Impossibility of Growing Quantum Bit Commitment

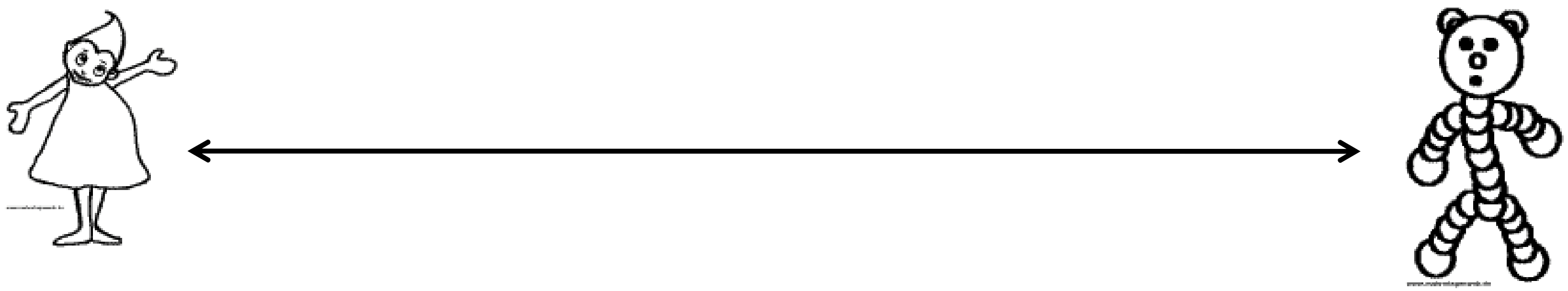
Severin Winkler, Marco Tomamichel, Stefan Hengl, Renato Renner

ETH Zurich

QCRYPT, September 13, 2011

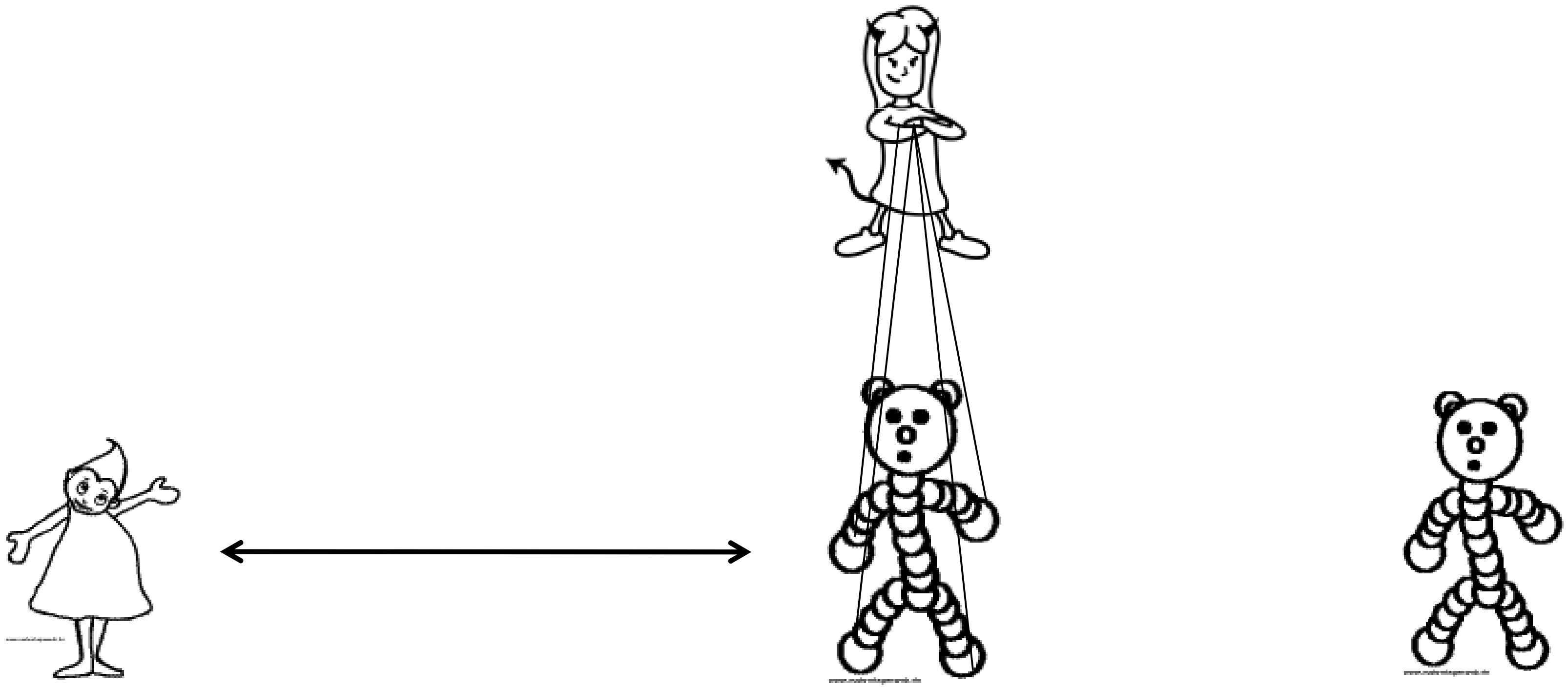
Motivation: QKD

- QKD over insecure channel is impossible:



