Quantum to Classical Randomness Extractors

Mario Berta, Omar Fawzi,
Stephanie Wehner

-

Full version preprint available at
arXiv:1111.2026v3

10/06/2012 - QCRYPT CQT, National University of Singapore

Outline

- (Classical to Classical) Randomness Extractors

Outline

- (Classical to Classical) Randomness Extractors
- <u>Main Contribution</u>: Quantum to Classical Randomness Extractors

Outline

- (Classical to Classical) Randomness Extractors
- Main Contribution: Quantum to Classical Randomness Extractors
- Application: Security in the Noisy-Storage Model

Outline

- (Classical to Classical) Randomness Extractors
- Main Contribution: Quantum to Classical Randomness Extractors
- Application: Security in the Noisy-Storage Model
- Entropic Uncertainty Relations with Quantum Side Information

Outline

- (Classical to Classical) Randomness Extractors
- Main Contribution: Quantum to Classical Randomness Extractors
- Application: Security in the Noisy-Storage Model
- Entropic Uncertainty Relations with Quantum Side Information
- Conclusions / Open Problems

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ **Ex:** $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ <u>Ex</u>: $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ <u>Ex</u>: $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$ <u>Ex</u>: $\Pr[N_i = 0] = \frac{2}{3} \quad \Pr[N_i = 1] = \frac{1}{3}$

$$M = f(N_1 N_2 N_3) = N_1 + N_2 + N_3 \mod 2$$

$$\Pr[M = 0] \approx 0.52$$

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ **Ex:** $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$ **Ex:** $\Pr[N_i = 0] = \frac{2}{3} \quad \Pr[N_i = 1] = \frac{1}{3}$

$$M = f(N_1 N_2 N_3) = N_1 + N_2 + N_3 \mod 2$$

$$\Pr[M = 0] \approx 0.52$$

- Only minimal guarantee about the randomness of the source, high min-entropy: $H_{\min}(N)_P = -\log \max_n P_N(n) = -\log p_{\text{guess}}(N)_P$.

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ **Ex:** $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$ **Ex:** $\Pr[N_i = 0] = \frac{2}{3} \quad \Pr[N_i = 1] = \frac{1}{3}$

$$M = f(N_1 N_2 N_3) = N_1 + N_2 + N_3 \mod 2$$

$$\Pr[M = 0] \approx 0.52$$

- Only minimal guarantee about the randomness of the source, high min-entropy: $H_{\min}(N)_P = -\log \max_n P_N(n) = -\log p_{\text{guess}}(N)_P$.
- Not possible to obtain randomness using a deterministic function, invest a small amount of perfect randomness:

N $\rightarrow$ f_D $\rightarrow$ $M = f_D(N)$

Seed D

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

  Source $\rightarrow$ $N = N_1, N_2, \ldots, N_q$ <u>Ex</u>: $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$ <u>Ex</u>: $\Pr[N_i = 0] = \frac{2}{3} \quad \Pr[N_i = 1] = \frac{1}{3}$

  $$M = f(N_1 N_2 N_3) = N_1 + N_2 + N_3 \mod 2$$

  $$\Pr[M = 0] \approx 0.52$$

- Only minimal guarantee about the randomness of the source, high min-entropy: $H_{\min}(N)_P = -\log \max_n P_N(n) = -\log p_{\text{guess}}(N)_P$.

- Not possible to obtain randomness using a deterministic function, invest a small amount of perfect randomness:

  $$\text{N} \rightarrow \boxed{f_D} \rightarrow M = f_D(N)$$

  Seed D $\uparrow$

- Lost randomness? Strong extractors: (M, D) are jointly uniform.

Classical to Classical (CC)-Randomness Extractors (I)

- Given an (unknown) weak source of classical randomness, how to convert it into uniformly random bits?

Source $\rightarrow N = N_1, N_2, \ldots, N_q$ **Ex:** $\Pr[N_1 = 0] = \frac{1}{2} + \delta_1, \quad \Pr[N_2 = 0] = \frac{1}{2} + \delta_2, \quad \ldots$

- Function: $f(N = N_1, \ldots, N_q) = M$ **Ex:** $\Pr[N_i = 0] = \frac{2}{3} \quad \Pr[N_i = 1] = \frac{1}{3}$

$$M = f(N_1 N_2 N_3) = N_1 + N_2 + N_3 \mod 2$$

$$\Pr[M = 0] \approx 0.52$$

- Only minimal guarantee about the randomness of the source, high min-entropy: $H_{\min}(N)_P = -\log \max_n P_N(n) = -\log p_{\text{guess}}(N)_P$.
- Not possible to obtain randomness using a deterministic function, invest a small amount of perfect randomness:

N $\rightarrow$ f_D $\rightarrow M = f_D(N)$

Seed D

- Lost randomness? Strong extractors: (M, D) are jointly uniform.
- Applications in information theory, cryptography and computational complexity theory [1,2].

[1] Nisan and Zuckerman, JCSS 52:43, 1996

[2] Vadhan, http://people.seas.harvard.edu/~salil/pseudorandomness/

Classical to Classical (CC)-Randomness Extractors (II)

- Deal with prior knowledge (trivial for classical side information [3]), in general problematic for quantum side information [4]! Source described by classical-quantum (cq)-state:

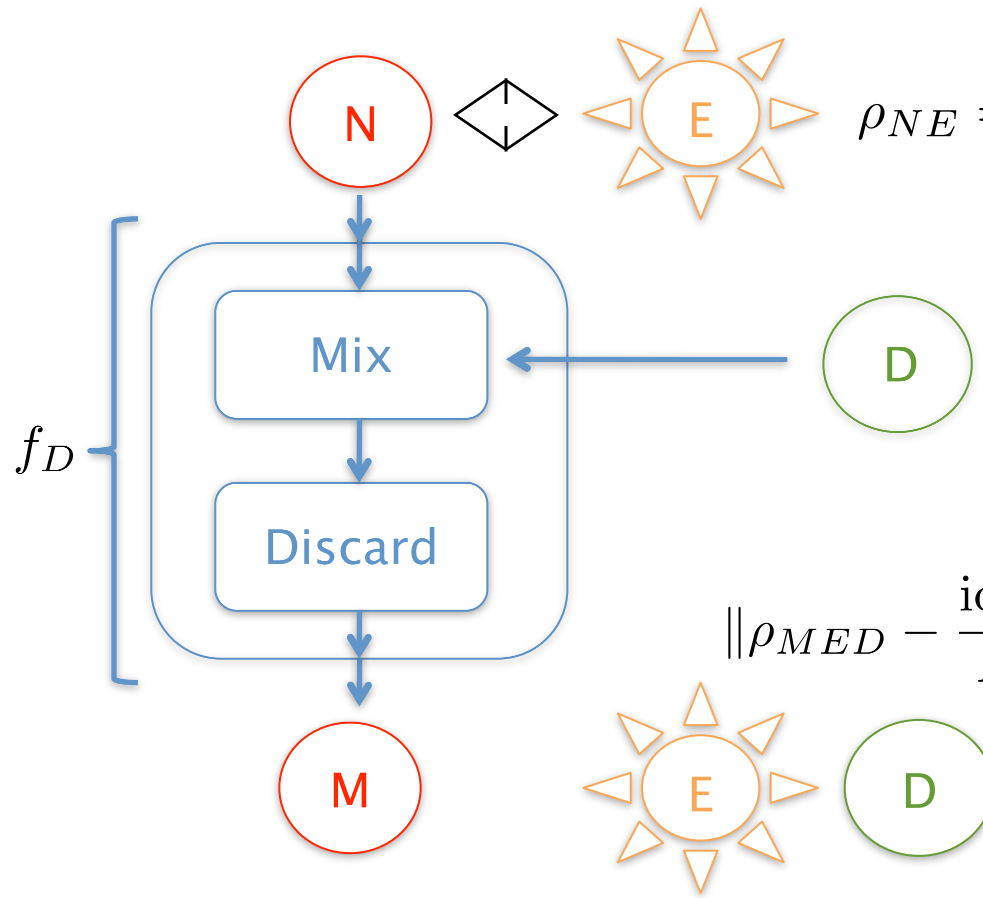
$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n .$$

[3] König and Terhal, IEEE TIT 54:749, 2008
[4] Gavinsky et al., STOC, 2007

Classical to Classical (CC)-Randomness Extractors (II)

- Deal with prior knowledge (trivial for classical side information [3]), in general problematic for <u>quantum side information</u> [4]! Source described by classical-quantum (cq)-state:

$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n .$$



$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n$$

$$\frac{\mathrm{id}_D}{D}$$

$$\|\rho_{MED} - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED}\|_1 \leq \varepsilon$$

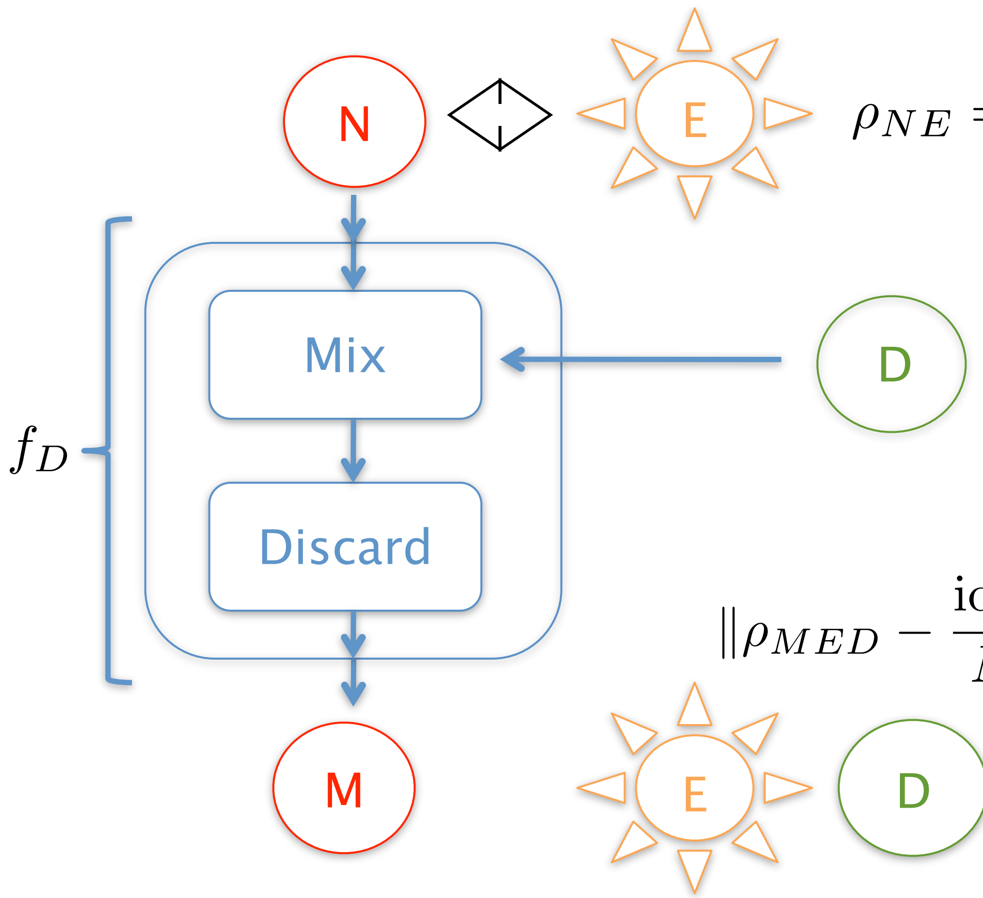
$$\|X\|_1 = \mathrm{tr}[\sqrt{X^\dagger X}]$$

[3] König and Terhal, IEEE TIT 54:749, 2008
[4] Gavinsky et al., STOC, 2007

Classical to Classical (CC)-Randomness Extractors (II)

- Deal with prior knowledge (trivial for classical side information [3]), in general problematic for <u>quantum side information</u> [4]! Source described by classical-quantum (cq)-state:

