QUANTUM TO CLASSICAL RANDOMNESS EXTRACTORS
OR
STRONG UNCERTAINTY RELATIONS WITH QUANTUM SIDE INFORMATION

Omar Fawzi (McGill University)

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

arXiv:1111.2026

General overview

- Uncertainty relations important in quantum cryptography
- We view uncertainty relations as special kind of randomness extractors (QC-extractors)
- Use techniques from the study of extractors

Outline

- Introduction
  - Getting to the definition
- Quantum to classical randomness extractors
  - Definition
  - Parameters
  - Constructions
- Application to security in noisy storage model
  - Model
  - Weak string erasure & link between security and quantum capacity

Randomness extraction

- Question: Given a weak source of randomness, how to convert it to private random bits?

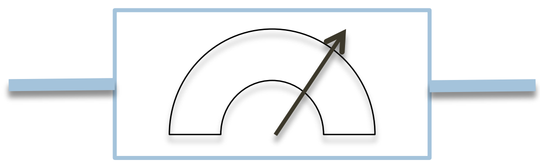
- Example: QKD
  - parameter estimation step → adversary has some uncertainty about bits of Alice and Bob
  - “privacy amplification” or “randomness extraction” step

- Important: Weak source of randomness: no control over the source

Randomness extractor from quantum source

- Here: source is a quantum system
- 1st try:

$$\frac{1}{\sqrt{2}}(|0> + |1>)$$

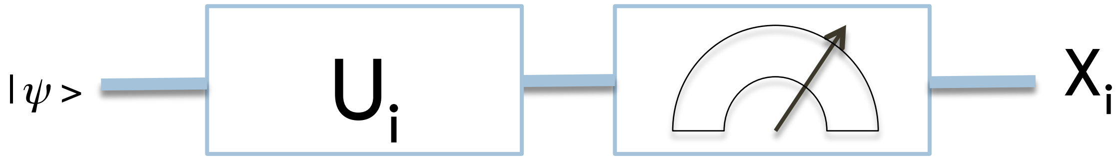


Random bit

- Not good enough: use the knowledge of the input state

QC-extraction: Better example

- Pick i in {0,1} at random



with $U_0 = I$ and $U_1 = H$

Theorem [Maassen and Uffink 1989]

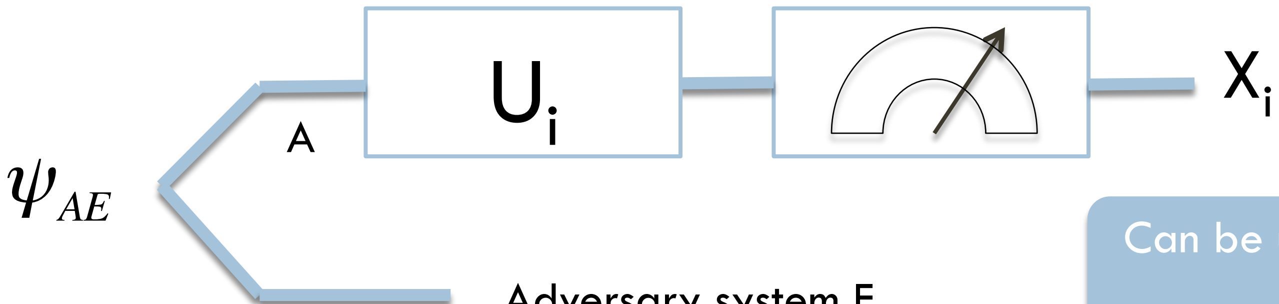
For *any input state*

$$\frac{1}{2}(H(X_0) + H(X_1)) \geq \frac{n}{2}$$

H: Shannon entropy (measure of uncertainty) $H(X) \in [0, n]$

QC-extraction: Better example continued

- Pick i in {0,1} at random with U_0= I and U_1 = H



Can be used to prove security of QKD

Theorem [Berta, Christandl, Colbeck, Renes, Renner 2010]

