Centre for Quantum Technologies

NUS National University of Singapore

A min entropy uncertainty relation for finite size cryptography

Nelly Ng Huei Ying

Centre for Quantum Technologies, Singapore

September 13, 2012

Joint work with:
Mario Berta (ETH, Zurich), Stephanie Wehner (CQT, Singapore)

Articles:
quant-ph/1205.0842, accepted by PRA

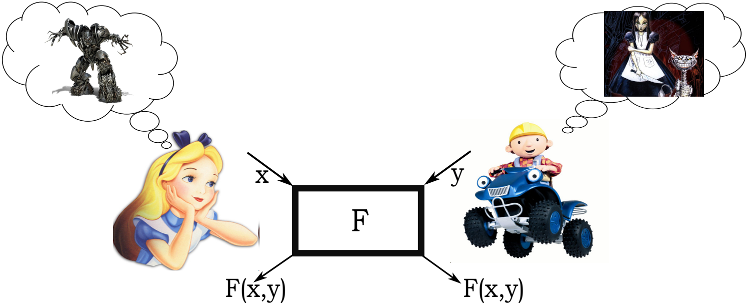
Table of Contents

The Cryptography World

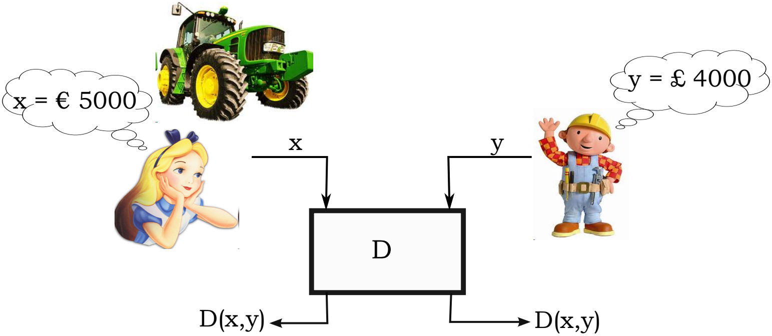
- Protection of information in a communication process.
- Conventional cryptography: protection against eavesdropping Eve.
- Main example: Key establishment
- QKD: information theoretic security based on quantum physics!

More challenges: two-party protocols

- Secure function evaluation, involving two distrustful parties.
- **No Eve!!**
- Security requirements: If one party is honest, the other possible cheating party cannot gain further information than provided by the outcome.



Example: Selling a tractor



$$D(x,y) = \begin{cases} \text{no if } x > y & \text{(Bob's offered price below Alice's asking price)} \\ y \text{ if } x \leq y & \text{(Sold at offered price, at least or higher than Alice's asking price)} \end{cases}$$

- Other examples: bit commitment, 1-2 oblivious transfer etc.

Are such fundamental 2-party protocols achievable by quantum cryptography?

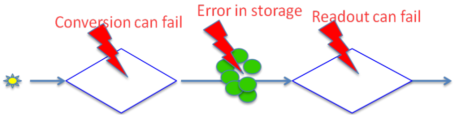
- Quantum bit commitment is impossible
  - H.K. Lo, H. F. Chau (quant-ph/9605026)
  - D. Mayers (quant-ph/9605044)
- One-sided two-party computations are impossible
  - H.K.Lo (quant-ph/9611031)
- Extension of impossibility proofs for bit commitment
  - G.M.D'Ariano, D. Kretschmann, D. Schlingemann, R.F.Werner (quant-ph/0605224)

Is this the end??

Quantum assumptions

- General limitations
  - Attacker cannot act on multiple qubits simultaneously (Salvail, http://www.cki.au.dk/pub/crypt.dvi)
  - Relativistic theory (Kent, quant-ph/1101.4620)
- Resource limitations
  - Bounded quantum storage (Damgaard, Fehr, Salvail, Schaffner, quant-ph/0508222)

Noisy Storage Model



- Quantum memory is in general bounded and subjected to noise. [1] (Wehner, Schaffner, Terhal, quant-ph/0711.2895)
- Quantum Protocol: Weak String Erasure
  - Provides Alice a random binary (classical) string X^n, and Bob a random substring $X_{\mathcal{I}}$ with the set of location indices $\mathcal{I}$.

[1] Not in contradiction with memories used for quantum repeaters.

