Physical Randomness Extractors

Yaoyun Shi
University of Michigan
joint works with Carl Miller (arXiv:1402.0489), Kai-Min Chung and Xiaodi Wu (arXiv:arXiv:1402.4797)

Carl Miller

Kai-Min Chung

Xiaodi Wu

1. Motivation

1. Motivation

- What's randomness?

1. Motivation

- What's randomness?
- Why is it difficult to get randomness?

1. Motivation

- What's randomness?
- Why is it difficult to get randomness?
- Why quantum and untrusted quantum devices?

Randomness = Secret

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: $XE = U_X \otimes E$, i.e. uniform on X and uncorrelated with E

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: $XE = U_X \otimes E$, i.e. uniform on X and uncorrelated with E
- (n, k)-source: best guessing probability of X using $E \leq 2^{-k}$

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: $XE = U_X \otimes E$, i.e. uniform on X and uncorrelated with E
- (n, k)-source: best guessing probability of X using E ≤ 2^{-k}
- k = n: uniform randomness

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: XE = $U_X \otimes E$, i.e. uniform on X and uncorrelated with E
- (n, k)-source: best guessing probability of X using E ≤ 2^{-k}
- k = n: uniform randomness
- k < n: weak randomness

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: XE = $U_X \otimes E$, i.e. uniform on X and uncorrelated with E
- (n, k)-source: best guessing probability of X using E ≤ 2^{-k}
  - k = n: uniform randomness
  - k < n: weak randomness
- Error parameter: deviation of XE from $U_X \otimes E$

Randomness = Secret

- A n-bit string X is random to a quantum system E if X cannot be perfectly guessed from E
- Uniform randomness: XE = $U_X \otimes E$, i.e. uniform on X and uncorrelated with E
- (n, k)-source: best guessing probability of X using E ≤ 2^{-k}
  - k = n: uniform randomness
  - k < n: weak randomness
- Error parameter: deviation of XE from $U_X \otimes E$
- True randomness: error → 0 (as other parameters grow)

We need randomness, a lot of it

We need randomness, a lot of it

- Randomness is critical

We need randomness, a lot of it

- Randomness is critical
  - Cryptography, privacy

We need randomness, a lot of it

- Randomness is critical
  - Cryptography, privacy
  - Fast randomized algorithms, e.g. physics simulation

We need randomness, a lot of it

- Randomness is critical
  - Cryptography, privacy
  - Fast randomized algorithms, e.g. physics simulation
  - Gambling, ...

We need randomness, a lot of it

- Randomness is critical
  - Cryptography, privacy
  - Fast randomized algorithms, e.g. physics simulation
  - Gambling, ...
- 1 T bits/day?

Central question

Central question

How do we get true randomness and know that we've got it?

We aren't always getting it: many security vulnerabilities

We aren't always getting it: many security vulnerabilities

- [Heninger+] broke ≧1% DSA keys downloaded

We aren't always getting it: many security vulnerabilities

- [Heninger+] broke ≥ 1% DSA keys downloaded
  - Share factors with another key

We aren't always getting it: many security vulnerabilities

- [Heninger+] broke ≧1% DSA keys downloaded
  - Share factors with another key
  - Not enough entropy to start with

We aren't always getting it: many security vulnerabilities

- [Heninger+] broke ≧1% DSA keys downloaded
    - Share factors with another key
    - Not enough entropy to start with
- Snowden: Hardware and software backdoors for RNGs

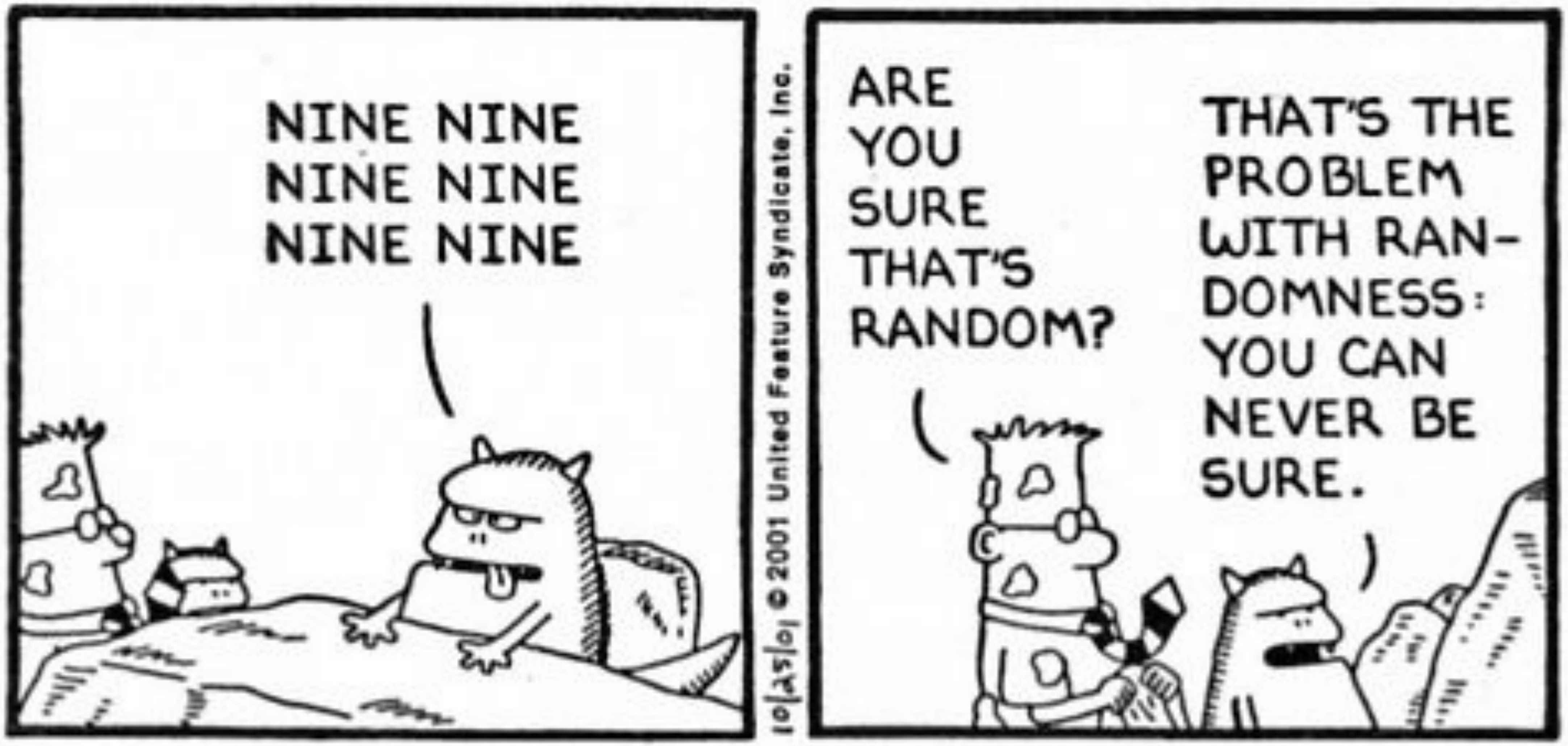
We aren't always getting it: many security vulnerabilities

- [Heninger+] broke ≧1% DSA keys downloaded
  - Share factors with another key
  - Not enough entropy to start with
- Snowden: Hardware and software backdoors for RNGs

"Ultimately the results of our study should serve as a wake-up call that secure random number generation continues to be an unsolved problem in important areas of practice."

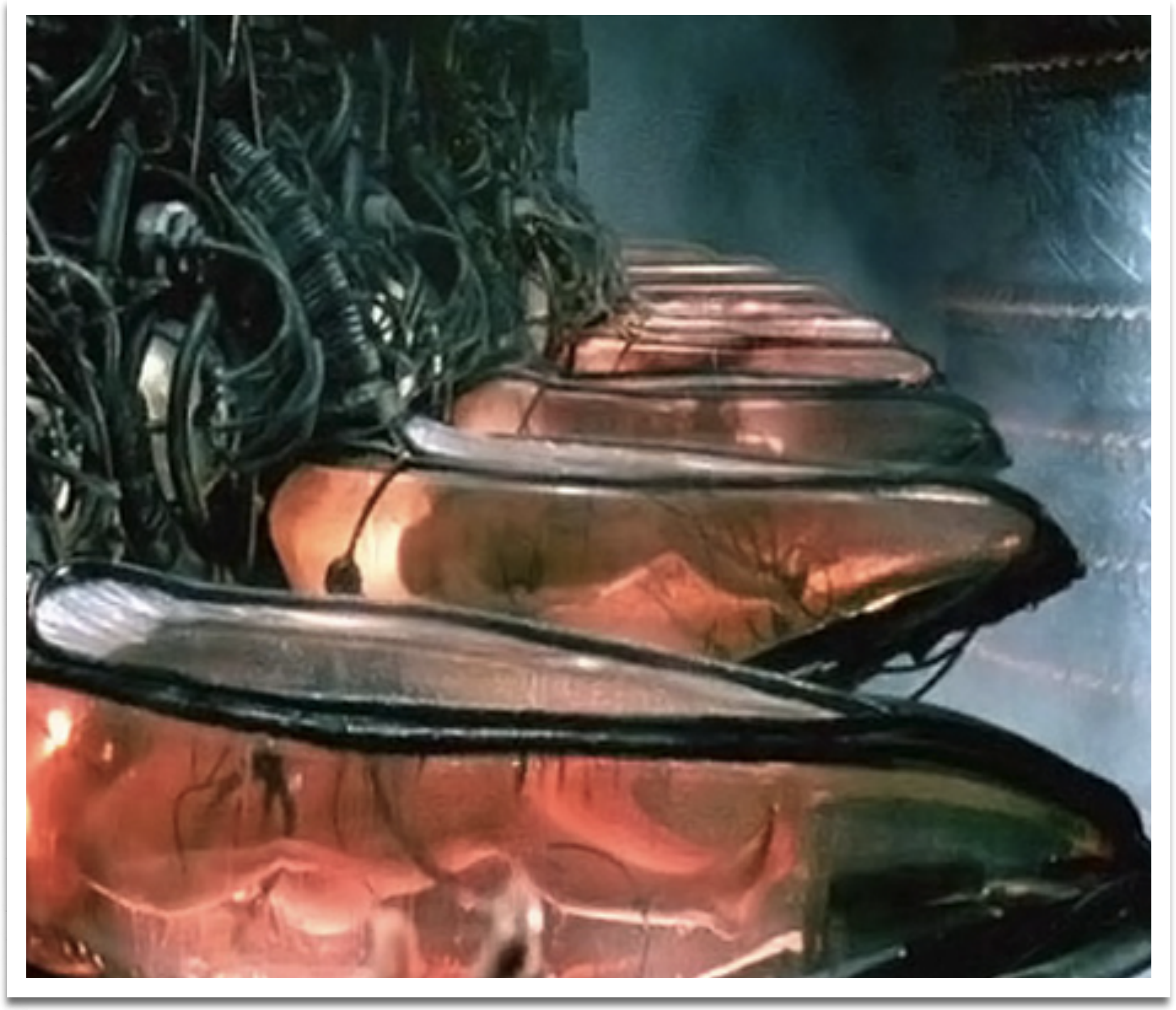
[Heninger+]

How can we be sure it's random?

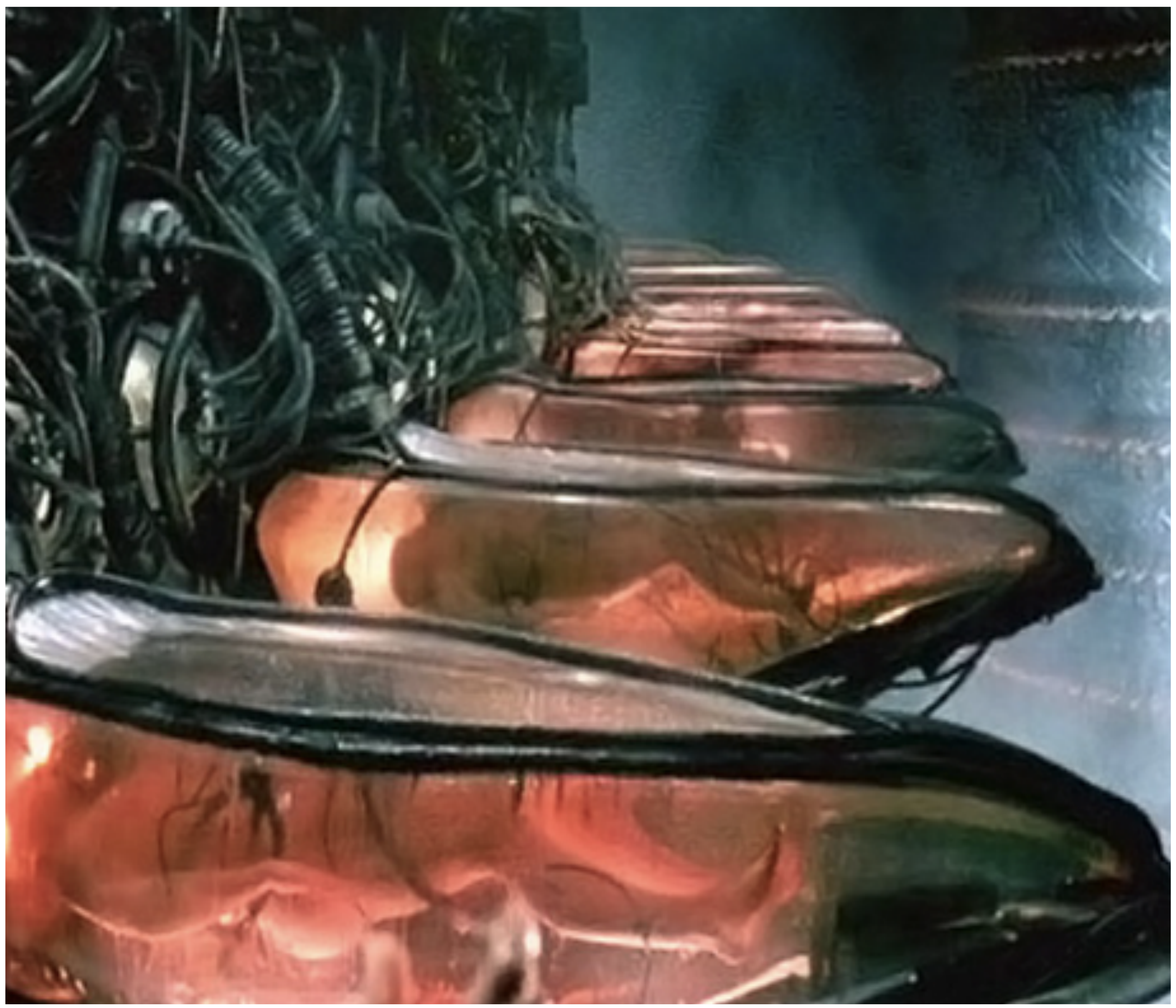


Motivation::randomness extractors

Also a deep physics question

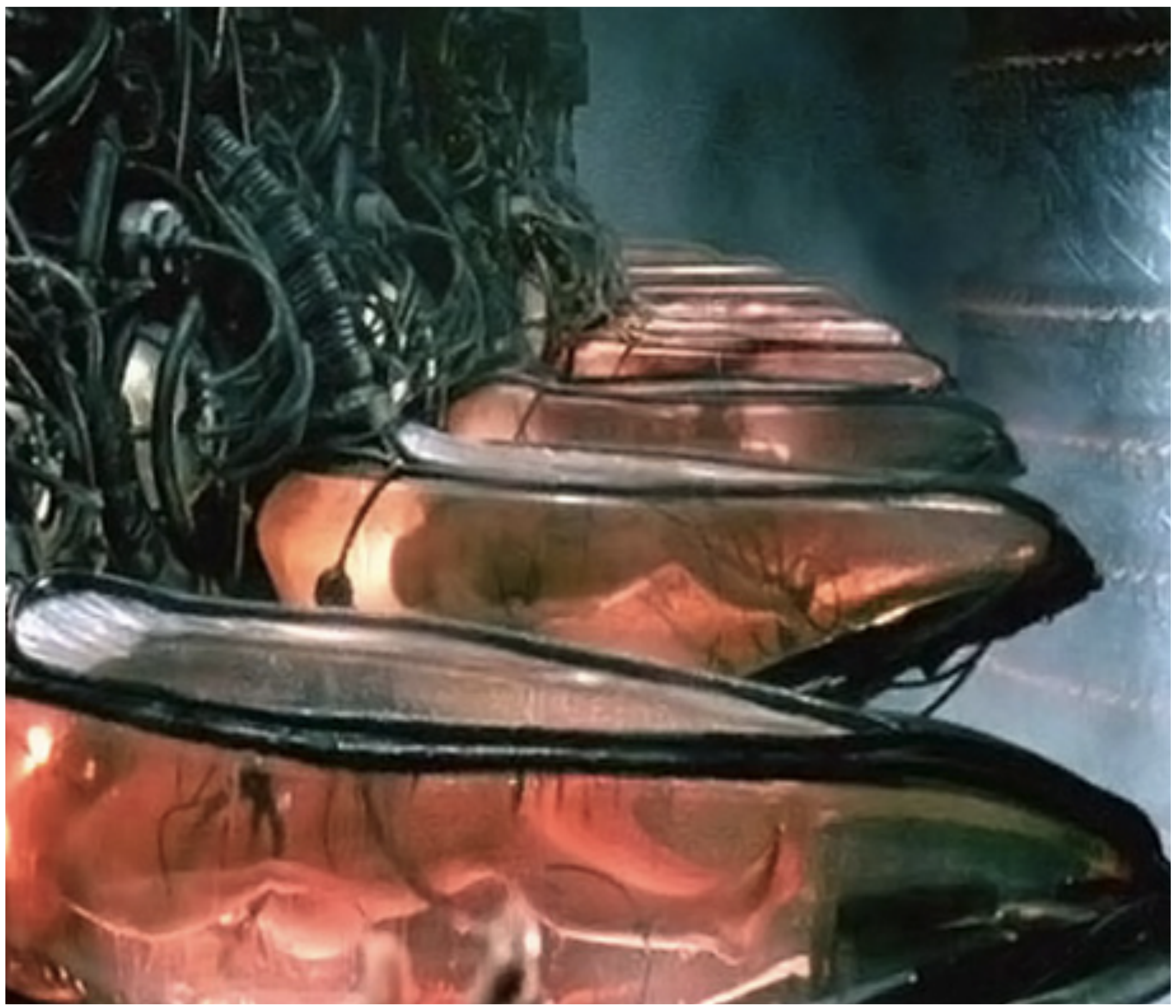


Also a deep physics question



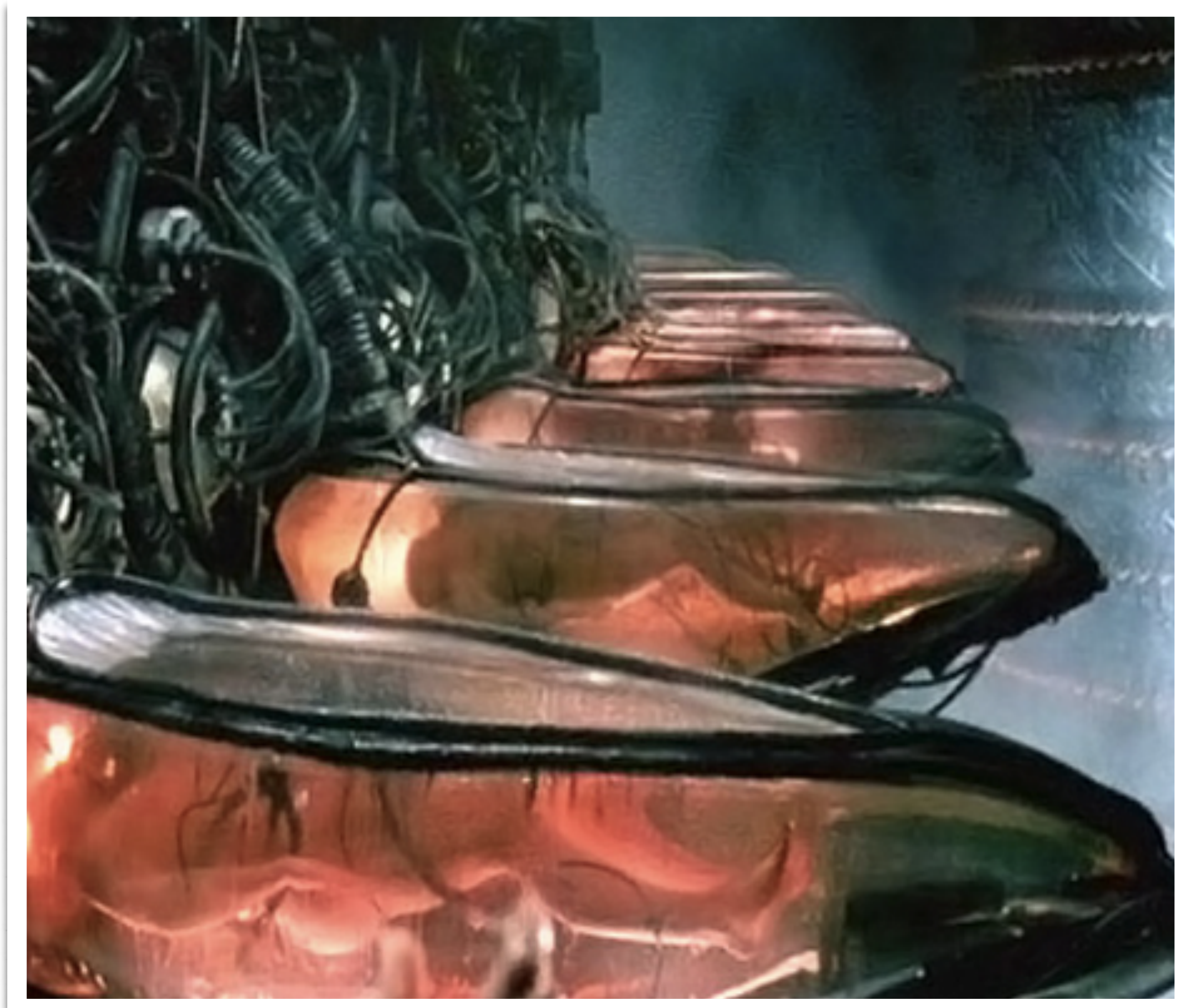
- Does randomness exist at all?