For *any input state*

$$\frac{1}{2}(H(X_0|E)+H(X_1|E)) \geq \frac{n}{2}+\frac{1}{2}H(A|E)$$

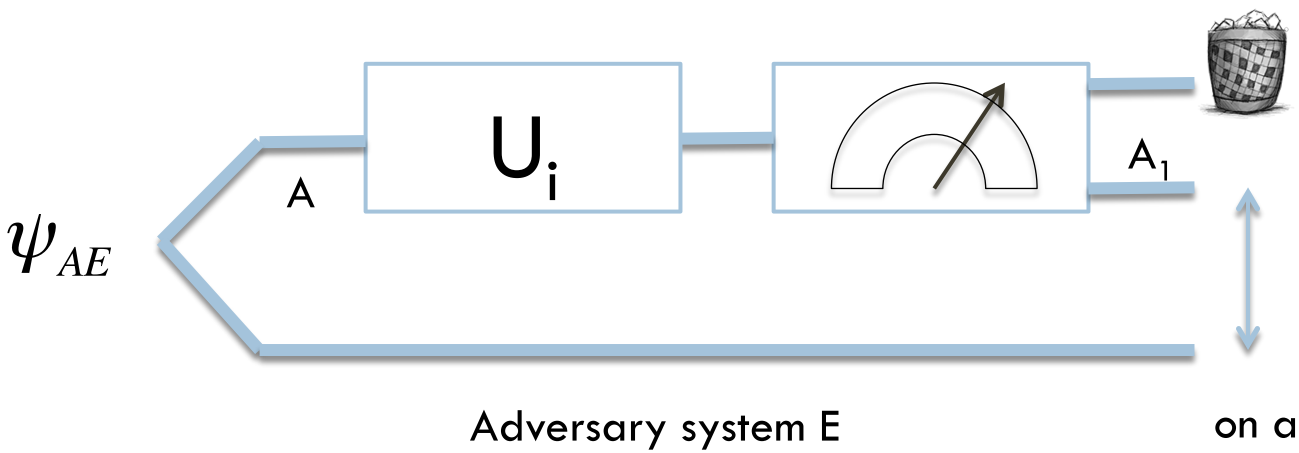
Uncertainty given E

=-n for max. entangled

QC-extractor: informal definition

- Shannon entropy: weak measure of uncertainty
- Want output indistinguishable from uniform random bits except with small probability ε
- Need L > 2 measurements

<u>Definition:</u> For all input states ρ_{AE} "not too entangled"



$$\approx_\varepsilon \frac{id_{A_1}}{|A_1|} \otimes \rho_E$$

on average over i in {1,…, L}

Measuring uncertainty relative to adversary

- Right measure:

$$H_{\min}(A|E) \in [-\log|A|, \log|A|]$$

$$H_{\min}(A|E) = \max\{\lambda : \rho_{AE} \leq 2^{-\lambda} id \otimes \rho_E\}$$

- Examples:

$$\rho_{AE} = |\psi\rangle\langle\psi|_A \otimes \rho_E \qquad H_{\min}(A|E) = 0$$

$$\rho_{AE} = \frac{id_A}{|A|} \otimes \rho_E \qquad H_{\min}(A|E) = \log|A|$$

$$|\rho\rangle_{AE} = \frac{1}{\sqrt{|A|}} \sum |j\rangle_A |j\rangle_E \qquad H_{\min}(A|E) = -\log|A|$$

Maximally entangled state

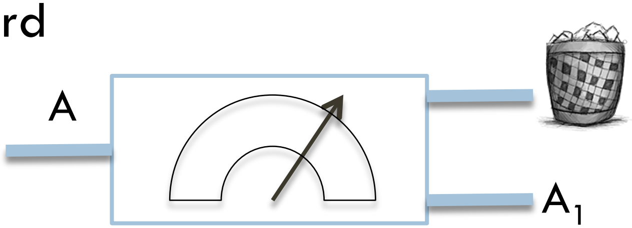
QC-extractor: more formal def

Definition

QC-extractor is a set of unitaries $\{U_1,\ldots,U_L\}$ such that for all ρ_{AE} such that Hmin(A|E) > k