(n, λ, ϵ)-WSE

t= t0

$X^n = \{0,0,1,1,0,1,0,1,0,\dots\}$

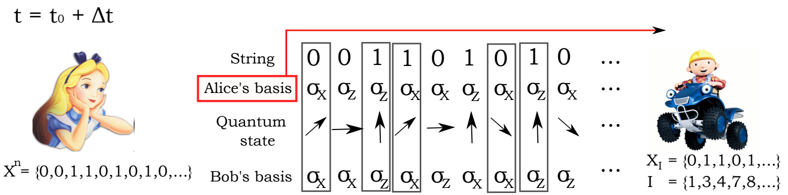
String	0	0	1	1	0	1	0	1	0	…
Alice's basis	σ_X	σ_Z	σ_Z	σ_X	σ_X	σ_Z	σ_X	σ_Z	σ_X	…
Quantum state	↗	→	↑	↗	→	↑	↘	↑	↘	…
Bob's basis	σ_X	σ_X	σ_Z	σ_X	σ_Z	σ_X	σ_X	σ_Z	σ_Z	…

$X_I = \{0,1,1,0,1,\dots\}$
$I = \{1,3,4,7,8,\dots\}$

- Security for Alice: Bob's knowledge of X^n is limited, i.e. $\boxed{\mathrm{H}^{\epsilon}_{\min}(X^n|B) \geq \lambda n.}$
- Security for Bob: Alice does not learn about $\mathcal{I}$.

- WSE protocol + classical information post-processing → fundamental secure 2-party protocols! (OT, BC etc)

(n, λ, ϵ)-WSE

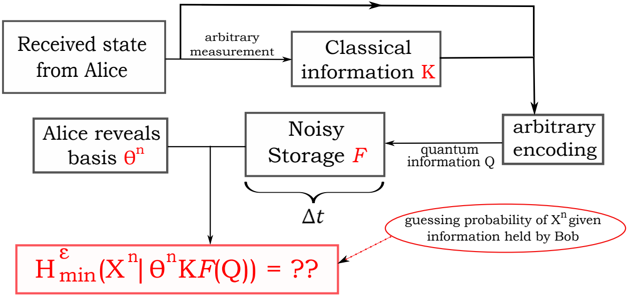


- Security for Alice: Bob's knowledge of X^n is limited, i.e. $\boxed{\mathrm{H}^{\epsilon}_{\mathrm{min}}(X^n|B) \geq \lambda n.}$
- Security for Bob: Alice does not learn about $\mathcal{I}$.

- WSE protocol + classical information post-processing $\rightarrow$ fundamental secure 2-party protocols! (OT, BC etc)

The Shield: Entropic Uncertainty Relations

- Fundamental principle: Description of the inherent randomness coming from the uncertainty in outcomes for non-commuting measurements.
- Importance: Bounds the amount of information that a possible adversary has access to.
- Quantities of interest:



Main Challenges

Goal: making min-entropy per bit large!
– more tolerance against losses and errors in implementations

- Tight/optimal bounds for quantum side information
  - Previously linked to channel capacities:
    – Classical capacity (quant-ph/0906.1030)
    – Entanglement cost (quant-ph/1108.5357)
  - WSE using six-states instead of BB84 can be linked to quantum capacity(quant-ph/1111.2026)
- Finite size effects
  - Tight bounds for in QKD (Tomamichel, Lim, Gisin, Renner/arXiv:1103.4130)

Approach:
Derive uncertainty relations w.r.t. classical information first, then include conditioning on quantum information by considering classical capacity of quantum channels obeying strong converse (better understood)

How much uncertainty can we obtain?

Scenario:
Consider an arbitrary n qubit state ρ, where Bob holds arbitrary classical information K about the state. An honest Alice performs random BB84 measurements upon the state, obtaining a string of outcomes $X^n \in \{0,1\}^n$. What is the min-entropy of Bob's total information about X^n?

Close to Shannon entropy!
(Damgaard, Fehr, Renner, Salvail, Schaffner, quant-ph/0612014)

$$\mathrm{H}^{\epsilon}_{\min}(X^n|\Theta^n K) \geq \left(\tfrac{1}{2} - \delta\right) n, \qquad \text{where } \epsilon = \exp\left[-\frac{\delta^2 n}{128(2+\log\frac{2}{\delta})^2}\right]$$

- Error parameter ϵ can be reasonably small in the large n limit.
- How large should n be? Ans: For small $\epsilon \approx 0.1$ and $\delta \approx 0.01$, $n \gtrsim 10^8$!

