東京大学
THE UNIVERSITY OF TOKYO

# Continuous Variable Entropic Uncertainty Relations in the Presence of Quantum Memory

QCRYPT 2013 - Waterloo - 9. Aug. 2013


Fabian Furrer

The University of Tokyo, Graduate School of Science

JOINT WORK WITH:

MARIO BERTA, VOLKHER SCHOLZ, MATTHIAS CHRISTANDL
**ETH ZURICH**

MARCO TOMAMICHEL
**CQT SINGAPORE**

## Motivation
# Some History

**Position and Momentum Operators:**

- Heisenberg's Uncertainty Relation

$$\sqrt{Var(Q)Var(P)} \geq \hbar/2$$

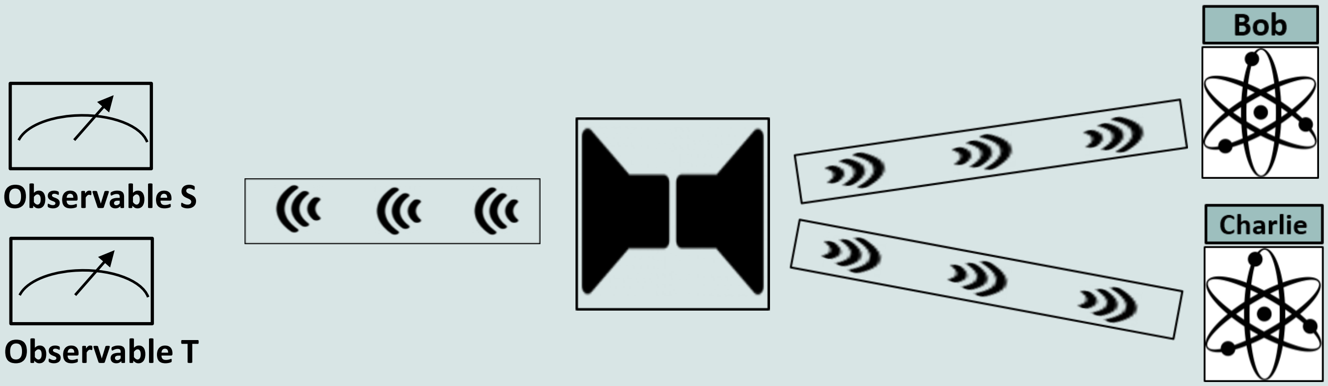
- Generalization to Entropies **(Beckner 75, I. Bialynicki-Birula and J. Mycielski. 75)**