Motivation: QKD

- QKD over insecure channel is impossible:
  - Eve can play the role of Bob



Motivation: QKD

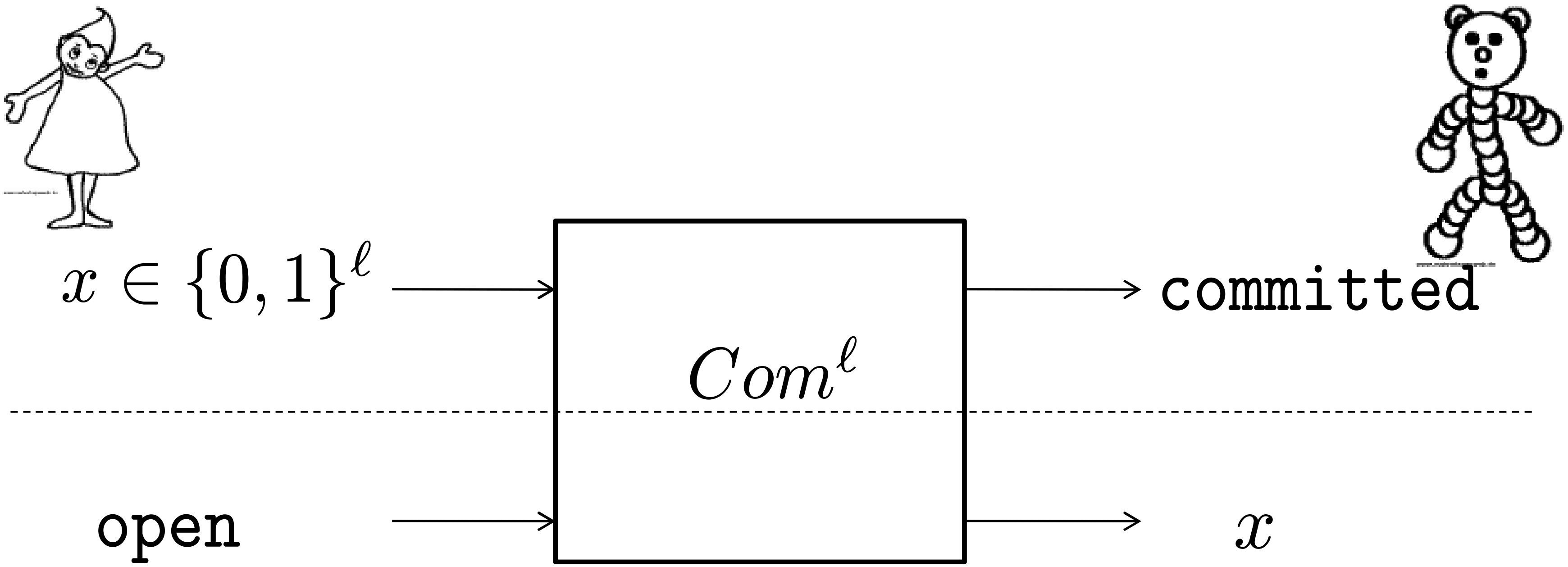
- QKD over insecure channel is impossible:
  - Eve can play the role of Bob
- Initial key can be used to authenticate channel
- QKD using an authenticated channel [BB84,Ekert'91]

$\rightarrow$ Quantum Key Growing is possible

Motivation: 2-Party Computation

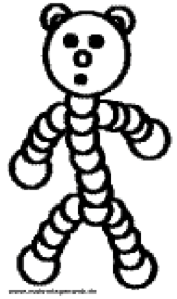
- Secure Coin Toss impossible [Lo,Chau'98, Kitaev'03]
- Coin Toss can be extended (Standalone Model) [Hofheinz,Müller-Quade,Unruh'06]
- Secure Commitments impossible [Mayers'97; Lo,Chau'97]
- Analogous Question for Commitments:
  – Commitment to large string from a smaller number of Bit Commitments?

Ideal String Commitment



- Statistically secure Oblivious Transfer / Multi-Party Computation [BBCS'92,DFLSS'09,Unruh'10]
- Zero-Knowledge Proofs and Secure CoinTossing

Commitment Protocol



$x \in \{0,1\}^\ell \longrightarrow$

Commit Phase

Open Phase

$\longrightarrow \tilde{x} \in \{0,1\}^\ell$

Security for Alice (Hiding):