$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n \,.$$



$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n$$

$$\frac{\mathrm{id}_D}{D}$$

$$\|\rho_{MED} - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED}\|_1 \leq \varepsilon$$

$$\|X\|_1 = \mathrm{tr}[\sqrt{X^\dagger X}]$$

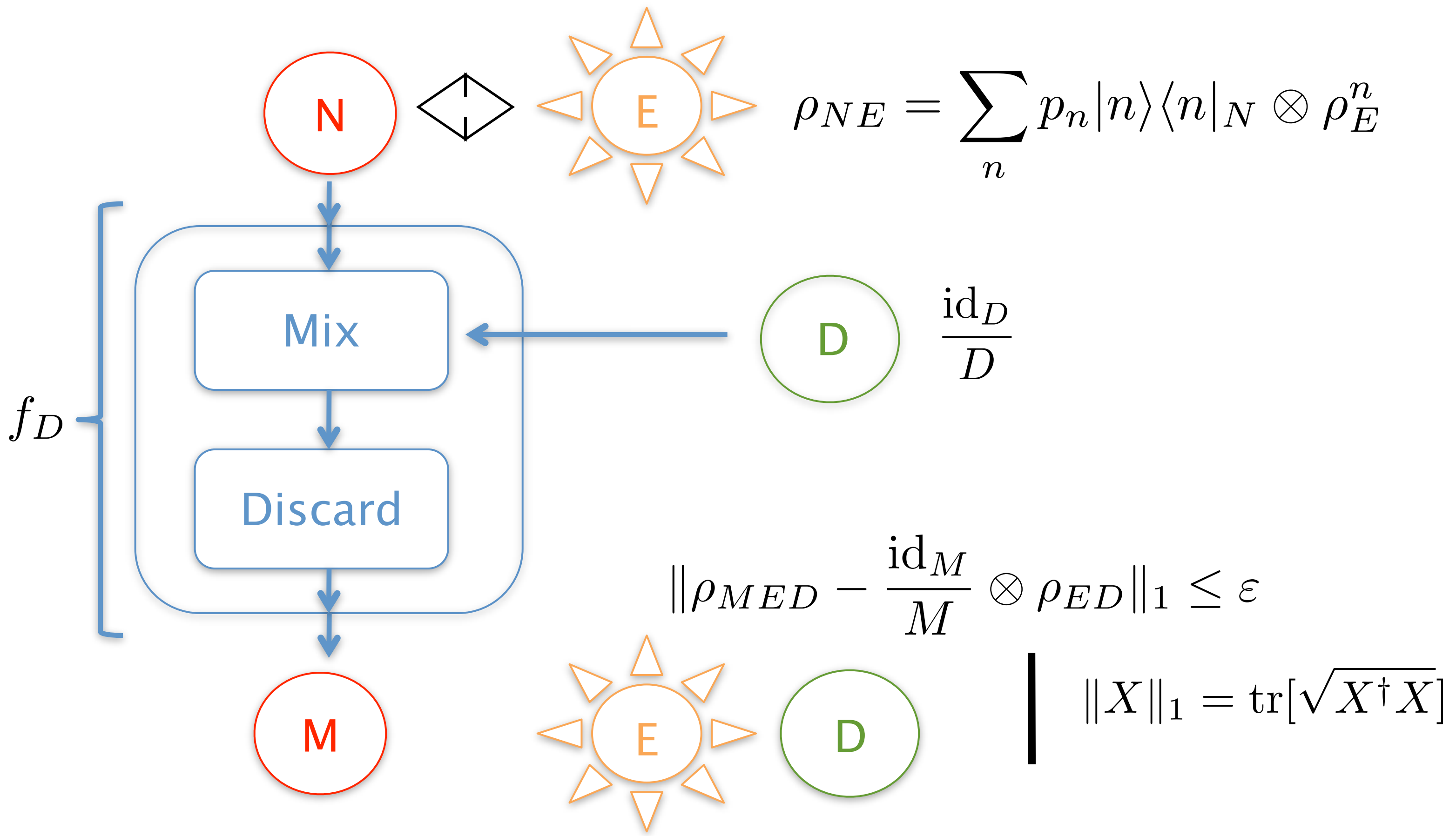
- Guarantee about conditional min-entropy of the source: $H_{\min}(N|E)_\rho = -\log p_{\text{guess}}(N|E)_\rho$.

[3] König and Terhal, IEEE TIT 54:749, 2008
[4] Gavinsky et al., STOC, 2007

Classical to Classical (CC)-Randomness Extractors (II)

- Deal with prior knowledge (trivial for classical side information [3]), in general problematic for <u>quantum side information</u> [4]! Source described by classical-quantum (cq)-state:

$$\rho_{NE} = \sum_n p_n |n\rangle\langle n|_N \otimes \rho_E^n \,.$$



- Guarantee about conditional min-entropy of the source: $H_{\min}(N|E)_\rho = -\log p_{\text{guess}}(N|E)_\rho$.
- <u>Ex</u>: Two-universal hashing / privacy amplification [5]. For all cq-states ρ_{NE} with

  $H_{\min}(N|E)_\rho \geq k$, we have $\|\rho_{MED} - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED}\|_1 \leq \varepsilon$ for $M = 2^k \cdot \varepsilon^2$.

  Strong (k, ε) extractor (against quantum side information), $D = O(N)$.

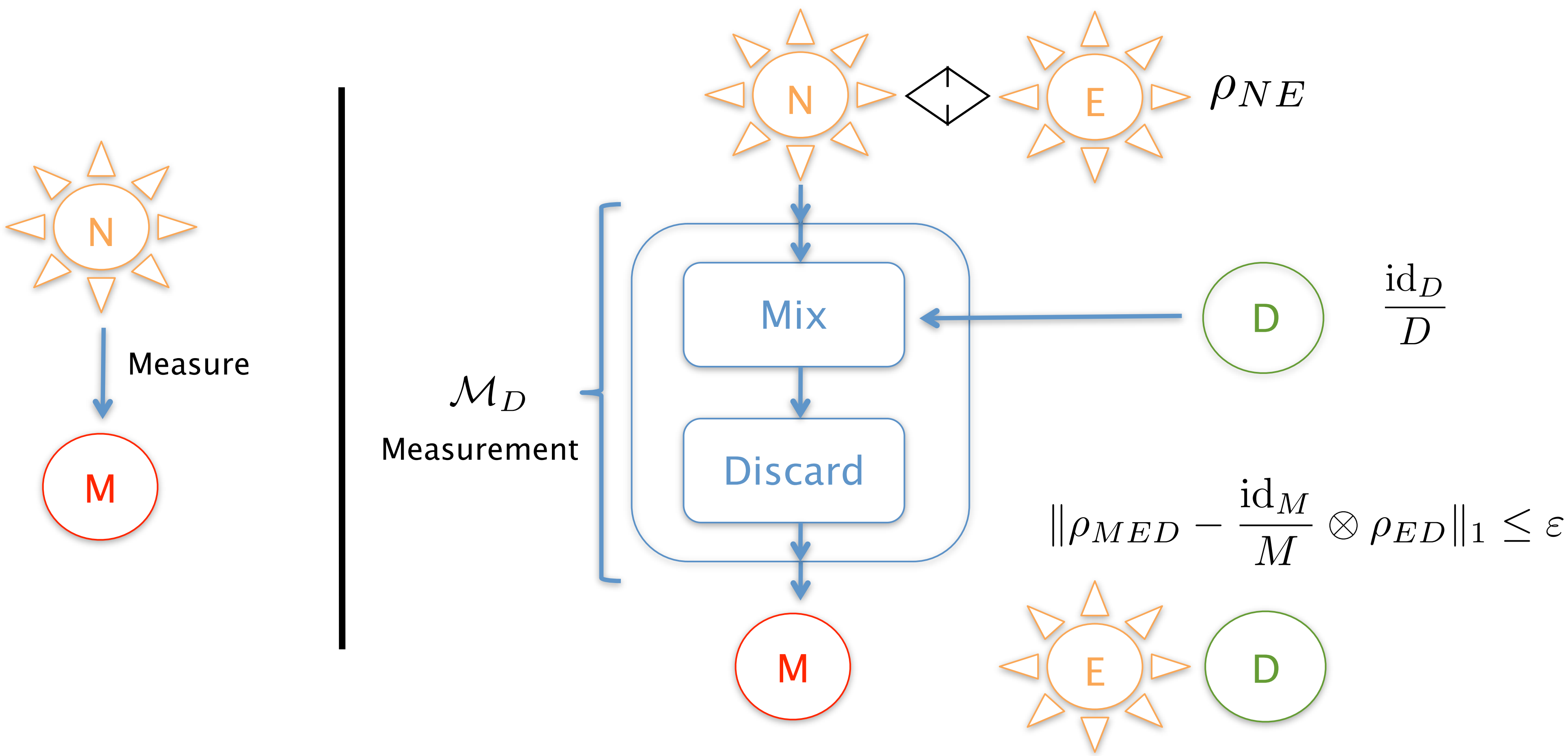
[3] König and Terhal, IEEE TIT 54:749, 2008
[4] Gavinsky et al., STOC, 2007
[5] Renner, PhD Thesis, ETHZ, 2005

Quantum to Classical (QC)-Randomness Extractors - Definition (I)

- Motivation: How to get weak randomness at first? How much randomness can be gained from a quantum source? Are all measurements equally “good” at obtaining randomness from a quantum system?

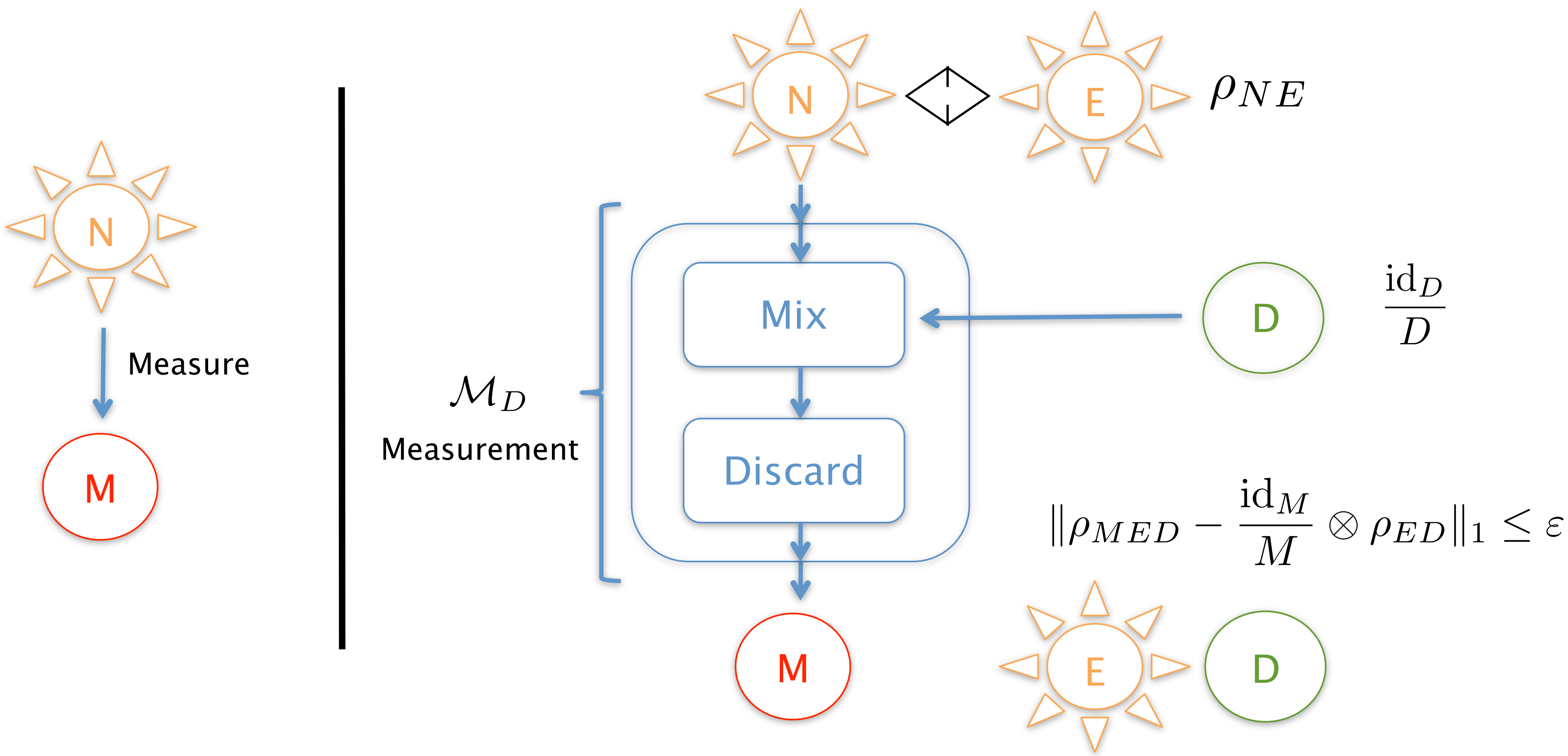
Quantum to Classical (QC)-Randomness Extractors - Definition (I)

- Motivation: How to get weak randomness at first? How much randomness can be gained from a quantum source? Are all measurements equally "good" at obtaining randomness from a quantum system?



Quantum to Classical (QC)-Randomness Extractors - Definition (I)

- <u>Motivation</u>: How to get weak randomness at first? How much randomness can be gained from a quantum source? Are all measurements equally "good" at obtaining randomness from a quantum system?