$$h(Q) + h(P) \geq \log e\pi$$

**Finite dimensional (Massen and Uffink 88):**

$$H(S) + H(T) \geq -\log c \qquad c = \max_{k.l} |< s_k|t_l >|^2$$

### Motivation:
# Uncertainty Principle in the Presence of Quantum Memory



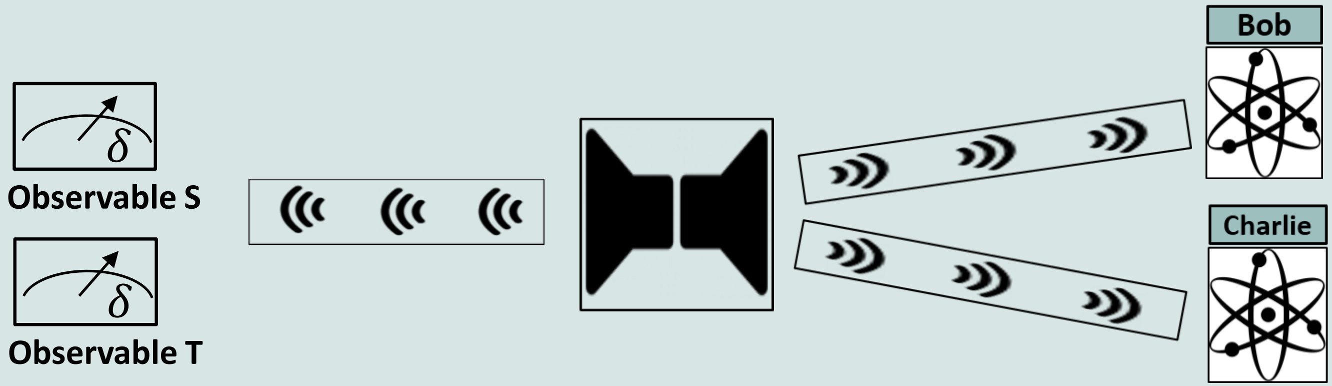

**Example: A & B share maximally entangled qubits and $S = \sigma_Z$ , $T = \sigma_X$**

- **no uncertainty for Bob**
- **maximal uncertainty for Charlie:** completely uncorrelated to Alice and Alice's state is maximally mixed

Combines uncertainty principle with monogomay of entanglement.

東京大学 THE UNIVERSITY OF TOKYO

**Motivation:**
# Uncertainty Principle in the Presence of Quantum Memory




Constraint on the sum of the uncertainty of Q w.r.t. Bob and P w.r.t. Eve:

$$H(S|B) + H(T|E) \geq -\log c$$

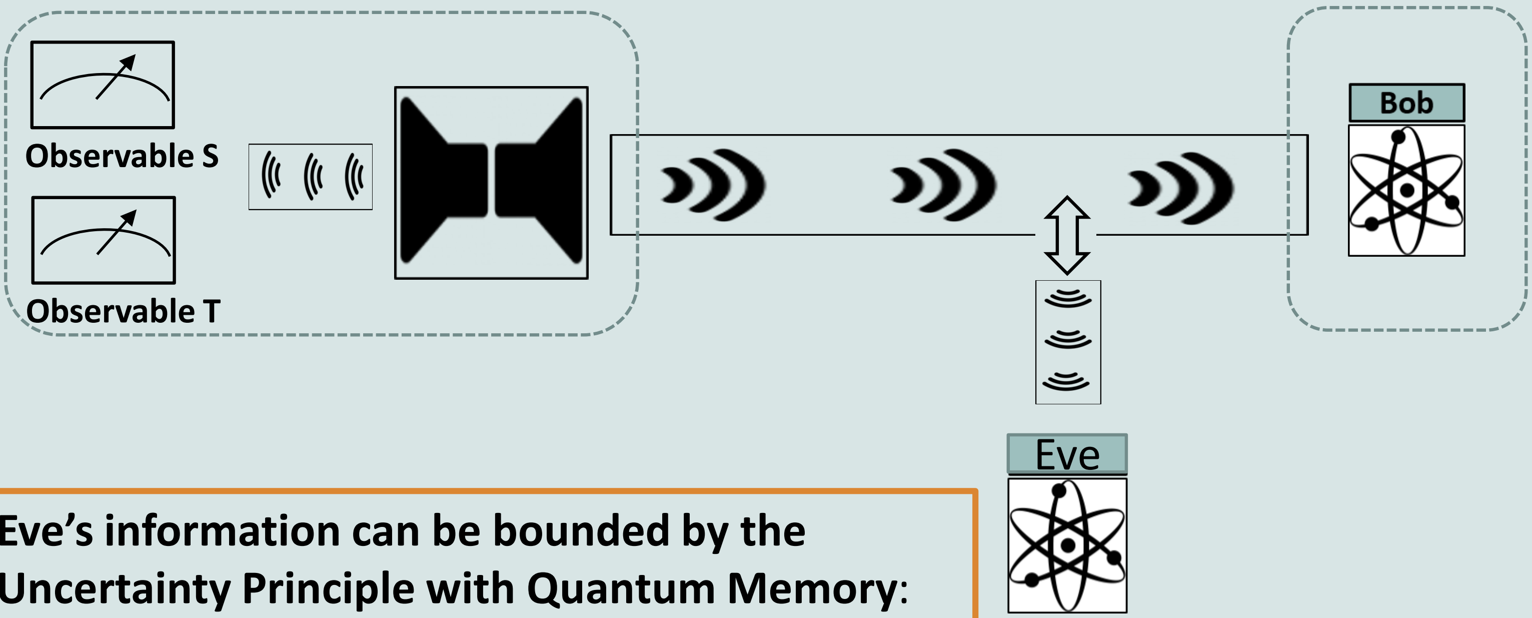
$H(S|B) = H(SB) - H(B)$ von conditional Neumann entropy of $\rho_{SB} = \sum_s P(s)|s >< s| \otimes \rho_B^s$ .