Also a deep physics question



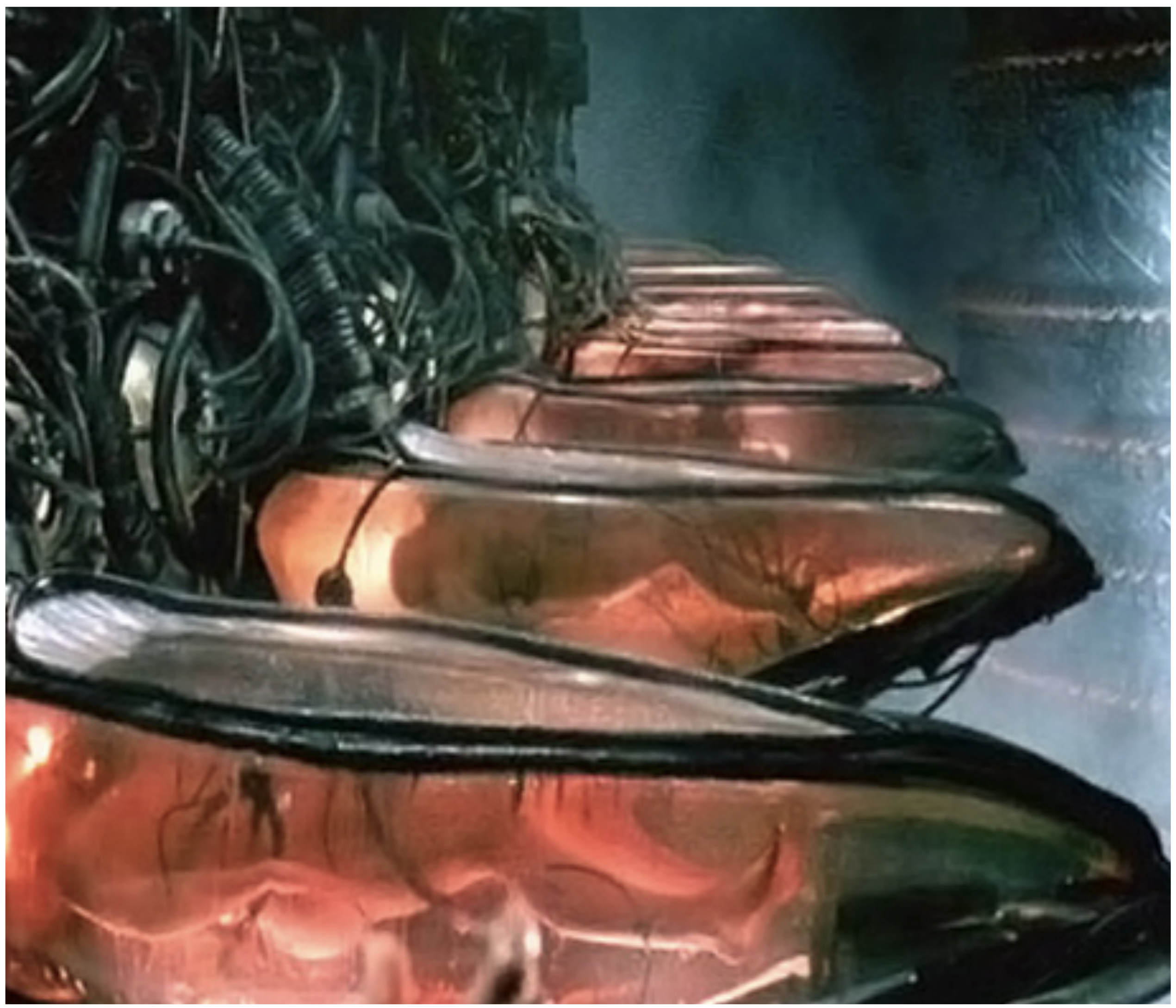
- Does randomness exist at all?
  - We can't possibly know

Also a deep physics question



- Does randomness exist at all?
  - We can't possibly know
- Assuming the world is not deterministic,
  Could there be almost perfect randomness?

Also a deep physics question



- Does randomness exist at all?
    - We can't possibly know
- Assuming the world is not deterministic,
  Could there be almost perfect randomness?
- Or, are we stuck with weak randomness?

Randomness extractors: classical theory

Randomness extractors: classical theory

- Model weak source by min-entropy

Randomness extractors: classical theory

- Model weak source by min-entropy
- Turn weak sources to true randomness

Randomness extractors: classical theory

- Model weak source by min-entropy
- Turn weak sources to true randomness
  - Ensure randomness whenever assumptions are met

Randomness extractors: classical theory

- Model weak source by min-entropy
- Turn weak sources to true randomness
  - Ensure randomness whenever assumptions are met
  - Excellent constructions for seeded extraction (i.e. one source is uniform)

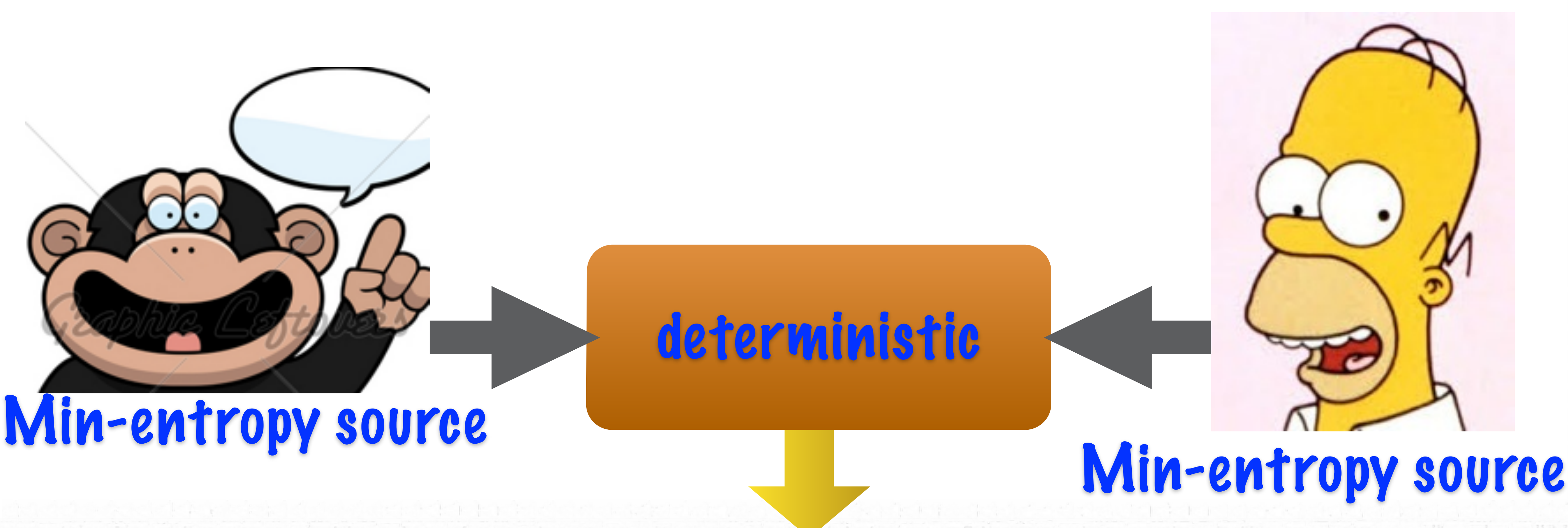
Limitation: two independent sources required

Limitation: two independent sources required

- Deterministic extraction, i.e. single source extraction, is impossible [Santha-Vazirani'86]

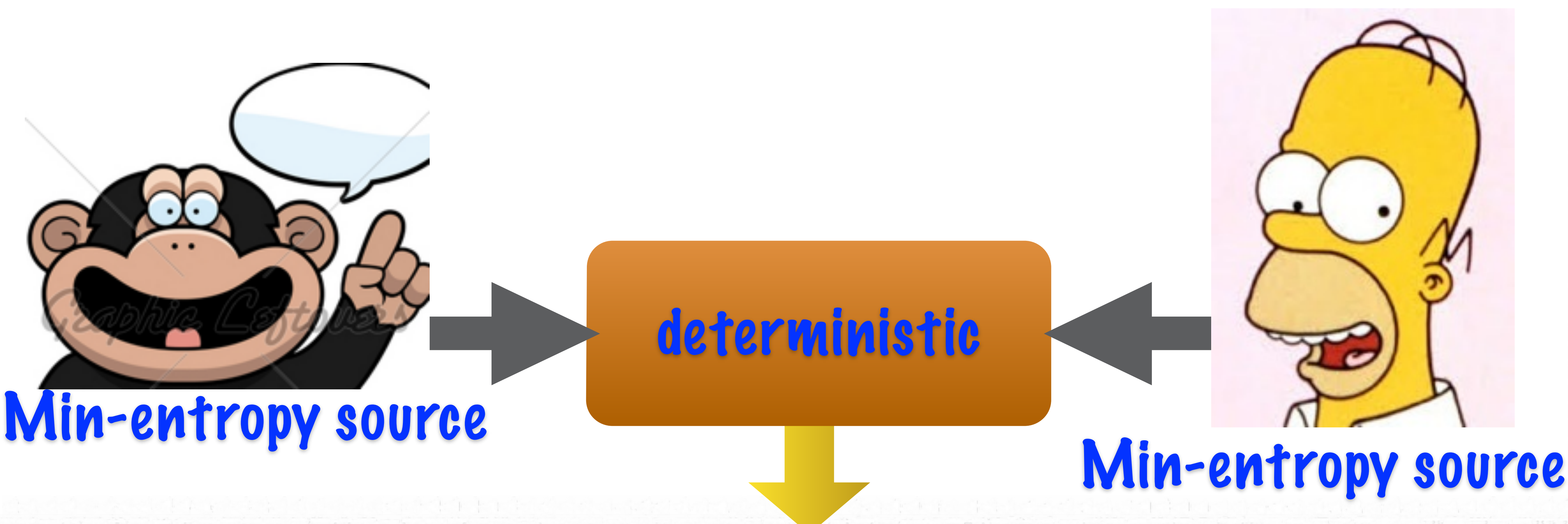
Limitation: two independent sources required

- Deterministic extraction, i.e. single source extraction, is impossible [Santha-Vazirani'86]
- Two independent sources are required



Limitation: two independent sources required

- Deterministic extraction, i.e. single source extraction, is impossible [Santha-Vazirani'86]
- Two independent sources are required
- Impossible to check independence



Limitation: two independent sources required

- Deterministic extraction, i.e. single source extraction, is impossible [Santha-Vazirani'86]
- Two independent sources are required
- Impossible to check independence

Quantum solution with trusted devices

Quantum solution with trusted devices

- Perfect randomness postulated in quantum theory

Quantum solution with trusted devices

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition $|0\rangle + |1\rangle$

Quantum solution with trusted devices

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition $|0\rangle + |1\rangle$
- Commercial products available

Quantum solution with trusted devices

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition $|0\rangle + |1\rangle$
- Commercial products available
- Trusted quantum device implies independence source

Quantum solution with trusted devices

- True quantum randomness (passes all randomness tests)
- High bit rate of 4Mbits/sec
- Affordable, compact and reliable
- Continuous status check

OEM

QUANTIS IS OFFICIALLY CERTIFIED

QUANTIS has been evaluated and certified by the Swiss Fed
METAS), the Swiss national organization in charge of measu

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition |0> + |1>
- Commercial products available
- Trusted quantum device implies independence source

Quantum solution with trusted devices

- True quantum randomness (passes all randomness tests)
- High bit rate of 4Mbits/sec
- Affordable, compact and reliable
- Continuous status check

OEM

QUANTIS IS OFFICIALLY CERTIFIED

QUANTIS has been evaluated and certified by the Swiss Fed
METAS), the Swiss national organization in charge of measu

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition |0> + |1>
- Commercial products available
- Trusted quantum device implies independence source

Quantum solution with trusted devices

- True quantum randomness (passes all randomness tests)
- High bit rate of 4Mbits/sec
- Affordable, compact and reliable
- Continuous status check

OEM

QUANTIS IS OFFICIALLY CERTIFIED

QUANTIS has been evaluated and certified by the Swiss Fed
METAS), the Swiss national organization in charge of measu

- Perfect randomness postulated in quantum theory
  - Fair coin from measuring superposition $|0\rangle + |1\rangle$
- Commercial products available
- Trusted quantum device implies independence source

Motivation::quantum approach

How do we know it works?

How do we know it works?

Motivation::quantum approach

How do we know it works?

- As classical beings, we cannot sense quantum directly

Motivation::quantum approach

How do we know it works?

- As classical beings, we cannot sense quantum directly
- Are we willing to trust the manufacturer or the certifying agency?

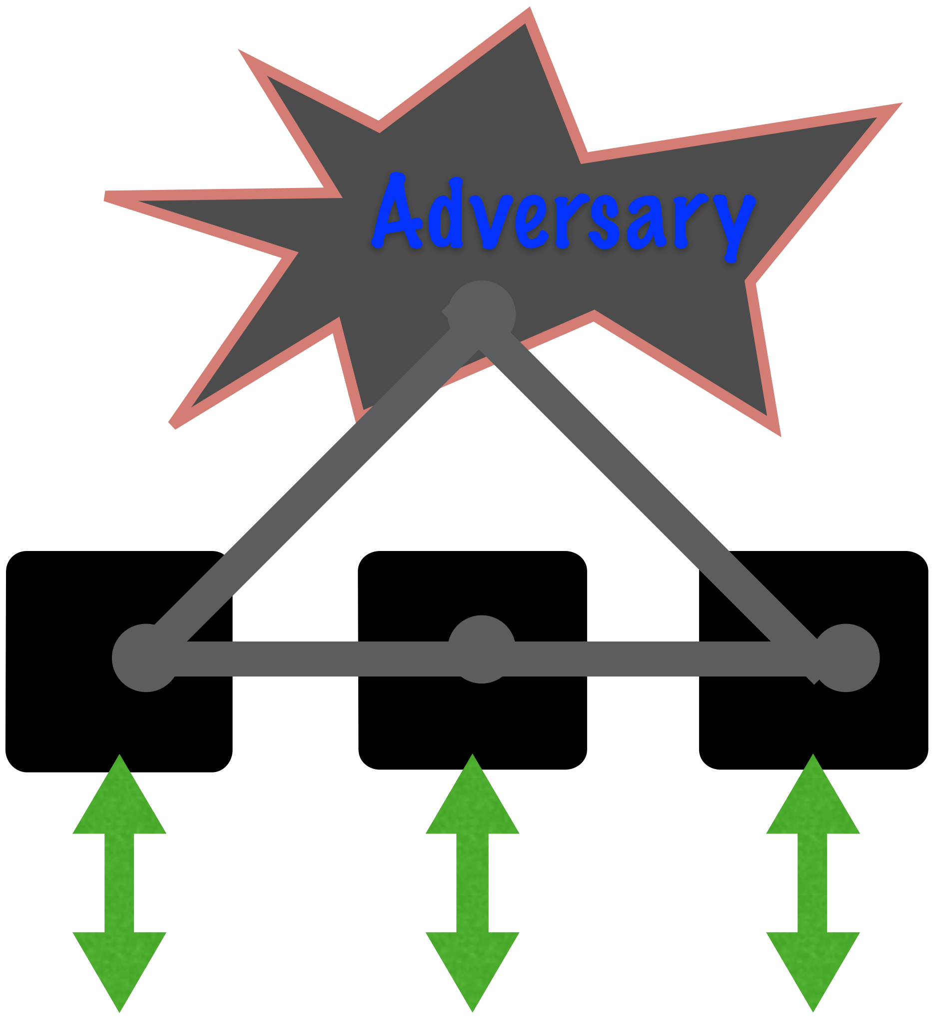
How do we know it works?

- As classical beings, we cannot sense quantum directly
- Are we willing to trust the manufacturer or the certifying agency?
- Even yes, devices may not be reliable.

How do we know it works?

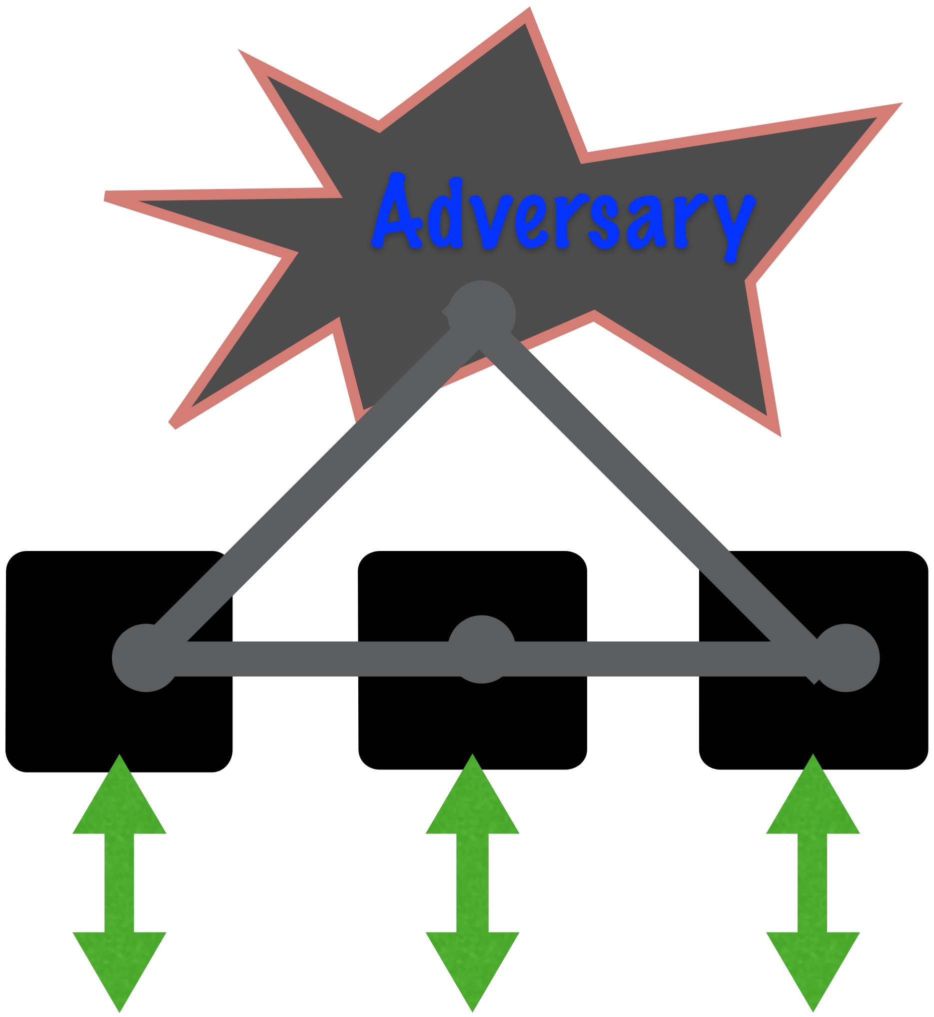
- As classical beings, we cannot sense quantum directly
- Are we willing to trust the manufacturer or the certifying agency?
- Even yes, devices may not be reliable.
    - Current technologies are prone to "noise"

Untrusted Quantum Devices



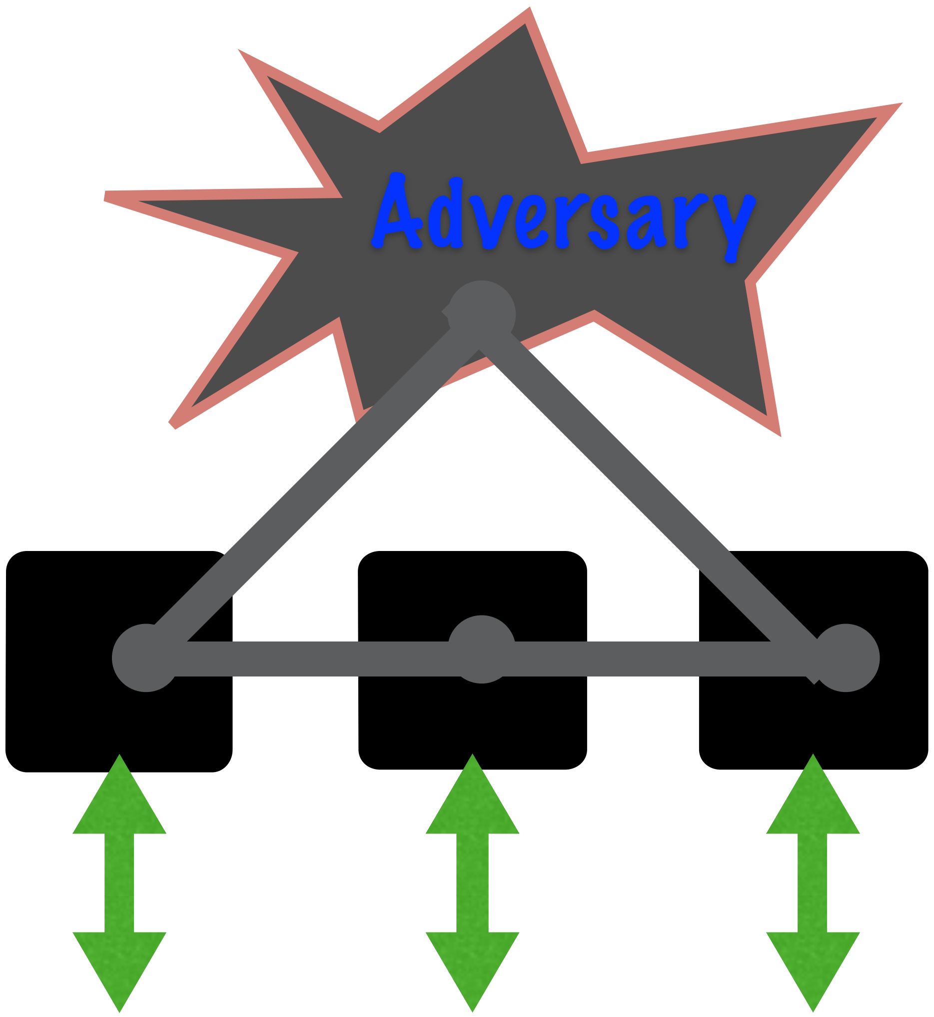
Motivation::quantum approach

Untrusted Quantum Devices



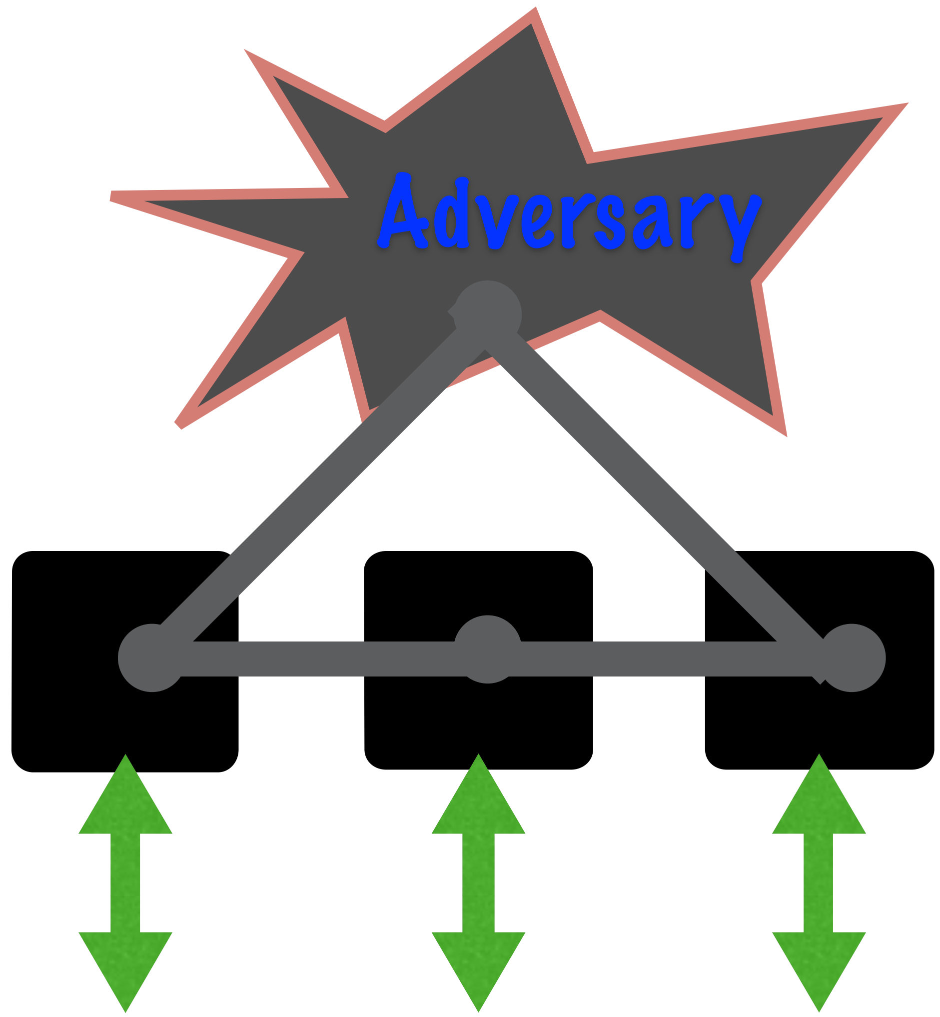
- Interact with quantum devices through classical interface