- <u>Idea</u>: Same setup as in the classical case (no control of the source)! Only guarantee about the conditional min-entropy [6]:

$$H_{\min}(N|E)_\rho = -\log N \max_{\Lambda_{E\to N'}} F(\Phi_{NN'}, (\mathrm{id}_N \otimes \Lambda_{E\to N'})(\rho_{NE}))$$

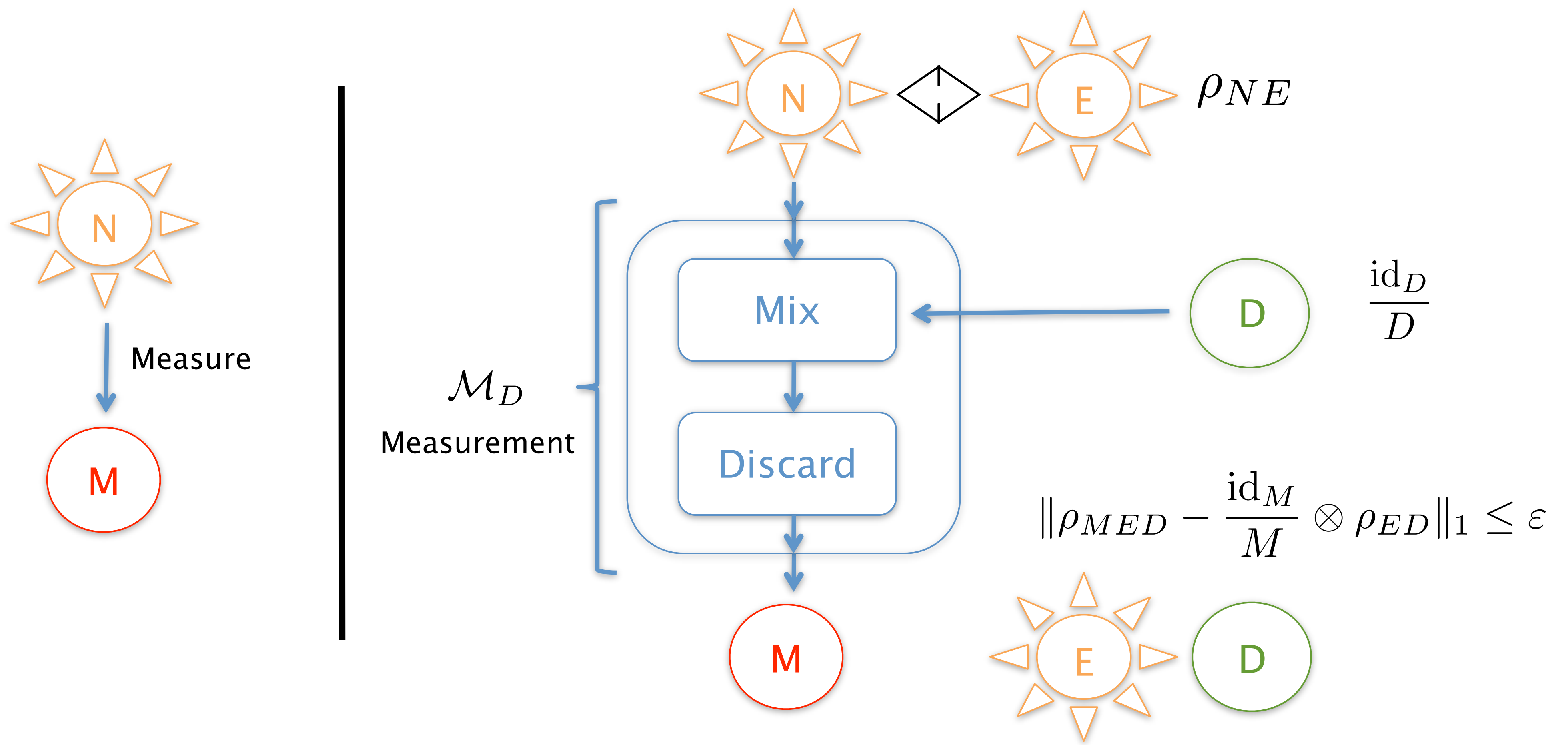
$$|\Phi\rangle_{NN'} = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle_N \otimes |n\rangle_{N'}$$

$$F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$$

[6] König et al., IEEE TIT 55:4674, 2009

Quantum to Classical (QC)-Randomness Extractors - Definition (I)

- <u>Motivation</u>: How to get weak randomness at first? How much randomness can be gained from a quantum source? Are all measurements equally "good" at obtaining randomness from a quantum system?



- <u>Idea</u>: Same setup as in the classical case (no control of the source)! Only guarantee about the conditional min-entropy [6]:

$$H_{\min}(N|E)_\rho = -\log N \max_{\Lambda_{E\to N'}} F(\Phi_{NN'}, (\mathrm{id}_N \otimes \Lambda_{E\to N'})(\rho_{NE}))$$

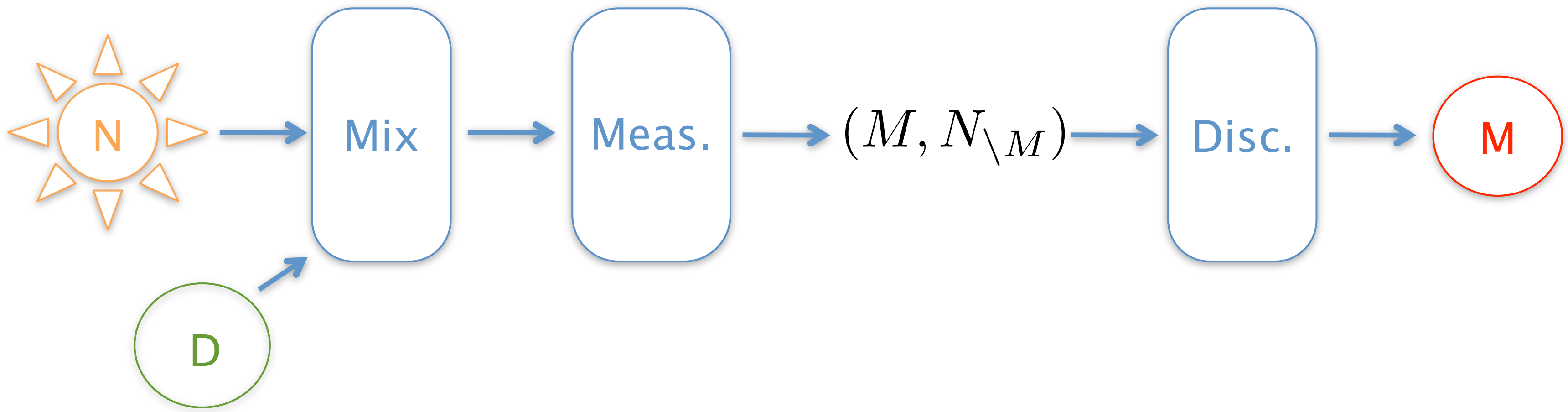
$$|\Phi\rangle_{NN'} = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle_N \otimes |n\rangle_{N'}$$

$$F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$$

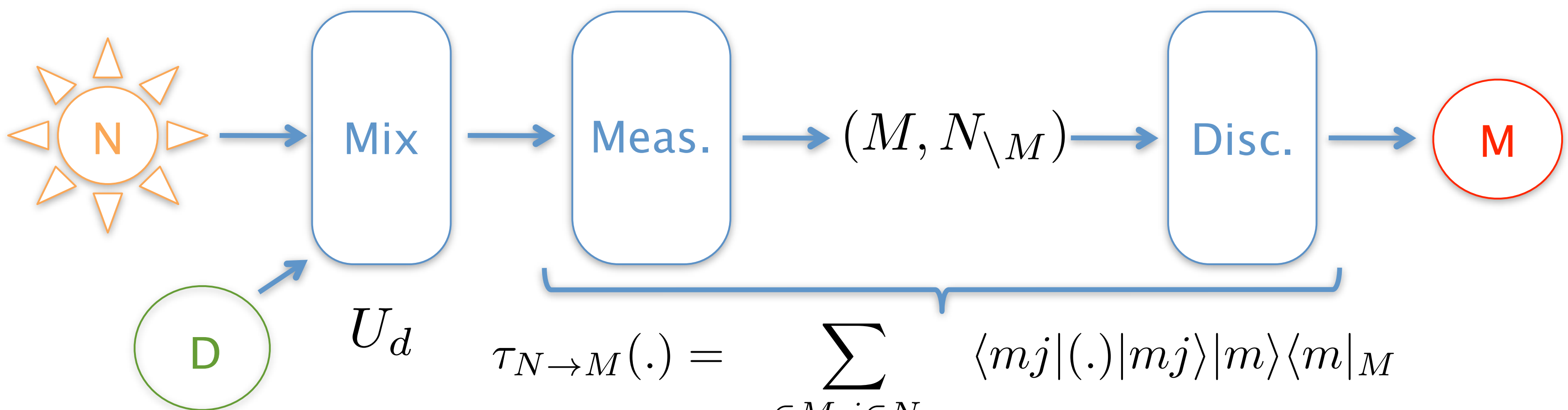
- Can get negative for entangled input states, in fact for MES: $H_{\min}(N|E)_\Phi = -\log N$.

[6] König et al., IEEE TIT 55:4674, 2009

Quantum to Classical (QC)-Randomness Extractors - Definition (II)

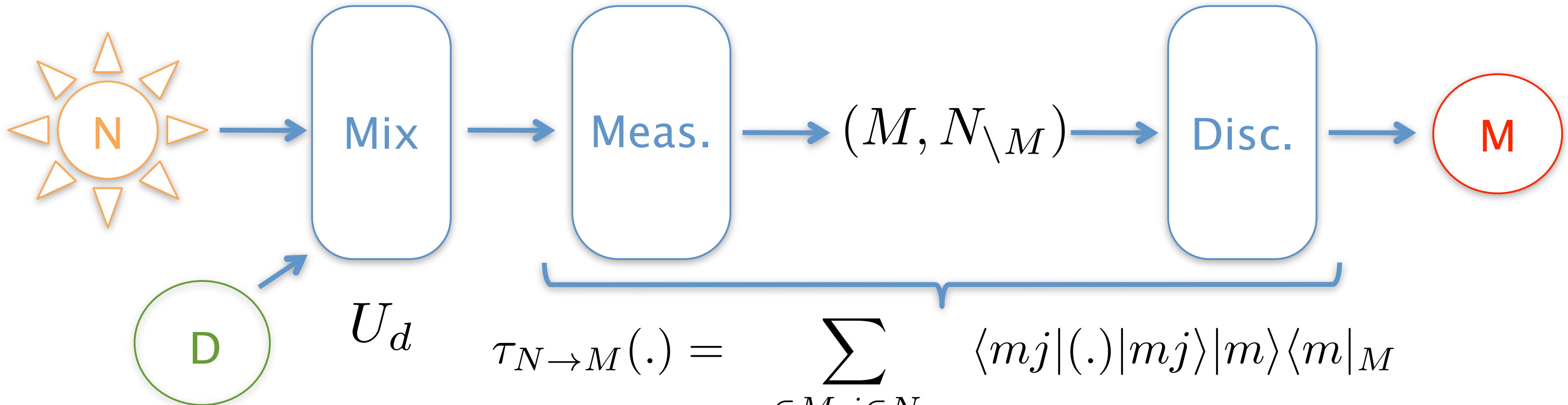


Quantum to Classical (QC)-Randomness Extractors - Definition (II)



$$\tau_{N\to M}(.) = \sum_{m\in M, j\in N_{\setminus M}} \langle mj|(.)|mj\rangle |m\rangle\langle m|_M$$

Quantum to Classical (QC)-Randomness Extractors - Definition (II)

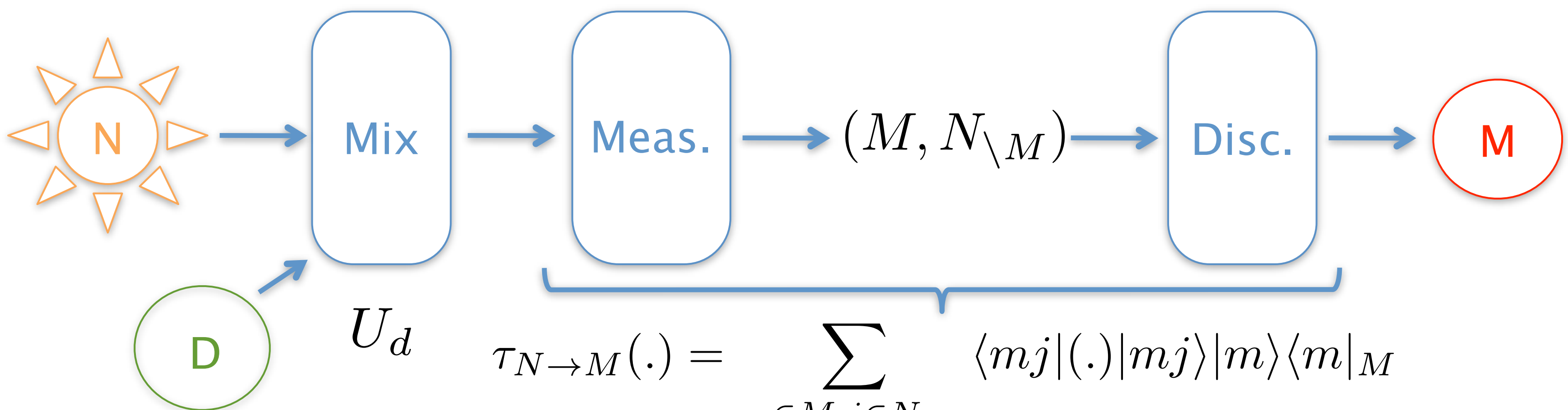


$$\tau_{N\to M}(.) = \sum_{m\in M, j\in N_{\setminus M}} \langle mj|(.)|mj\rangle |m\rangle\langle m|_M$$