**Exactly what we use in Quantum Key Distribution Protocols!**

M. Berta et al., Nature Physics 6, 2010

**Motivation:**

# The connection between QKD and the Uncertainty Principle with Quantum Memory




**Eve's information can be bounded by the Uncertainty Principle with Quantum Memory**:

$$H(S|E) \geq -\log c - H(T|B)$$

東京大学 THE UNIVERSITY OF TOKYO

**Motivation:**

# Application of the Uncertainty Principle with Quantum Memory in QKD Security Proofs

## *Discrete Protocol:*

Security of BB84 Protocol against coherent attacks including finite-size effects
**M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. 3, 634 (2012).**

## *Continuous Variable Protocol:*

Security of two-mode squeezed state against coherent attacks including finite-size effects **FF, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. 109, 100502 (2012)**

- first quantitative analyses against coherent attacks!
- using a binning of the continuous outcomes measurements into a finite number of outcomes
- Implementation:

**Realization of finite-size continuous-variable quantum key distribution based on Einstein-Podolsky-Rosen entanglement**
Tobias Eberle, and Vitus Händchen, Fabian Furrer, Torsten Franz, Jörg Duhme, Reinhard F. Werner, and Roman Schnabel
Abstract Extended abstract

# Our Contribution

**Generalize Uncertainty Principle to**

- continuous outcomes (e.g., Position-Momentum Operators)
- arbitrary (infinite-dimensional) quantum memories

**Entropy Measures:**

- generalize differential conditional von Neumann entropy (**asymptotic limit**)
- introduce differential conditional min-/max-entropy (**finite-size QKD!**)

**Related work:**

- For restricted definition of diff. cond. von Neumann entropy: **R. L. Frank, E. H. Lieb, arXiv:1204.0825**
- For min-/max-entropy with arbitrary quantum memories but finite number of outcomes: **M. Berta, FF, V. Scholz, arXiv:1107.5460**

東京大学 THE UNIVERSITY OF TOKYO

# Our Contribution

**Generalize Uncertainty Principle to**

- continuous outcomes (e.g., Position-Momentum Operators)
- arbitrary (infinite-dimensional) quantum memories

**Entropy Measures:**

- generalize differential conditional von Neumann entropy (**asymptotic limit**)
- introduce differential conditional min-/max-entropy (**finite-size QKD!**)

**Related work:**

- For restricted definition of cond. von Neumann entropy: **R. L. Frank, E. H. Lieb, arXiv:1204.0825**
- For min-/max-entropy with arbitrary quantum memories but finite number of outcomes: **M. Berta, FF, V. Scholz, arXiv:1107.5460**

# Outlook

I. **Continuous Variable Systems**
   - **Position and Momentum Operators**

II. **Differential Conditional von Neumann Entropy**
   - **Approximation by finer and finer coarse graining**

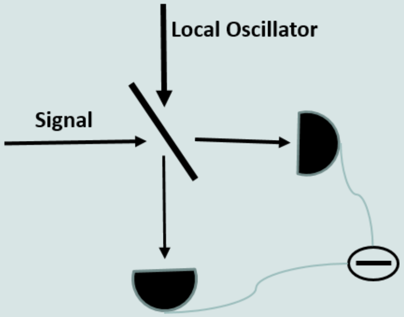
III. **Uncertainty Relations in Presence of Quantum Memory**
   - **Finite precision position-momentum measurements**
   - **Infinite precision position-momentum measurements**

