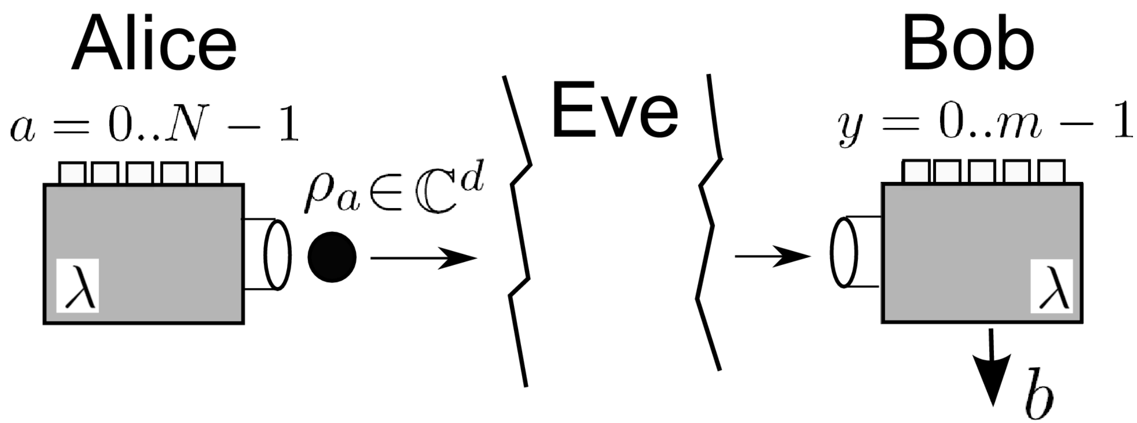
  Exponential separation
  Family of data tables: QM → dim d
  Classicaly → dim ≥ 2^d

  The universe is not exponentially complicated

  Barrett,NB,Gallego,Gogolin (in preparation)

- Security proof for semi DI QKD

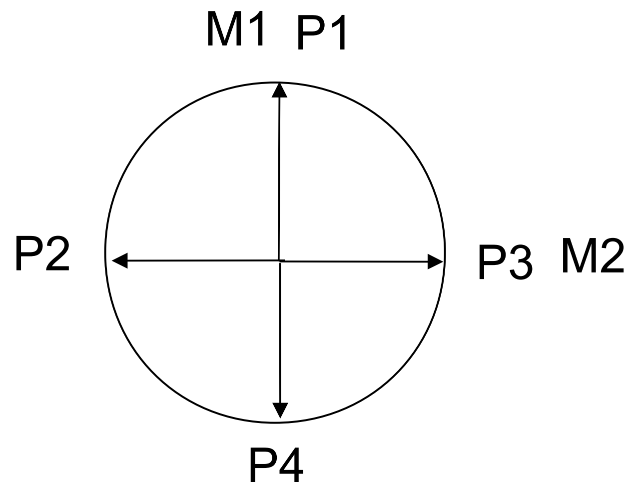
# Semi DI QKD



# BB84

4 qubit preparations (|+z>, |-z>, |+x>, |-x>) and 2 measurements (Z,X)

| | M1 | M2 |
|---|---|---|
| P1 | +1 | 0 |
| P2 | 0 | -1 |
| P3 | 0 | +1 |
| P4 | -1 | 0 |




Does not violate any 2-dim classical witness!

Can be reproduced by sending a classical bit

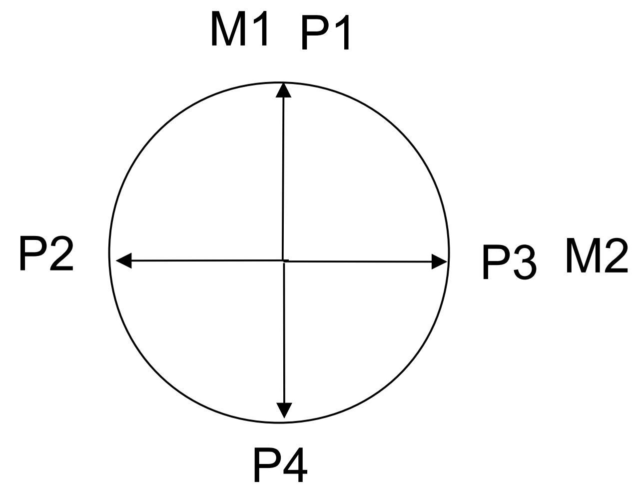
**No security in a semi-DI scenario**

# BB84

4 qubit preparations ($|{+z}\rangle$, $|{-z}\rangle$, $|{+x}\rangle$, $|{-x}\rangle$) and 2 measurements (Z,X)

basis outcome

| a0 | a1 | | M1 | M2 |
|---|---|---|---|---|
| 0 | 0 | P1 | +1 | 0 |
| 1 | 0 | P2 | 0 | -1 |
| 1 | 1 | P3 | 0 | +1 |
| 0 | 1 | P4 | -1 | 0 |




Does not violate any 2-dim classical witness!

