Achieving the limits of the noisy-storage model using entanglement sampling

Frédéric Dupuis
Aarhus Universitet

Joint work with
Omar Fawzi (ETH Zürich)
Stephanie Wehner (National University of Singapore)

August 6, 2013

Outline

- Bit commitment and the bounded quantum storage model
- Min-entropy
- Main result: bounding the min-entropy of channel outputs
- Application to BQSM

Bit commitment

- Bit commitment: basic cryptographic primitive for two-party cryptography
- What it should do:

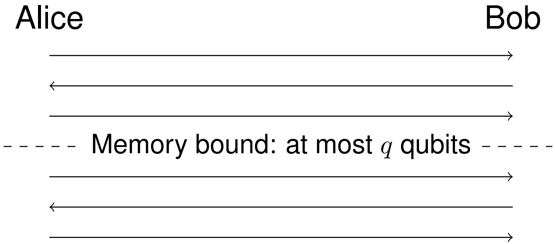
Quantum bounded storage model

Assumptions needed for bit commitment:

- Complexity assumptions
- Physical assumptions (bounded storage, noisy channel, etc)
- This talk: bounded *quantum* storage

Bounded quantum storage model (BQSM)

At some point in the protocol, all parties are assumed to have at most q qubits of storage (but unlimited classical storage).



- In the BQSM, there is a protocol to do bit commitment [DFSS05].

[Damgård, Fehr, Salvail, and Schaffner 2005]

Previous work on the BQSM

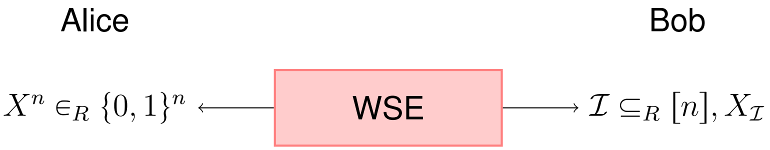
n: number of qubits sent, q: memory bound

- Damgård, Fehr, Salvail, Schaffner 2005; Damgård, Fehr, Renner, Salvail, Schaffner 2007: $q \approx n/4$
- König, Wehner, Wullschleger 2009: $q \approx n/2$
- Mandayam, Wehner 2011: $q \approx 2n/3$

This talk: $q = n - O(\log^2 n)$: essentially optimal

Weak string erasure

Bit commitment can in turn be reduced to *weak string erasure* [König, Wehner, Wullschleger 2009]:



For security, we want:

- $\mathcal{I}$ is distributed uniformly over $[n]$ and is independent of anything Alice has.
- If Bob is dishonest, then $\frac{1}{n} H_{\min}(X^n|B)_\sigma \geqslant \lambda$, where $\sigma_{X^n B}$ is the state at the end of the protocol.

Weak string erasure

Given a protocol for weak string erasure with

$$\lambda \geqslant \Omega\left(\frac{\log n}{n}\right),$$

we can do bit commitment.

Protocol for weak string erasure

Alice | Bob

$x^n \in_R \{0,1\}^n$
$\theta^n \in_R \{+,\times\}^n$

$\tilde{\theta}^n \in_R \{+,\times\}^n$

$|x^n\rangle_{\theta^n}$ →

Measure in basis $\tilde{\theta}^n$, get $\tilde{x}^n$

- - - - - - - - - Memory bound applies - - - - - - - - -

θ^n →

Output: x^n

Output: $\mathcal{I} = \{i : \theta_i = \tilde{\theta}_i\}$, $\tilde{x}_{\mathcal{I}}$