# Continuous Variable (CV) Systems

Most Important Example in Quantum Information processing:

**Quadratures of em-field** (continuous degree of freedom)

Measurement: **Homodyne detection**




**Model for one mode:**

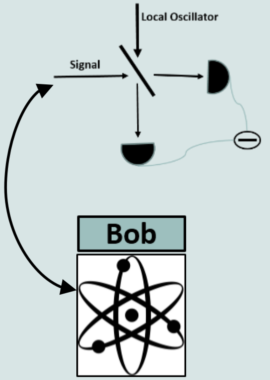
- Equivalent to Harmonic Oscillator
- Infinite-dimensional Hilbert space (square integrable functions)
- Quadrature Measurement with phase shift $\phi = \frac{\pi}{2}$: P, Q satisfying

$$[Q, P] = i$$

**Position & Momentum Operators: Continuous spectrum!**

# Position & Momentum Mesurements

**Continuous Outcomes (infinite precision):**




**Outcome:**

$x \in X$ = Real Line

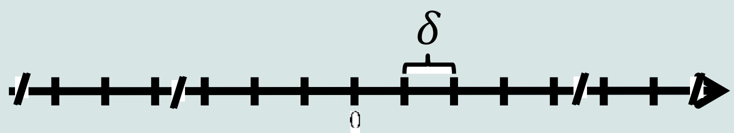
$\rho_B(x)$ = post-measurement state

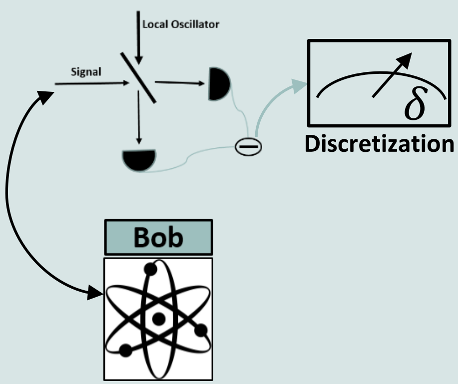
**Continuous probability distribution & set of post-measurement states:**

$\rho_{XB}$ "=" $P(x), \{\rho_B(x)\}$

# Position & Momentum Mesurements

**Discrete Outcomes (finite precision):**

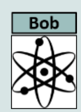



**Outcome:**

$k \in X_\delta$={0,1,2,…}

$\rho_B^k$

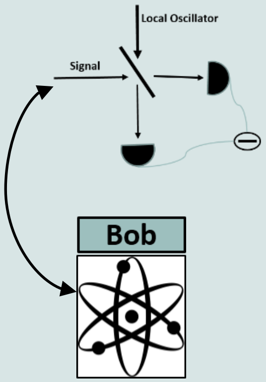



**Discrete probability distribution & set of post-measurement states:**

$$\rho_{X_\delta B} \ \text{"="} \ p_k, \{\rho_B^k\}$$

# Position & Momentum Mesurements

**Continuous Outcomes (infinite precision):**




**Outcome:**

$x \in X$ = Real Line

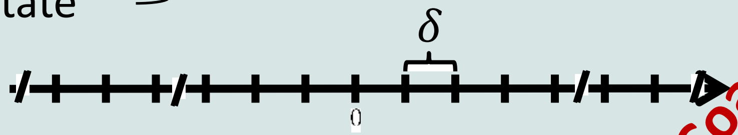
$\rho_B(x)$ = post-measurement state

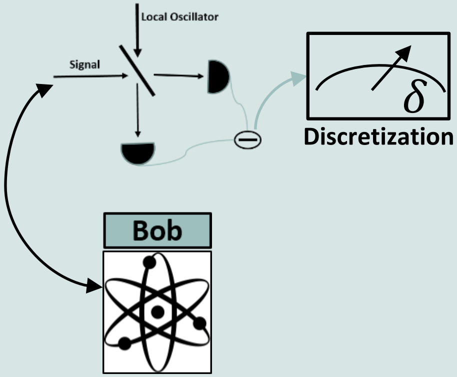
**Continuous probability distribution & set of post-measurement states:**