Can be reproduced by sending a classical bit

⇨ **No security in a semi-DI scenario**

**Strategy** $\lambda=0$: Alice sends $m=a0+a1$, Bob outputs $b=m+y$

If $y=a0$, then $b=a1$ else $b=a1+1$

$\lambda=1$: Alice sends $m=a1$, Bob outputs $b=m=a1$

# Dimension witness and random access codes

| | M1 | M2 |
|---|---|---|
| P1 | + | + |
| P2 | + | - |
| P3 | - | + |
| P4 | - | - |

$\leq 4$ (for classical bits)

# Dimension witness and random access codes

| a0 | a1 | | M1 | M2 |
|---|---|---|---|---|
| 0 | 0 | P1 | + | + |
| 0 | 1 | P2 | + | - |
| 1 | 0 | P3 | - | + |
| 1 | 1 | P4 | - | - |

$\leq 4$ (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

$\Rightarrow$ P_guess = (I + 8) / 16

I ≤ 4 corresponds to P_guess ≤ ¾

(classical limit for RAC)

# Dimension witness and random access codes

| a0 | a1 | | M1 | M2 |
|---|---|---|---|---|
| 0 | 0 | P1 | + | + |
| 0 | 1 | P2 | + | - |
| 1 | 0 | P3 | - | + |
| 1 | 1 | P4 | - | - |

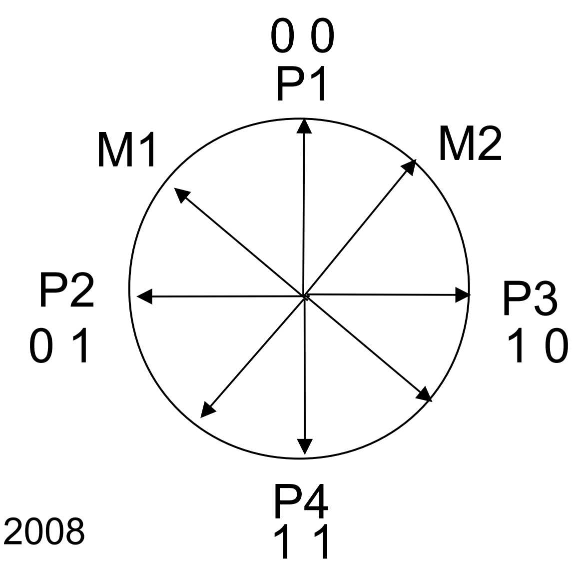
$\leq 4$ (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

P_guess = (I + 8) / 16

I $\leq$ 4 corresponds to P_guess $\leq$ ¾
(classical limit for RAC)

For qubits, P_guess <= $\cos^2(\pi/8) \sim 0.85$




See also S. Wehner, M. Christandl, A. Doherty, PRA 2008

# Security proof

Individual attacks: Csiszar & Korner (1978) $I(A:B) > I(A:E)$

$P_B > P_E$ ⇒ Positive key rate

Proof based on a result by R. König (PhD thesis)

$F_n$ : set of balanced boolean functions on n-bit strings

Alice receives a (uniformly chosen) n-bit string; Bob receives a function in $F_n$
Alice sends s qubits to Bob. Bob's probability of guessing is bounded by

$$P_n \leq \frac{1}{2}\left(1+\sqrt{\frac{2^s-1}{2^n-1}}\right)$$

# Security proof

We have n=2, s=1 $$P_B(a_0) + P_B(a_1) + P_B(a_0 \oplus a_1) \le \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Assume Bob and Eve collaborate

$$P_{BE}(a_0) + P_{BE}(a_1) + P_{BE}(a_0 \oplus a_1) \ge 2P_B(a_0) + 2P_E(a_1) - 1$$

$$\boxed{\begin{aligned} P_{BE}(a_0 \oplus a_1) &\ge P_{BE}(a_0, a_1) \\ &\ge P_{BE}(a_0) + P_{BE}(a_1) - 1 \end{aligned}}$$

$$P_{BE}(a_i) \ge P_B(a_i)$$

$$\Rightarrow P_B(a_0) + P_E(a_1) \le \frac{5+\sqrt{3}}{4} \Rightarrow P_B + P_E \le \frac{5+\sqrt{3}}{4}$$

$$\Rightarrow P_B > P_E$$ when $$P_B > \frac{5+\sqrt{3}}{8} \approx 0.8415$$

# Security proof

We have n=2, s=1 $$P_B(a_0) + P_B(a_1) + P_B(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Assume Bob and Eve collaborate

$$P_{BE}(a_0) + P_{BE}(a_1) + P_{BE}(a_0 \oplus a_1) \geq 2P_B(a_0) + 2P_E(a_1) - 1$$

$$\begin{aligned} P_{BE}(a_0 \oplus a_1) &\geq P_{BE}(a_0, a_1) \\ &\geq P_{BE}(a_0) + P_{BE}(a_1) - 1 \end{aligned}$$

$$P_{BE}(a_i) \geq P_B(a_i)$$

$$\Rightarrow \quad P_B(a_0) + P_E(a_1) \leq \frac{5+\sqrt{3}}{4} \quad \Rightarrow \quad P_B + P_E \leq \frac{5+\sqrt{3}}{4}$$

$$\Rightarrow \quad P_B > P_E$$ when $$P_B > \frac{5+\sqrt{3}}{8} \approx 0.8415$$

**Security**

Qubits can reach $$P_B = \cos^2(\pi/8)) \approx 0.8536$$

# Relevance of the semi-DI approach?

**Conceptual interest**

proof not based on entanglement

**Practical viewpoint**

Not fully DI (side-channels?)

Relaxation compared to usual security proofs
Alice is Semi-DI (preparations of given dimension but non-characterized)
Bob is fully DI

# Open questions

**Practical**

What about more general attacks?

Larger key rates?

Can security be guaranteed with qubits under the assumption that d>2?

**Conceptual**

Does violation of a dimension witness imply security?

Link to contextuality?
Is preparation contextuality a resource for semi-DI QKD?