Our results:

$$\mathrm{H}_{\min}^{\epsilon}(X^n|\Theta^n K) \geq c_{BB84}\, n,$$

$$c_{BB84} := \max_{s\in(0,1]} \frac{1}{s}\left[1 + s - \log(1+2^s) - \frac{1}{sn}\log\frac{2}{\epsilon^2}\right]$$

- Crucial idea: Bounding the min-entropy by a class of conditional Renyi entropies, and maximizing over all obtained bounds.
- How large should n be? Ans: For $\epsilon \approx 0.1$, $\delta \approx 0.01$, $n \gtrsim 10^4$ is sufficient!
- Similarly tight results obtained for six-state measurements.

Steps in proof: (a rough sketch)

$$H_\alpha(X \mid \Theta)$$
$$\downarrow$$
$$H_\alpha(X^n \mid \Theta^n)$$
$$\downarrow$$
$$H_\alpha(X^n \mid \Theta^n K)$$
$$\downarrow$$
$$H^\varepsilon_{\min}(X^n \mid \Theta^n K)$$

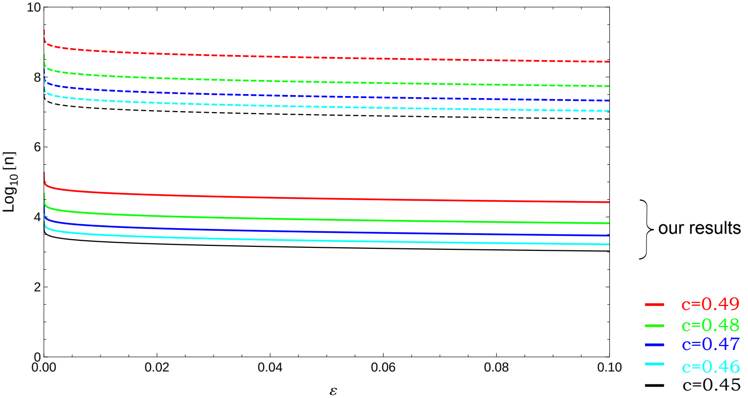
1. Theoretical optimization over all states of conditional α-Renyi entropies, for a single qubit.
   - Reformulation in terms of spherical coordinates.
   - Invoking the Bloch sphere condition as constraint for an arbitrary single-qubit density matrix.
2. Generalization to an arbitrary n-qubit state ρ.
3. Further conditioning on classical information K.
   - Coincides with $H_\alpha(X^n|\Theta^n)_\rho$, due to the fact that Θ^n and K are independent from each other.
4. Link to min-entropy.
   - Tomamichel, Colbeck, Renner/arXiv:0811.1221

extension to quantum side information

Let F be a quantum channel satisfying strong converse. Then

$$\boxed{H^\varepsilon_{\min}(X^n|\Theta^n KF(Q)) \geq -\log P^F_{succ}[\,H^{\varepsilon/2}_{\min}(X^n|\Theta^n K) - \log(2/\varepsilon)\,]}$$

A new bound for min-entropy

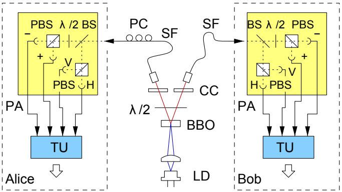


$$\mathsf{c} = \frac{\mathrm{H}^{\epsilon}_{\min}(X^n|\Theta^n K)}{n}$$

Application: Bit Commitment in Noisy Storage Model

Ng, Joshi, Chia, Kurtseifer, Wehner/arXiv:1205.3331

- For security, we need $H^{\epsilon}_{min}(X^n|B) \gtrsim 0.47n$.
- Reasons: 1) Making protocol robust against QBER = 4.1%.
  2) Minimal classical information processing while considering finite size effects.
- Perform bit commitment by sending 2.5×10^5 qubits during WSEE[2].



[2]Modified version of WSE to include robustness against losses and errors

Conclusion

- New uncertainty relation provides improved bounds, substantially decreasing the amount of information post-processing required.
- For $n = 2.5 \times 10^5$, $\epsilon = 2 \times 10^{-5}$, we performed secure bit commitment under a quantum storage assumption of 972 qubits undergoing low depolarizing noise of r=0.9 (or 928 qubits stored in noiseless memory).

Comments and Open problems

- Demonstrates feasibility of fundamental two-party protocols in NSM.
  - Motivates more construction of useful protocols using WSE, for ex: secure identification.
- Tight relations for quantum side information
  - To prove security of WSE for a larger range of quantum channels.

The End

Thank you!