Untrusted Quantum Devices



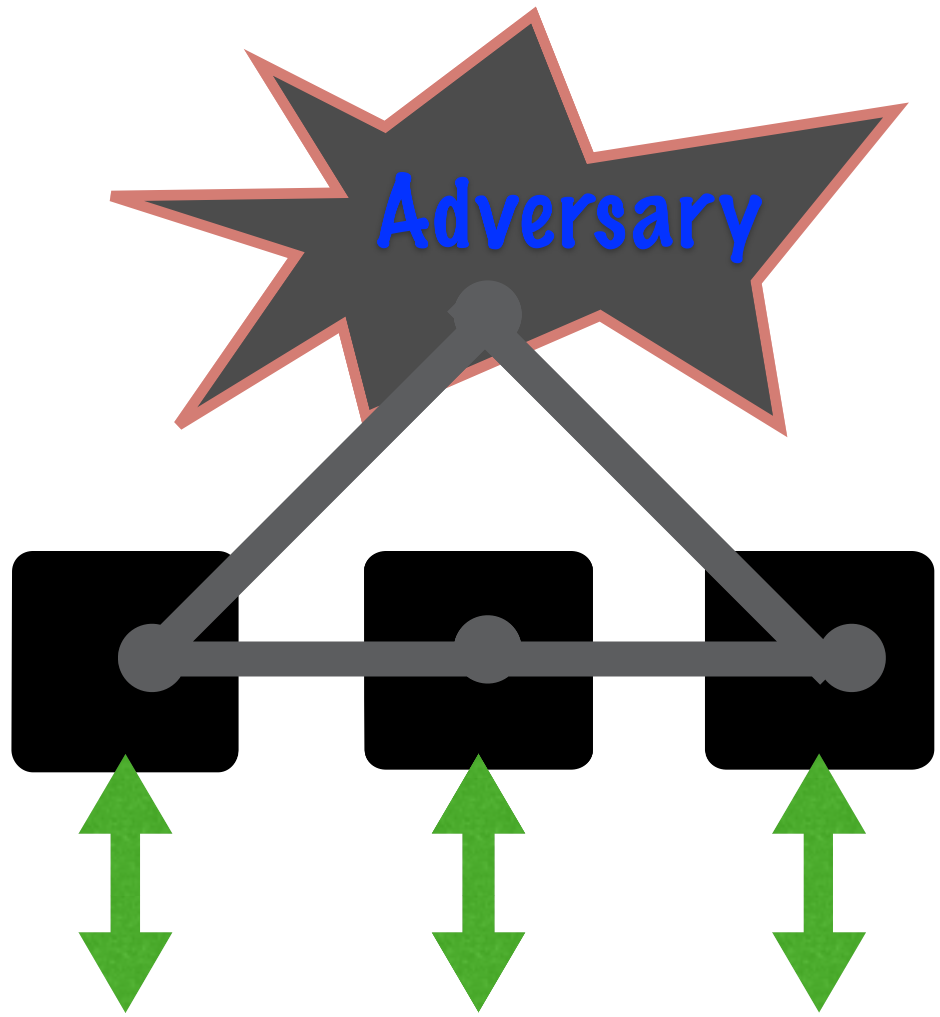
- Interact with quantum devices through classical interface
- No assumption on the quantum inner-working

Untrusted Quantum Devices



- Interact with quantum devices through classical interface
- No assumption on the quantum inner-working
  - Device can be imperfect or even malicious

Untrusted Quantum Devices



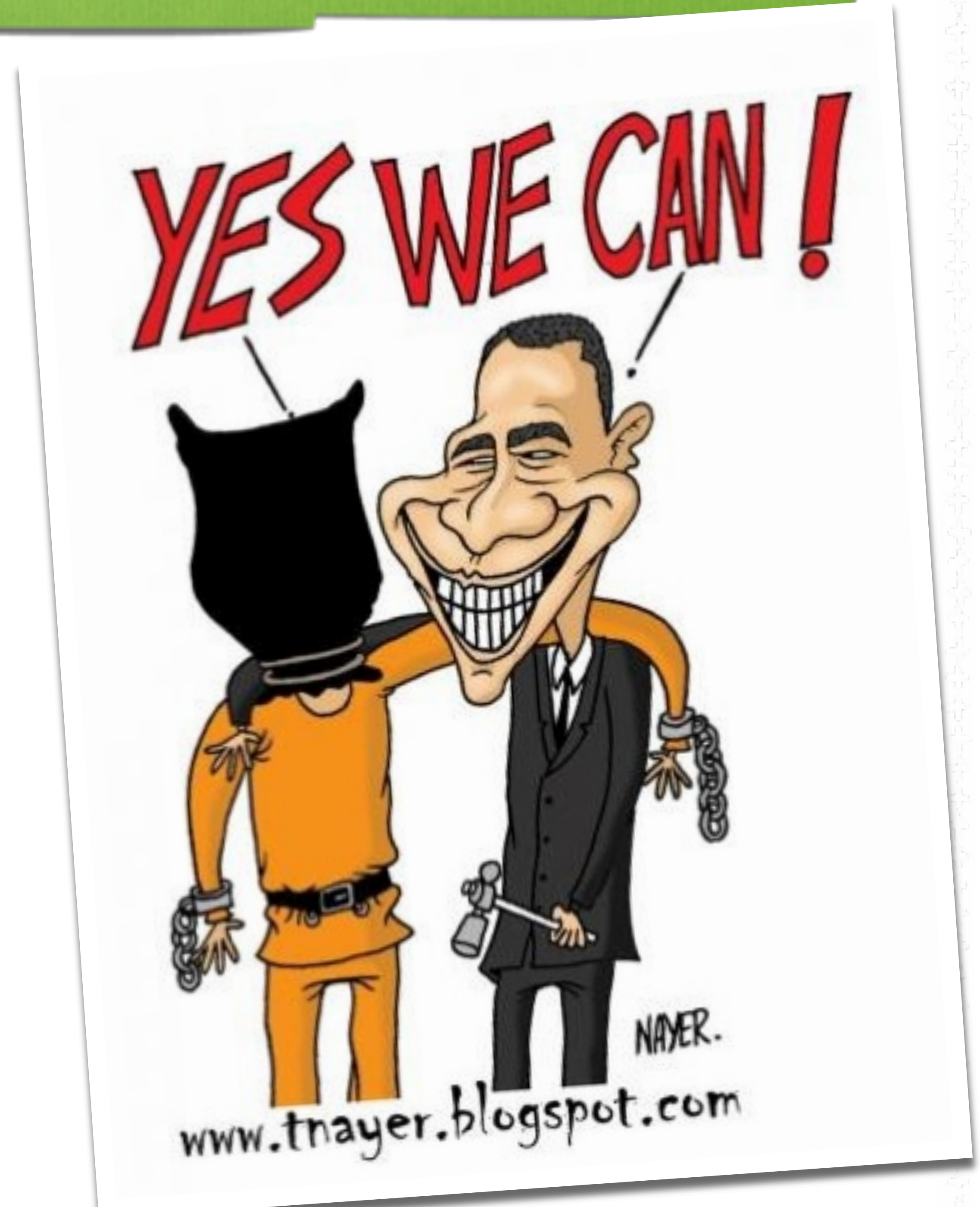
- Interact with quantum devices through classical interface
- No assumption on the quantum inner-working
  - Device can be imperfect or even malicious
  - May be in quantum correlation with the adversary and each others

Motivation::quantum approach

Can we still reap the quantum benefits without trusting the device?

Motivation::quantum approach

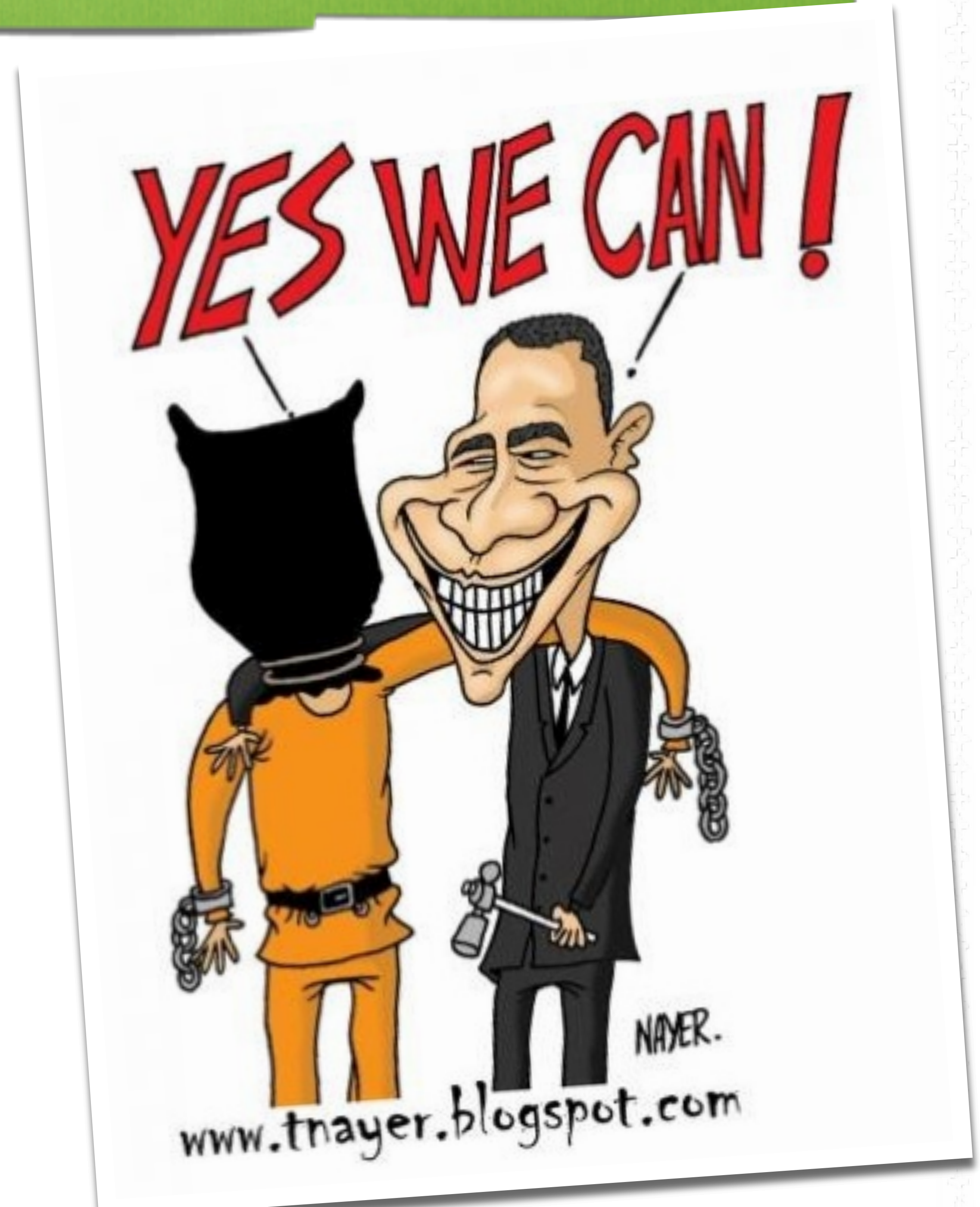
Can we still reap the quantum benefits without trusting the device?



Motivation::quantum approach

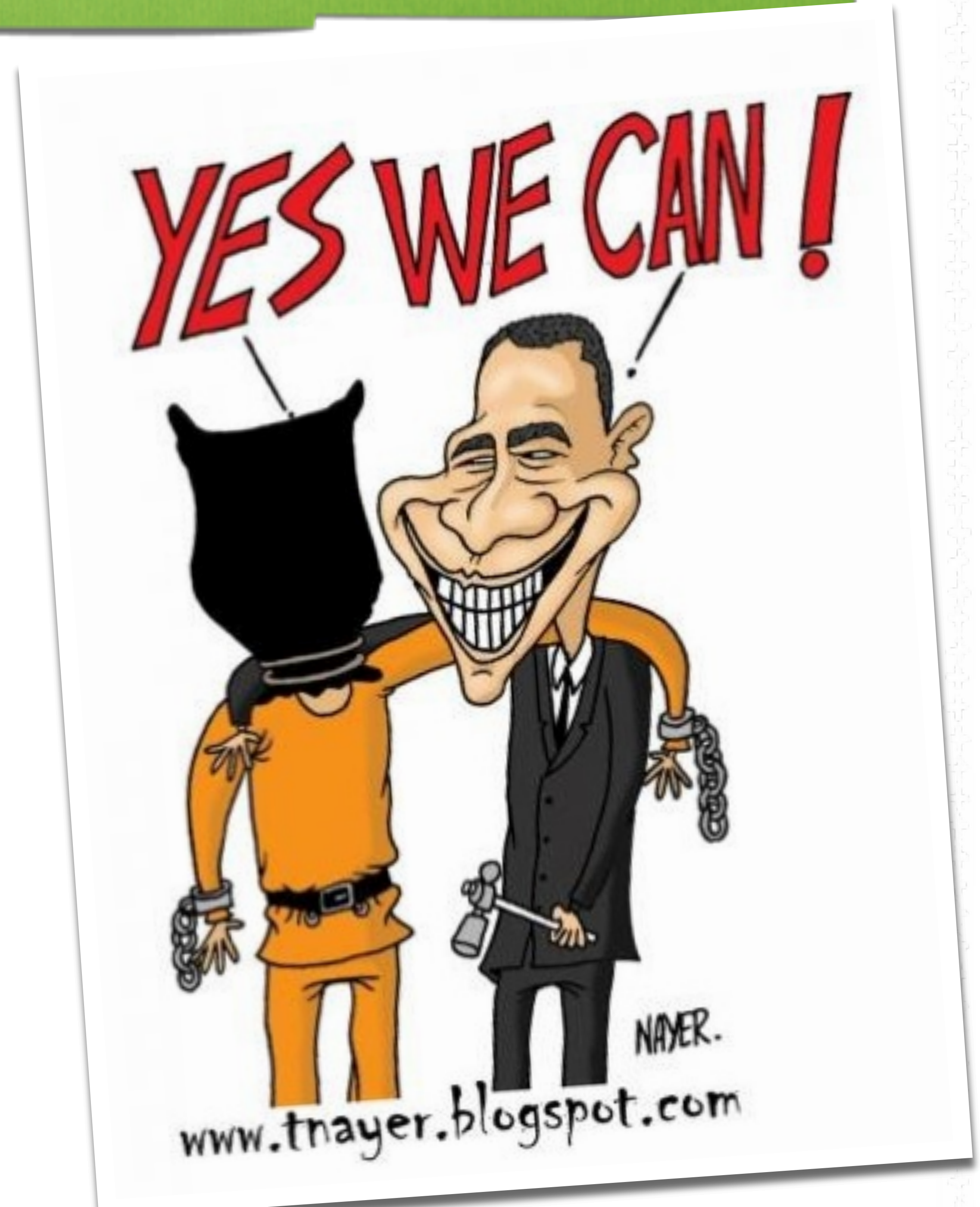
Can we still reap the quantum benefits without trusting the device?

- Untrusted-device quantum cryptography



Can we still reap the quantum benefits without trusting the device?

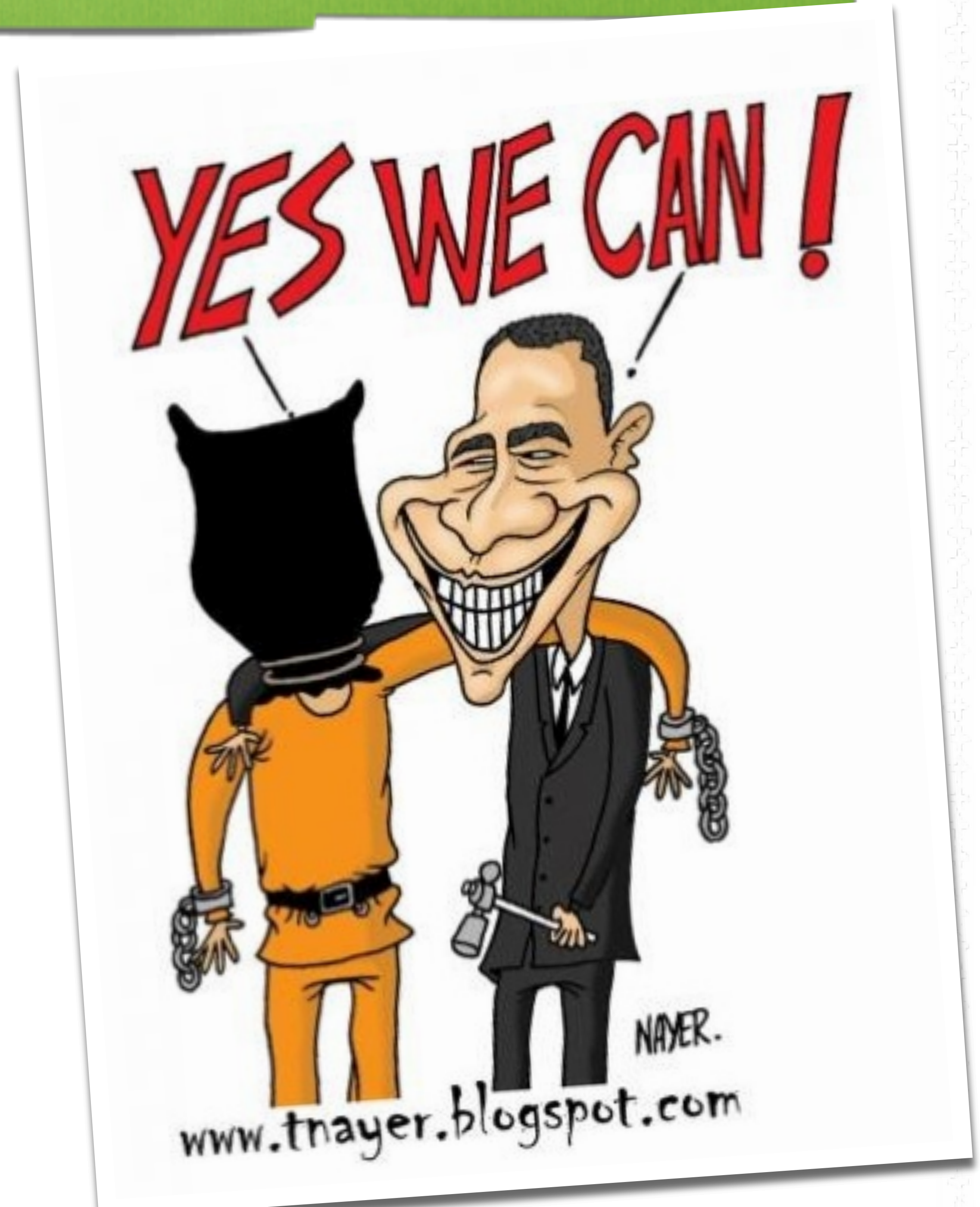
- Untrusted-device quantum cryptography
  - Started with Quantum Key Distribution [Mayers-Yao'98, Barrett-Hardy-Kent'05]



Motivation::quantum approach

Can we still reap the quantum benefits without trusting the device?

- Untrusted-device quantum cryptography
  - Started with Quantum Key Distribution [Mayers-Yao'98, Barrett-Hardy-Kent'05]
  - Many recent works



Goal

Create and expand true randomness using a single classical source and untrusted quantum devices

2. Model and Results

2. Model and Results

- What's been done?