- **Definition:** A set of unitaries $\{U_1, \ldots, U_D\}$ defines a strong (k, ε) qc-extractor (against quantum side information) if for any state ρ_{NE} with $H_{\min}(N|E)_\rho \geq k$,

$$\|\frac{1}{D}\sum_{i=1}^{D} \tau_{N\to M}(U_i \rho_{NE} U_i^\dagger) \otimes |i\rangle\langle i|_D - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED}\|_1 \leq \varepsilon \ .$$

Quantum to Classical (QC)-Randomness Extractors - Definition (II)



$$\tau_{N\to M}(.) = \sum_{m\in M, j\in N_{\setminus M}} \langle mj|(.)|mj\rangle |m\rangle\langle m|_M$$

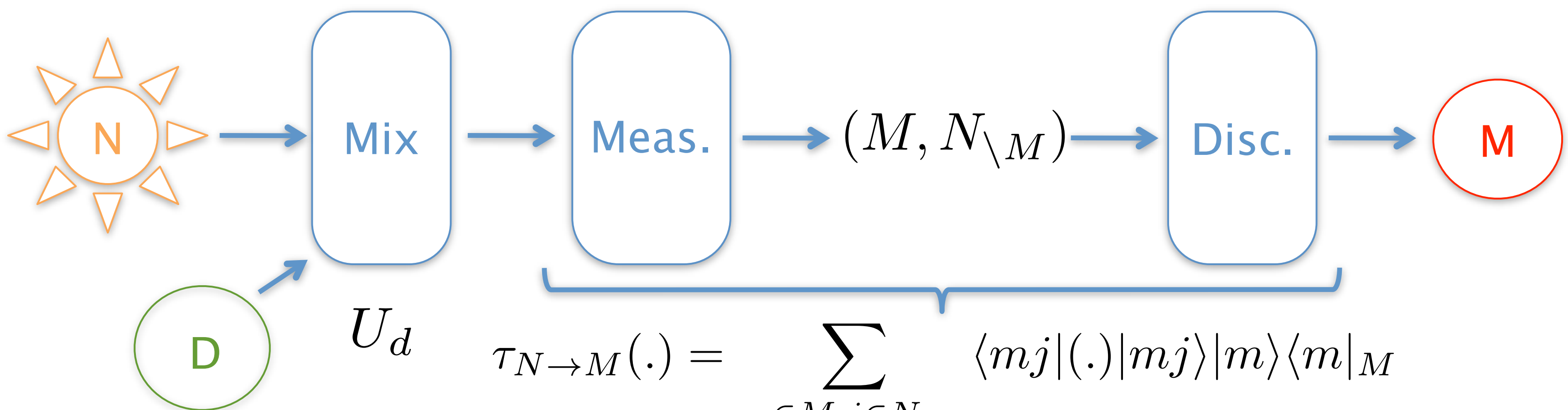
- **Definition:** A set of unitaries $\{U_1, \ldots, U_D\}$ defines a strong (k, ε) qc-extractor (against quantum side information) if for any state ρ_{NE} with $H_{\min}(N|E)_\rho \geq k$,

$$\| \frac{1}{D} \sum_{i=1}^{D} \tau_{N\to M}(U_i \rho_{NE} U_i^\dagger) \otimes |i\rangle\langle i|_D - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED} \|_1 \leq \varepsilon \, .$$

- Without side information, this corresponds to ε-metric uncertainty relations [7].

[7] Fawzi et al., STOC, 2011

Quantum to Classical (QC)-Randomness Extractors - Definition (II)

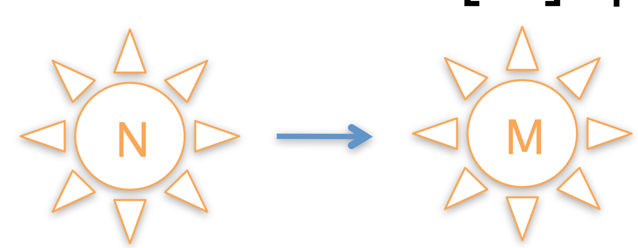


$$\tau_{N\to M}(.) = \sum_{m\in M, j\in N_{\setminus M}} \langle mj|(.)|mj\rangle |m\rangle\langle m|_M$$

- <u>Definition</u>: A set of unitaries $\{U_1, \ldots, U_D\}$ defines a strong (k, ε) qc-extractor (against quantum side information) if for any state ρ_{NE} with $H_{\min}(N|E)_\rho \geq k$,
$$\left\| \frac{1}{D} \sum_{i=1}^{D} \tau_{N\to M}(U_i \rho_{NE} U_i^\dagger) \otimes |i\rangle\langle i|_D - \frac{\mathrm{id}_M}{M} \otimes \rho_{ED} \right\|_1 \leq \varepsilon \, .$$

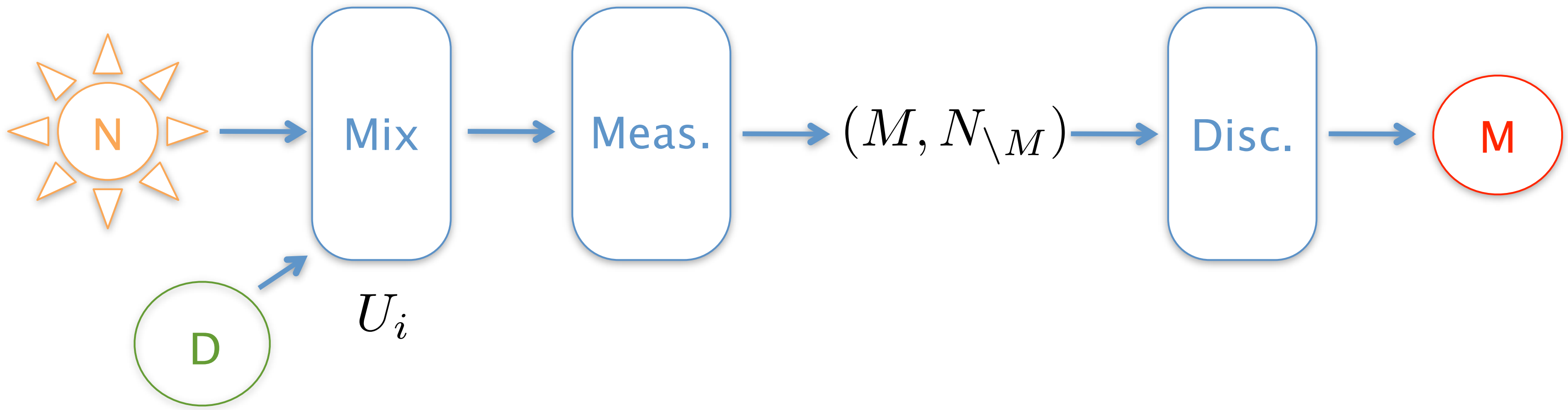
- Without side information, this corresponds to ε-metric uncertainty relations [7].

- Fully quantum versions of this: decoupling theorems (quantum coding theory) [8], quantum state randomization [9], quantum extractors [10]: <u>quantum to quantum (qq)-randomness extractors</u>!



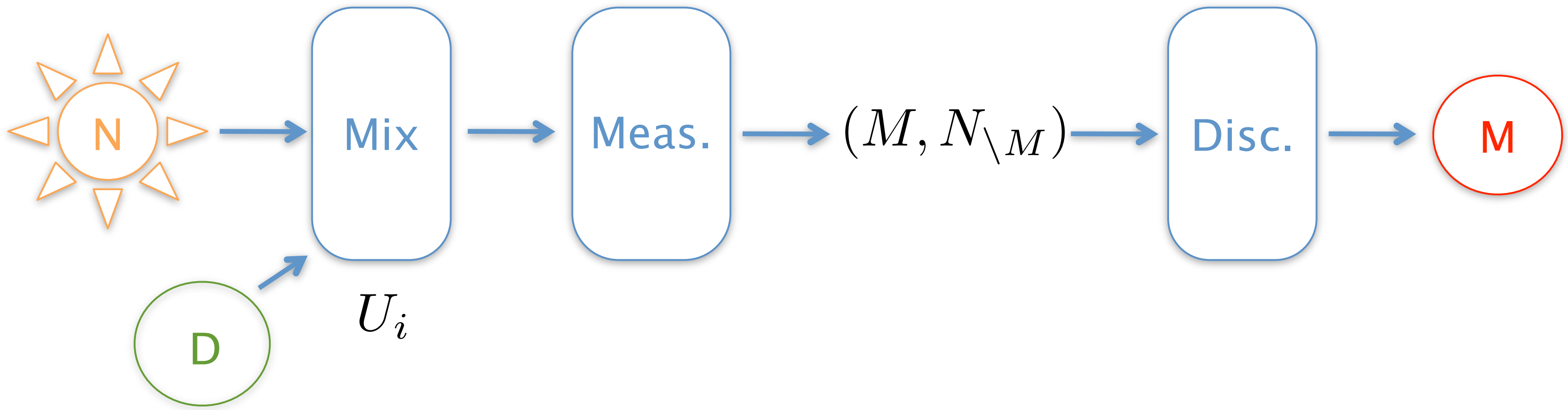
[7] Fawzi et al., STOC, 2011
[8] Dupuis, PhD Thesis, McGill, 2009
[9] Hayden et al., CMP 250:371, 2004
[10] Ben-Aroya et al., TOC 6:47, 2010

Quantum to Classical (QC)-Randomness Extractors - Parameters



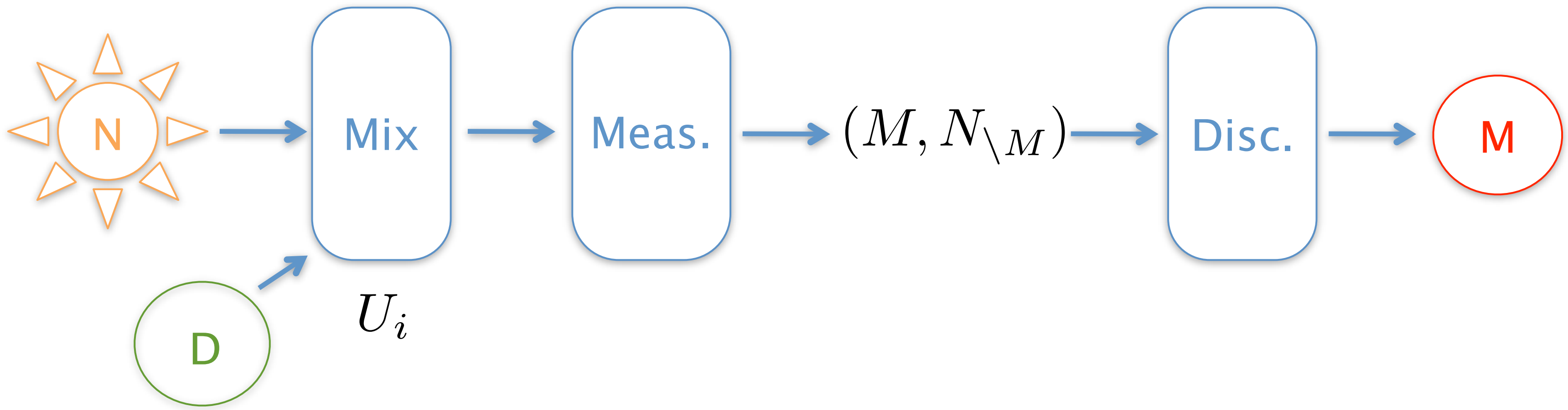
- Probabilistic construction (random unitaries).

Quantum to Classical (QC)-Randomness Extractors - Parameters



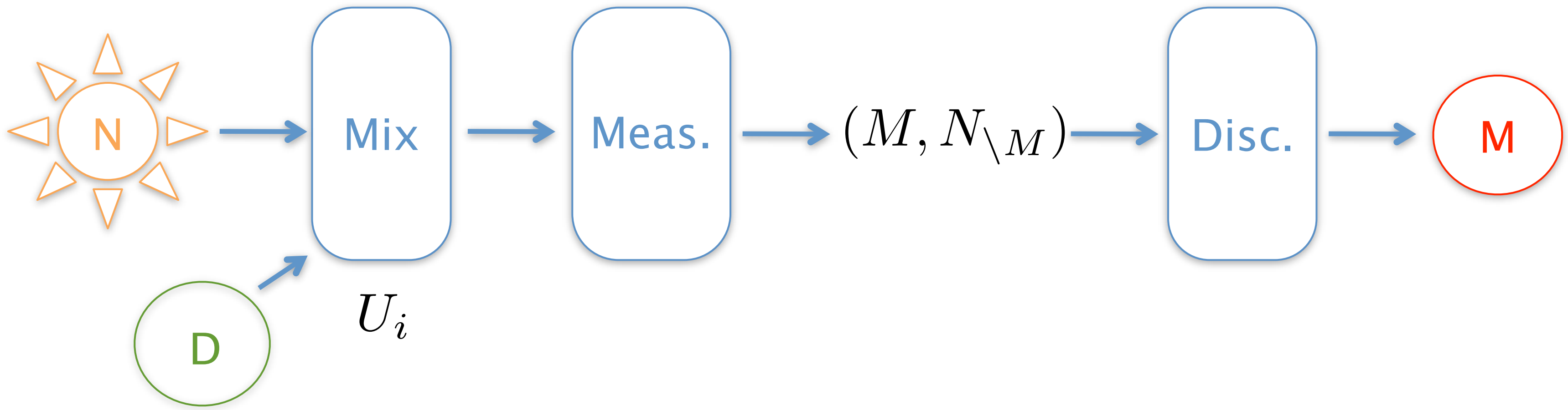
- Probabilistic construction (random unitaries).
  - Output size: $M = \min\{N, N \cdot 2^k \cdot \epsilon^4\}$
  - Seed size: $D = M \cdot \log N \cdot \varepsilon^{-4}$

Quantum to Classical (QC)-Randomness Extractors - Parameters



- Probabilistic construction (random unitaries).
  - Output size: $M = \min\{N, N \cdot 2^k \cdot \epsilon^4\}$
  - Seed size: $D = M \cdot \log N \cdot \varepsilon^{-4}$
- Converse bounds.