Bob has no information about committed value before Open

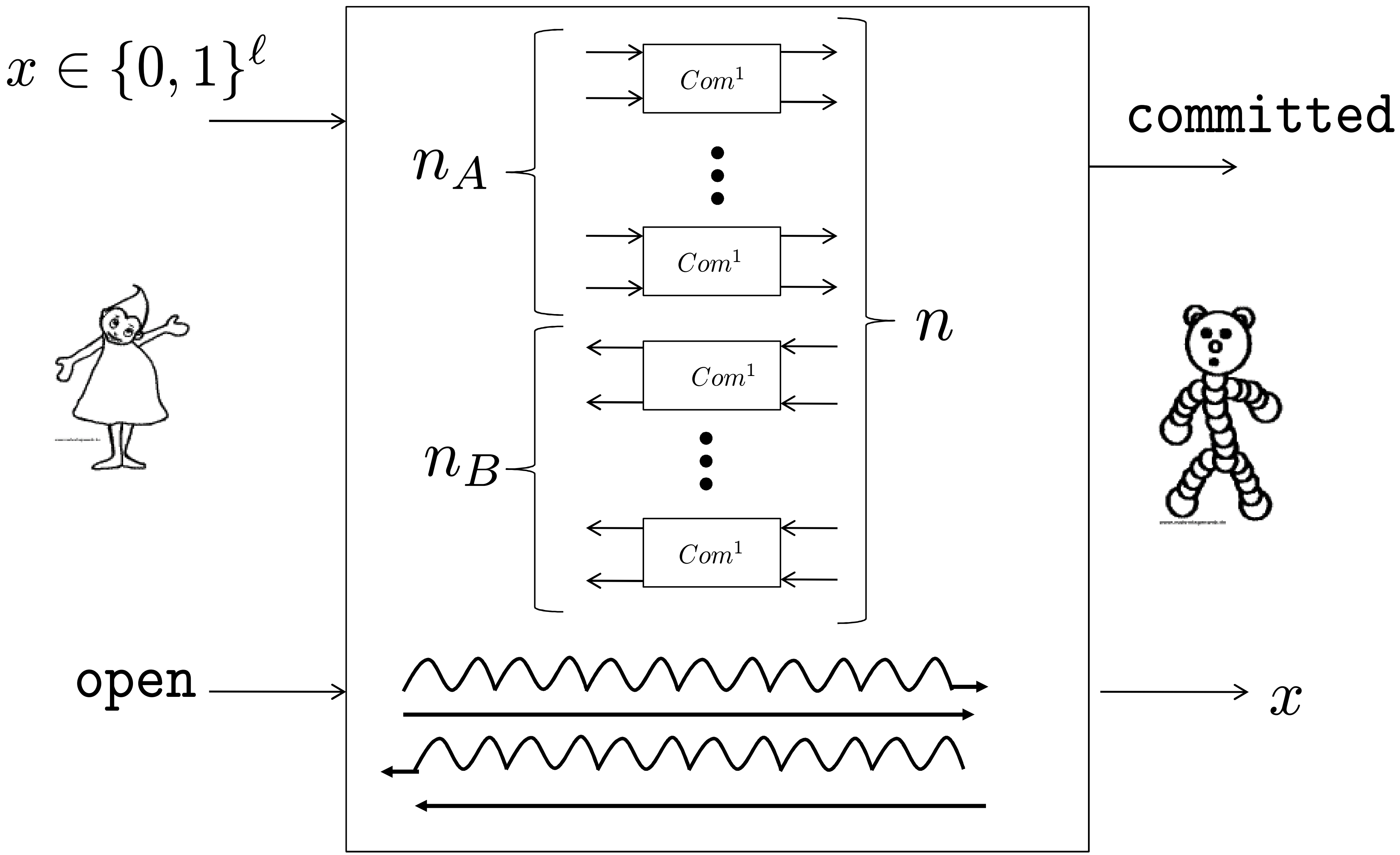
Security for Bob (Binding):

Alice cannot change committed value

Model

- (Noiseless) Quantum Channel
- (Noiseless) Classical Channel
  - Measures input and sends result to receiver
- Arbitrary quantum operations on whole system (conditioned on classical data)
- Players have unlimited computing power
  - QBSM/NSM [DFSS05,DFRSS07], [WST08,STW08,KWW09]
- No Relativistic Protocols [Kent'99,Kent'05, Kent'11]
- Ideal Bit Commitments as a Resource

Growing Commitments



Main Result

- Any protocol implementing a string commitment of lenght ℓ:
  - quantum and classical communication
  - using $n = n_A + n_B$ Bit Commitments
  - unconditionally hiding and binding with a small (constant) error

  must satisfy $\ell \lesssim n$.
- Weaker result follows from lower bounds for oblivious transfer reductions [WW10]

Part 2: Proof Ideas

Purified Protocol

- Purify operations of players:
  - Introduce larger space (ancillas)
  - Unitary operations (Stinespring)
- Purified protocol is equivalent
- Joint state ρ_{AB} at the end of commit phase is pure conditioned on (symmetric) classical information

Commit to Superposition

- Alice can purify random choice of input
- Commit to uniform superposition of strings from a set $\mathcal{X}_0 \subseteq \{0,1\}^\ell$:
  - Prepare the state $\frac{1}{\sqrt{|\mathcal{X}_0|}} \sum_{x \in \mathcal{X}_0} |x\rangle_X \otimes |x'\rangle_{X'}$
  - Input register X to the protocol
  - Keep register X'
- Measure X' to obtain x after commit
- Open x