2. Model and Results

- What's been done?
- Physical Extractors [Chung-Shi-Wu]: a unifying framework for extracting from physical systems

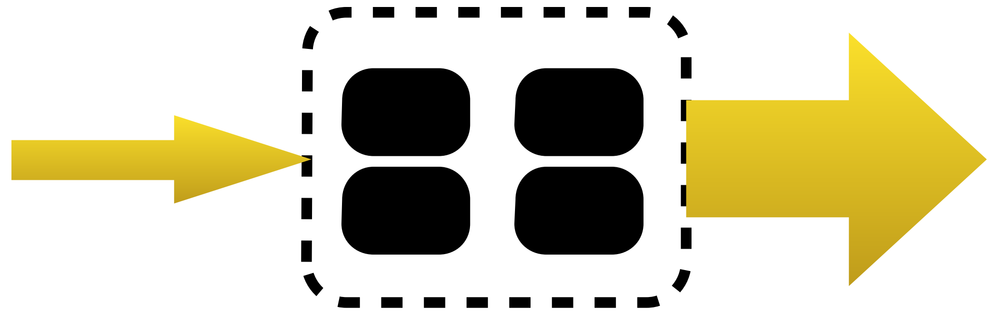
2. Model and Results

- What's been done?
- Physical Extractors [Chung-Shi-Wu]: a unifying framework for extracting from physical systems
- Our results [Miller-Shi, Chung-Shi-Wu]

Randomness Expansion [Colbeck'06, Colbeck-Kent'11]

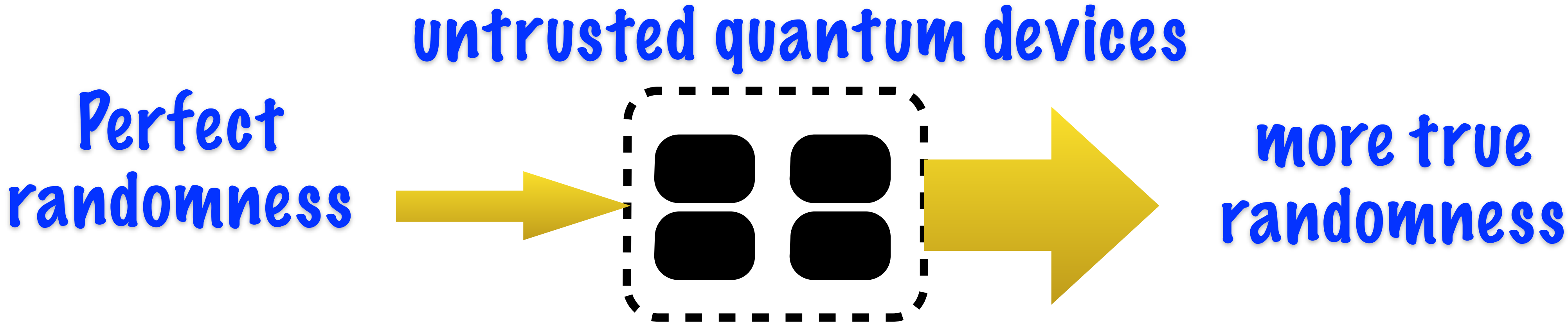
untrusted quantum devices

Perfect randomness



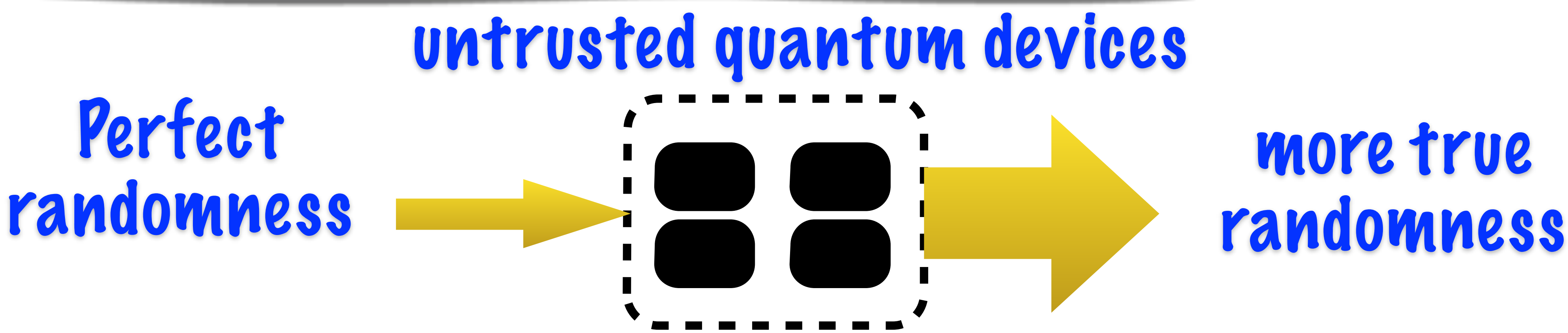
more true randomness

Randomness Expansion [Colbeck'06, Colbeck-Kent'11]



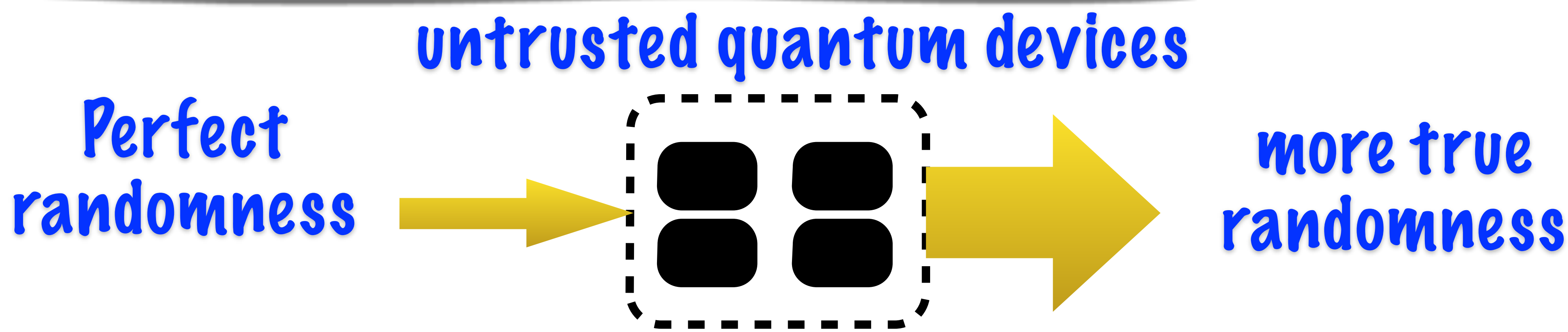
- Turn an initial (uniform) seed to a longer true randomness

Randomness Expansion [Colbeck'06, Colbeck-Kent'11]



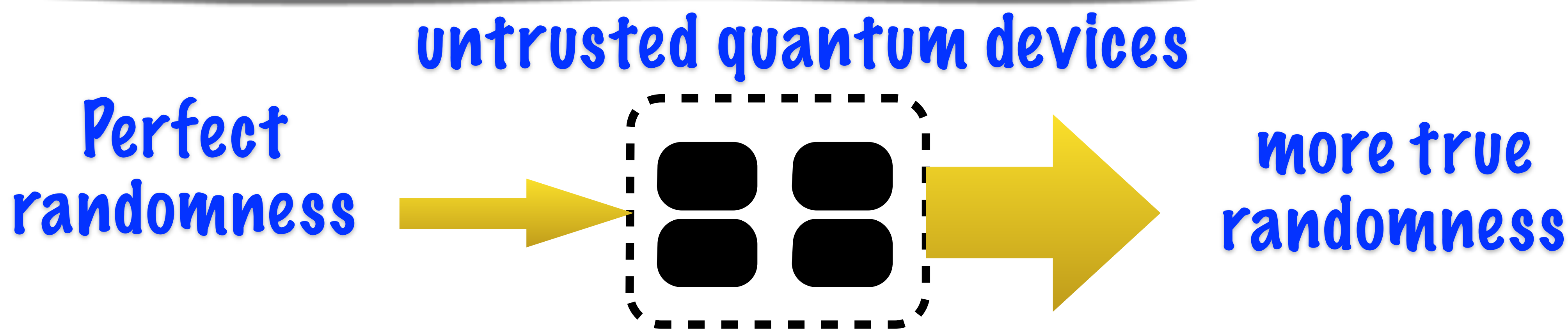
- Turn an initial (uniform) seed to a longer true randomness
- Classical or restricted security proved by [Pironio+'10, Pinorio-Massar'13, Fehr+'13, Coudron+'13]

Randomness Expansion [Colbeck'06, Colbeck-Kent'11]



- Turn an initial (uniform) seed to a longer true randomness
- Classical or restricted security proved by [Pironio+'10, Pinorio-Massar'13, Fehr+'13, Coudron+'13]
- Quantum security proved by [Vazirani-Vidick'12]

Randomness Expansion [Colbeck'06, Colbeck-Kent'11]

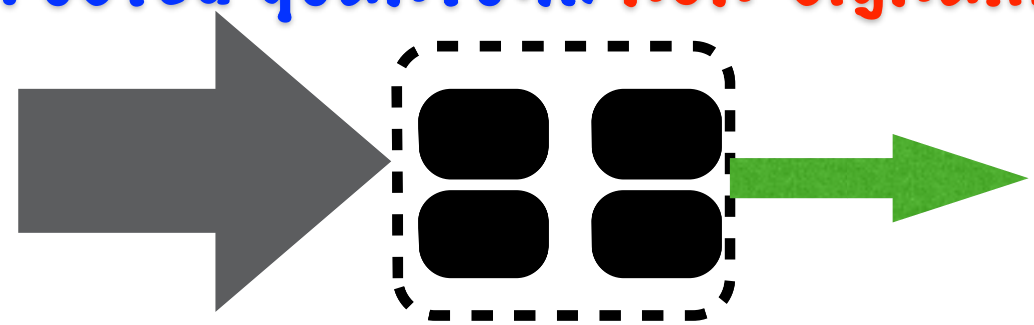


- Turn an initial (uniform) seed to a longer true randomness
- Classical or restricted security proved by [Pironio+'10, Pinorio-Massar'13, Fehr+'13, Coudron+'13]
- Quantum security proved by [Vazirani-Vidick'12]
  - Also exponentially expanding: k bits -> exp(k^c) bits

Randomness Amplification [Colbeck-Renner'12]

untrusted quantum/non-signaling devices

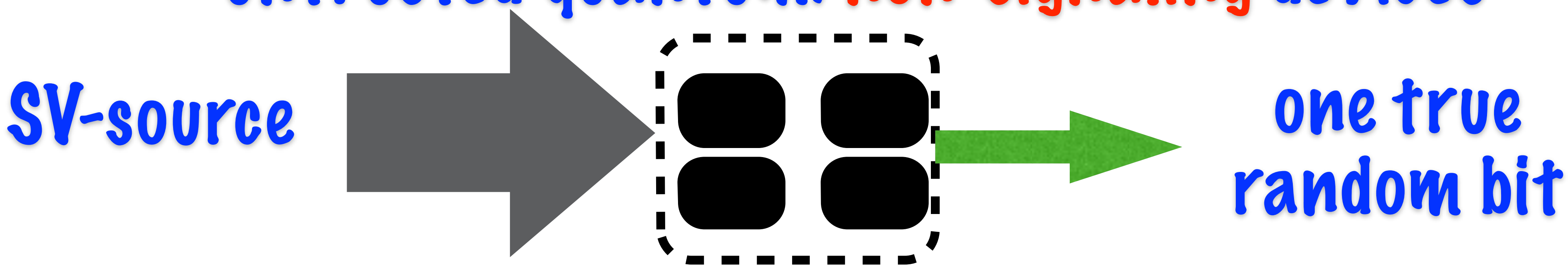
SV-source



one true random bit

Randomness Amplification [Colbeck-Renner'12]

untrusted quantum/non-signaling devices

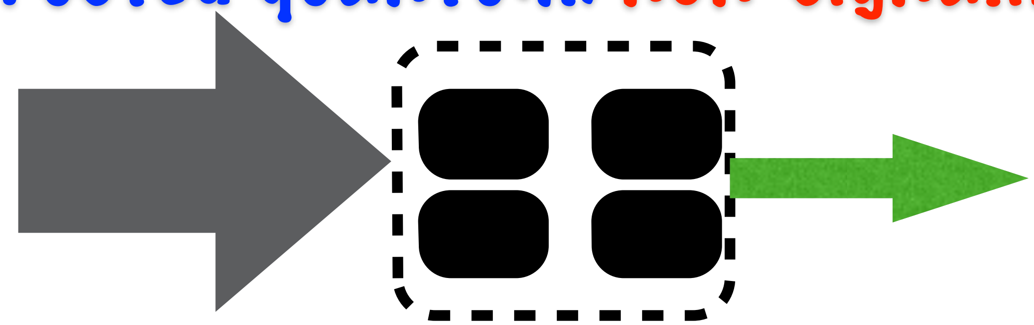


- Q: "Are there fundamentally random processes in Nature?"

Randomness Amplification [Colbeck-Renner'12]

untrusted quantum/non-signaling devices

SV-source



one true random bit

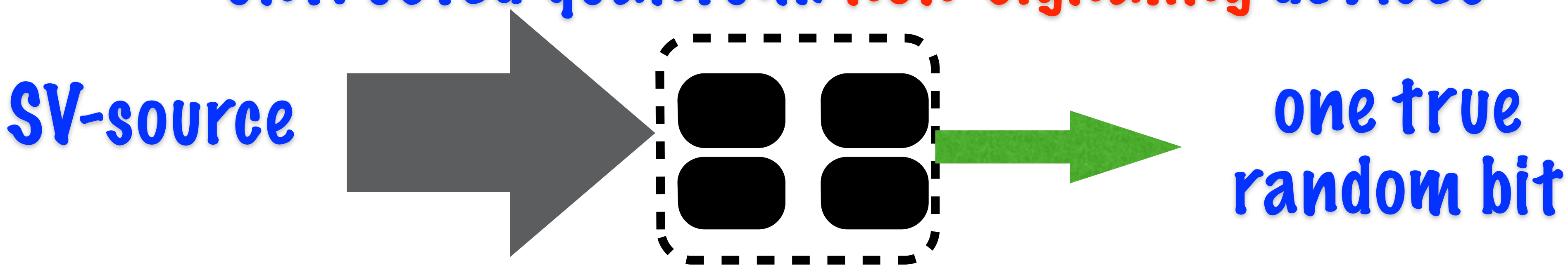
- Q: "Are there fundamentally random processes in Nature?"

- Model weak randomness as an Santha-Vazirani (SV) source: $x_1, x_2, \ldots., x_n$, s.t. for a constant ϵ and any adversary's side information e, $\mathrm{Prob}[x_i = 1 \mid x_1, x_2, \ldots, x_{i-1}, e] \in [1/2-\epsilon, 1/2+\epsilon]$.

Model and Results::history

Randomness Amplification [Colbeck-Renner'12]

untrusted quantum/non-signaling devices



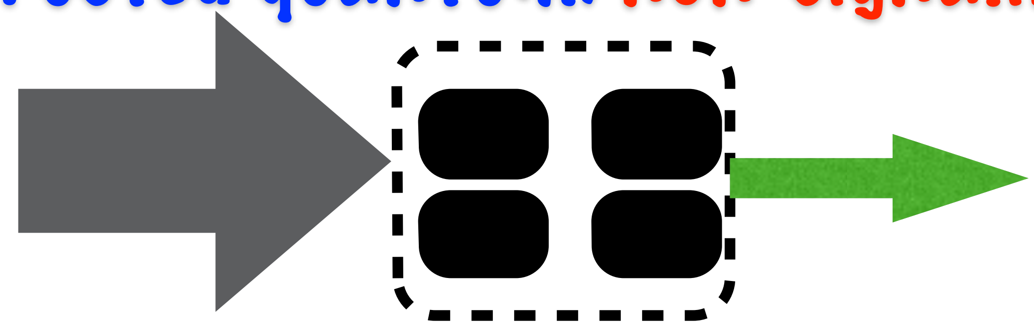
- Q: "Are there fundamentally random processes in Nature?"
- Model weak randomness as an Santha-Vazirani (SV) source: $x_1, x_2, \ldots, x_n$, s.t. for a constant ϵ and any adversary's side information e, $\mathrm{Prob}[x_i = 1 \mid x_1, x_2, \ldots, x_{i-1}, e] \in [1/2-\epsilon, 1/2+\epsilon]$.
- [Colbeck-Renner'12]: sufficiently small ϵ; [Gallego+'13]: any $\epsilon<1/2$; [Brandao'14]: constant number of devices

Model and Results::history

Randomness Amplification [Colbeck-Renner'12]

untrusted quantum/non-signaling devices

SV-source

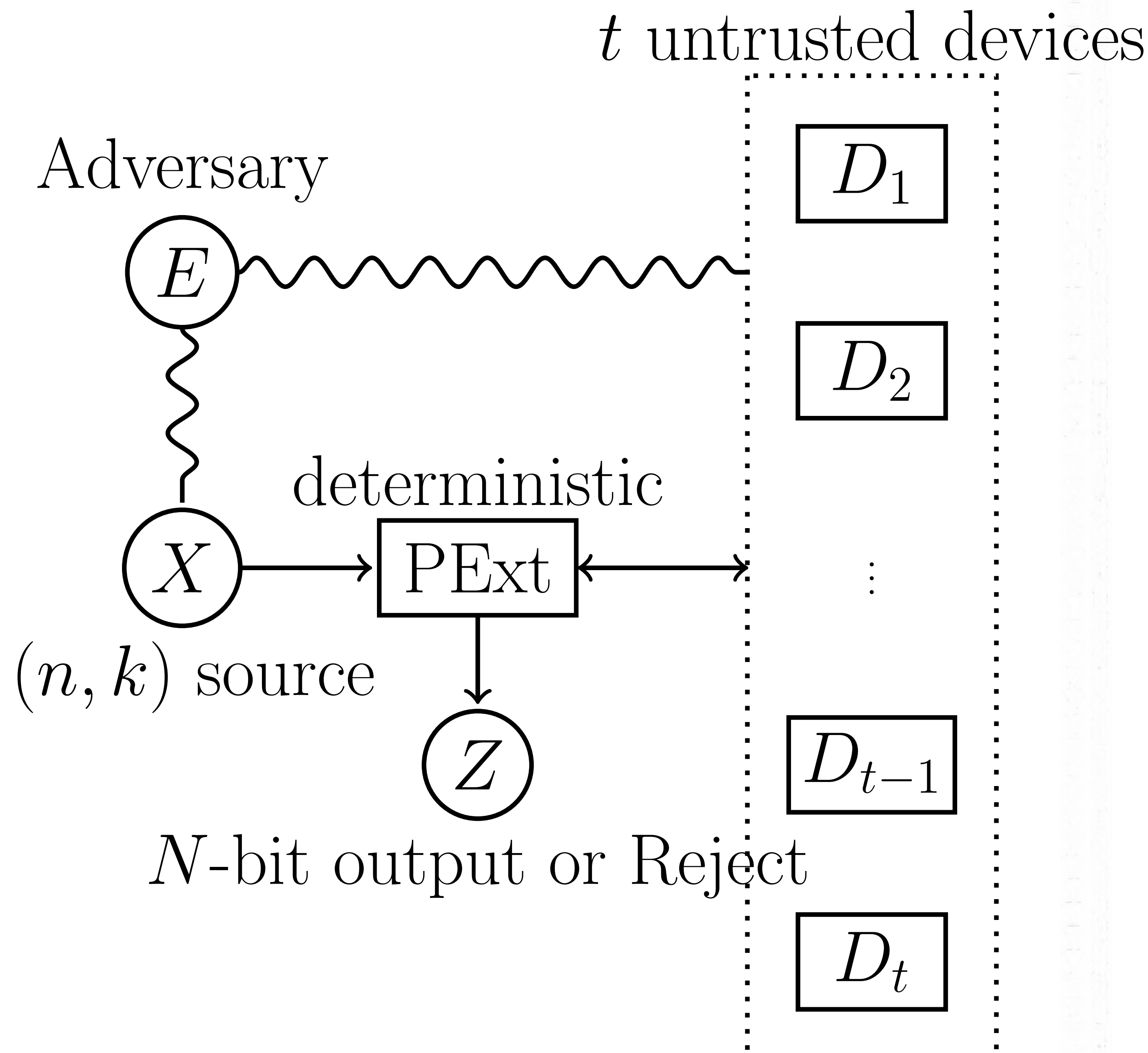


one true random bit

- Q: "Are there fundamentally random processes in Nature?"
- Model weak randomness as an Santha-Vazirani (SV) source: $x_1, x_2, \ldots, x_n$, s.t. for a constant ϵ and any adversary's side information e, $\mathrm{Prob}[x_i = 1 \mid x_1, x_2, \ldots, x_{i-1}, e] \in [1/2-\epsilon, 1/2+\epsilon]$.
- [Colbeck-Renner'12]: sufficiently small ϵ;
  [Gallego+'13]: any $\epsilon<1/2$;
  [Brandao'14]: constant number of devices
  - All assume independence of the SV-source and the device conditioned on e.