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathcal{T}_{A\to A_1}(U_i\rho_{AE}U_i^\dagger)-\frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1\leq\varepsilon\ .$$

- $\mathcal{T}$: Measurement + discard



- Parameters:
  - k : how much uncertainty is needed in the input
  - log|A1|: size of output
  - ε : statistical error
  - L: number of unitaries

Parameters: Output size $|A_1|$

Proposition

We can extract at most

$$\log|A_1| \leq \log|A| + H_{\min}^{\sqrt{\varepsilon}}(A|E)\ .$$

Example:

- If pure state on A: at most log|A|
- If maximally entangled Hmin(A|E) = -log |A|: cannot extract anything

Parameters: seed size L

Proposition

Size of output

$$\log(1/\varepsilon) \le \log L \le \log |A_1| + small$$

Simple argument

Probabilistic construction
$\{U_1,\ldots,U_L\}$ random unitaries

Huge gap! I suspect log L = O(log log |A|) might be possible

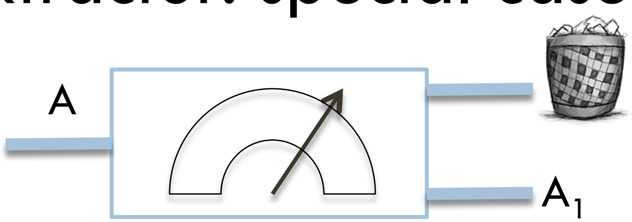
QC-extractors: constructions from decoupling

- Decoupling unitaries [Dupuis et. al. 2010]
  - Random unitaries (Haar measure)
  - Unitary two-design (Reproduce second moment of Haar measure)
- Works for any map $\mathcal{T}$

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathcal{T}_{A\to A_1}(U_i\rho_{AE}U_i^{\dagger}) - \frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \varepsilon \ .$$

