GAP Optique Geneva University

From Bell’s theorem to secure key distribution

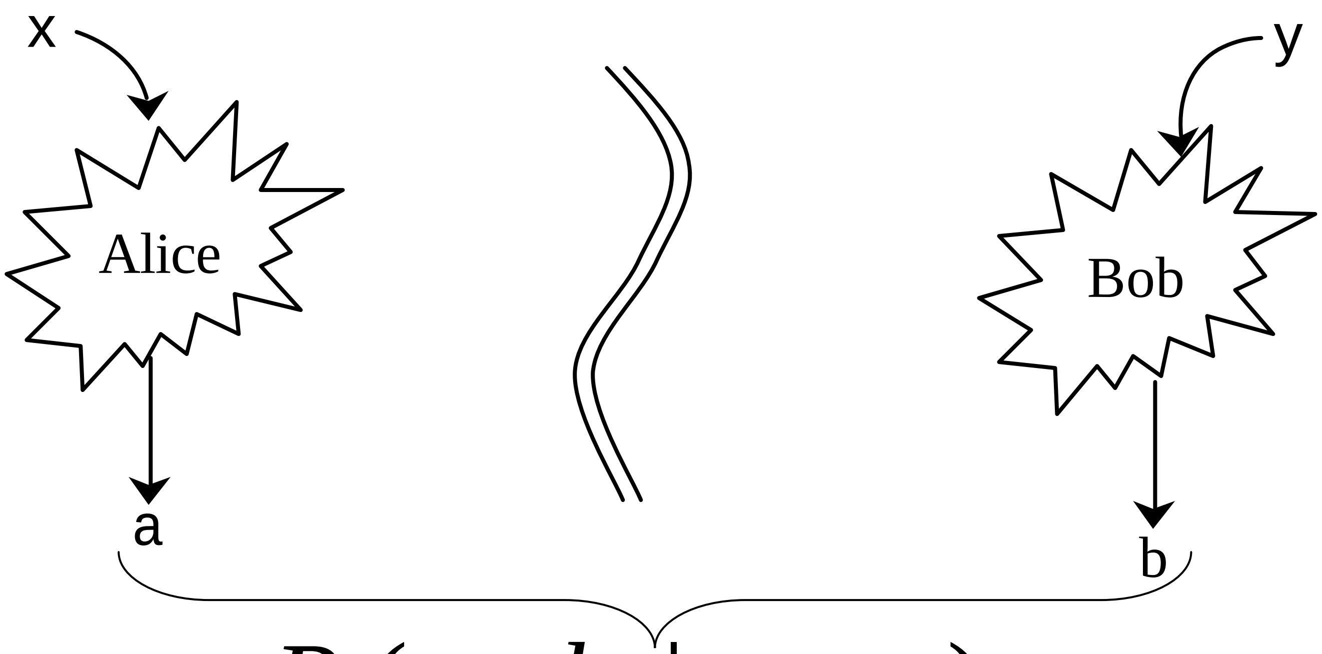
Nicolas Gisin, Valerio Scarani, Geneva

Antonio Acin, Barcelona

Lluis Masanes, Bristol

- Key distribution: abstract setting
- Assumptions in security proofs of “unconditional” QKD
- Security against individual attacks from no-signaling
- Heisenberg uncertainty for non-signaling correlations

Key distribution: abstract setting



$$P(a,b\,|\,x,y)$$

assumptions about Eve's power

$$P(a,b,e\,|\,x,y,z)$$

key distillation Þ **secret key**

Assumptions in security proofs of "unconditional" QKD

$$P\,(\underbrace{a\,,\,b}_{\text{measurements outcomes}}\;|\;\underbrace{x\,,\,y}_{\text{bases choices}})$$