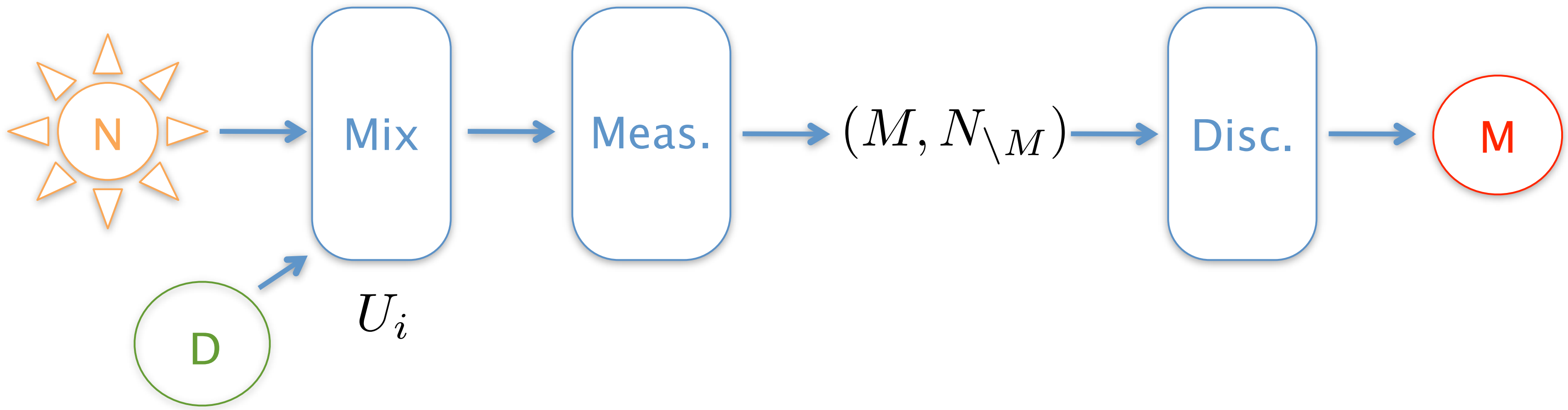
Quantum to Classical (QC)-Randomness Extractors - Parameters



- Probabilistic construction (random unitaries).
  - Output size: $M = \min\{N, N \cdot 2^k \cdot \epsilon^4\}$
  - Seed size: $D = M \cdot \log N \cdot \varepsilon^{-4}$
- Converse bounds.
  - Output size: $M \leq N \cdot 2^{k_\varepsilon}$, where $2^{k_\varepsilon} = H_{\min}^{\varepsilon}(N|E)_\rho = \max_{\bar{\rho} \in \mathcal{B}_\varepsilon(\rho)} H_{\min}(N|E)_{\bar{\rho}}$ (smooth entropies [5,11]).
  - Seed size: $D \geq \varepsilon^{-1}$

[5] Renner, PhD Thesis, ETHZ, 2005
[11] Tomamichel, PhD Thesis ETHZ, 2012

Quantum to Classical (QC)-Randomness Extractors - Parameters

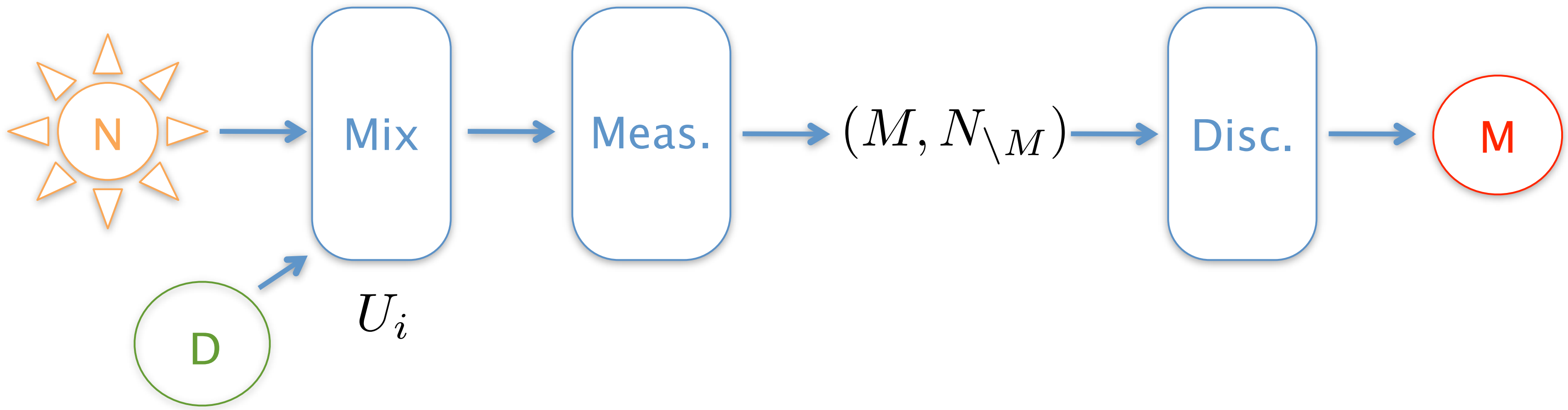


- Probabilistic construction (random unitaries).
  - Output size: $M = \min\{N, N \cdot 2^k \cdot \epsilon^4\}$
  - Seed size: $D = M \cdot \log N \cdot \varepsilon^{-4}$
- Converse bounds.
  - Output size: $M \leq N \cdot 2^{k_\varepsilon}$, where $2^{k_\varepsilon} = H_{\min}^{\varepsilon}(N|E)_\rho = \max_{\bar{\rho} \in \mathcal{B}_\varepsilon(\rho)} H_{\min}(N|E)_{\bar{\rho}}$ (smooth entropies [5,11]).
  - Seed size: $D \geq \varepsilon^{-1}$

Huge gap! We know that our proof technique can only yield $D \geq \varepsilon^{-2} \cdot \min\{N \cdot 2^{-k-1}, M/4\}$ [12].

[5] Renner, PhD Thesis, ETHZ, 2005
[11] Tomamichel, PhD Thesis ETHZ, 2012
[12] Fawzi, PhD Thesis, McGill, 2012

Quantum to Classical (QC)-Randomness Extractors - Parameters



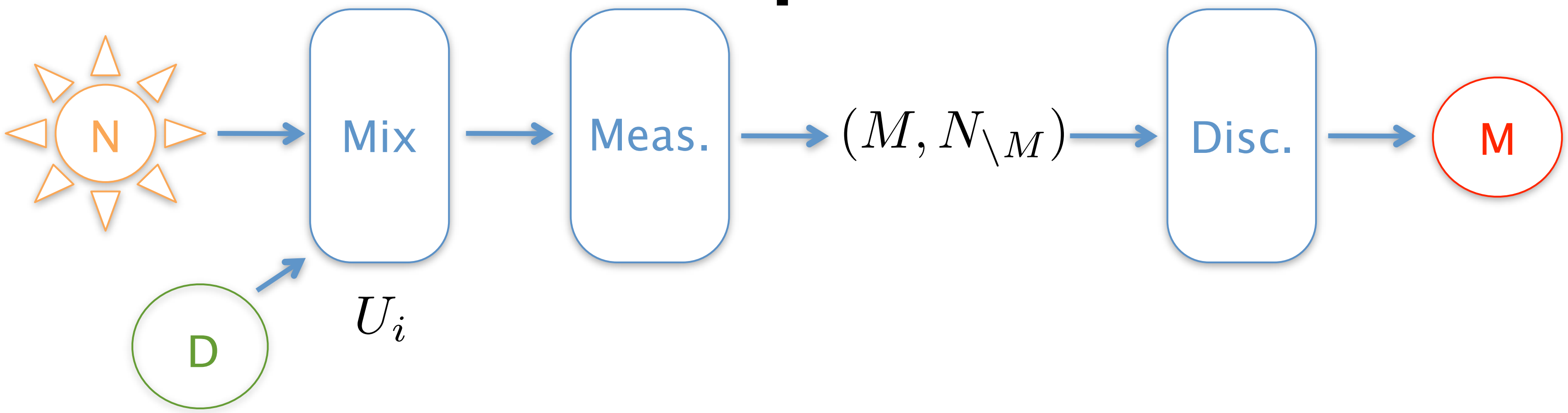
- Probabilistic construction (random unitaries).
  - Output size: $M = \min\{N, N \cdot 2^k \cdot \epsilon^4\}$
  - Seed size: $D = M \cdot \log N \cdot \varepsilon^{-4}$
- Converse bounds.
  - Output size: $M \leq N \cdot 2^{k_\varepsilon}$, where $2^{k_\varepsilon} = H_{\min}^{\varepsilon}(N|E)_\rho = \max_{\bar{\rho} \in \mathcal{B}_\varepsilon(\rho)} H_{\min}(N|E)_{\bar{\rho}}$ (smooth entropies [5,11]).
  - Seed size: $D \geq \varepsilon^{-1}$

Huge gap! We know that our proof technique can only yield $D \geq \varepsilon^{-2} \cdot \min\{N \cdot 2^{-k-1}, M/4\}$ [12].

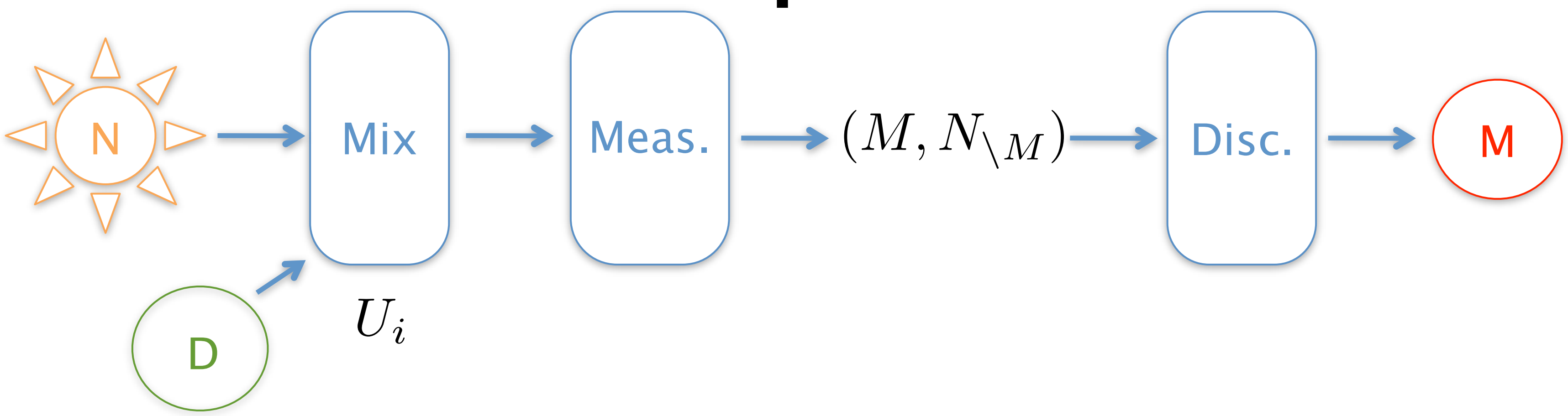
- Find explicit constructions!