- QC-extractor: special case

$\mathcal{T}$ =

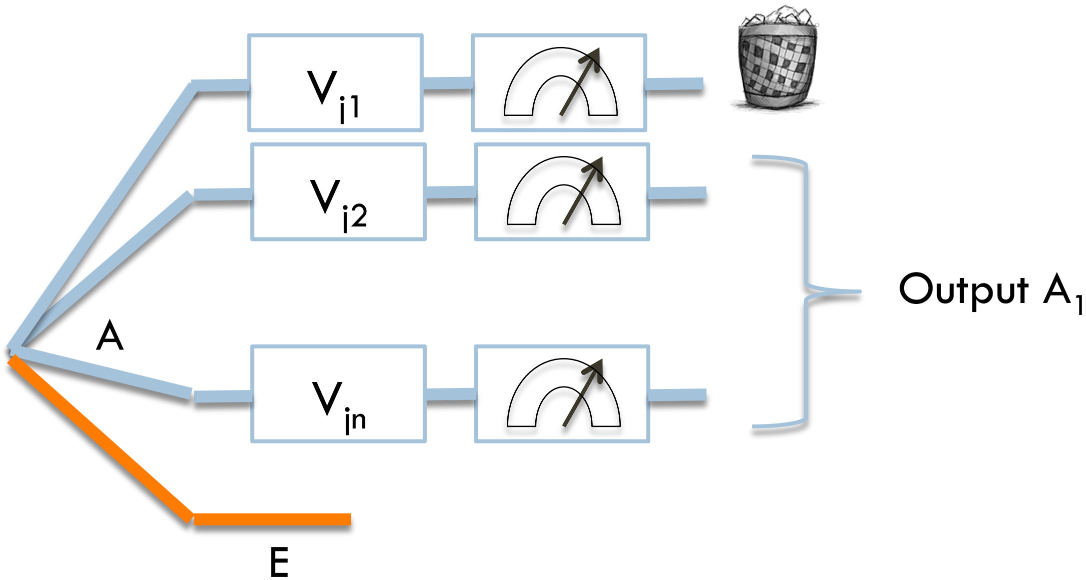


QC-extractors: constructions from decoupling

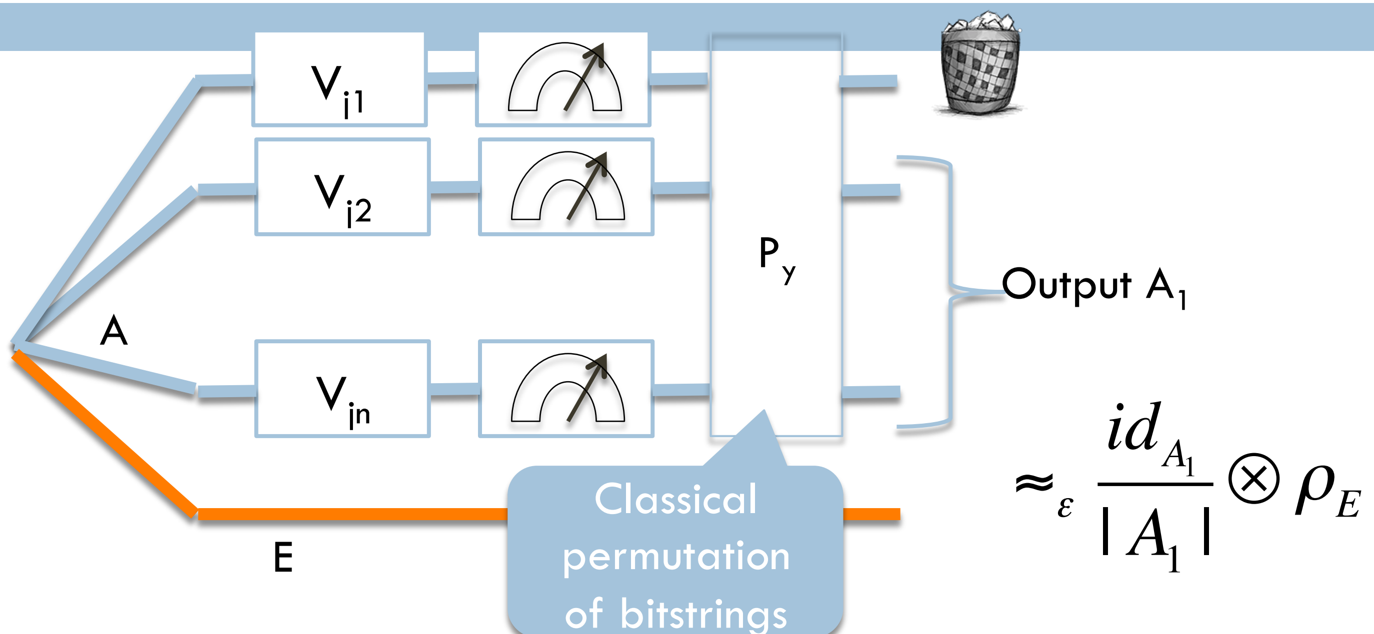
- Decoupling unitaries [Dupuis et. al. 2010]
  - Random unitaries (Haar measure)
  - Unitary two-design (Reproduce second moment of random unitaries) evenly distributed unitaries
- Parameters:
  - Output size: $\log |A| + H_{min}(A|E)$ (optimal)
  - Seed size: $\log L = 4 \log |A|$ (probably far from optimal)
  - Unitaries can be implemented by polytime quantum circuits

QC-extractor: simpler construction

- For cryptographic applications, we want **simpler** unitaries: only **single-qubit** gates