Protocol for weak string erasure

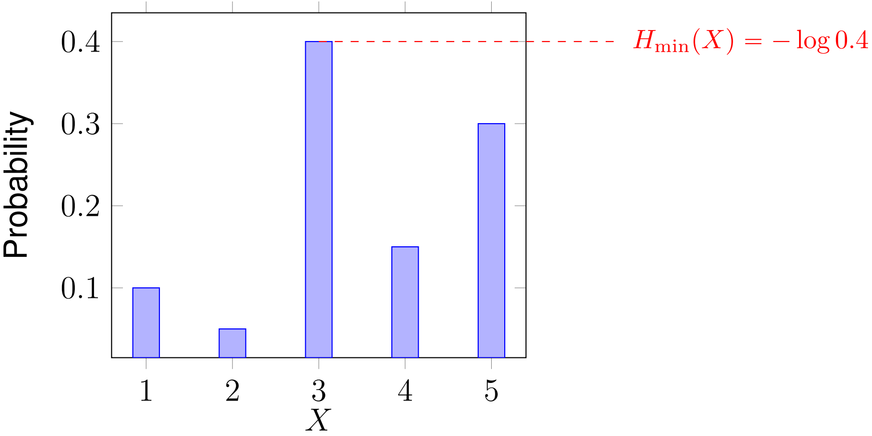
Does this protocol satisfy the security definition?

- $\mathcal{I}$ uniform and independent. Yes: $\mathcal{I}$ only depends on the XOR of θ^n and $\tilde{\theta}^n \Rightarrow$ Alice has no control over it.
- We need that, for a dishonest Bob, $\frac{1}{n} H_{\min}(X^n|B)_\sigma \geqslant \lambda$.

We need our theorem to guarantee the second point.

Min-entropy

Min-entropy



$H_{\min}(X) = -\log($probability of guessing $X)$.

Conditional min-entropy

- $H_{\min}(X|B) = -\log($probability of guessing X given $B)$.
- If B is quantum, then it is the probability of guessing X after doing the optimal measurement on B.
- Let ρ_{XB} be a classical-quantum state:

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_B^x.$$

- We define the min-entropy as the best probability of correctly guessing X by measuring B:

$$2^{-H_{\min}(X|B)_\rho} := \sup_{\{M_B^x\}} \sum_x p_x \operatorname{Tr}[M_B^x \rho_B^x],$$

where we optimize over POVMs $\{M_B^x\}$.

Min-entropy: definition for general states

What about general states?

- Let ρ_{AB} be any quantum state.
- We define the min-entropy as the best fidelity with a maximally entangled state:

$$2^{-H_{\min}(A|B)_\rho} := \sup_{\{\mathcal{D}_{B\to A'}\}} \langle\Phi|(\mathbb{1}\otimes\mathcal{D})(\rho_{AB})|\Phi\rangle.$$

  where we optimize over CPTP maps from B to A', and where

$$|\Phi\rangle_{AA'} := \sum_i |i\rangle_A \otimes |i\rangle_{A'}$$

Min-entropy: definition for general states

- Note that $|\Phi\rangle$ is not normalized.
- So: $-\log d_A \leqslant H_{\min}(A|B)_\rho \leqslant \log d_A$.
- If $H_{\min}(A|B)_\rho = -\log d_A$, then we can recover $\Phi_{AA'}$ by acting on B alone.
- If $H_{\min}(A|B)_\rho = \log d_A$, then $\rho_{AB} = \frac{\mathbb{1}_A}{d_A} \otimes \rho_B$.

The fine print: $H_{\min}$ vs H_2

As it turns out, it is easier to obtain results for the 2-entropy instead of the min-entropy:

Definition

Given a quantum state ρ_{AB}*,*

$$2^{-H_2(A|B)_\rho} := \mathrm{Tr}\left[\left((\mathbb{1}_A \otimes \rho_B^{-\frac{1}{4}})\rho_{AB}(\mathbb{1}_A \otimes \rho_B^{-\frac{1}{4}})\right)^2\right].$$

Big advantage: we have an explicit expression.