Example of BB84: P(a=b|x=y) ≈ 1

Eve's power limited only by quantum laws ⇒ ~~secure secret key~~

and Alice and Bob's Q systems are 2-dimensional ⇒ secure secret key

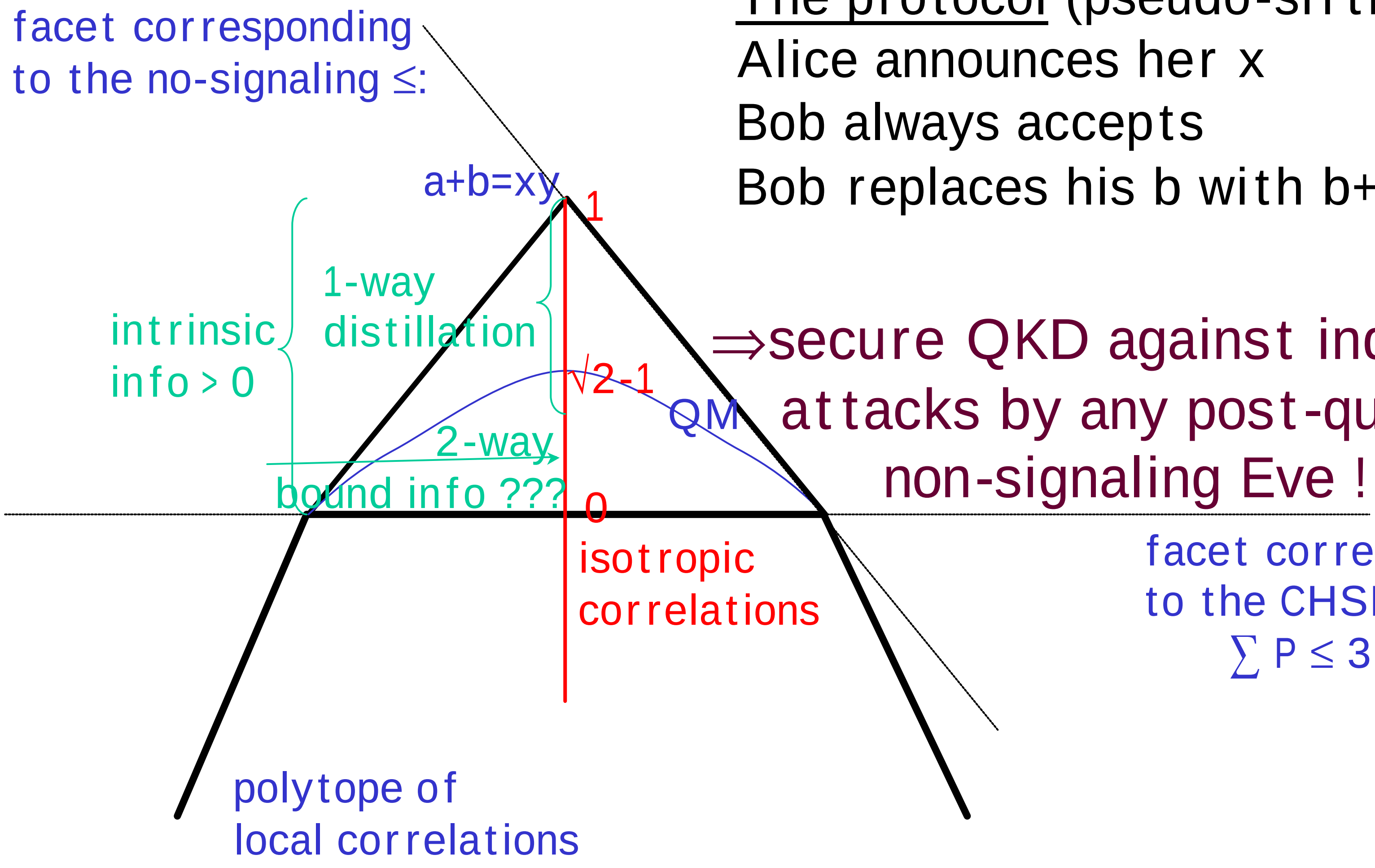
$$\frac{1}{4}\Big(|0,0\rangle_{ab}\langle 0,0| + |1,1\rangle_{ab}\langle 1,1|\Big)_z \otimes \Big(|0,0\rangle_{ab}\langle 0,0| + |1,1\rangle_{ab}\langle 1,1|\Big)_x$$

This is a real thread to actual implementations of QKD, known as « side channels ».

Security against individual attacks from no-signaling

J.Barrett et al, PRL'05
A.Acin, L.Masanes, NG
quant-ph/0510094

Eve distributes the correlation.
For each realization she produces one of the vertices with fixed prob.



The protocol (pseudo-sifting):
Alice announces her x
Bob always accepts
Bob replaces his b with b+xy

⇒secure QKD against individual attacks by any post-quantum non-signaling Eve !

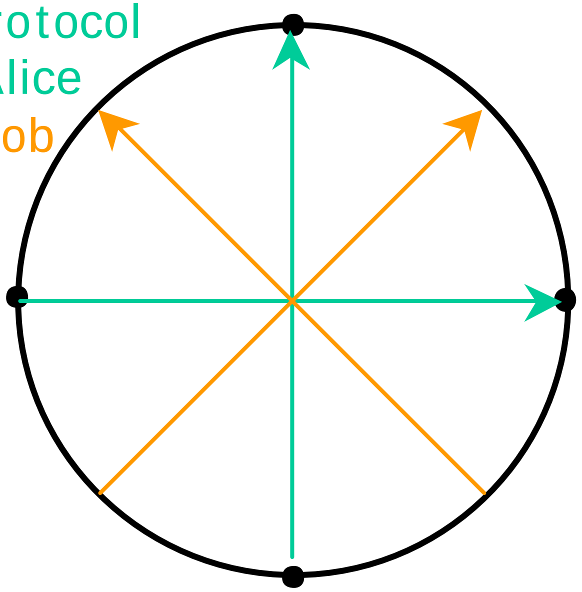
Security against individual attacks from no-signaling