QC-extractor: simpler construction



Theorem

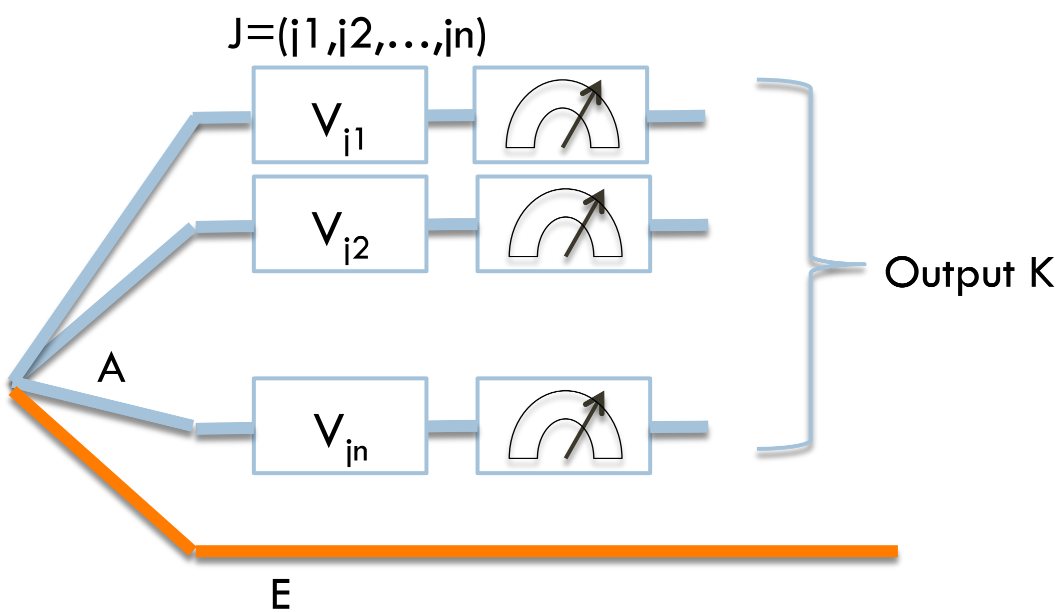
$\{P_y V_j\}_{yj}$ is a QC-extractor with