[5] Renner, PhD Thesis, ETHZ, 2005
[11] Tomamichel, PhD Thesis ETHZ, 2012
[12] Fawzi, PhD Thesis, McGill, 2012

Quantum to Classical (QC)-Randomness Extractors - Explicit Constructions



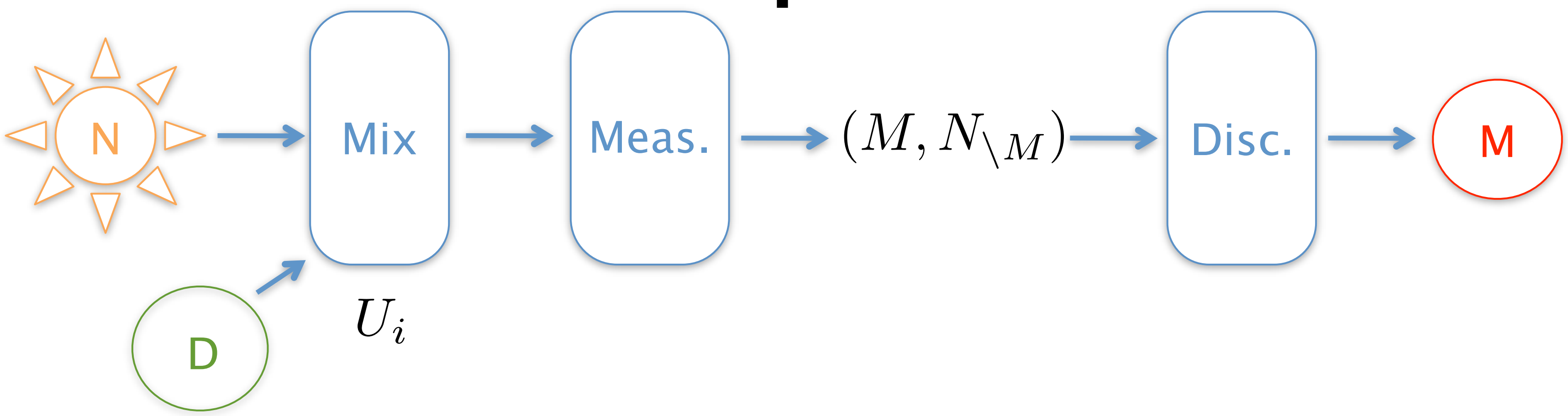
Quantum to Classical (QC)-Randomness Extractors - Explicit Constructions



- (Almost) unitary two-designs reproduce second moment of random unitaries [8,13]: $M = \min\{N, N \cdot 2^k \cdot \epsilon^2\}$ $\quad D = O(N^4)$

[8] Dupuis, PhD Thesis, McGill, 2009
[13] Szehr et al., arXiv:1109.4348v1

Quantum to Classical (QC)-Randomness Extractors - Explicit Constructions



- (Almost) unitary two-designs reproduce second moment of random unitaries [8,13]:

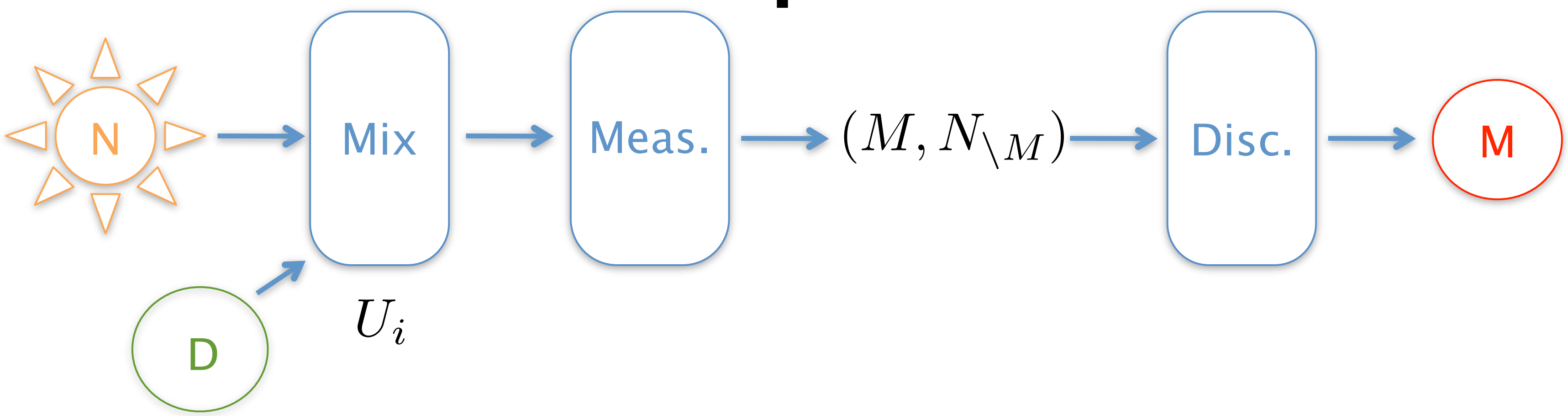
$$M = \min\{N, N \cdot 2^k \cdot \epsilon^2\} \qquad D = O(N^4)$$

- Set of unitaries defined by a full set of mutually unbiased bases together with two-wise independent permutations:

$$M = \min\{N, N \cdot 2^k \cdot \epsilon^2\} \qquad D = N \cdot (N+1)^2$$

[8] Dupuis, PhD Thesis, McGill, 2009
[13] Szehr et al., arXiv:1109.4348v1

Quantum to Classical (QC)-Randomness Extractors - Explicit Constructions



- (Almost) unitary two-designs reproduce second moment of random unitaries [8,13]: $M = \min\{N, N \cdot 2^k \cdot \epsilon^2\}$ $D = O(N^4)$
- Set of unitaries defined by a full set of mutually unbiased bases together with two-wise independent permutations:

$$M = \min\{N, N \cdot 2^k \cdot \epsilon^2\} \qquad D = N \cdot (N+1)^2$$

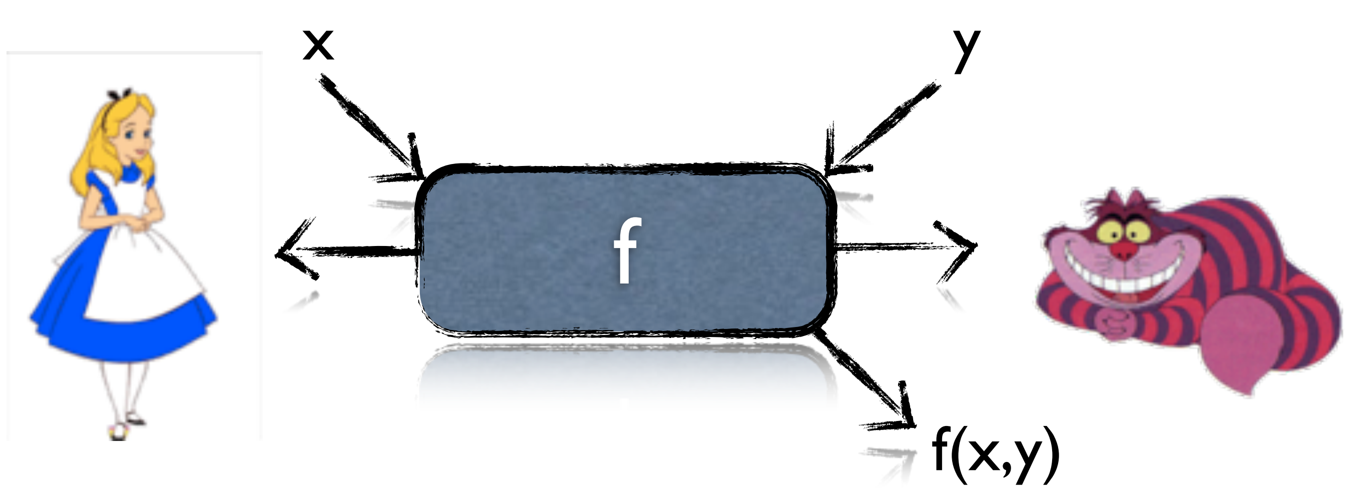
- Bitwise qc-extractors! Let $N = 2^n$, $M = 2^m$. Set of unitaries defined by a full set of mutually unbiased bases for each qubit, $\{\sigma_X, \sigma_Y, \sigma_Z\}^{\otimes n}$, together with two-wise independent permutations:

$$M = O(N^{\log 3 - 1} \cdot \varepsilon^4) \cdot \min\{1, 2^k\} \qquad D = N \cdot (N-1) \cdot 3^{\log N}$$

[8] Dupuis, PhD Thesis, McGill, 2009
[13] Szehr et al., arXiv:1109.4348v1

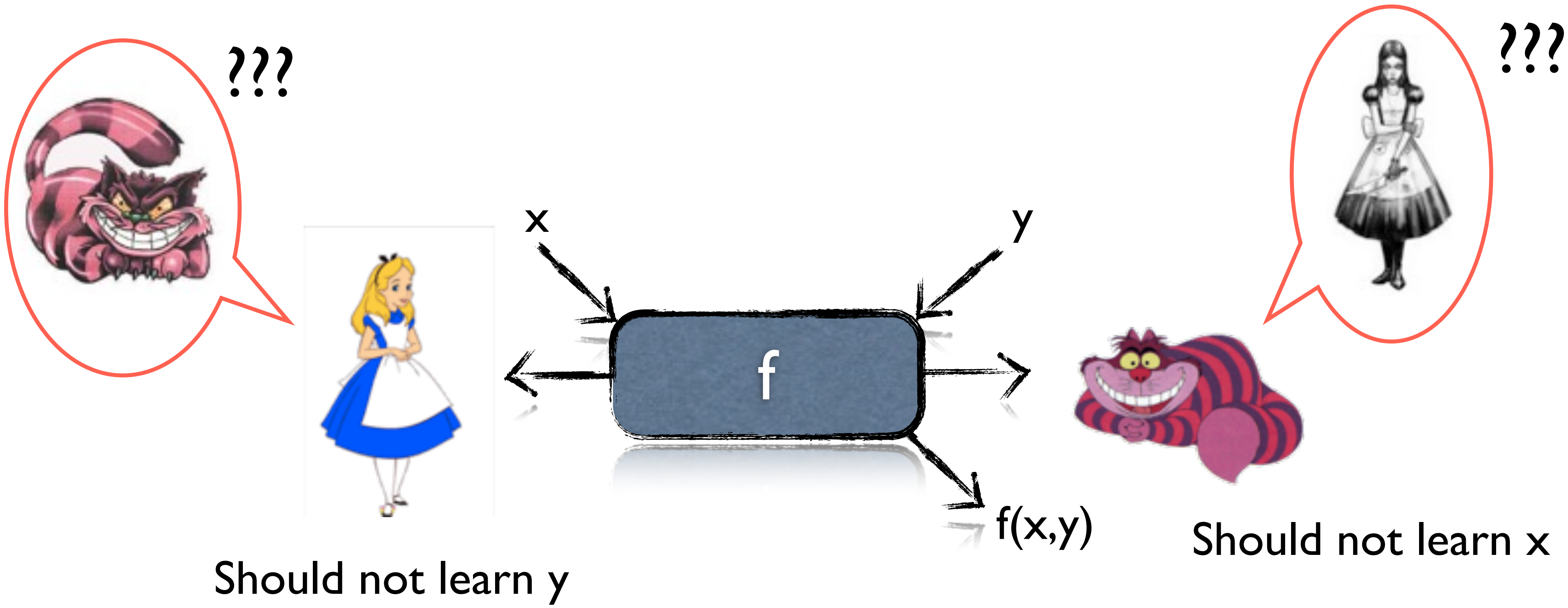
Application: Two-Party Cryptography

- Example: secure function evaluation.



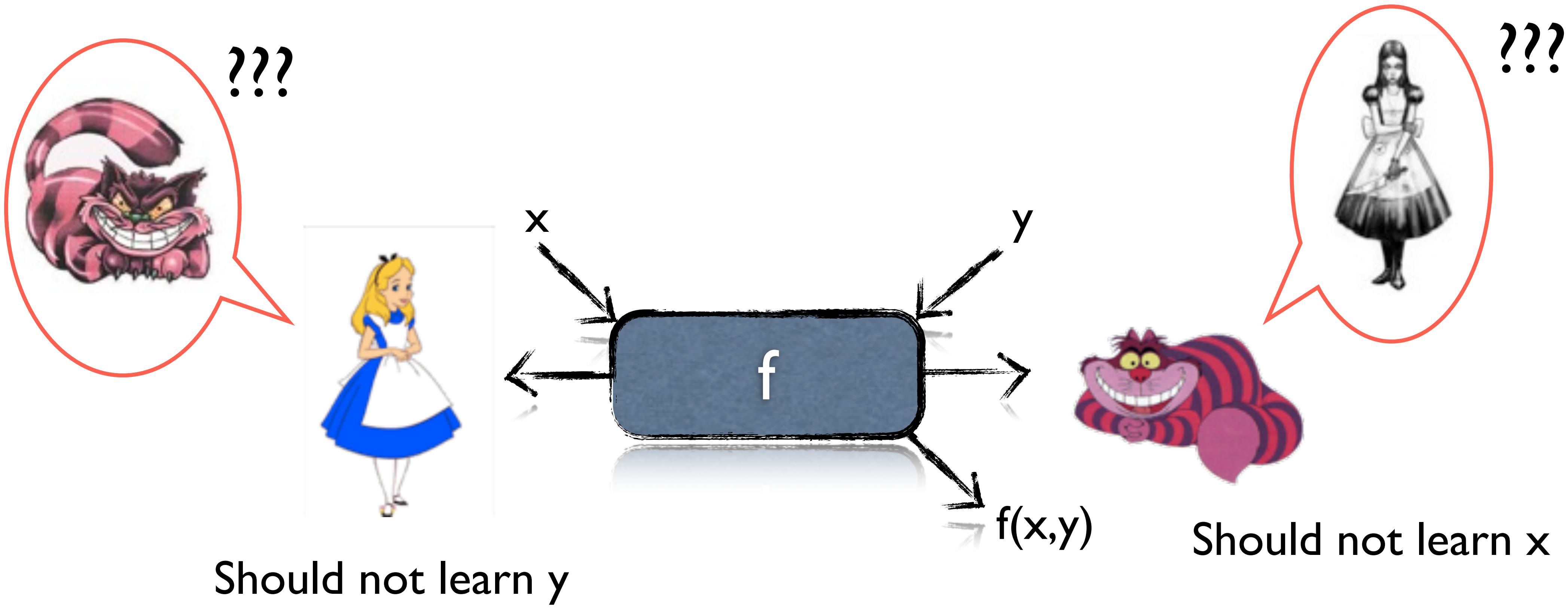
Application: Two-Party Cryptography

- Example: secure function evaluation.