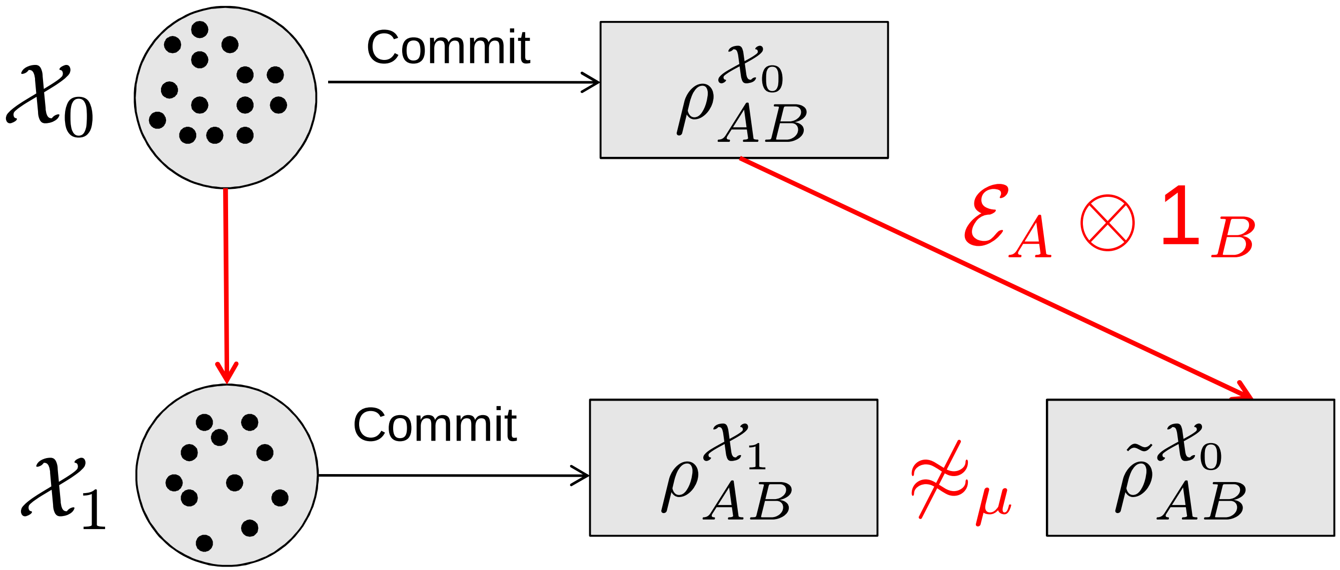
Security: Hiding

- We use two security properties that follow from any sensible security definition
- Relaxed (e.g. no arbitrary malicious strategies)→stronger impossibility
- (Weakly) ϵ-Hiding:
  - For uniform X, the committed strings X are close to uniform w.r.t. B

$$\rho_{XB} \approx_\epsilon \frac{1}{|X|} \mathbb{1}_X \otimes \sigma_B$$

Security: Binding

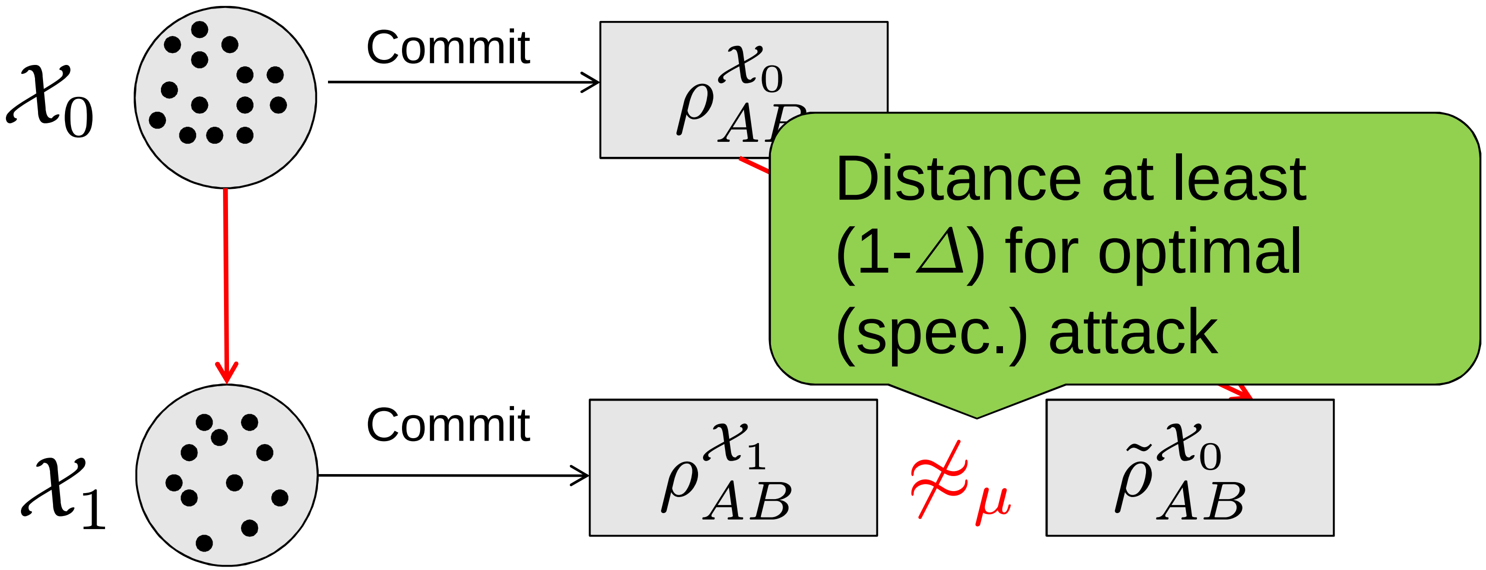
- (Weakly) Δ-Binding:



- (1-Δ) = distance μ minimized over disjoint sets $\mathcal{X}_0, \mathcal{X}_1$ and maps $\mathcal{E}_A$ on Alice's system

Security: Binding

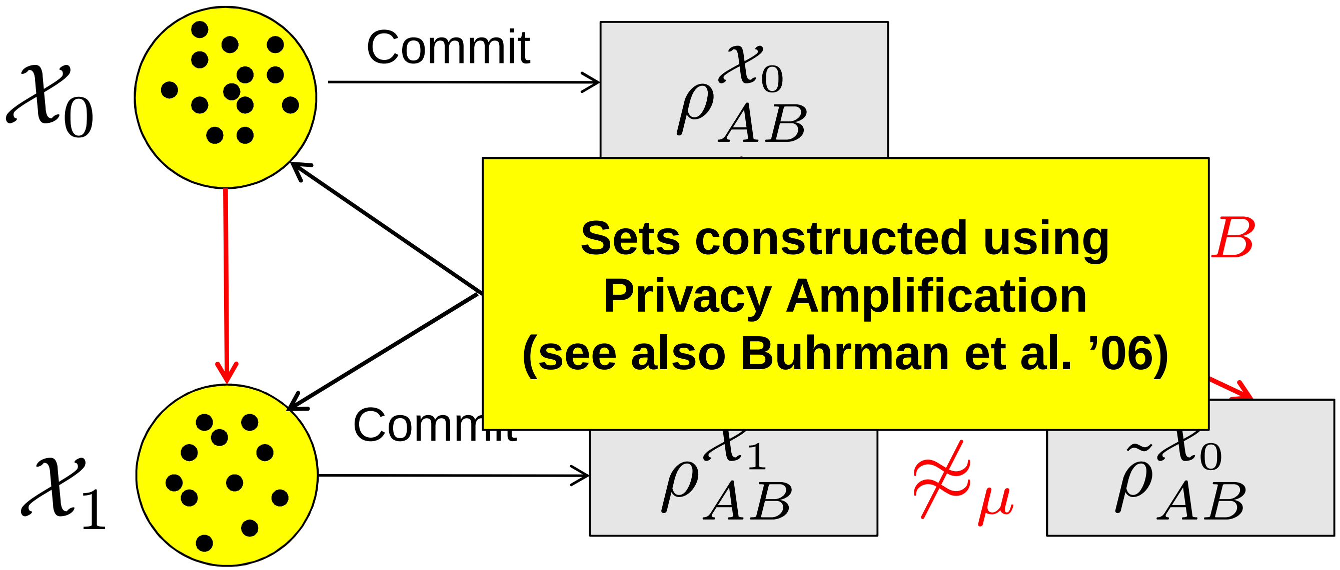
- (Weakly) Δ-Binding:



- (1-Δ) = distance μ minimized over disjoint sets $\mathcal{X}_0, \mathcal{X}_1$ and maps $\mathcal{E}_A$ on Alice's system