$$\varepsilon \approx \sqrt{2^{-0.58n + \log|A_1| - H_{\min}(A|E)}}$$

Min-entropy uncertainty relation

Theorem

$$H_{\min}(K \mid EJ) \geq 0.58n + H_{\min}(A \mid E)$$

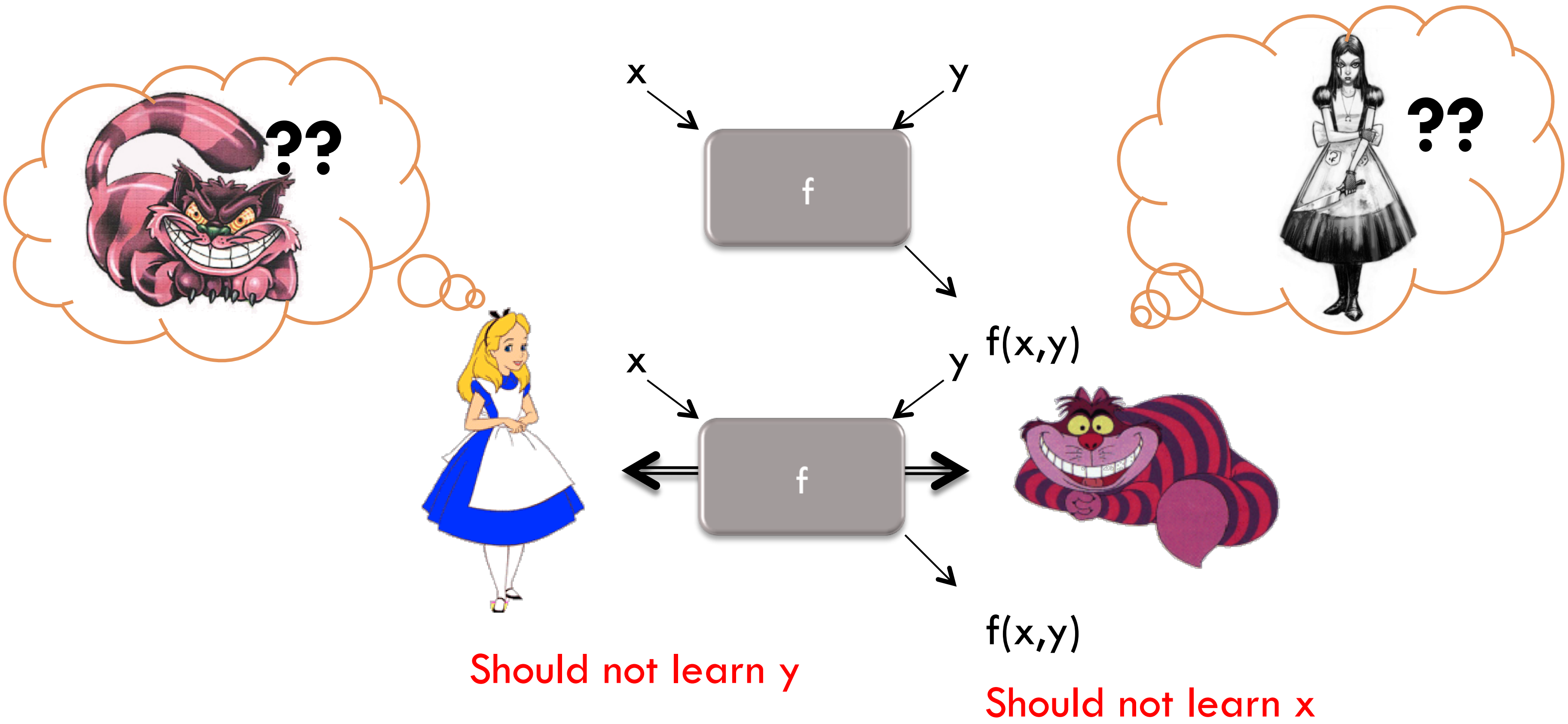


Proof idea

- Use 2-norm instead of the 1-norm
- Similar to leftover hash lemma* with more technicalities

* Leftover hash lemma: **two**-universal hash functions are good randomness extractors

Applications to cryptography: secure function evaluation



Secure function evaluation

- Not possible to solve without assumptions [Lo 97]
- Classical assumptions are typically computational assumptions (eg factoring is hard)

- Memory assumption: bounded **quantum** storage [Damgaard, Fehr, Salvail, Schaffner 2005]
  - Secure function evaluation possible if parties have limited quantum storage
  - Honest parties do not need any quantum storage

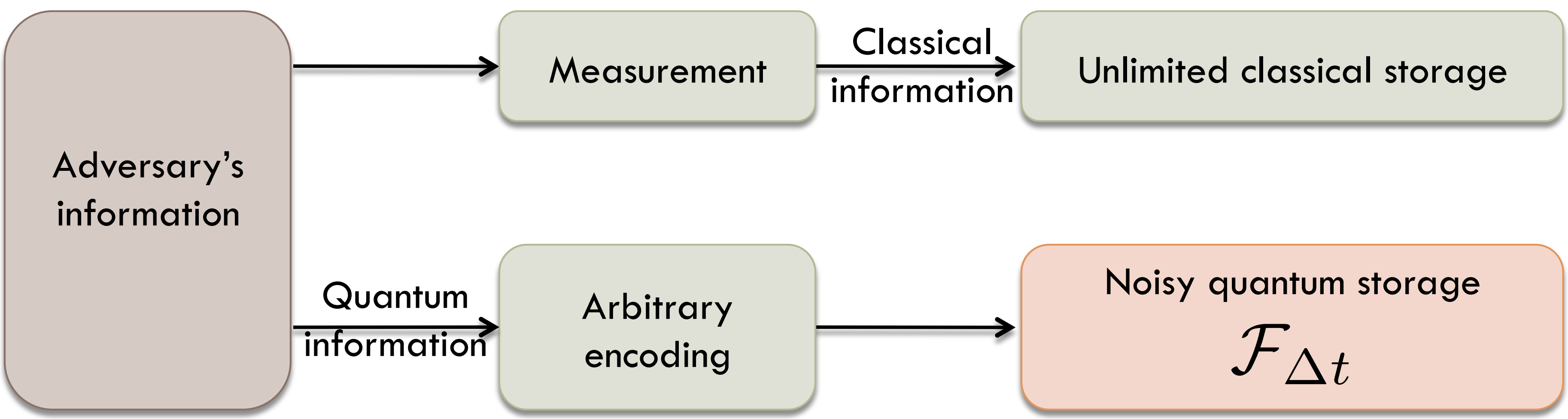
Noisy storage model [Wehner, Schaffner, Terhal 08]