Model and Results::history

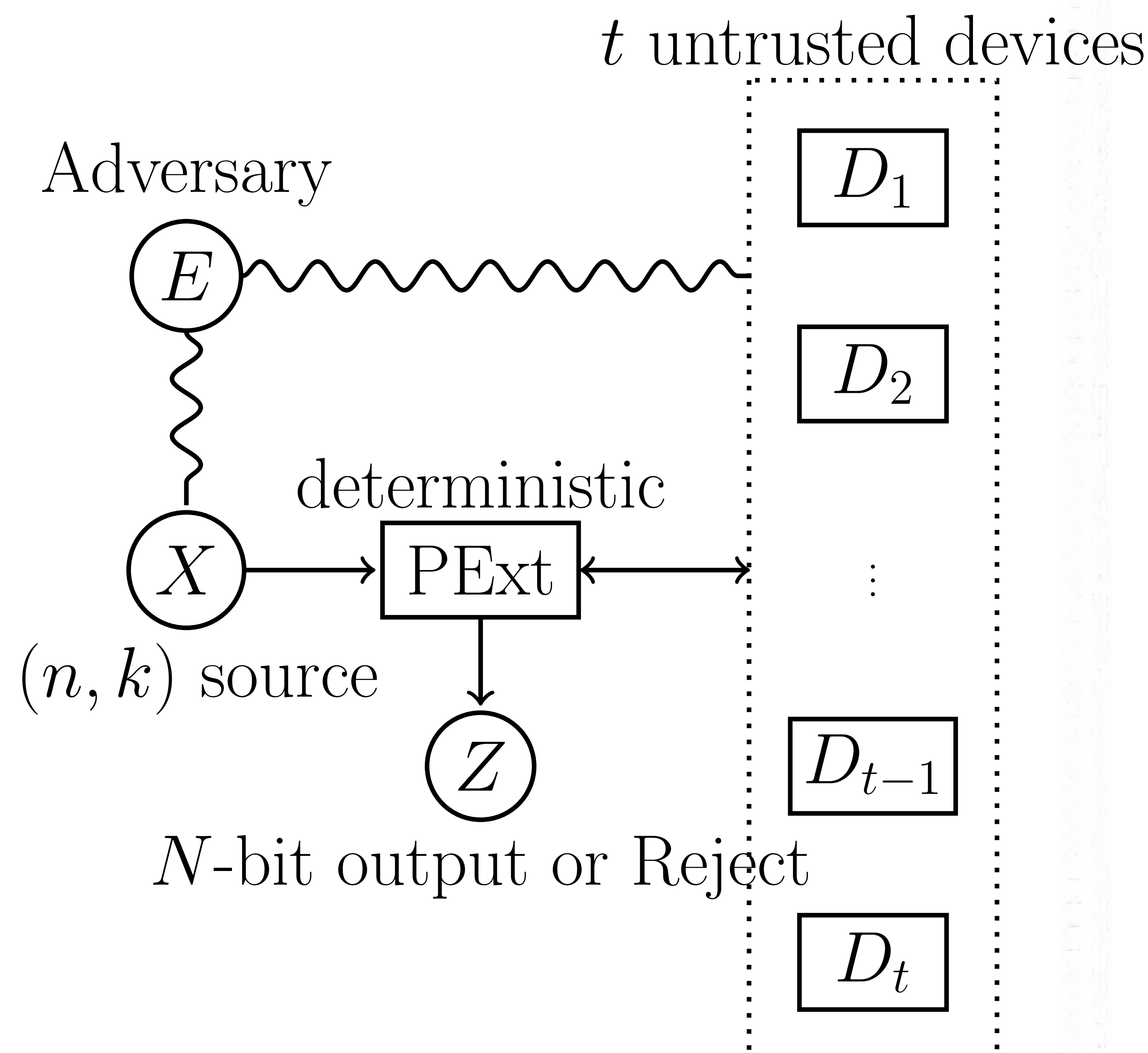
Physical Extractors: a unifying quantum framework



Model and Results::unifying model

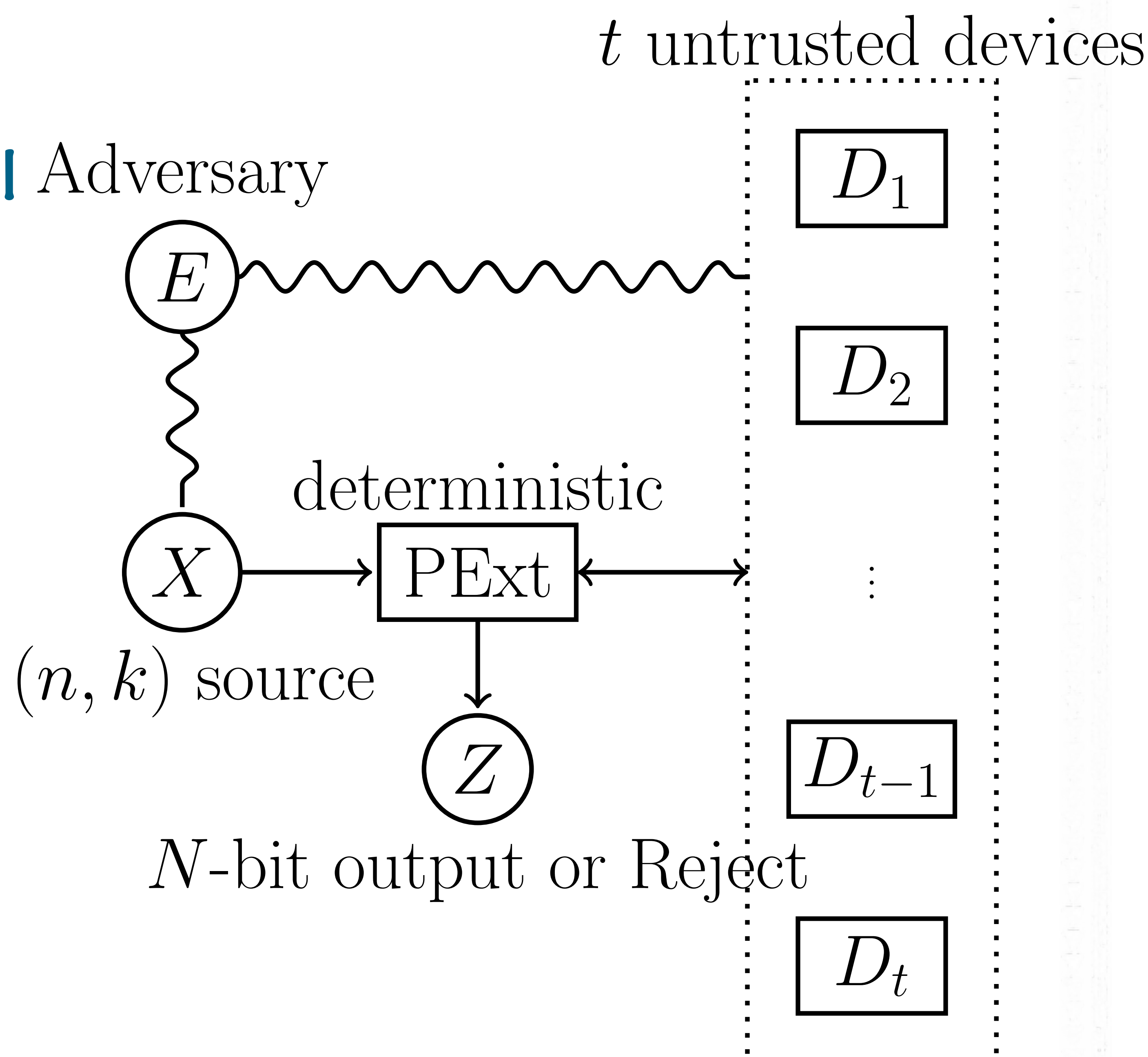
Physical Extractors: a unifying quantum framework

- **Protocol: deterministic**



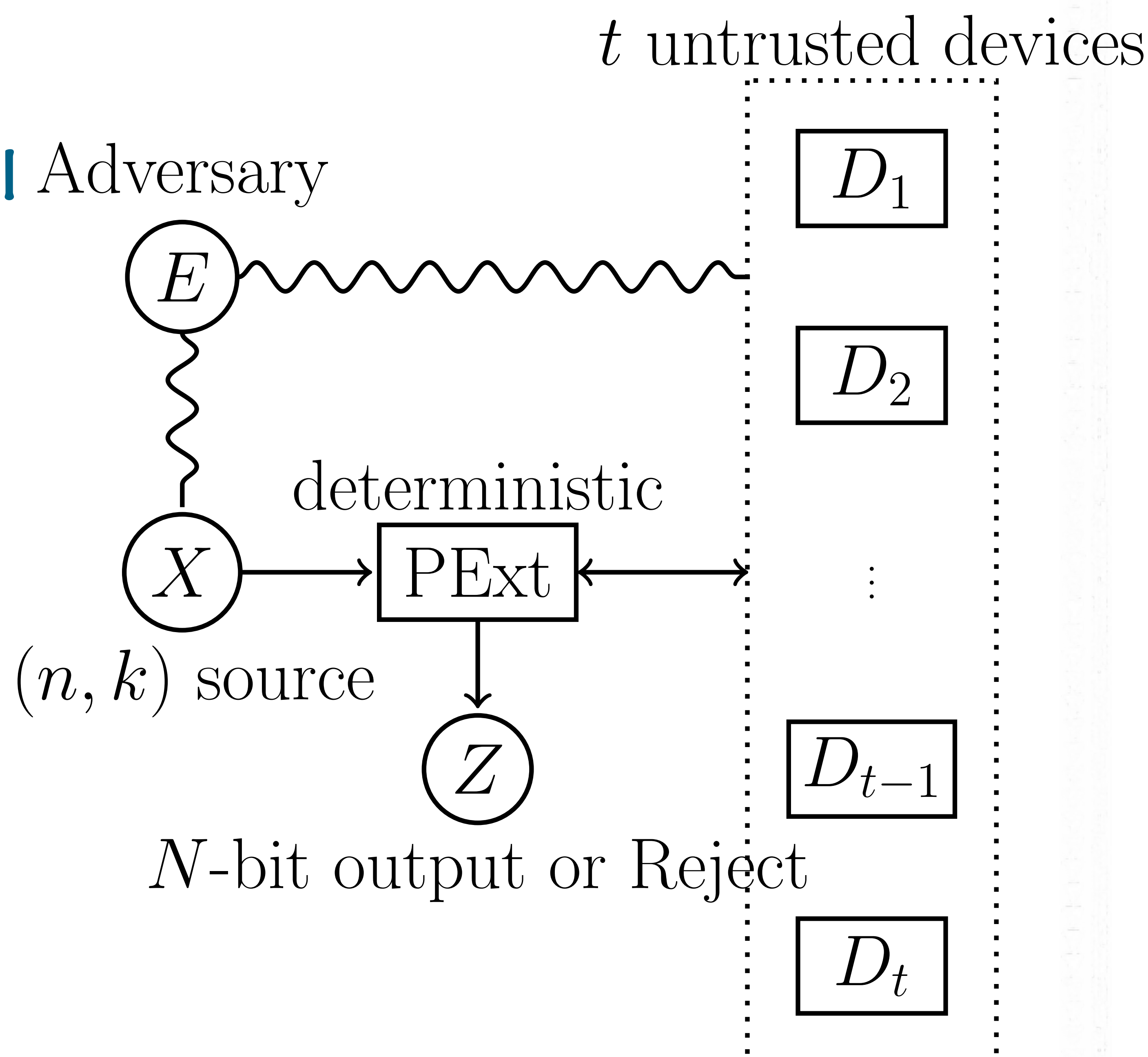
Physical Extractors: a unifying quantum framework

- Protocol: deterministic
- Adversary: quantum and all powerful



Physical Extractors: a unifying quantum framework

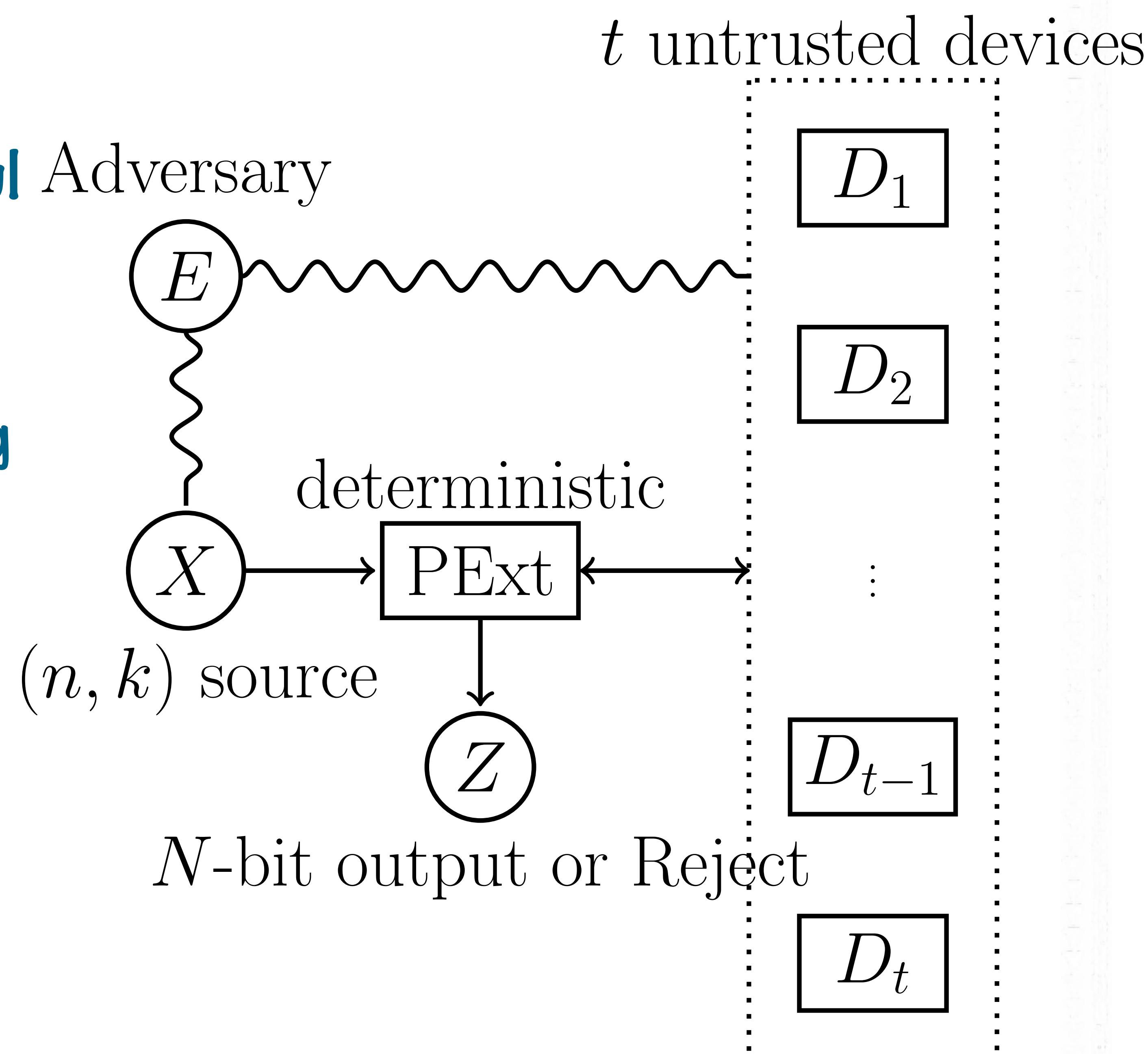
- Protocol: deterministic
- Adversary: quantum and all powerful
  - Prepares/entangled with devices



Model and Results::unifying model

Physical Extractors: a unifying quantum framework

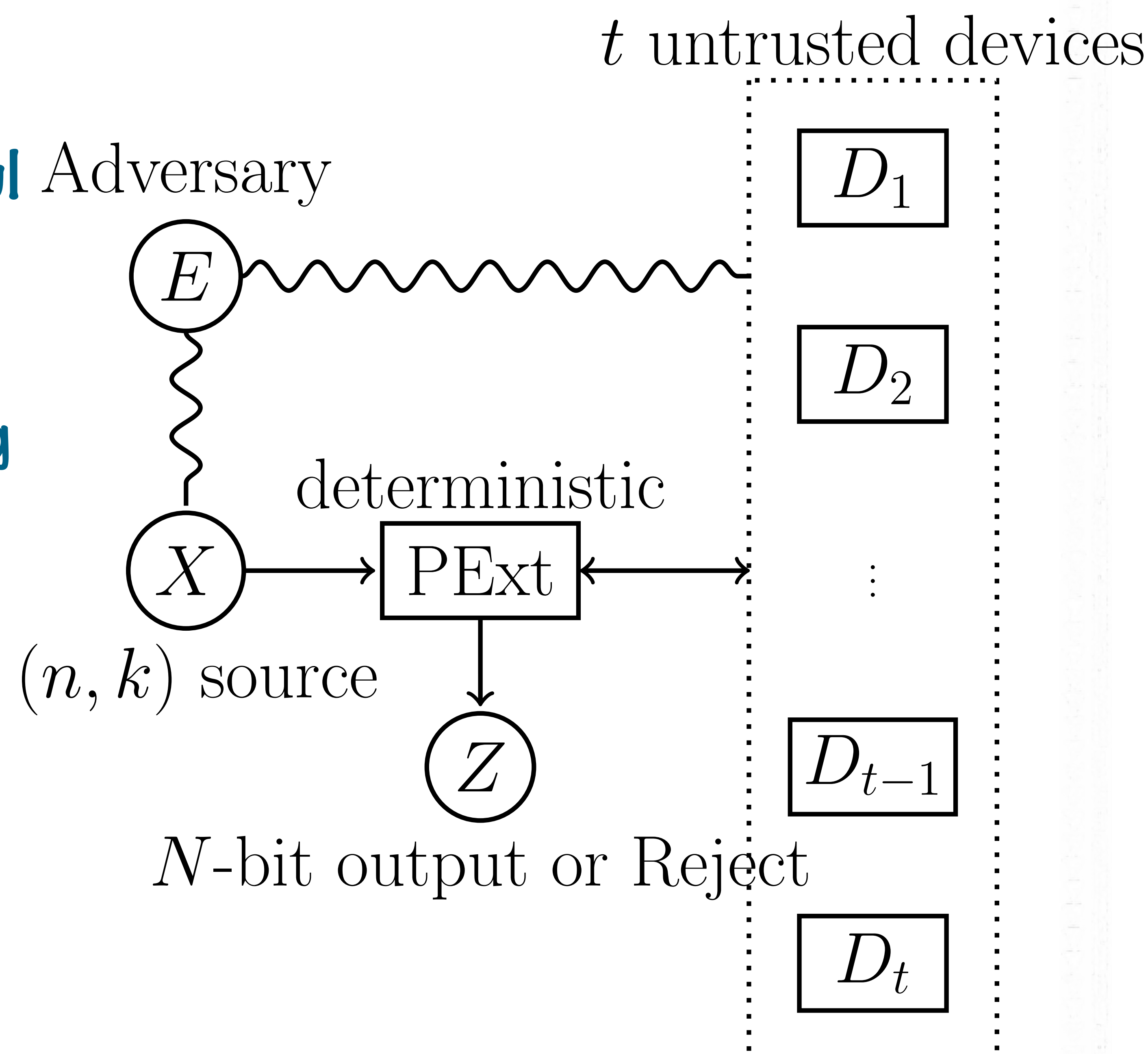
- Protocol: deterministic
- Adversary: quantum and all powerful
    - Prepares/entangled with devices
    - Can't interact with devices during protocol



Model and Results::unifying model

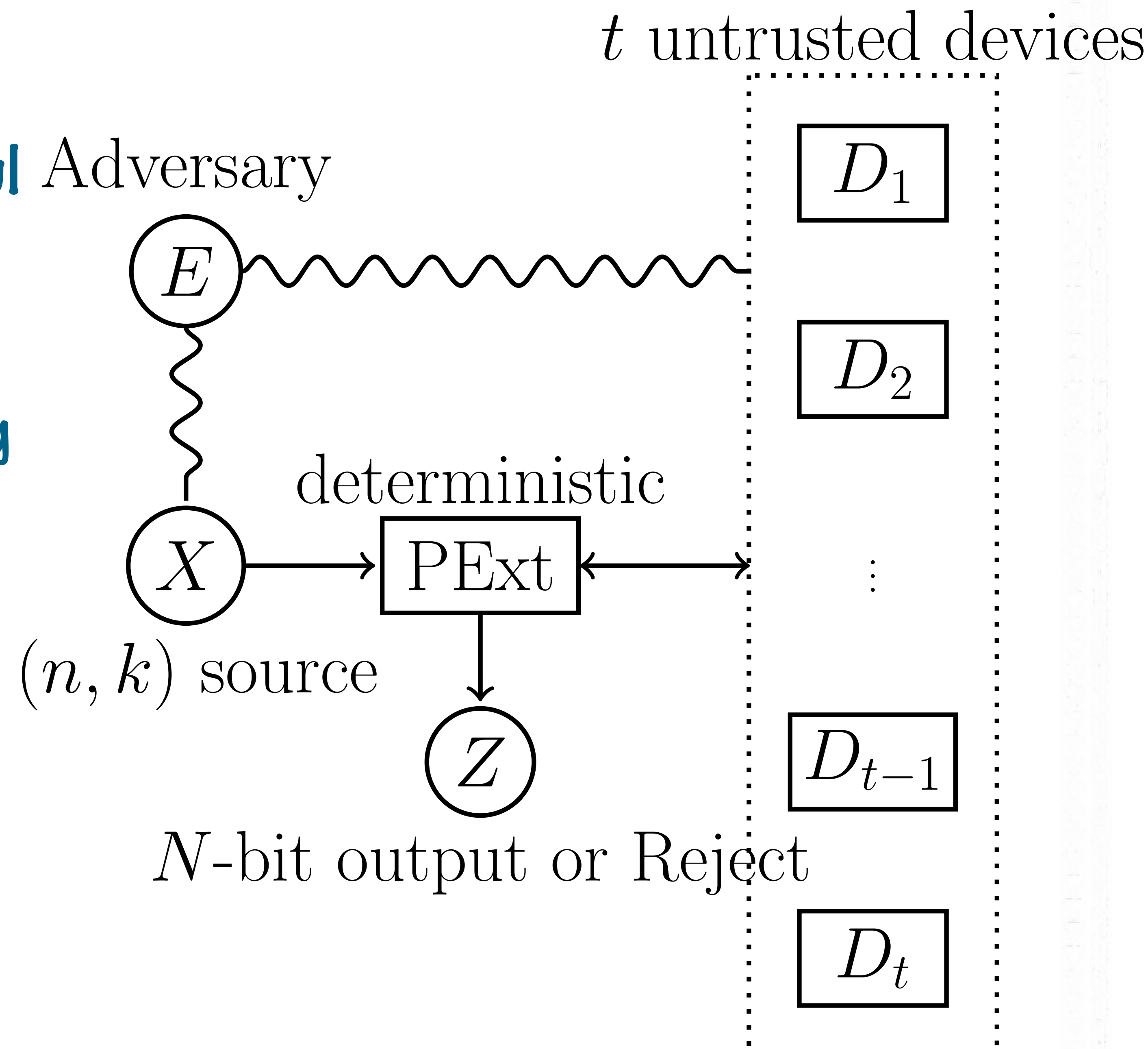
Physical Extractors: a unifying quantum framework

- Protocol: deterministic
- Adversary: quantum and all powerful
    - Prepares/entangled with devices
    - Can't interact with devices during protocol
- Devices: non-interacting



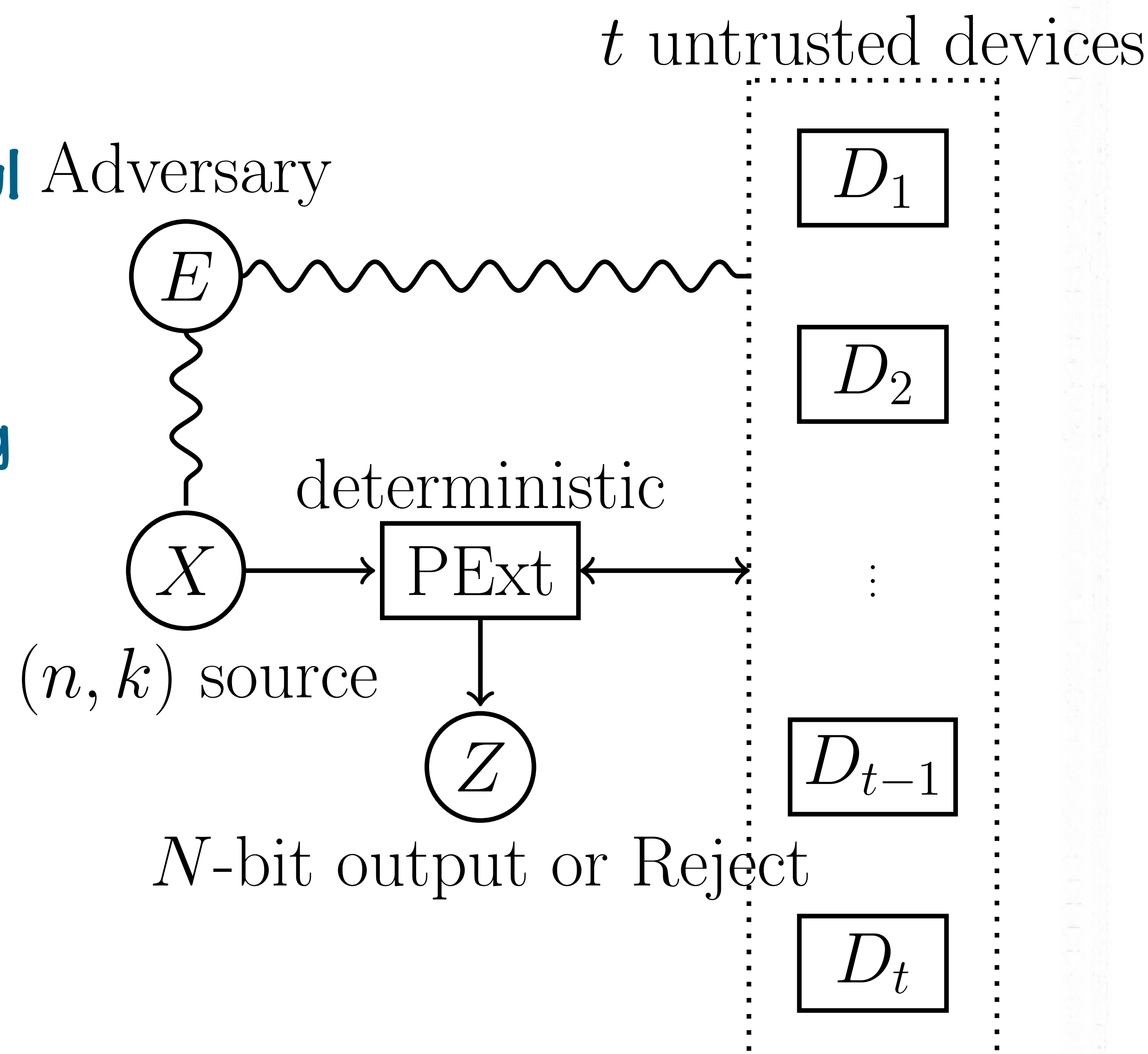
Physical Extractors: a unifying quantum framework