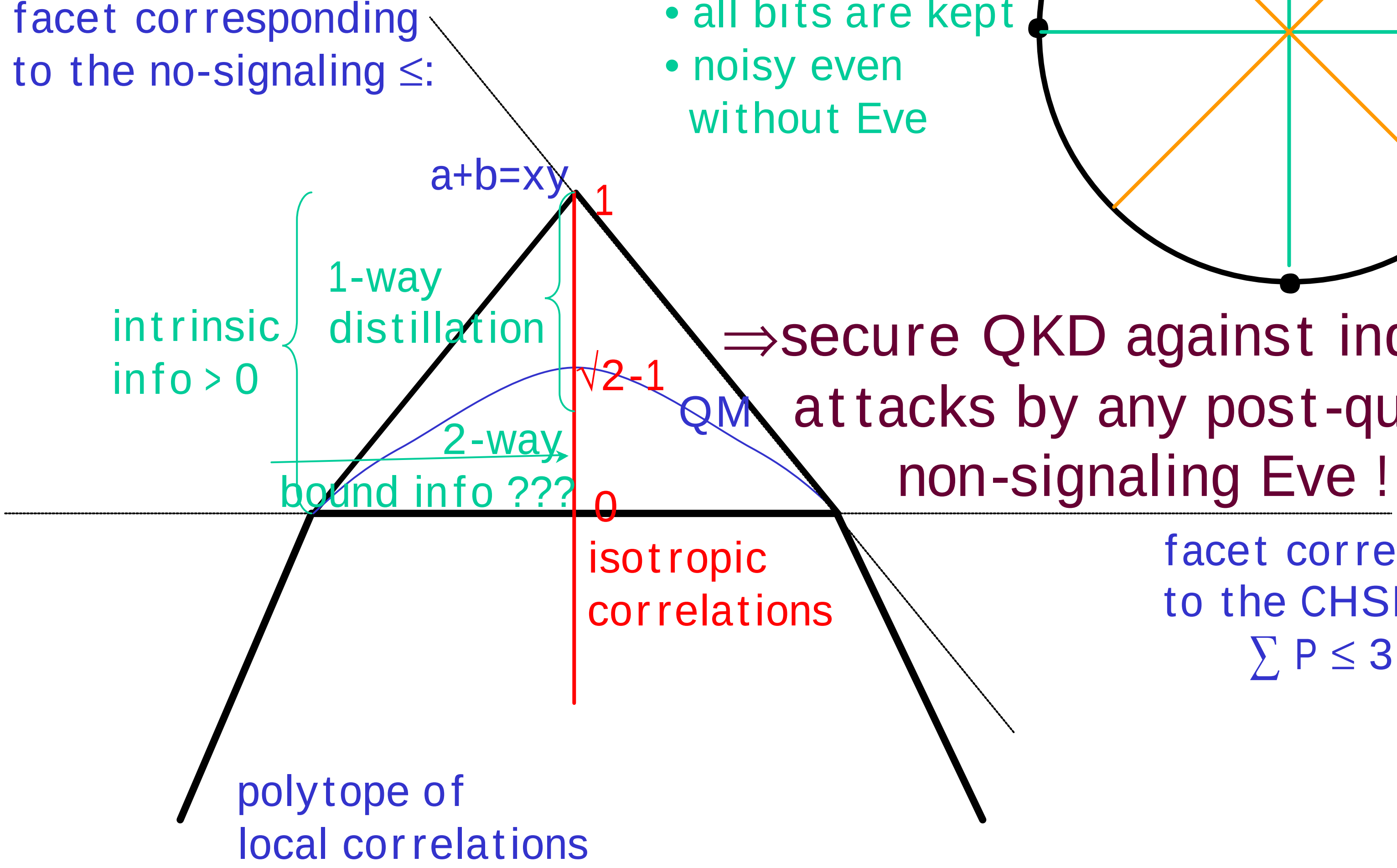
A.Acin, L.Masanes, NG
quant-ph/0510094

CHSH Q-crypto protocol

pseudo-sifting:

- 1-way
- all bits are kept
- noisy even without Eve





⇒secure QKD against individual attacks by any post-quantum non-signaling Eve !

Heisenberg uncertainty for non-signaling correlations

QBER for a given input x on Alice side: $Q_x = P(a \neq b|x)$

Eve's information gain: $I(E,B|x)$

Information gain versus disturbance trade-off:

$$I(E,B|x=0) = \frac{1}{2} Q_{x=1} \qquad\qquad I(E,B|x=1) = \frac{1}{2} Q_{x=0}$$

Conclusions

- Correlations that do not violate any Bell inequality can not be distilled to a secret key without assumptions on the Hilbert space dimensions.
- Any correlation that violates some Bell inequality has a positive intrinsic information.
- In the binary case, security is proven against individual attacks for most nonlocal correlations, including some Q correlations.
- In the binary case, the Heisenberg trade-off bw information gain and disturbance holds for all non-signaling correlations.