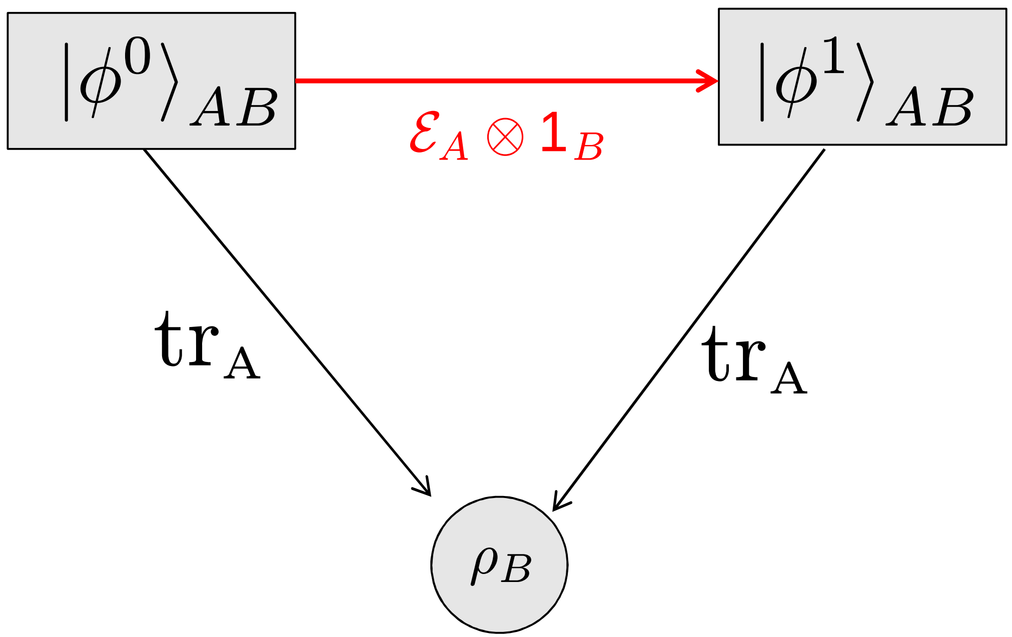
(Relaxed) Security: Binding

- (Weakly) Δ-Binding:



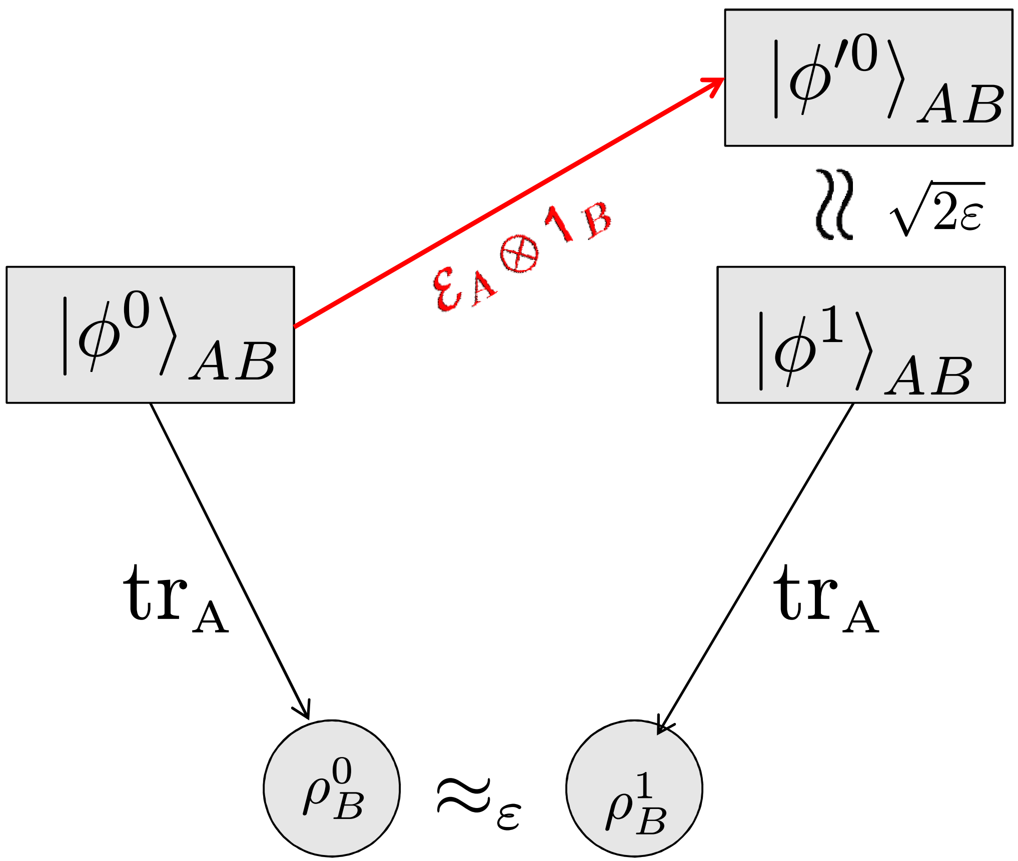
- (1-Δ) = distance μ minimized over disjoint sets $\mathcal{X}_0, \mathcal{X}_1$ and maps $\mathcal{E}_A$ on Alice's system

Alice‘s Attack (perfectly hiding)



- Application of Uhlmann’s Theorem

Attack: non-perfectly hiding



- same attack if states are pure conditioned on symmetric classical data

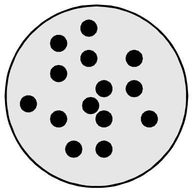
Min-Entropy and Privacy Amplification

- Relate $H_{\min}^{\varepsilon}(X|B)_{\rho}$ to success probability of Alice's attack
- $H_{\min}^{\varepsilon}(X|B)_{\rho}$ = min-entropy of X conditioned on B
- We extract one secret bit f(X) using a two-universal function f
- Secrecy of f(X) increases with $H_{\min}^{\varepsilon}(X|B)_{\rho}$