$$\rho_{XB} \text{ "=" } P(x), \{\rho_B(x)\}$$

Coarse-Graining

**Discrete Outcomes (finite precision):**




**Outcome:**

$k \in X_\delta$ =

$\rho_B^k$

**Discrete probability distribution & set of post-measurement states:**

$$\rho_{X_\delta B} \text{ "=" } p_k, \{\rho_B^k\}$$

# II. Differential Conditional Entropies

**Our approach to differential conditional entropies:**

***A unified definition of conditional entropies continuous in the limit of finer and finer coarse graining!***

**Further:**

- Most General Setting
- No restriction on the states (important for QKD)

東京大学 THE UNIVERSITY OF TOKYO

# II. Differential Conditional Entropies:
## The Conditional von Neumann Entropy

**Y finite discrete, B finite-dimensional system:**

$$\boldsymbol{H(Y|B) = H(YB) - H(B)}$$

- $\rho_{YB} = \sum_y p_y |y><y| \otimes \rho_B^y$ “=“ $p_y, \{\rho_B^y\}$, $H(\rho) = -tr\, \rho \log \rho$
- $\mathrm{H(Y}|B) = -\sum_y D(p_y \rho_B^y || \rho_B)$ with $D(\rho||\sigma) = tr\rho \log\rho - tr\rho \log \sigma$ quantum relative entropy (arbitrary quantum systems, Araki ‘76)

***Definition:*** $(\boldsymbol{X}, \boldsymbol{\mu})$ **measure space**

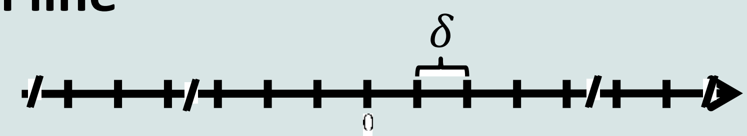
$$\boldsymbol{h(X|B) = -\int D(P(x)\rho_B(x)||\rho_B)d\mu(x)}$$

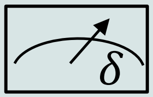
- X = real line: $h(X|B) = -\int D(P(x)\rho_B(x)||\rho_B)dx$ : **differential entropy**
- X = discrete: $H(X|B) = -\sum_x D(p_x \rho_B^x||\rho_B)$ (capital letter)

# II. Differential Conditional Entropies: Discrete Approximation

**Continuous Variable X = real line**

I. Coarse Graining with $\delta$:




**Observable S**

$X_\delta$=discrete and conditional entropy $H(X_\delta|B)$

II. Infinte Precision:

$X$= real line and conditional entropy $\mathrm{h}(\mathrm{X}_\delta|\mathrm{B})$

**Approximaton Theorem:**

$$h(X|B) = \lim_{\delta \to 0} \left( H(X_\delta|B) + log\delta \right)$$

- Assumptions: $h(X|B) \succ -\infty$ and $H(X_\delta|B) < \infty$ for an arbitrary $\delta$.

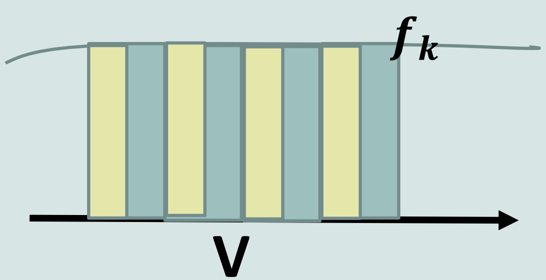
# II. Differential Conditional Entropies:
Discrete Approximation