- Computationally all-powerful
- Unlimited classical storage

What the adversary can do

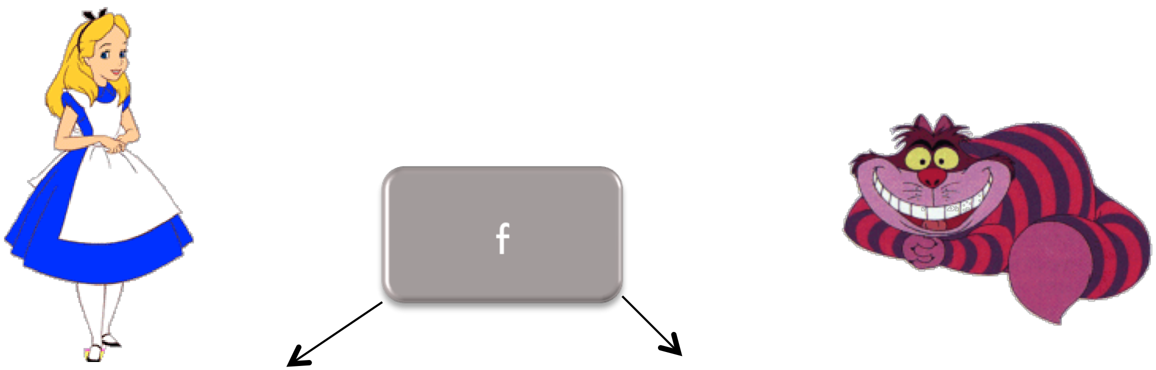
- Noisy quantum storage

Protocol will have waiting times Δt in which noisy-storage must be used:



Weak string erasure [Konig, Wehner, Wullschleger 10]