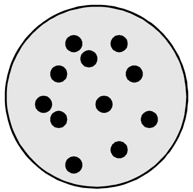
Alice’s Attack

- Secrecy of f(X) increases with $H^{\varepsilon}_{\min}(X|B)_{\rho}$

$f^{-1}(0)$

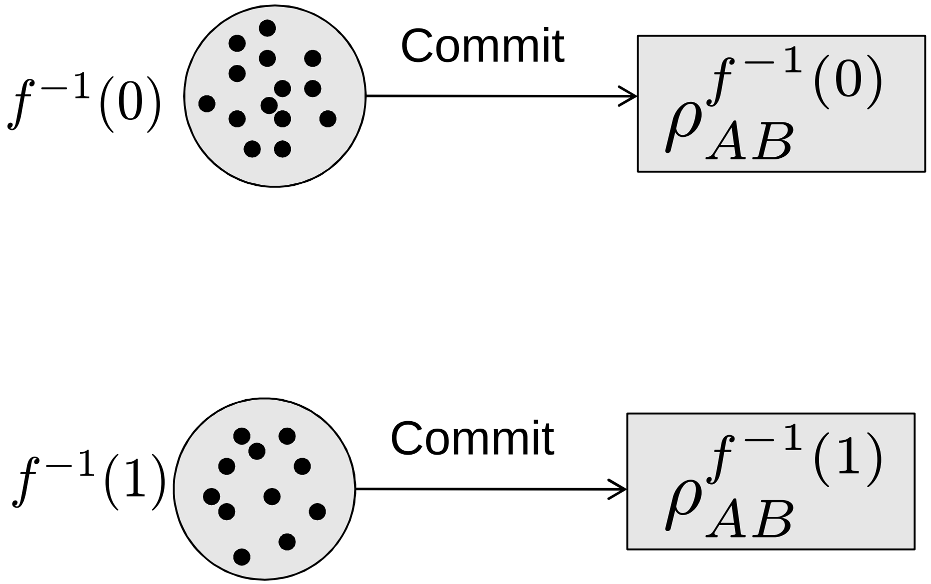


$f^{-1}(1)$



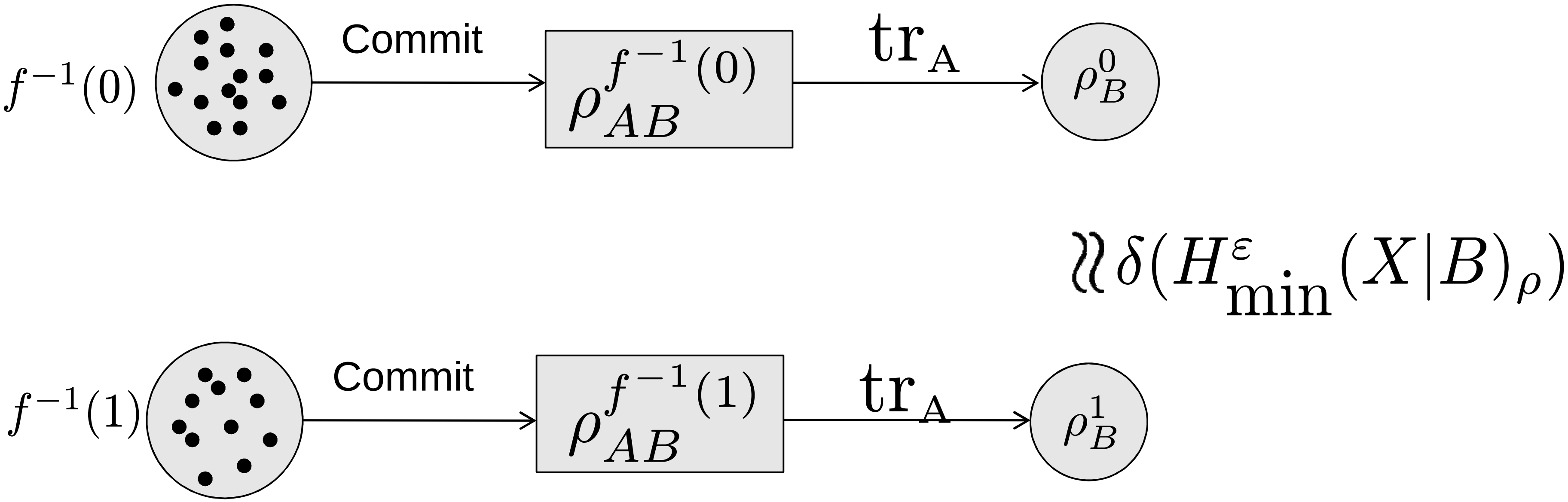
Alice’s Attack

- Secrecy of f(X) increases with $H_{\min}^{\varepsilon}(X|B)_{\rho}$



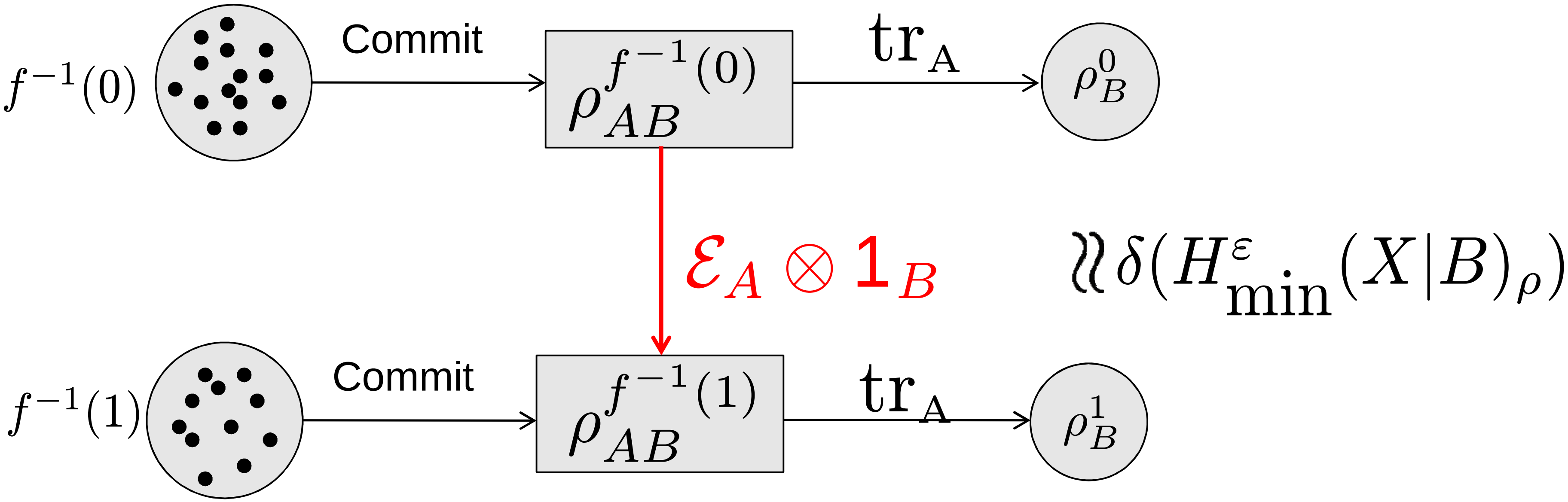
Alice's Attack

- Secrecy of f(X) increases with $H_{\min}^{\varepsilon}(X|B)_\rho$



Alice's Attack

- Secrecy of f(X) increases with $H_{\min}^{\varepsilon}(X|B)_\rho$



- Success probability. of Alice's attack increases with $H_{\min}^{\varepsilon}(X|B)_\rho$

Proof Sketch with Resources

- Hiding implies $H^{\epsilon}_{\min}(X|B)_\rho \geq \ell$
- Modified Protocol without Resource:
  - Alice sends committed bits to Bob (C_A)
  - Bob purifies measure. of committed bits (C_B)
  - Bob more powerful in the modified protocol
  - Pure state conditioned on classical data
- Smooth Min-Entropy Calculus implies:

$$H^{\epsilon}_{\min}(X|BC_AC_B)_\rho \geq \ell - n$$

n = #resource bit commitments

Main Result

- n Bit Commitments as Resource
- Implemented commitment has length ℓ
- ϵ-hiding and Δ-binding implies

$$\ell \leq n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\epsilon}\right) - 1$$

For example $\varepsilon = \Delta = 0.01$ implies $\ell \leq n + 5$