**Approximaton Theorem:**

$$h(X|B) = \lim_{\delta \to 0} \left( H(X_\delta|B) + log\delta \right)$$

$$2^{h(X|B)} = \lim_{\delta \to 0} \frac{2^{H(X_\delta|B)}}{\delta}$$

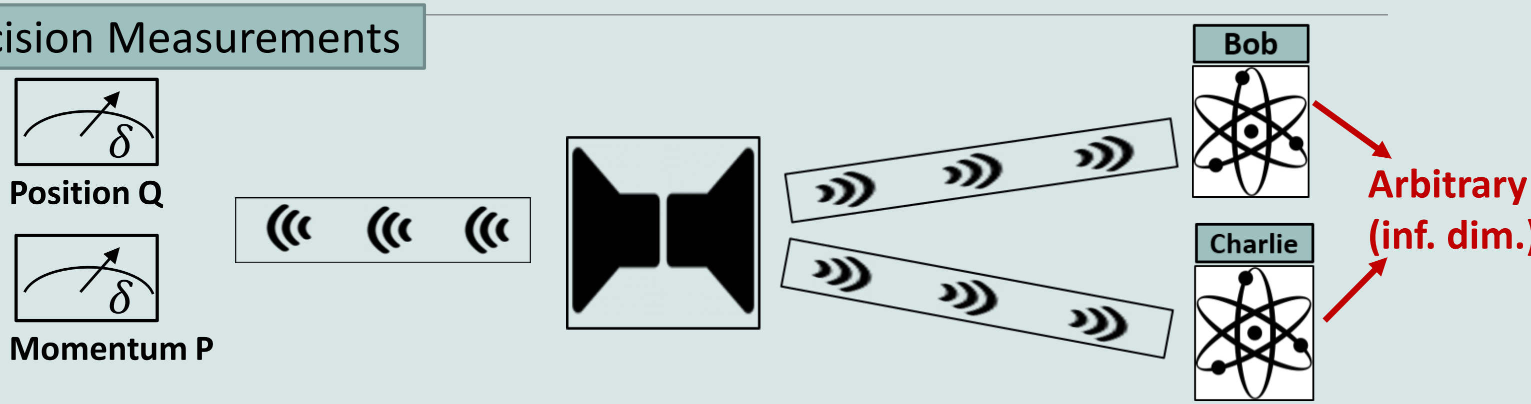
- Operational Approach
- Practical (computations)
- Intuition: It converges for $\delta$ small enough such that function looks constant




Entropy in V $= -\frac{V}{\delta} * (\delta f_k) \log \delta f_k =$
$- V f_k \log f_k - V f_k \log \delta$

# III. Uncertainty Relation in Presence of Quantum Memory
## P-Q Measurements with Finite Precision

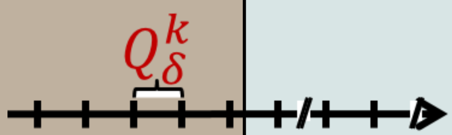
### Finite Precision Measurements




***Uncertainty Relation (finite precision):***

$$H(Q_\delta|B) + H(P_\delta|C) \geq -\log c(\delta)$$

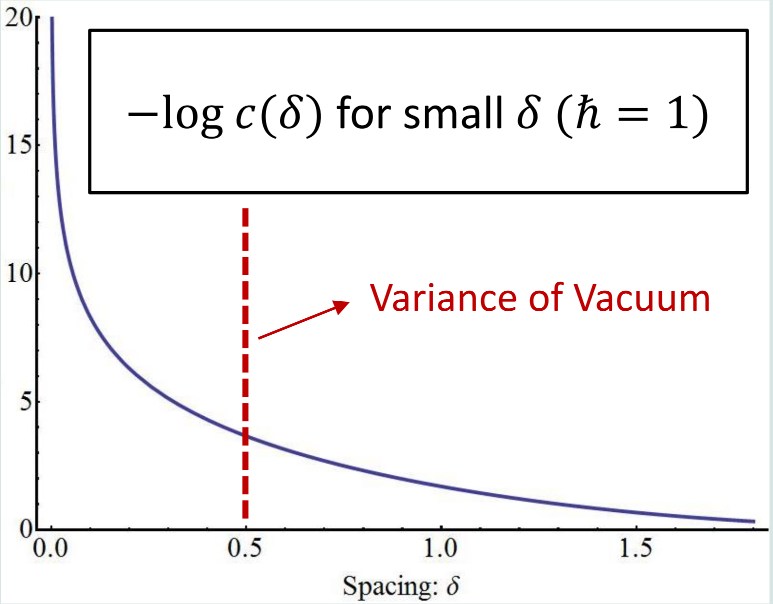
$$c(\delta) = \sup_{k,l} \left\| \sqrt{Q_\delta^k} \sqrt{P_\delta^l} \right\|^2 \approx \frac{\delta^2}{2\pi\hbar}$$