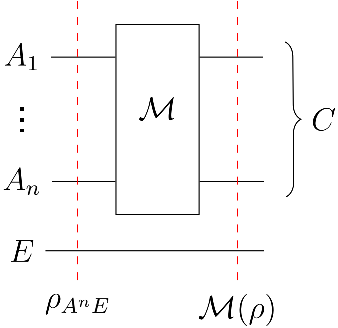
The fine print: $H_{\min}$ vs H_2

H_2 is closely related to $H_{\min}$:

- For any ρ_{AB}, $H_{\min}(A|B)_\rho \leqslant H_2(A|B)_\rho$.
- For any CQ ρ_{XB}, $H_2(X|B)_\rho \leqslant 2H_{\min}(X|B)_\rho$.
- For any ρ_{AB}, $H_2(A|B)_\rho + \log d_A \leqslant 2(H_{\min}(A|B)_\rho + \log d_A)$.
- (Much better bounds when we use *smoothing*.)

Main result

Bounding the 2-entropy of channel outputs



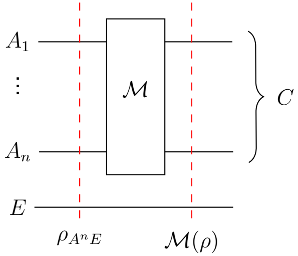
The A_i's are of dimension d.

Main theorem

Theorem (Main theorem)

Let $\mathcal{M}_{A^n \to C}$ be a CP map and let $\rho_{A^n E}$ be a state. Then for any partition $[d^2]^n = \mathfrak{S}_+ \cup \mathfrak{S}_-$ into subsets $\mathfrak{S}_+$ and $\mathfrak{S}_-$, we have*

$$2^{-H_2(C|E)_{\mathcal{M}(\rho)}} \leqslant \sum_{s \in \mathfrak{S}_+} \lambda_s 2^{-H_2(A^n|E)_\rho} + \left(\max_{s \in \mathfrak{S}_-} \lambda_s \right) d^n.$$



*such that $((\mathcal{M}^\dagger \circ \mathcal{M})_{A^n} \otimes \mathrm{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \sum_{s \in [d^2]^n} \lambda_s \Phi_s$

Main theorem: Corollaries

By choosing some specific $\mathcal{M}$, we can get the following:

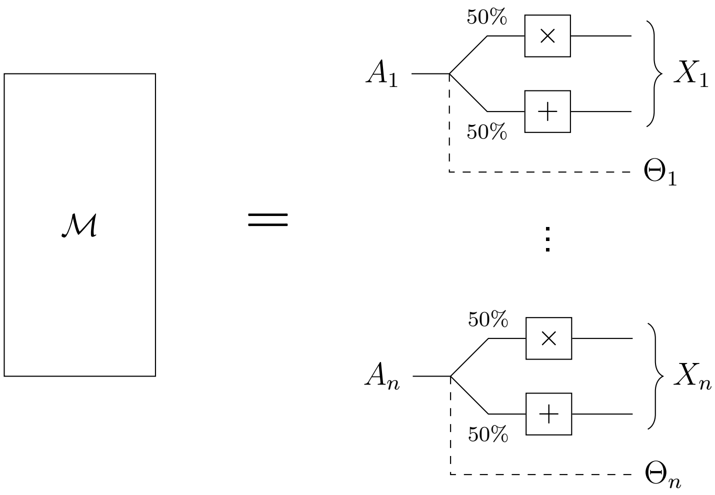
- Sampling k out of n subsystems
  - Yields results on random-access codes
- Measuring each subsystem in either the $+$ or the $\times$ basis

Main theorem: Corollaries

By choosing some specific $\mathcal{M}$, we can get the following:

- Sampling k out of n subsystems
  - Yields results on random-access codes
- Measuring each subsystem in either the $+$ or the $\times$ basis

Min-entropy of measured states

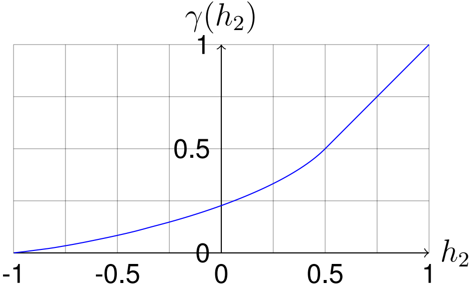


Min-entropy of measured states

Theorem

Let $\rho_{A^n B}$ be a state (each A is a qubit), and let $\sigma_{X^n \Theta^n B} = \mathcal{M}_{A \to \Theta X}^{\otimes n}(\rho)$, where $\mathcal{M}$ measures in BB84 bases, records the result in X, and the basis chosen in Θ. Then,

$$\frac{1}{n} H_2(X^n | B \Theta^n)_\sigma \geqslant \gamma\left(\frac{1}{n} H_2(A^n|B)_\rho\right) - \frac{1}{n}\log 3.$$