Primitive: weak string erasure



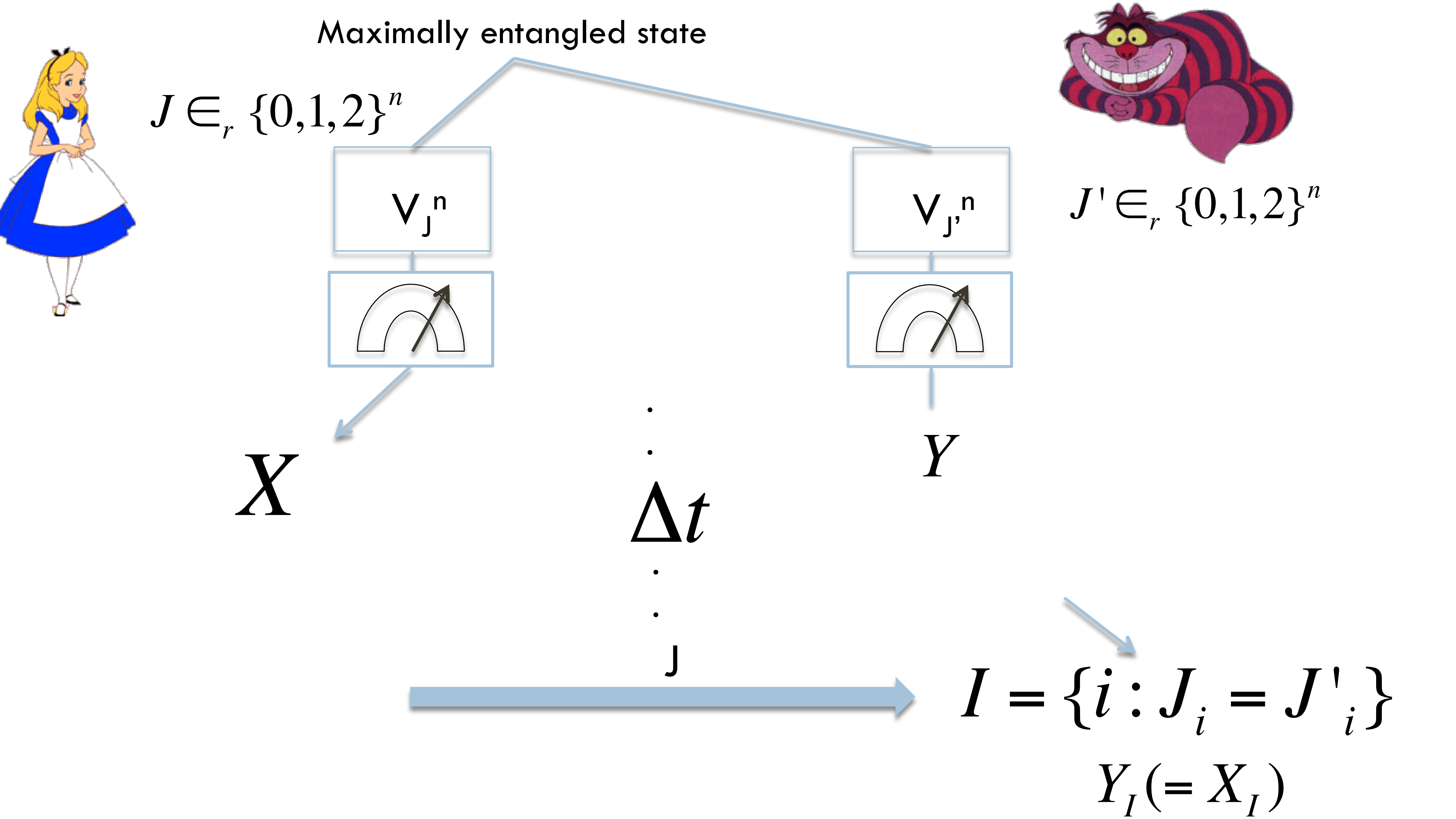
$X \in_r \{0,1\}^n$ $\quad$ $I \subset_r \{1,\ldots,n\}$ and $X_I \in \{0,1\}^{|I|}$

Security criterion

- Cheating Alice does not learn I
- Cheating Bob Hmin(X|B) > λ n

It is for this condition that we use the limitation on Bob's storage

Protocol for weak string erasure in the noisy storage model



Security statement

- Cheating Alice
  - Protocol unconditionally secure

- Cheating Bob
  - Provided

$$\mathrm{BestSuccProb}(\ \mathscr{F}\ ) \leq 2^{-(1-0.58+\delta)n}$$

The protocol is secure

Summary

- Viewed uncertainty relations as some kind of randomness extractor

- Using techniques from extractors and decoupling, we give new uncertainty relations

- Use it to relate security to capacity of device to maintain entanglement

Open problems

- Ideally, want security provided

$$\mathrm{BestSuccProb}(\ \mathscr{F}\ ) \leq 2^{-\delta n}$$

Should improve

From
$$H_{\min}(K \mid EJ) \geq 0.58n + H_{\min}(A \mid E)$$

To
$$H_{\min}(K \mid EJ) \geq 0.58n + 0.58 H_{\min}(A \mid E)$$

Related to (quantum) min-entropy sampling

- Number of unitaries needed for a QC-extractor not well understood
  - Is there a QC-extractor with log L = O(log log |A|)?
  - More generally, are there decoupling unitaries with logL = O(log log |A|)?