- Protocol: deterministic
- Adversary: quantum and all powerful
    - Prepares/entangled with devices
    - Can't interact with devices during protocol
- Devices: non-interacting
- Min-entropy source: necessary to prevent cheating

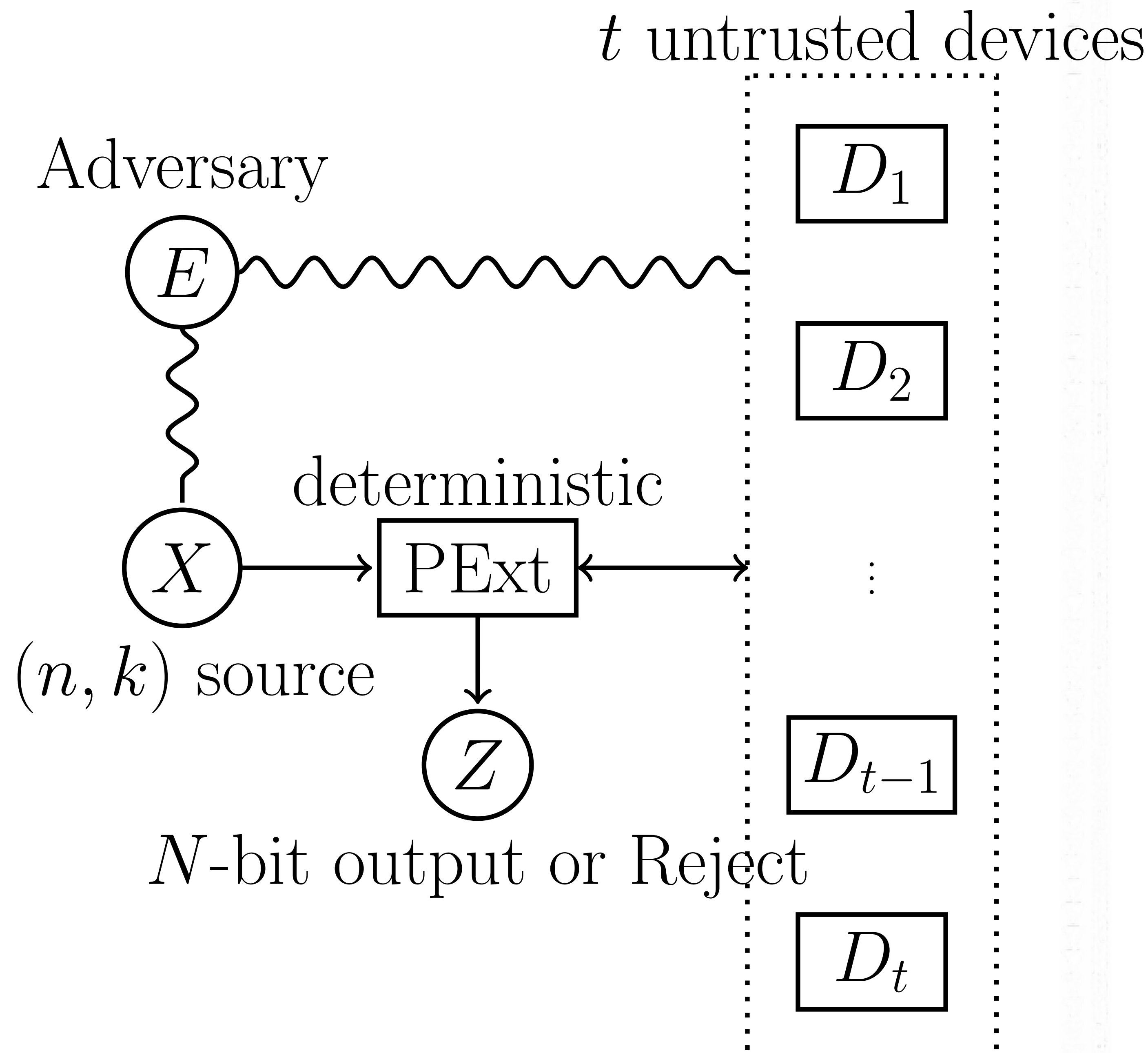


Physical Extractors: a unifying quantum framework

- Protocol: deterministic
- Adversary: quantum and all powerful
  - Prepares/entangled with devices
  - Can't interact with devices during protocol
- Devices: non-interacting
- Min-entropy source: necessary to prevent cheating
  - Min-entropy w.r.s.t. Adversary +Device



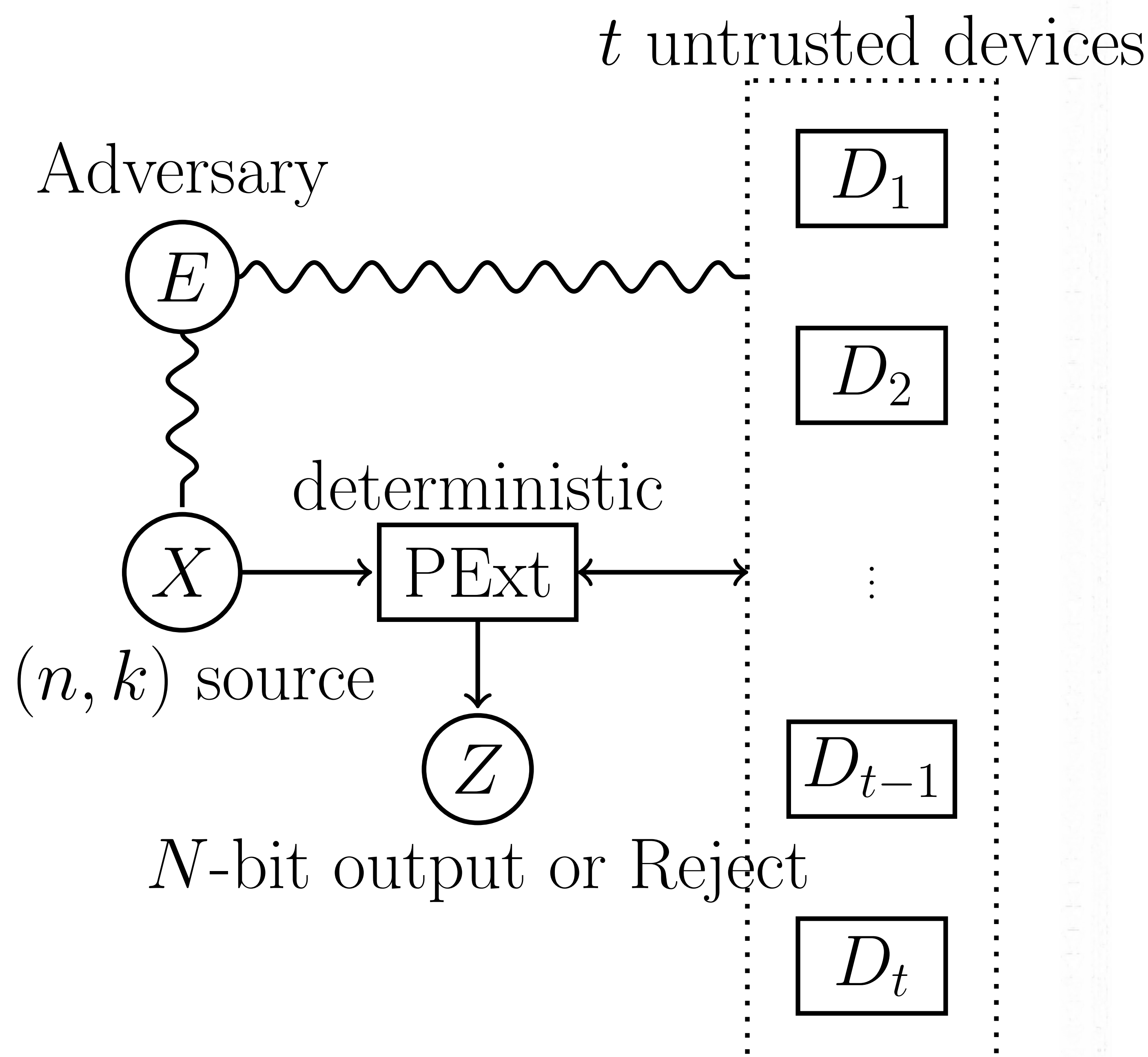
Expansion and amplification as physical extractors



Model and Results::a unifying framework

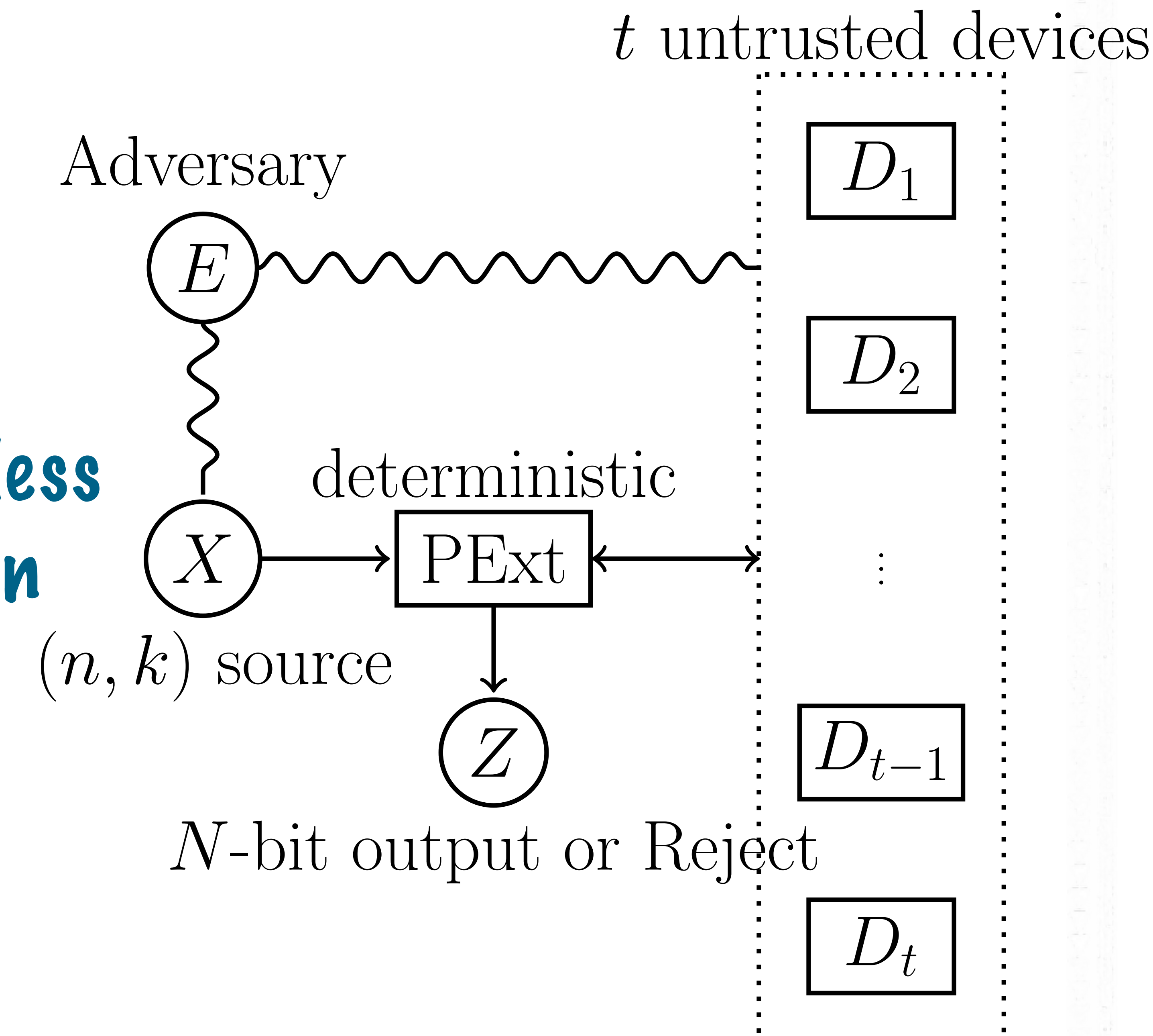
Expansion and amplification as physical extractors

- **Expansion: seeded extraction**



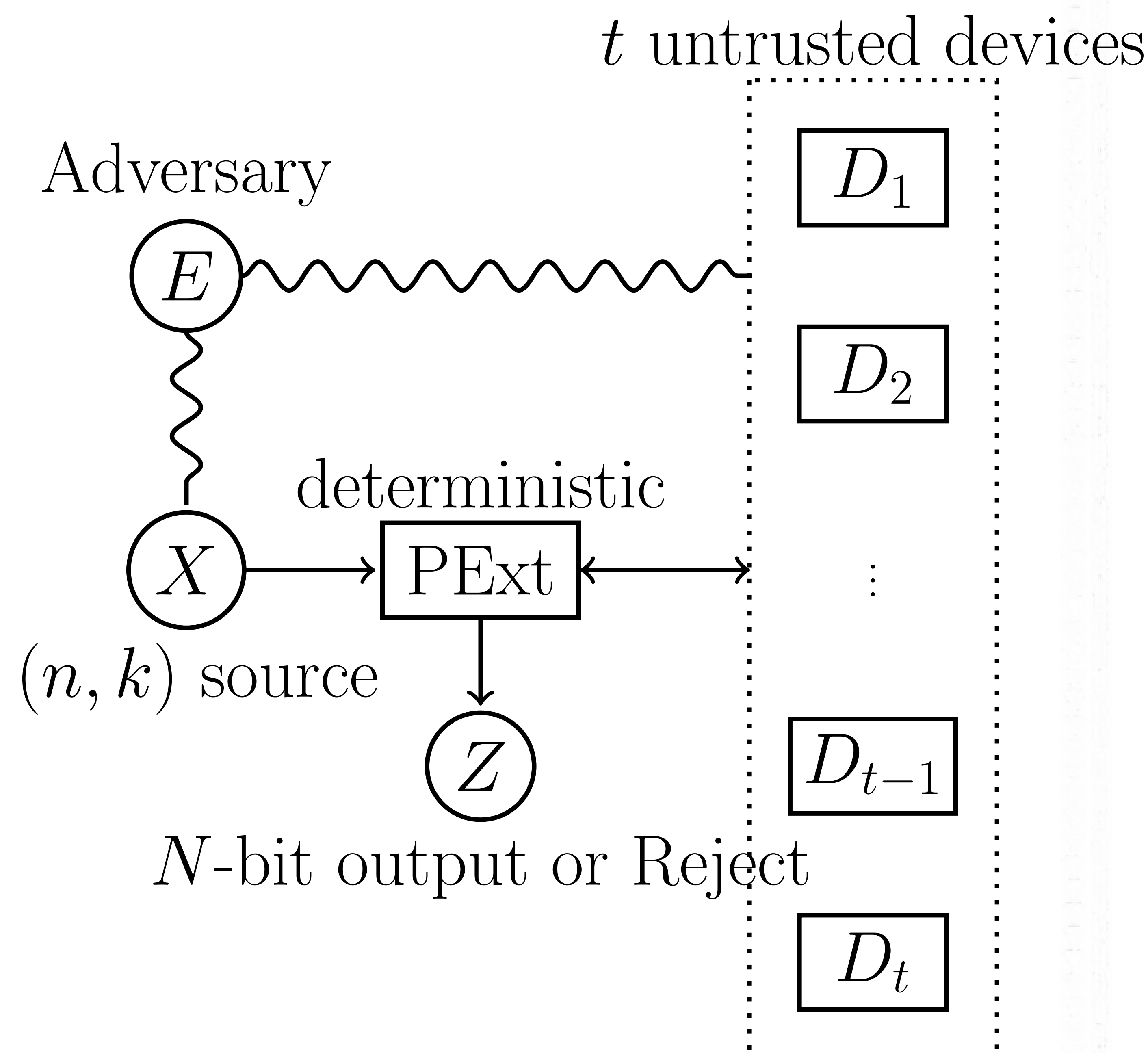
Expansion and amplification as physical extractors

- **Expansion: seeded extraction**
- **Amplification: 1-bit seedless extraction with a certain strong SV-source and conditional-independent input-device**