Application to weak string erasure

Alice | Bob

$x^n \in_R \{0,1\}^n$
$\theta^n \in_R \{+,\times\}^n$

$\tilde{\theta}^n \in_R \{+,\times\}^n$

$|x^n\rangle_{\theta^n}$ →

Measure in basis $\tilde{\theta}^n$, get $\tilde{x}^n$

- - - - - - - - - Memory bound applies - - - - - - - - -

θ^n →

Output:
x^n

Output:
$\mathcal{I} = \{i : \theta_i = \tilde{\theta}_i\}$
$\tilde{x}_{\mathcal{I}}$

Protocol for weak string erasure

Consider this equivalent protocol:

Alice		Bob
$\|\Phi\rangle_{AA'}^{\otimes n}$ $\theta^n \in_R \{+, \times\}^n$		$\tilde{\theta}^n \in_R \{+, \times\}^n$
	$\xrightarrow{A'^{\otimes n}}$	Measure A'^n in basis $\tilde{\theta}^n$, get $\tilde{x}^n$
	- - - - - - Memory bound: q qubits max - - - - - -	
Measure A^n in basis θ^n, get x^n		
	$\xrightarrow{\theta^n}$	
Output: x^n		Output: $\mathcal{I} = \{i : \theta_i = \tilde{\theta}_i\}, \tilde{x}_{\mathcal{I}}$

Protocol for weak string erasure

And now consider a dishonest Bob:

Alice	Bob
$\|\Phi\rangle_{AA'}^{\otimes n}$ $\theta^n \in_R \{+, \times\}^n$	???

$A'^{\otimes n}$ →

------ Memory bound: q qubits max ------

$\rho_{A^n B_Q B_C}$

$d_{B_Q} = 2^q$

Measure A^n in basis θ^n, get x^n

θ^n →

Output:	Output:
x^n	$\mathcal{I} = \{i : \theta_i = \tilde{\theta}_i\}, \tilde{x}_{\mathcal{I}}$

Protocol for weak string erasure

We apply our theorem to $\rho_{A^n B_Q B_C}$:

Theorem

Let $h_2 = \frac{1}{n} H_2(A^n | B_Q B_C)_\rho$*, and let*

$$\sigma_{X^n \Theta^n B_Q B_C} = \mathcal{M}_{A \to \Theta X}^{\otimes n}(\rho),$$

where $\mathcal{M}$ *measures in BB84 bases, records the result in* X*, and the basis chosen in* Θ*. Then,*

$$\frac{2}{n} H_{\min}(X^n | B_Q B_C \Theta^n)_\sigma \geqslant \frac{1}{n} H_2(X^n | B_Q B_C \Theta^n)_\sigma \geqslant \gamma(h_2) - \frac{1}{n} \log 3.$$

How do we bound h_2? $H_2(A^n | B_Q B_C) \geqslant -\log d_{B_Q} \geqslant -q$. Hence,

$$\frac{1}{n} H_{\min}(X^n | B_Q B_C \Theta^n)_\sigma \geqslant \frac{1}{2}\gamma(-q/n) - \frac{1}{2n} \log 3 =: \lambda.$$

Protocol for weak string erasure

- To get bit commitment, it enough for to require q to be at most
$$n - c\log^2 n - c\log n \log(1/\varepsilon).$$
- Since for $q = n$ we cannot have security, this is essentially optimal.
- Previous best: security for $q \approx 2n/3$.
- Also works for any other model in which we get a nontrivial bound on $H_2(A^n|B)_\rho$ (noisy memory model, etc).

Thank you!

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS ·

Centre for Quantum Technologies

National University of Singapore