Application: Two-Party Cryptography

- Example: secure function evaluation.

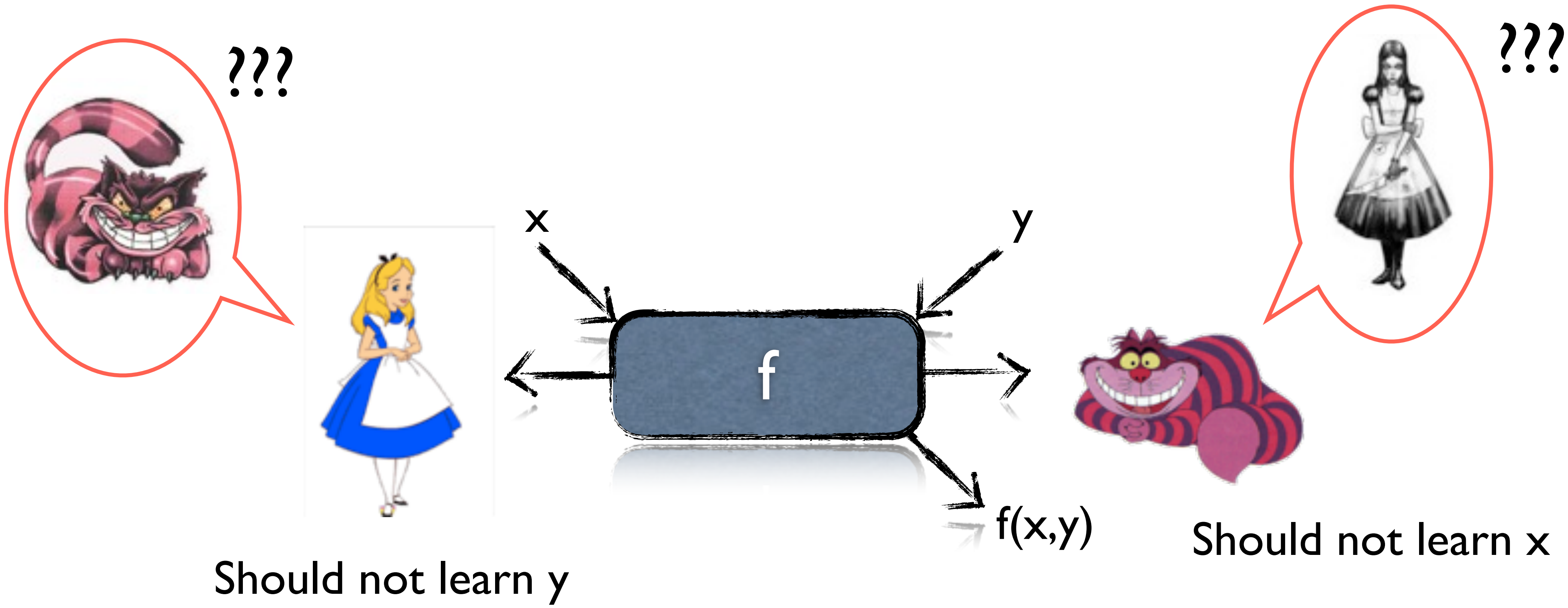


  - Not possible to solve without assumptions [17].

[17] Lo, PRA 56:1154, 1997

Application: Two-Party Cryptography

- Example: <u>secure function evaluation</u>.

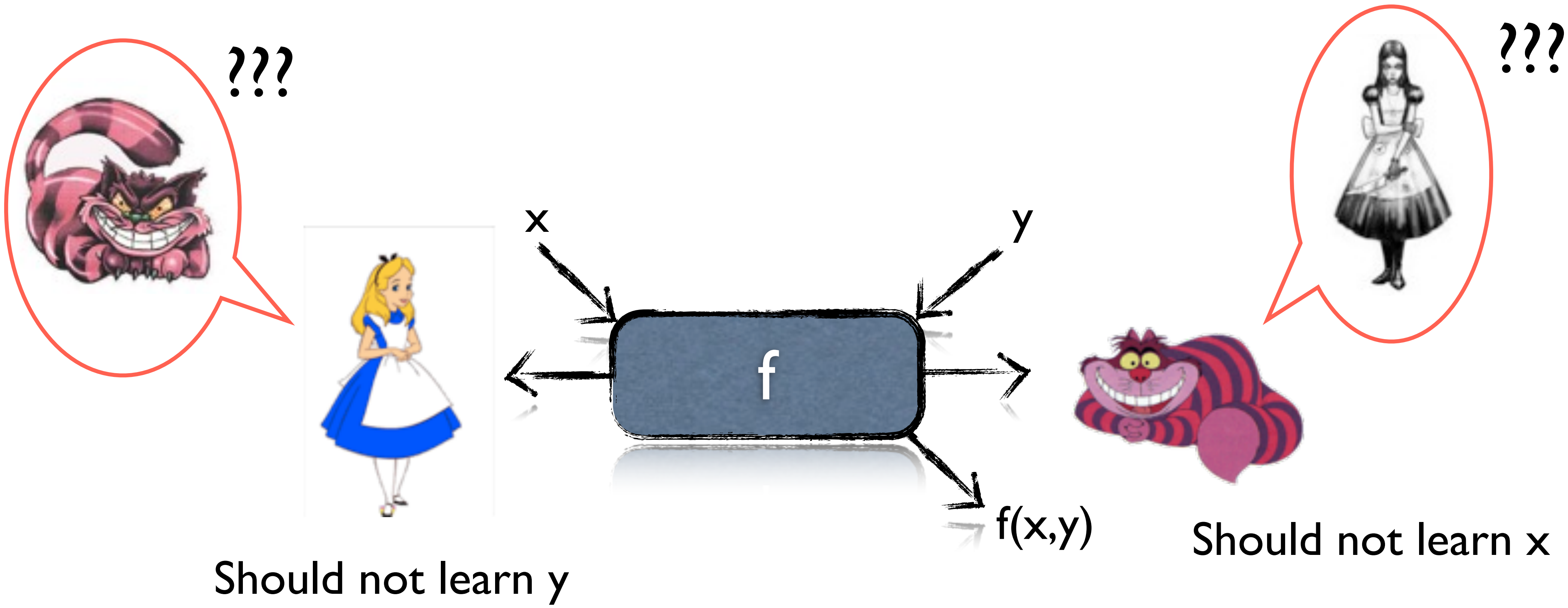


  - Not possible to solve without assumptions [17].
  - Classical assumptions are typically computational assumptions (e.g. factoring is hard).

[17] Lo, PRA 56:1154, 1997

Application: Two-Party Cryptography

- Example: secure function evaluation.



  - Not possible to solve without assumptions [17].
  - Classical assumptions are typically computational assumptions (e.g. factoring is hard).
  - Physical assumption: bounded quantum storage [18], secure function evaluation becomes possible [19].

[17] Lo, PRA 56:1154, 1997
[18] Damgård et al., CRYPTO, 2007
[19] König et al., IEEE TIT 58:1962, 2012

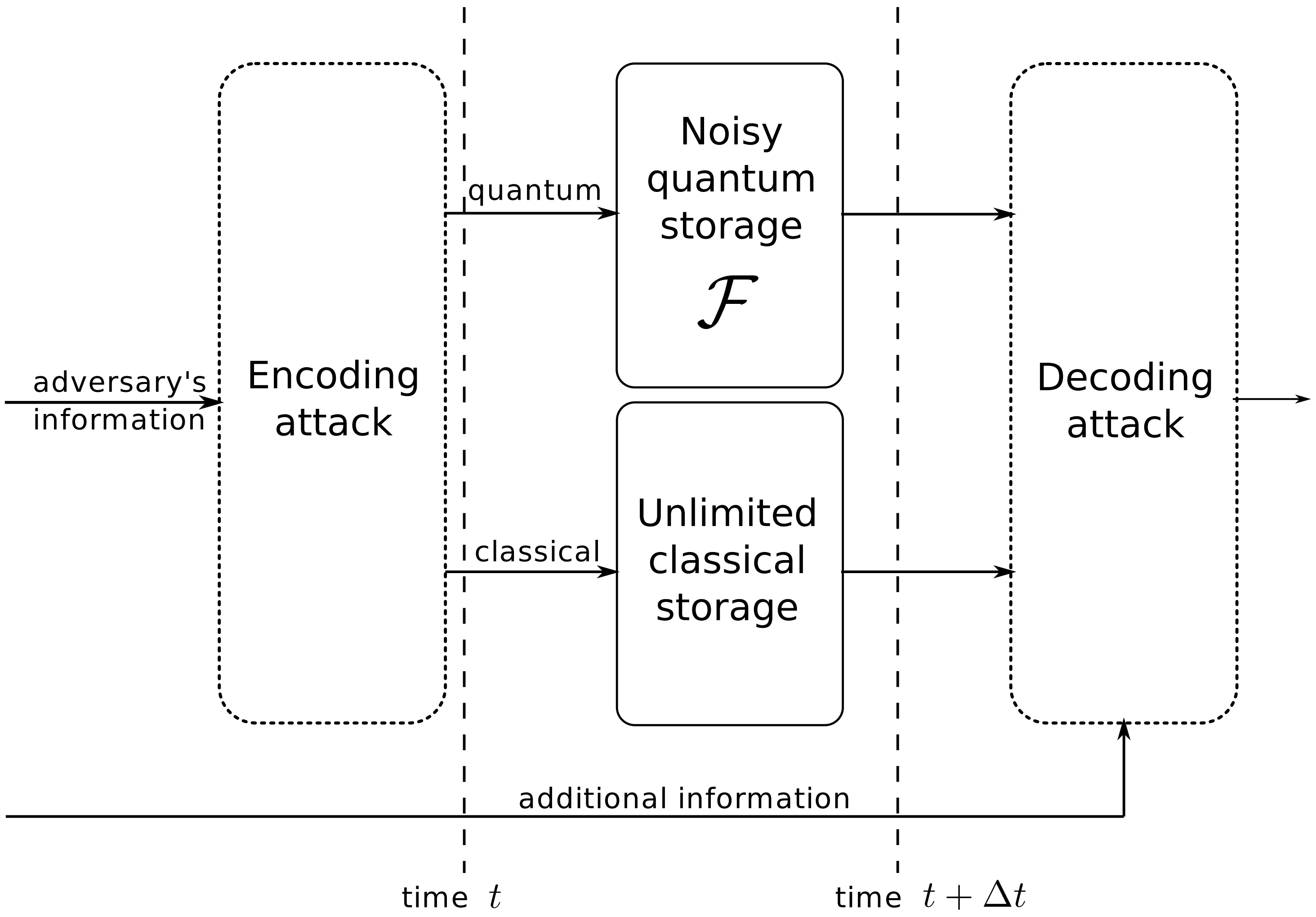
Application: Security in the Noisy-Storage Model [20]

- What the adversary can do: computationally all powerful, unlimited classical storage, actions are instantaneous, **BUT** noisy (bounded) quantum storage.

[20] Wehner et al., PRL 100:220502, 2008

Application: Security in the Noisy-Storage Model [20]

- What the adversary can do: computationally all powerful, unlimited classical storage, actions are instantaneous, **BUT** noisy (bounded) quantum storage.