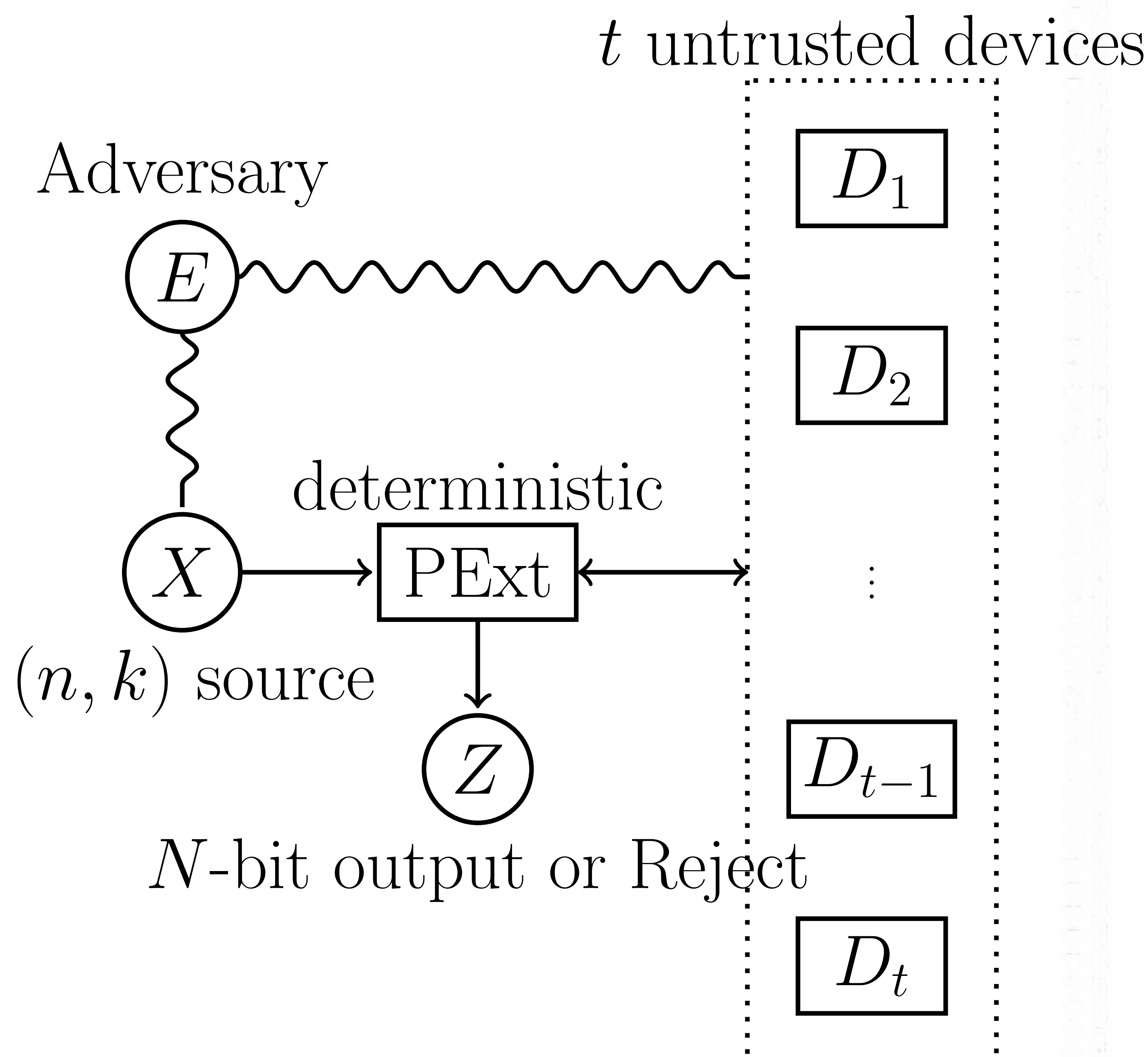
Model and Results::a unifying framework

Goals for physical extractors



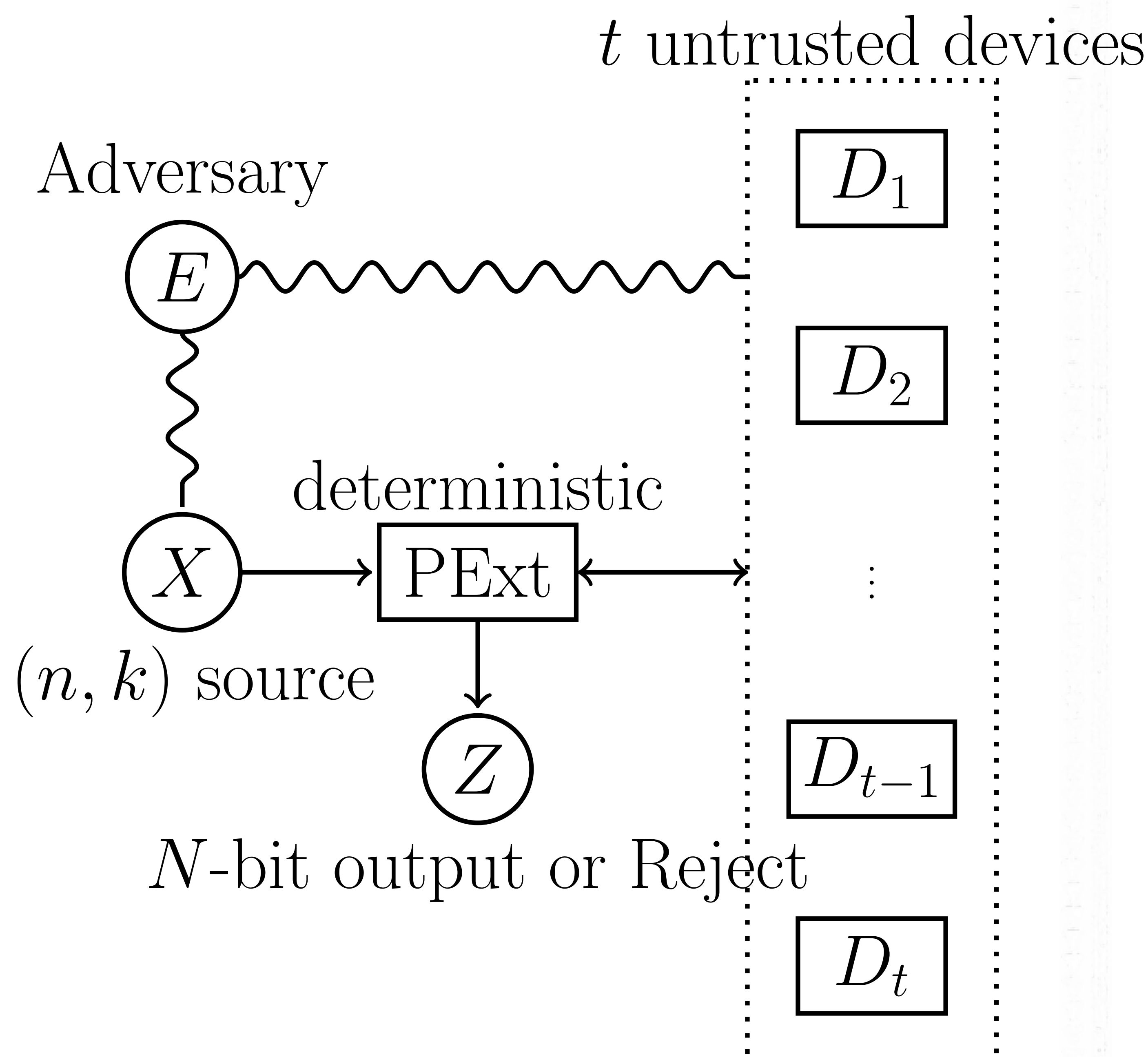
Goals for physical extractors

1. **Security: quantum**



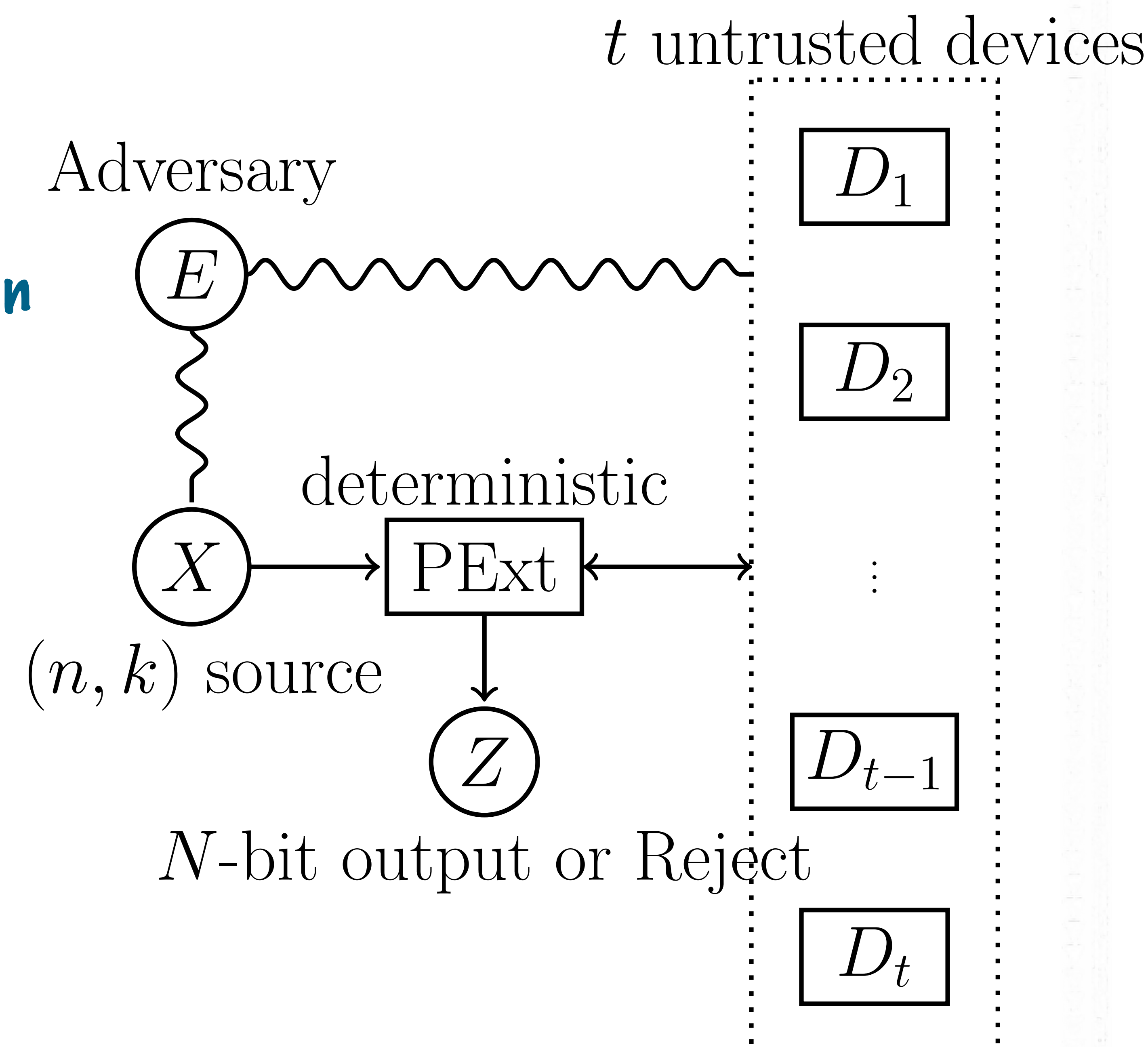
Goals for physical extractors

1. Security: quantum
2. Quality: small errors



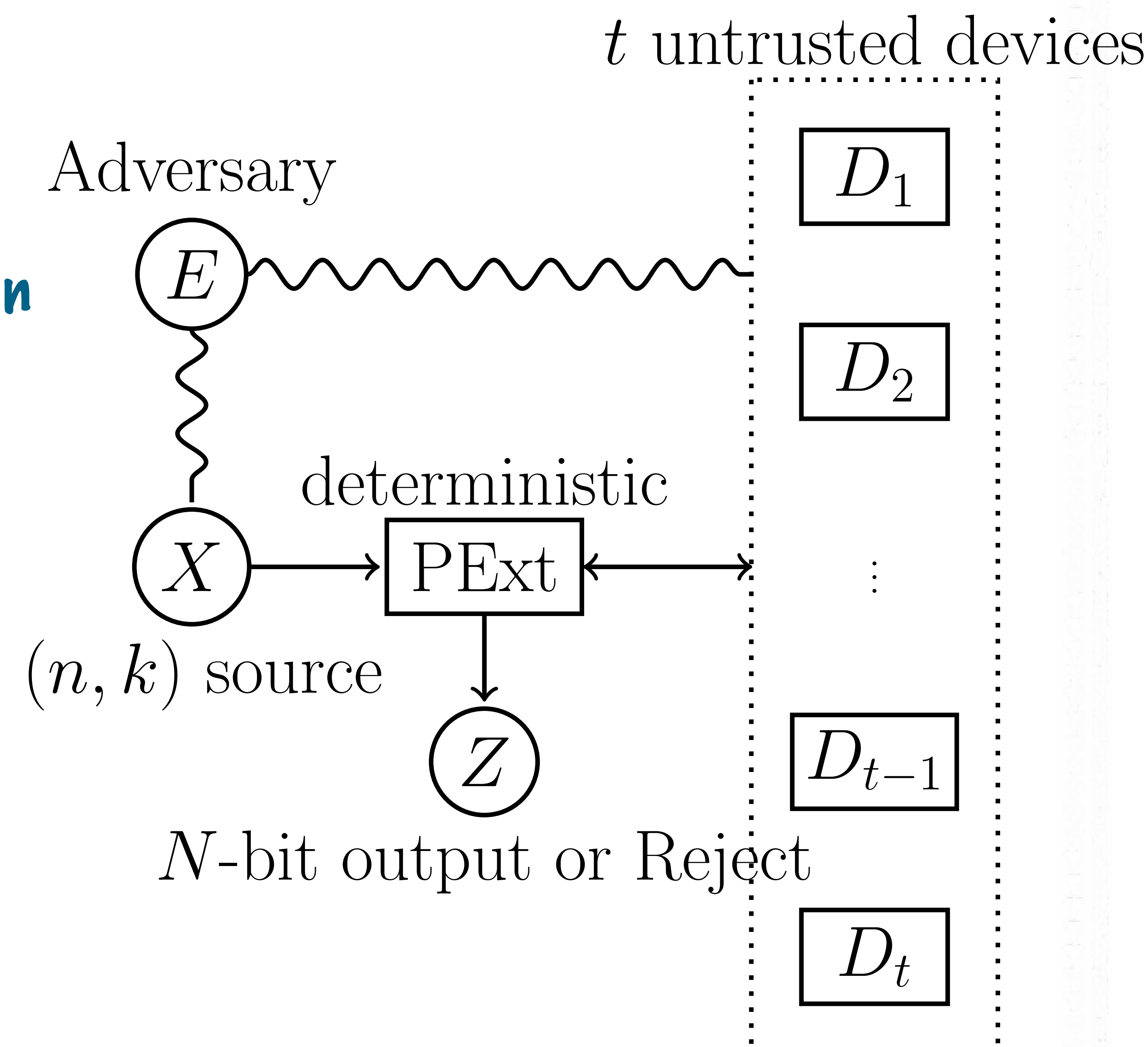
Goals for physical extractors

1. Security: quantum
2. Quality: small errors
3. Output length: "all" randomness in devices



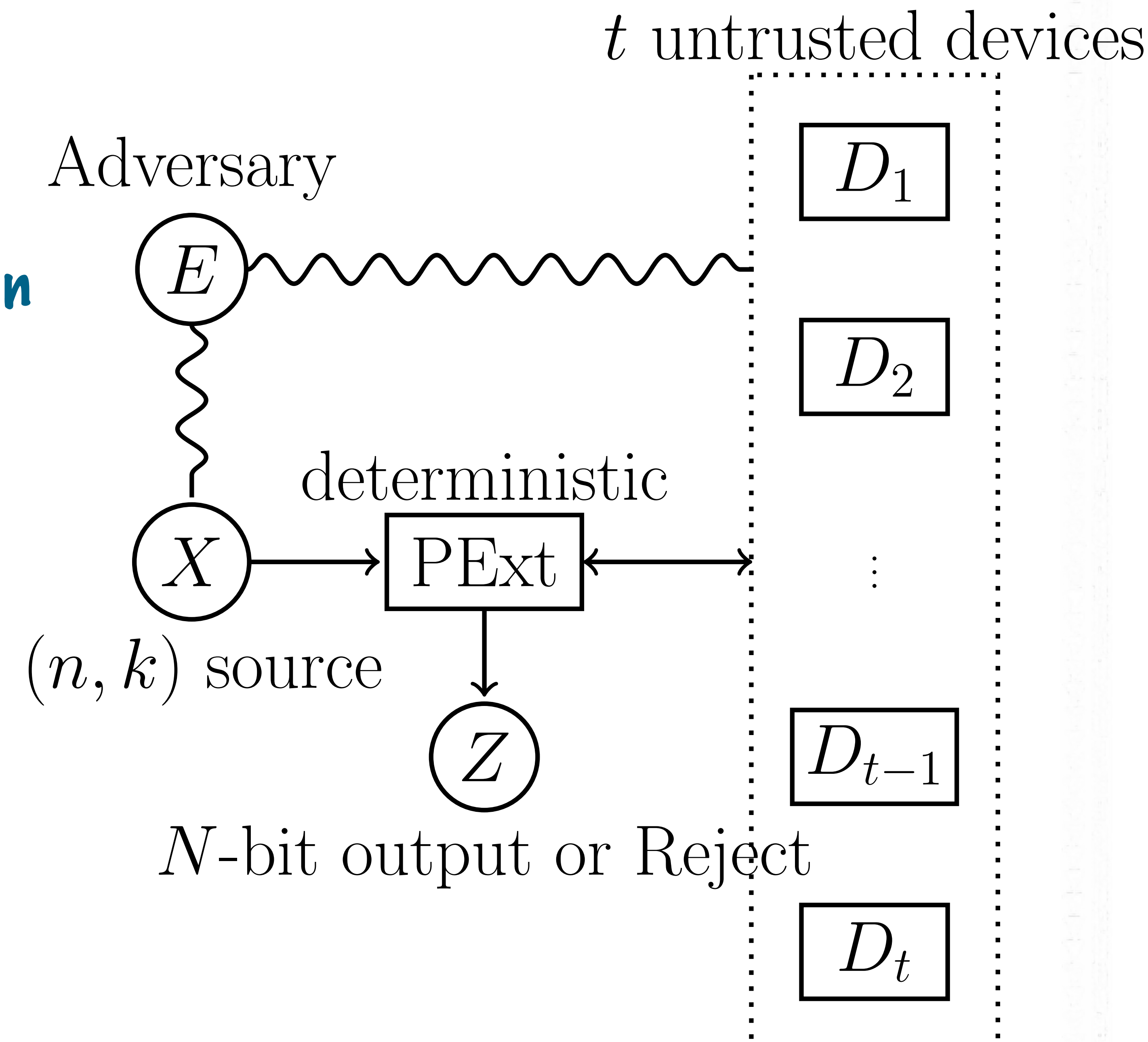
Goals for physical extractors

1. Security: quantum
2. Quality: small errors
3. Output length: "all" randomness in devices
4. Classical source: arbitrary min-entropy



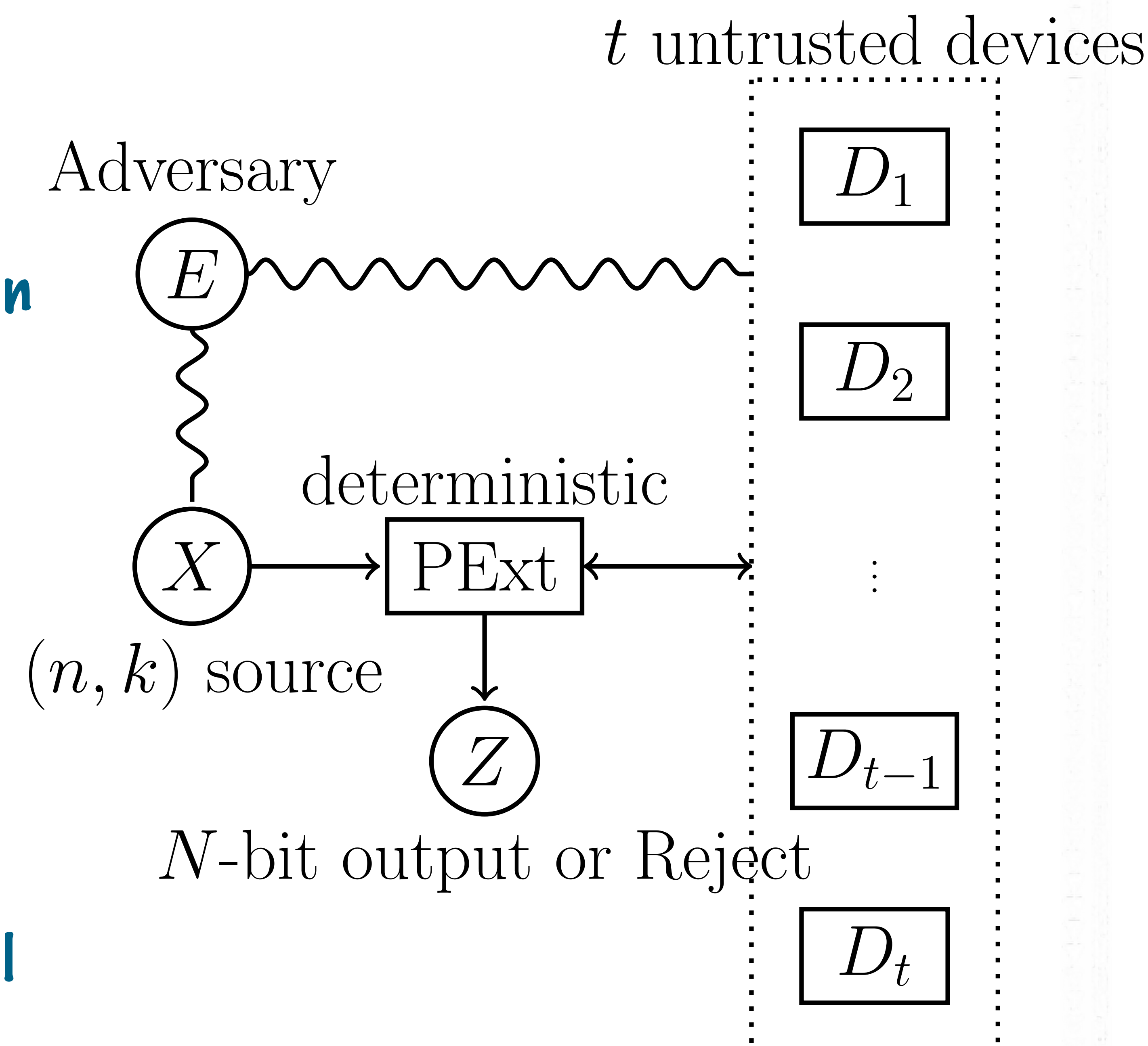
Goals for physical extractors

1. Security: quantum
2. Quality: small errors
3. Output length: "all" randomness in devices
4. Classical source: arbitrary min-entropy
5. Robustness: tolerate a constant level of noise



Goals for physical extractors

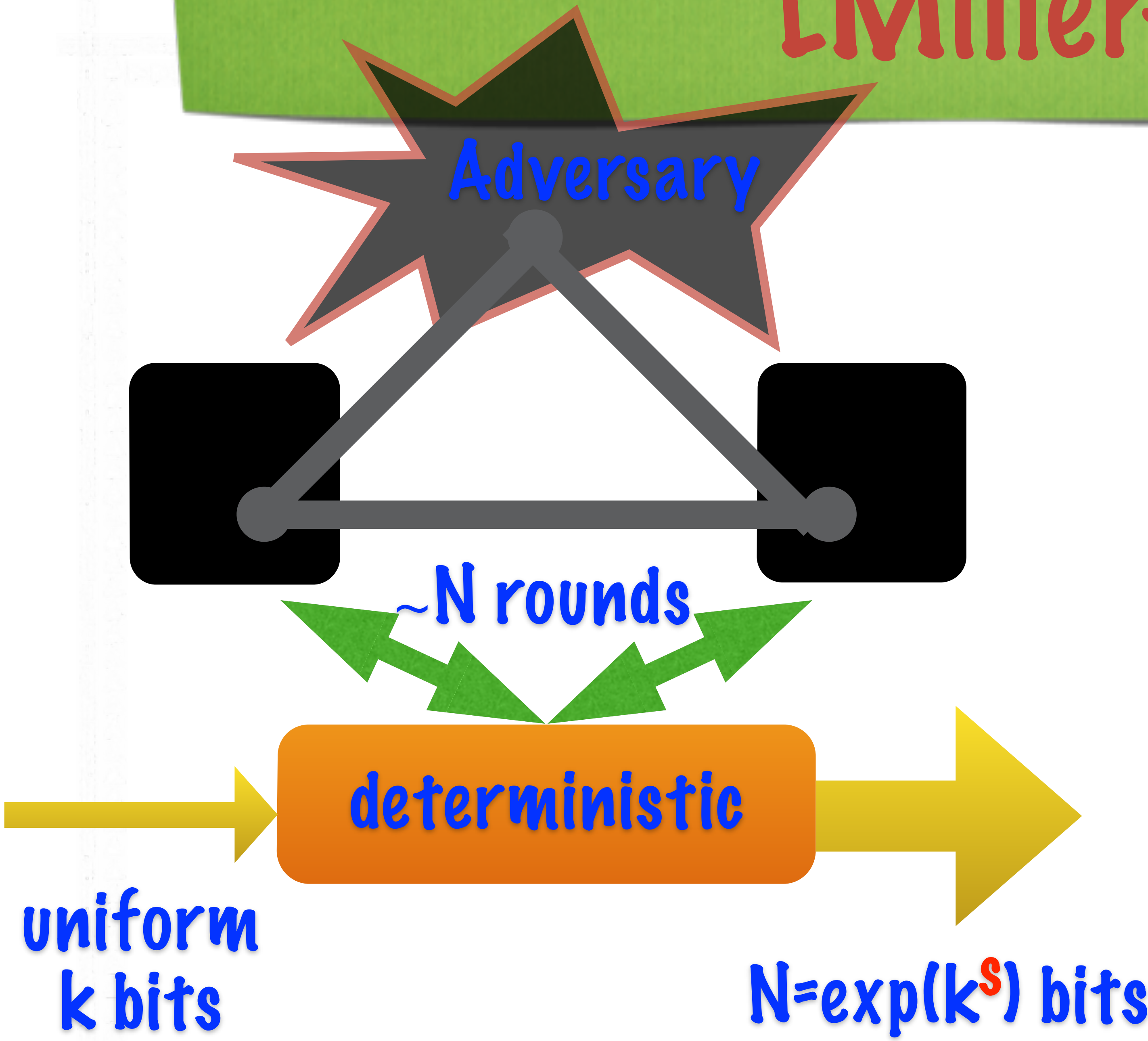
1. Security: quantum
2. Quality: small errors
3. Output length: "all" randomness in devices
4. Classical source: arbitrary min-entropy
5. Robustness: tolerate a constant level of noise
6. Efficiencies: Quantum memory, number of devices, computational complexity