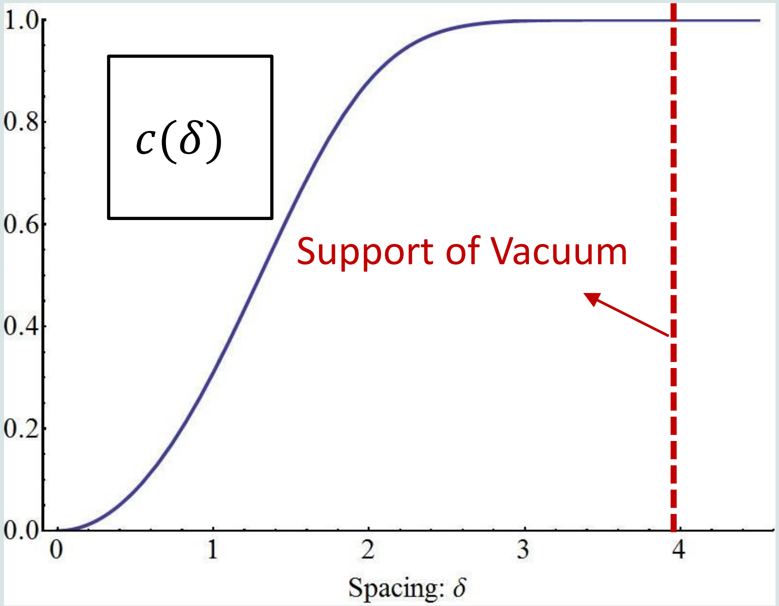


III. Uncertainty Relation in Presence of Quantum Memory

# The Complementarity Constant

***Complementarity:*** $c(\delta) = \sup_{k,l} \left\| \sqrt{Q_\delta^k}\sqrt{P_\delta^l} \right\|^2 \approx \frac{\delta^2}{2\pi\hbar}$



東京大学 THE UNIVERSITY OF TOKYO

## III. Uncertainty Relation in Presence of Quantum Memory

# P-Q Measurements with Infinite Precision

Discrete Approximation Theorem:

$$H(Q_\delta|B) + \log\delta \ + H(P_\delta|C) + \ \log\delta \geq \log\frac{c(\delta)}{\delta^2}$$

$$\delta \to 0\,, \quad h(X|B) = \lim_{\delta\to 0} \left( H(X_\delta|B) + log\delta \ \right)$$

***Uncertainty Relation (continuous case):***

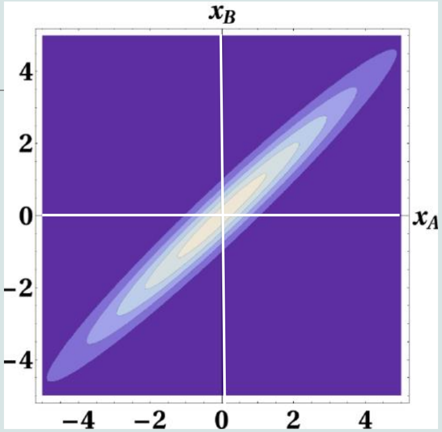
$$h(Q|B) + h(P|C) \geq \log 2\pi\hbar$$

**Is it sharp (exists a state for which equality holds)?**

- Not sharp without quantum memory: (Beckner, Ann. of Math., 102:159, 1975)