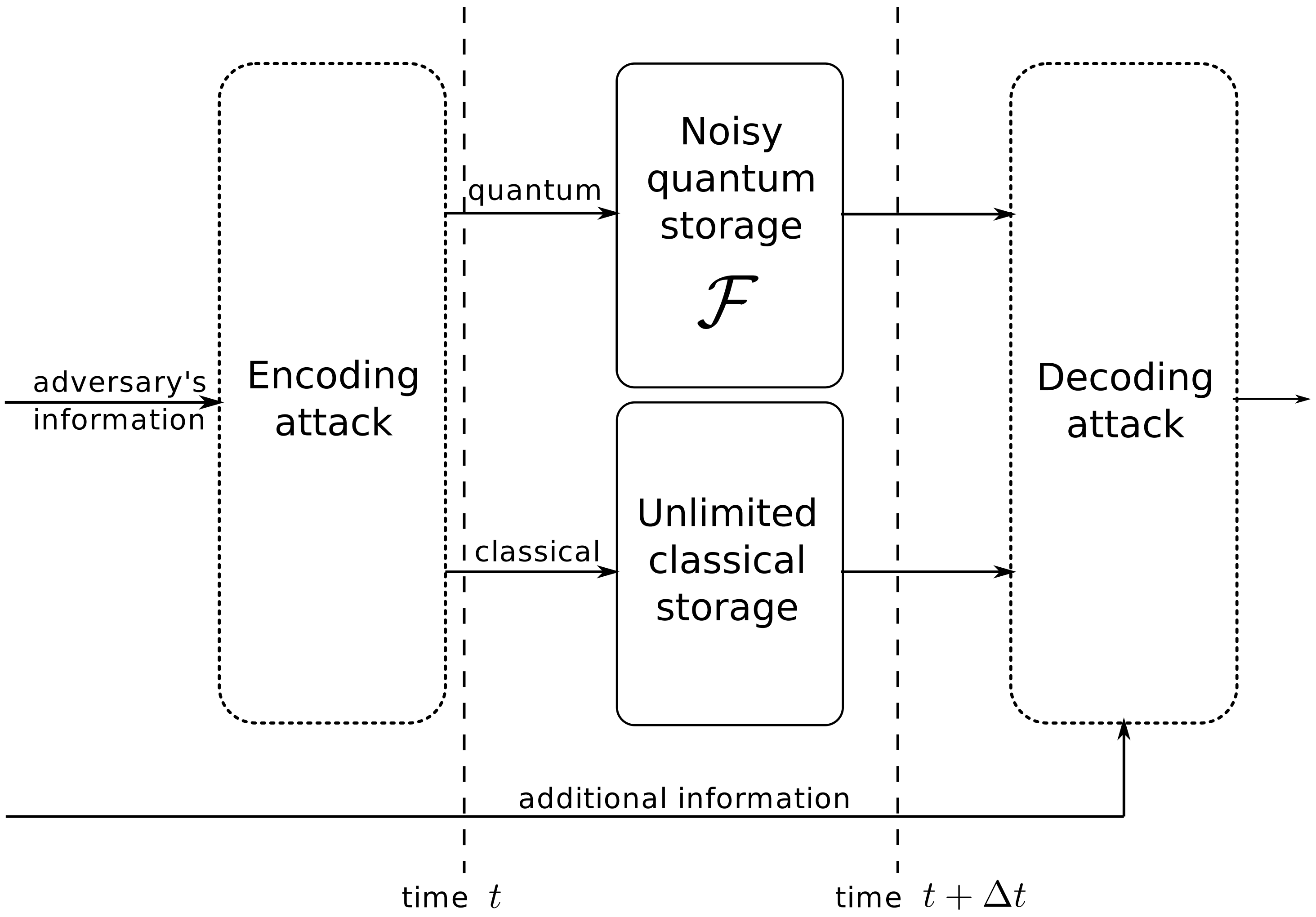


[20] Wehner et al., PRL 100:220502, 2008

Application: Security in the Noisy-Storage Model [20]

- What the adversary can do: computationally all powerful, unlimited classical storage, actions are instantaneous, **BUT** noisy (bounded) quantum storage.

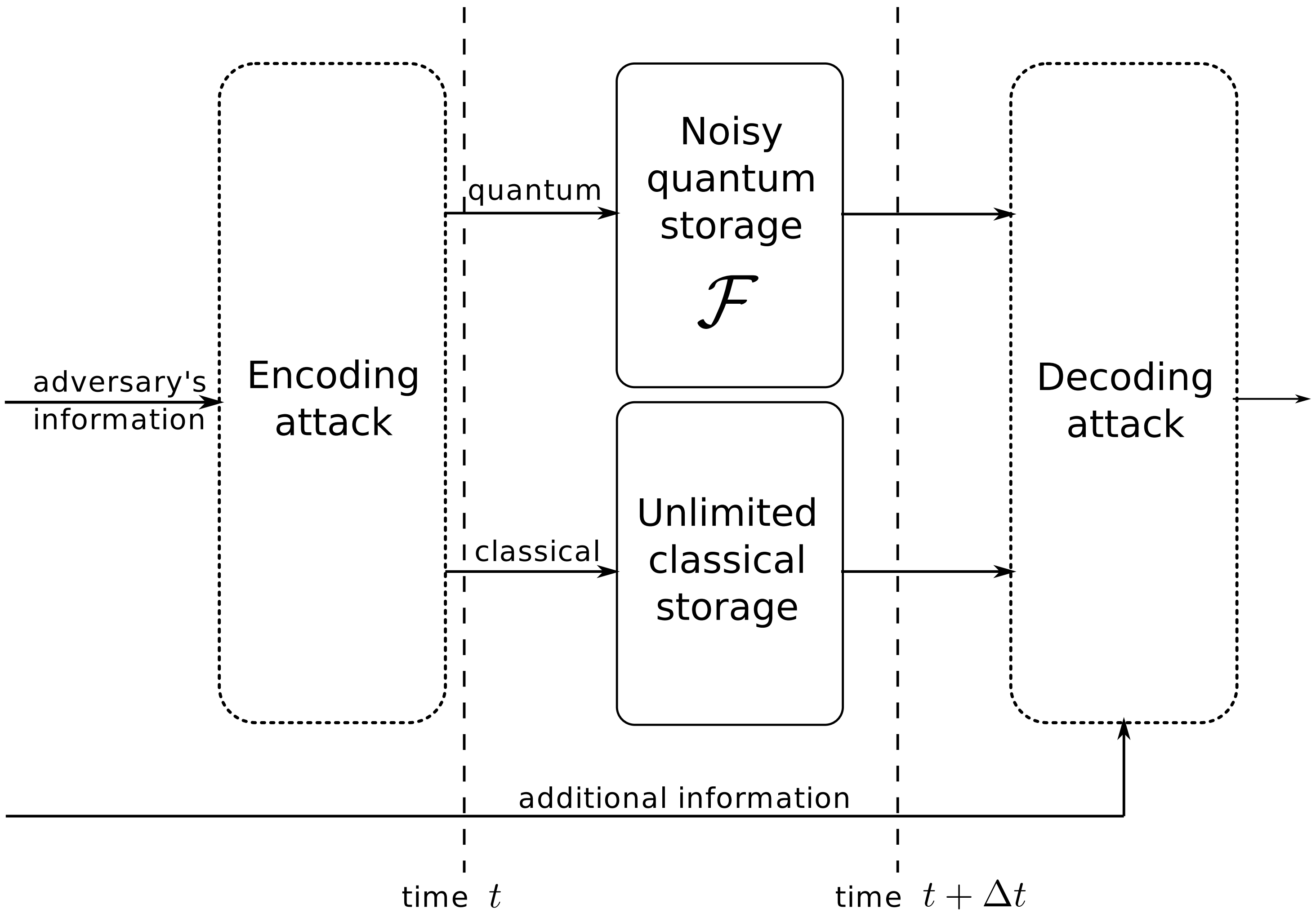
- Basic idea: protocol will have have waiting times, in which noisy storage must be used!



[20] Wehner et al., PRL 100:220502, 2008

Application: Security in the Noisy-Storage Model [20]

- What the adversary can do: computationally all powerful, unlimited classical storage, actions are instantaneous, **BUT** noisy (bounded) quantum storage.



- Basic idea: protocol will have have waiting times, in which noisy storage must be used!

- Implement task 'weak string erasure' (sufficient [21]). Using bitwise qc-randomness extractors, we can link security to the entanglement fidelity (quantum capacity) of the noisy quantum storage (improves [19,22])!

[20] Wehner et al., PRL 100:220502, 2008
[21] Kilian, STOC, 1998
[19] König et al., IEEE TIT 58:1962, 2012
[22] B. et al., IEEE ISIT, 2012

Entropic Uncertainty Relations with Quantum Side Information

- Review article [14]. Given a quantum state ρ and a set of measurements$\{K_1, \ldots, K_D\}$ these relations usually take the form (where $H(.)$ denotes e.g. the Shannon entropy):

$$H(K|D) = \frac{1}{D}\sum_{i=1}^{D} H(K_i|D = i) \geq \mathrm{const}(K)\,.$$

[14] Wehner and Winter., NJP 12:025009, 2010

Entropic Uncertainty Relations with Quantum Side Information

- Review article [14]. Given a quantum state ρ and a set of measurements $\{K_1, \ldots, K_D\}$ these relations usually take the form (where $H(.)$ denotes e.g. the Shannon entropy):

$$H(K|D) = \frac{1}{D}\sum_{i=1}^{D} H(K_i|D=i) \geq \mathrm{const}(K)\,.$$

- Idea of [15]: add quantum side information! Start with a bipartite quantum state ρ_{AE} and a set of measurements $\{K_1, \ldots, K_D\}$ on A:

$$\boxed{H(K|ED) = \frac{1}{D}\sum_{i=1}^{D} H(K_i|ED=i) \geq \mathrm{const}(K) + H(A|E)\,,}$$

here $H(A)_\rho = -\mathrm{tr}[\rho_A \log \rho_A]$, the von Neumann entropy, and its conditional version $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$ (which can get negative for entangled input states!).

[14] Wehner and Winter., NJP 12:025009, 2010
[15] B. et al., NP 6:659, 2010

Entropic Uncertainty Relations with Quantum Side Information

- Review article [14]. Given a quantum state ρ and a set of measurements $\{K_1, \ldots, K_D\}$ these relations usually take the form (where $H(.)$ denotes e.g. the Shannon entropy):

$$H(K|D) = \frac{1}{D}\sum_{i=1}^{D} H(K_i|D=i) \geq \mathrm{const}(K)\,.$$

- Idea of [15]: add quantum side information! Start with a bipartite quantum state ρ_{AE} and a set of measurements $\{K_1, \ldots, K_D\}$ on A:

$$\boxed{H(K|ED) = \frac{1}{D}\sum_{i=1}^{D} H(K_i|ED=i) \geq \mathrm{const}(K) + H(A|E)\,,}$$

here $H(A)_\rho = -\mathrm{tr}[\rho_A \log \rho_A]$, the von Neumann entropy, and its conditional version $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$ (which can get negative for entangled input states!).

- QC-extractors (against quantum side information) give entropic uncertainty relations with quantum side information!
- Entropic uncertainty relations with quantum side information together with cc-extractors give qc-extractors (against quantum side information) [16]!

[14] Wehner and Winter., NJP 12:025009, 2010 [16] B./Wehner/Coles, unpublished
[15] B. et al., NP 6:659, 2010

Conclusions / Open Problems

- Definition of quantum to classical (qc)-randomness extractors.
- Probabilistic and explicit constructions as well as converse bounds.
- Security in the noisy-storage model linked to the quantum capacity.
- Close relation to entropic uncertainty relations with quantum side information.

Conclusions / Open Problems

- Definition of quantum to classical (qc)-randomness extractors.
- Probabilistic and explicit constructions as well as converse bounds.
- Security in the noisy-storage model linked to the quantum capacity.
- Close relation to entropic uncertainty relations with quantum side information.

- Relation between qq-, qc-, and cc-extractors?

Conclusions / Open Problems

- Definition of quantum to classical (qc)-randomness extractors.
- Probabilistic and explicit constructions as well as converse bounds.
- Security in the noisy-storage model linked to the quantum capacity.
- Close relation to entropic uncertainty relations with quantum side information.

- Relation between qq-, qc-, and cc-extractors?
- Seed length: $\varepsilon^{-1} \leq D \leq M \cdot \log N \cdot \varepsilon^{-4}$. We believe that at least $D = \mathrm{polylog}(N)$ might be possible (cf. cc-extractors against quantum side information [23]). However, our proof technique can only yield $D \geq \varepsilon^{-2} \cdot \min\{N \cdot 2^{-k-1}, M/4\}$ [12].

[23] Ve et al., arXiv:0912.5514v3
[12] Fawzi, PhD Thesis, McGill, 2012

Conclusions / Open Problems

- Definition of quantum to classical (qc)-randomness extractors.
- Probabilistic and explicit constructions as well as converse bounds.
- Security in the noisy-storage model linked to the quantum capacity.
- Close relation to entropic uncertainty relations with quantum side information.

- Relation between qq-, qc-, and cc-extractors?
- Seed length: $\varepsilon^{-1} \leq D \leq M \cdot \log N \cdot \varepsilon^{-4}$. We believe that at least $D = \mathrm{polylog}(N)$ might be possible (cf. cc-extractors against quantum side information [23]). However, our proof technique can only yield $D \geq \varepsilon^{-2} \cdot \min\{N \cdot 2^{-k-1}, M/4\}$ [12].
- Bitwise qc-randomness extractor for $\{\sigma_X, \sigma_Z\}^{\otimes n}$ (BB84) encoding? Improve bound for $\{\sigma_X, \sigma_Y, \sigma_Z\}^{\otimes n}$ (six-state) encoding for large n?

[23] Ve et al., arXiv:0912.5514v3
[12] Fawzi, PhD Thesis, McGill, 2012