Conclusions

- Impossible to extend commitments with quantum protocols:
  - no commitment to larger string or
  - no larger number of bit commitments

  from smaller number of bit commitments.
- Similar result holds for quantum commitment resource

Thank you

Full version:

http://arxiv.org/abs/0811.3589

Problem???

- Can we extend a given cryptographic primitive?
- Interesting from the theoretical point of view
- Relevant in practice:
  - Resources might be costly
  - Lower amortized costs per instance

Positive Results

- Unconditionally Secure Commitments
  - Bounded Storage Model [DFSS05,DFRSS07]
  - Noisy Storage [WST08,STW08,KWW09]
  - Relativistic Protocols [Kent'99,Kent'05, Kent'11]
  - Trusted Resources
    - Noisy Correlations [IMNW04,IMNW06]
    - Noisy Channels [Crépeau'97, Winter et al. 03]
  - String Commitments with weak security [BCHLW'06]

Impossibility Results

- Impossibility Results for Quantum Protocols:
  - No Bit Commitment [Mayers'97; Lo,Chau'97]
  - ??No Secure Coin Toss [Lo,Chau'98,Kitaev'03]
  - ??No Oblivious Transfer / One-Sided SFE [Lo'97]
  - String commitments w. relaxed security [Buhrman, Christandl, Hayden, Lo, Wehner'06]
  - Impossible to extend Oblivious Transfer [WW10]
  - Lower Bound on the number of commitments to implement OT [WW10]