$$h(Q) + h(P) \geq \log e\pi\hbar$$

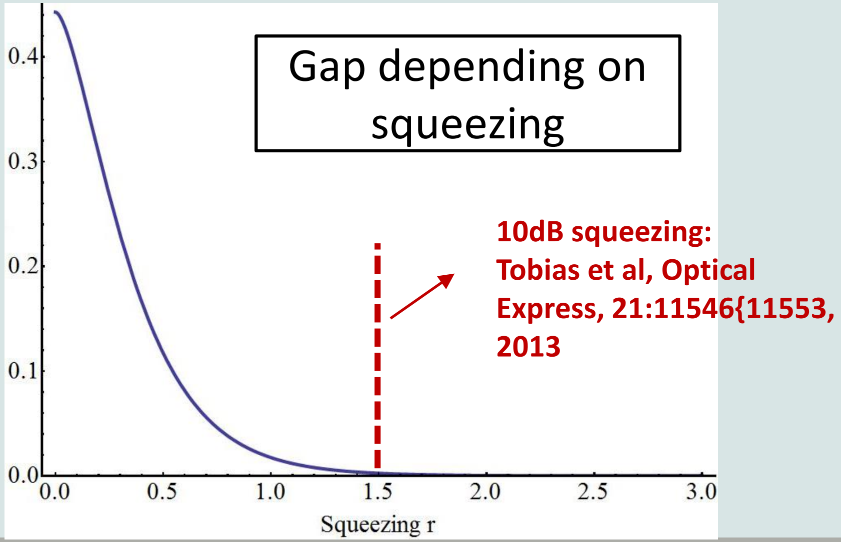
# III. Uncertainty Relation in Presence of Quantum Memory
## Sharpness of the Uncertainty Relation

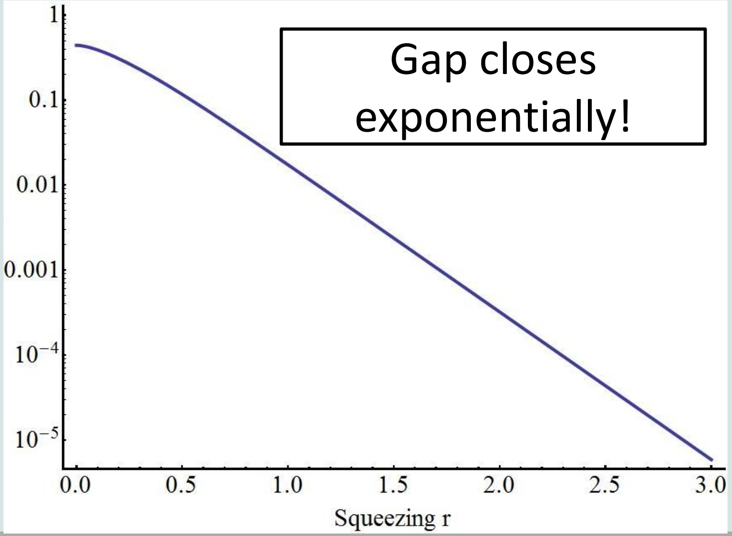



**Sharp with quantum memory:**

- **EPR-state on A and B for Infinite squeezing !**

(EPR-state = pure two-mode squeezed Gaussian state with maximally correlated quadratures)



東京大学 THE UNIVERSITY OF TOKYO

# Conclusion and Outlook

**Summary**

- introduced general differential conditional entropy measures
- derived uncertainty relations for coarse-grained and continuous outcomes.
- Same uncertainty relations for min- and max-entropies (tight for finite and infinite precision measurements)
- tight in the continuous case

**Outlook:**

- Possible applications in QKD: no discretization needed (extremality of Gaussian attacks)
- Approximation of discrete entropies: $H(X_\delta|B) \geq h(X|B) - log\delta$
- **…**

# THANK YOU FOR YOUR ATTENTION

soon on arXiv!

MARIO BERTA, VOLKHER SCHOLZ, MATTHIAS CHRISTANDL
**ETH ZURICH**

MARCO TOMAMICHEL
**CQT SINGAPORE**