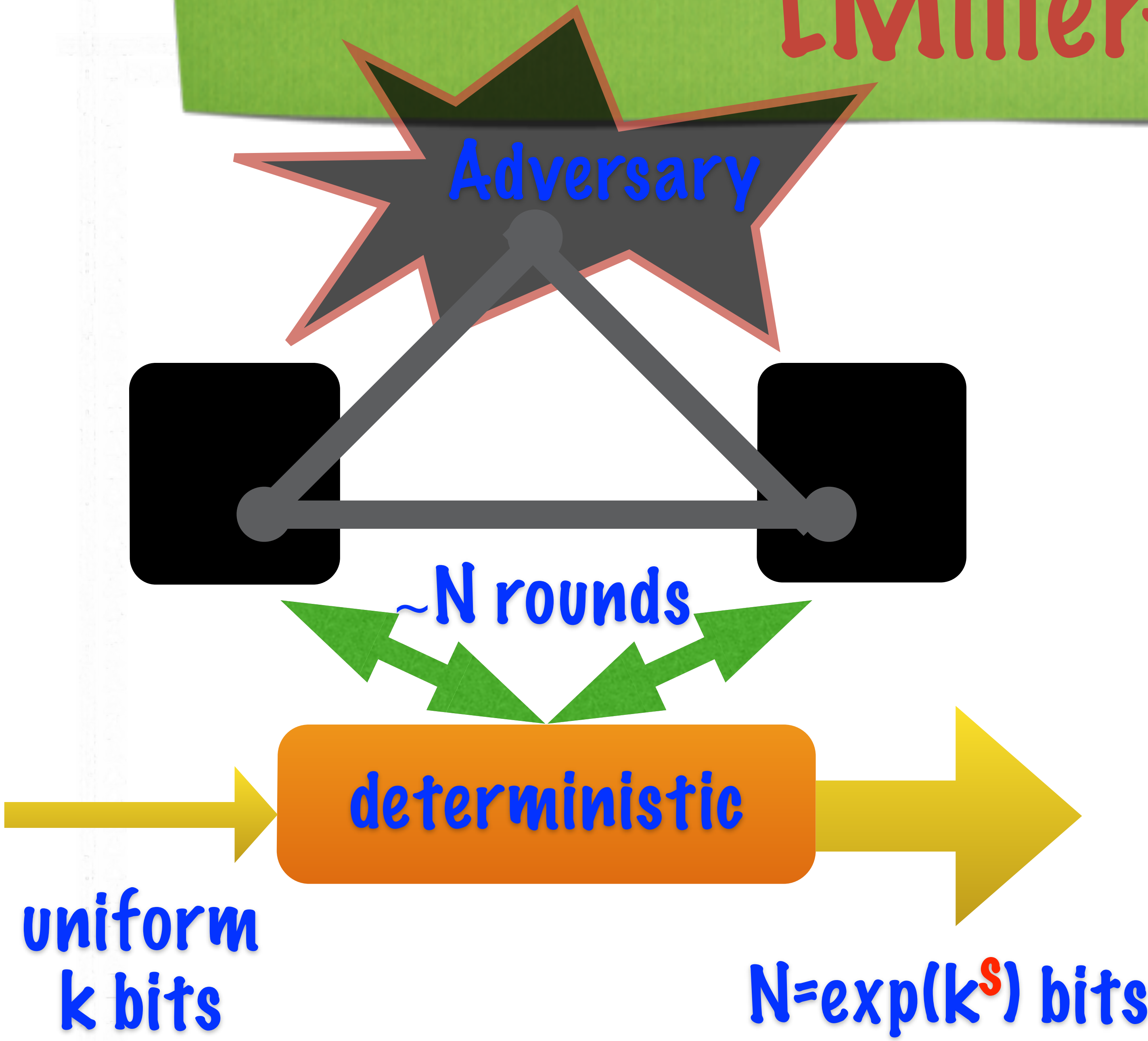
Open problems::Physical Extractors

Result: seeded extraction [Miller-Shi]

Result: seeded extraction [Miller-Shi]

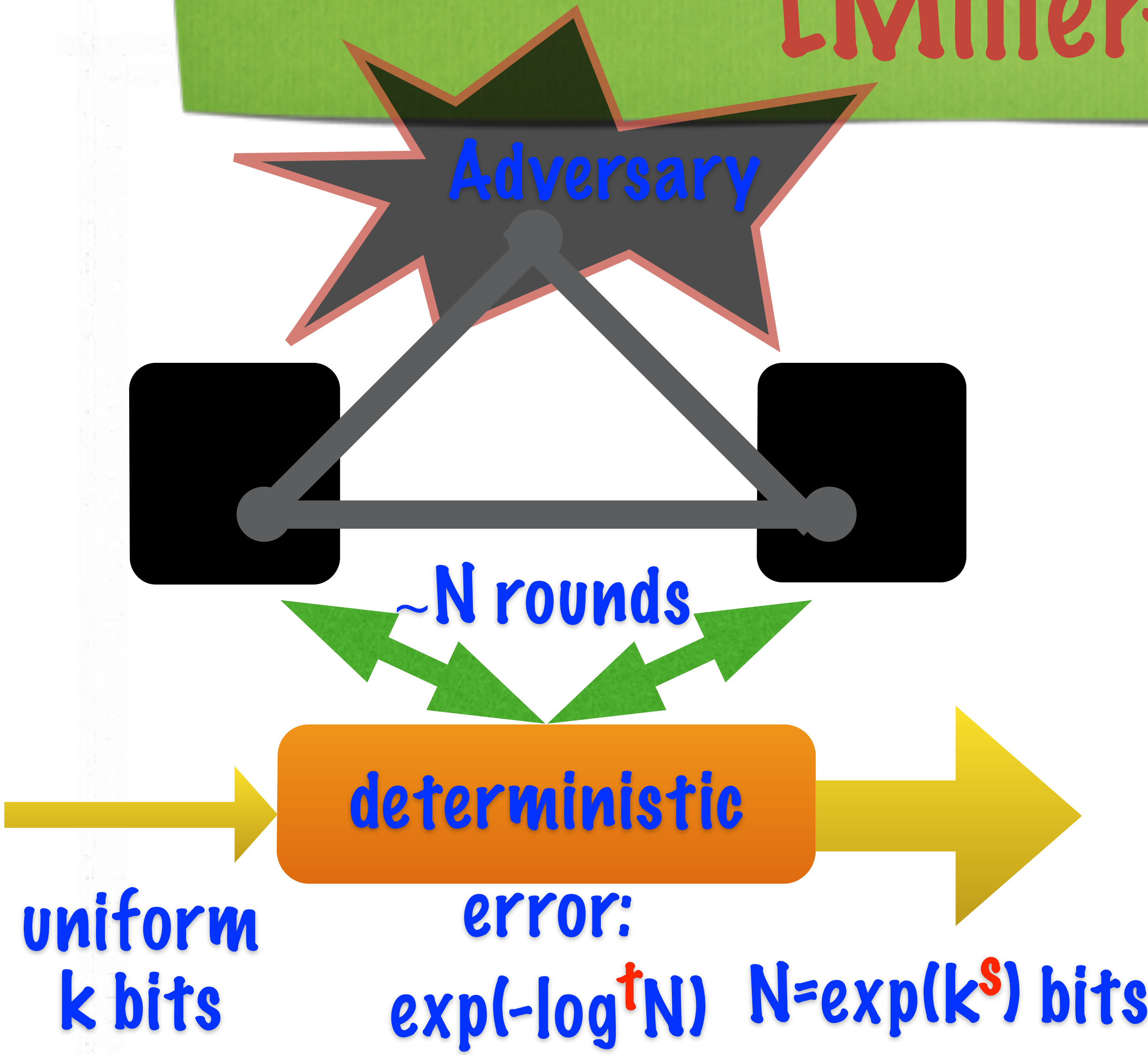


Result: seeded extraction [Miller-Shi]



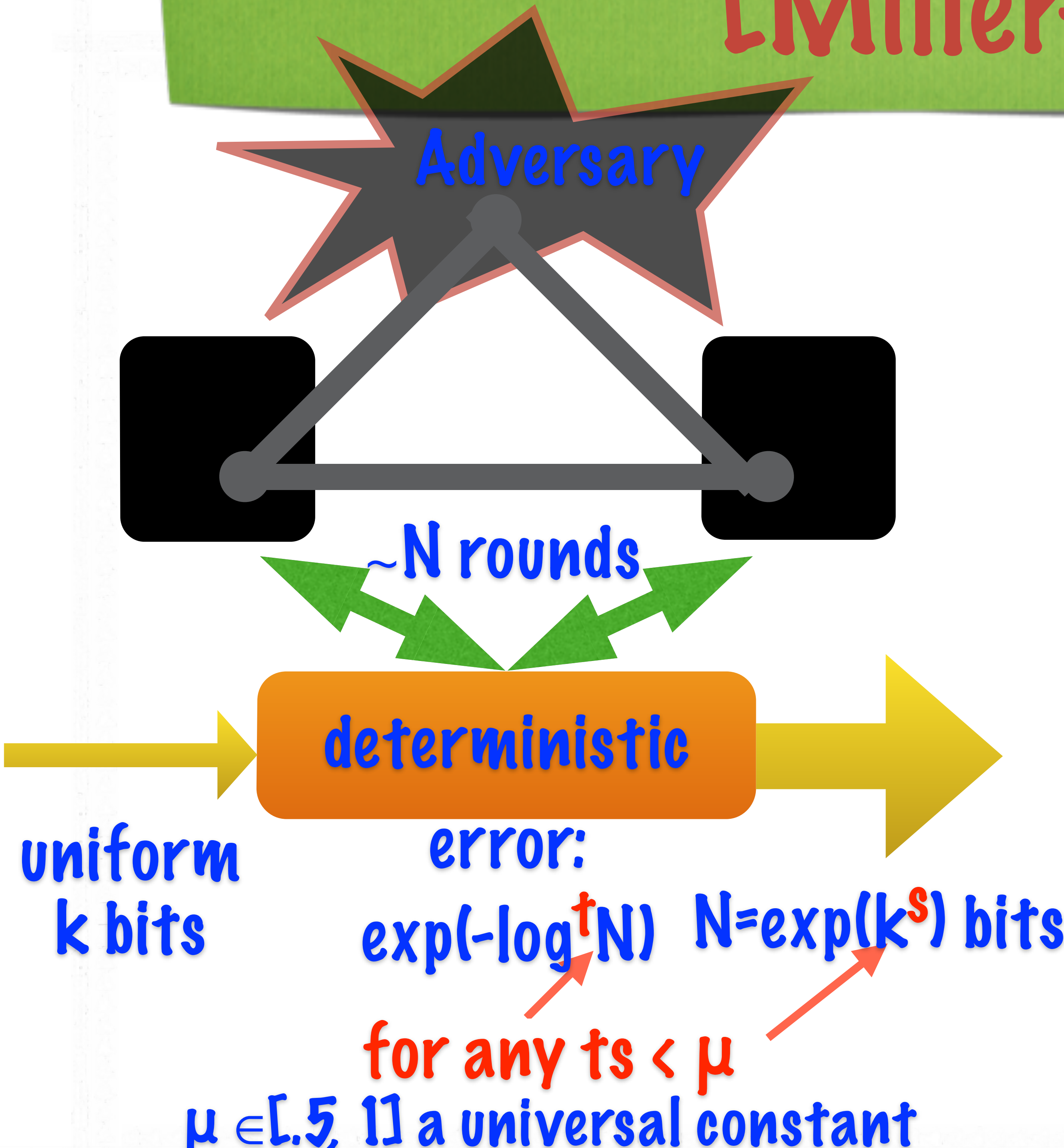
- 2 devices, exponential expanding, quantum security (match VV'12)

Result: seeded extraction [Miller-Shi]



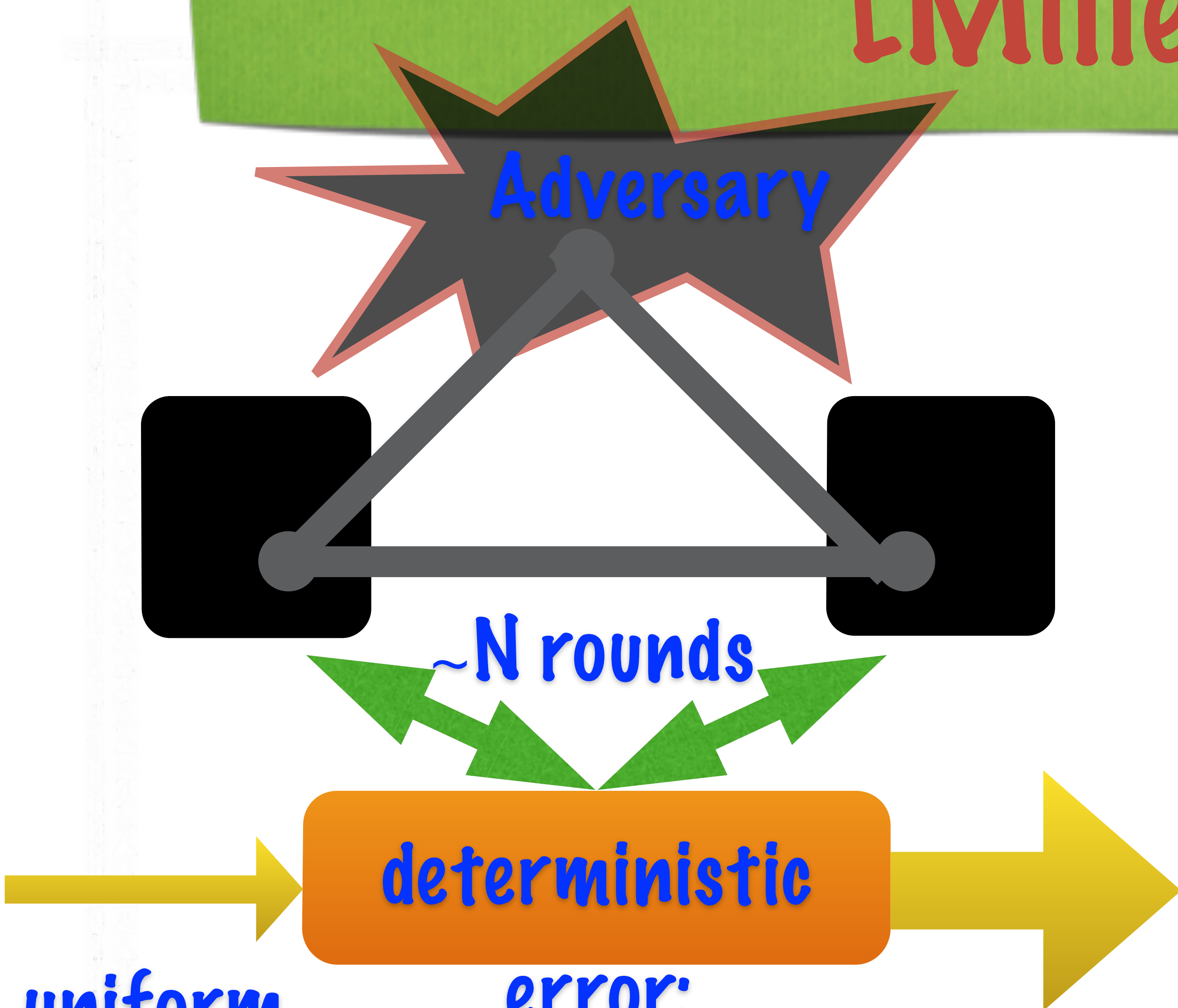
- 2 devices, exponential expanding, quantum security (match VV'12)
- Cryptographic security: errors = negligible in running time

Result: seeded extraction [Miller-Shi]



- 2 devices, exponential expanding, quantum security (match VV'12)
- Cryptographic security: errors = negligible in running time

Result: seeded extraction [Miller-Shi]



uniform k bits

error: $\exp(-\log^t N)$

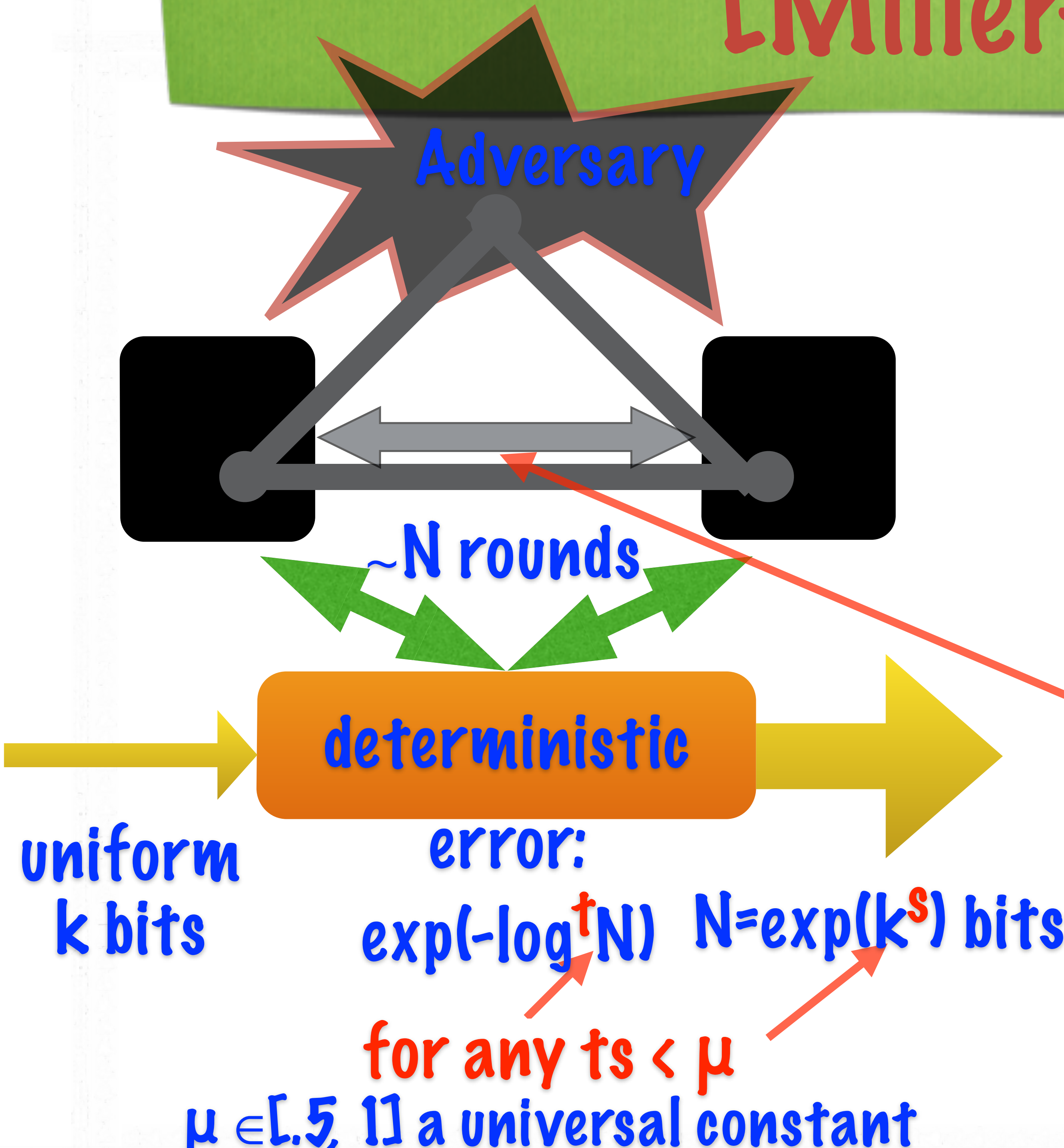
$N = \exp(k^s)$ bits

for any $ts < \mu$

$\mu \in [.5, 1]$ a universal constant

- 2 devices, exponential expanding, quantum security (match VV'12)
- Cryptographic security: errors = negligible in running time
- Robustness: constant level of noise

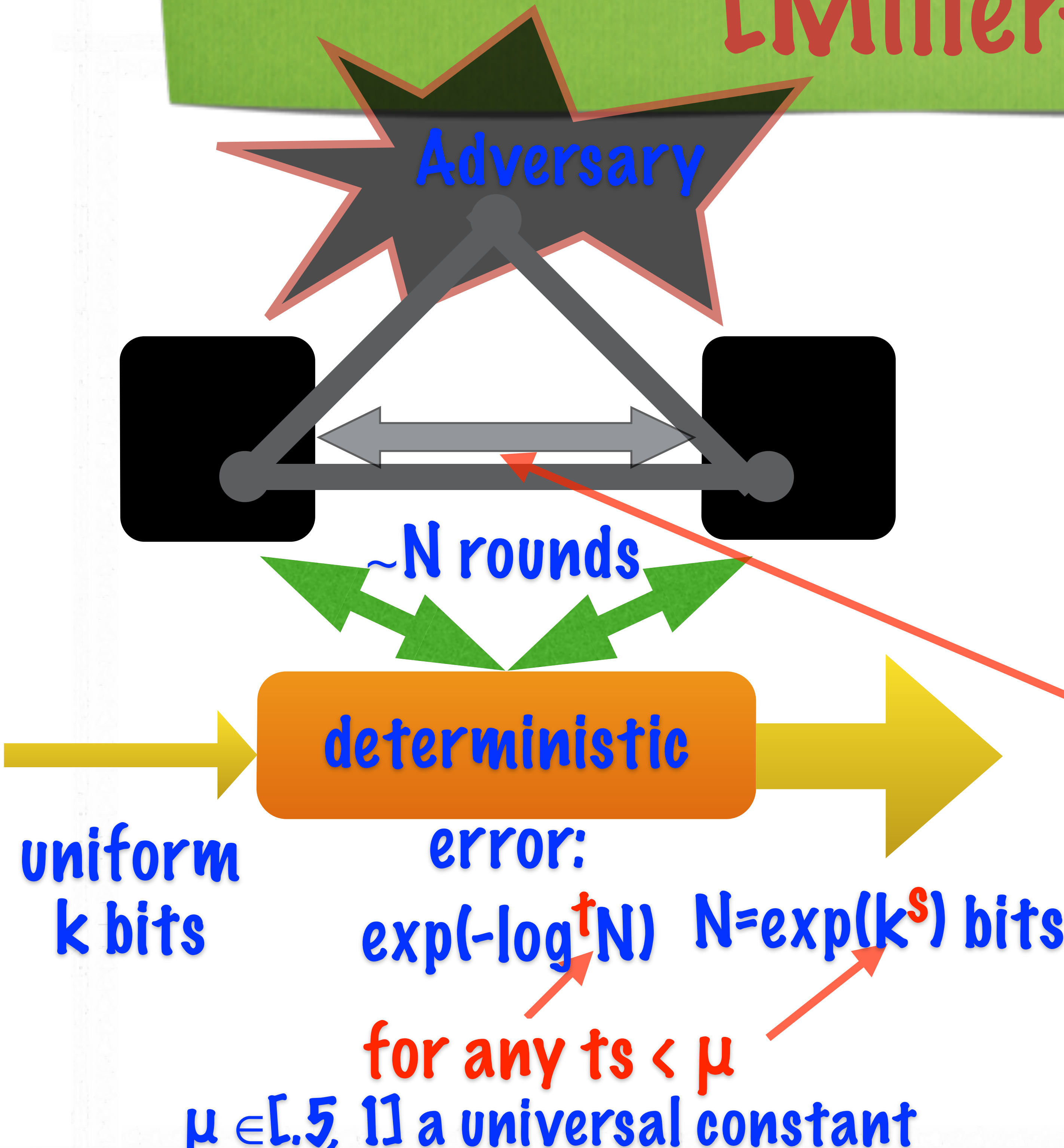
Result: seeded extraction [Miller-Shi]



- 2 devices, exponential expanding, quantum security (match VV'12)
- **Cryptographic security**: errors = negligible in running time
- **Robustness**: constant level of noise
- **Unit size quantum memory**: allow in-between-rounds of communication

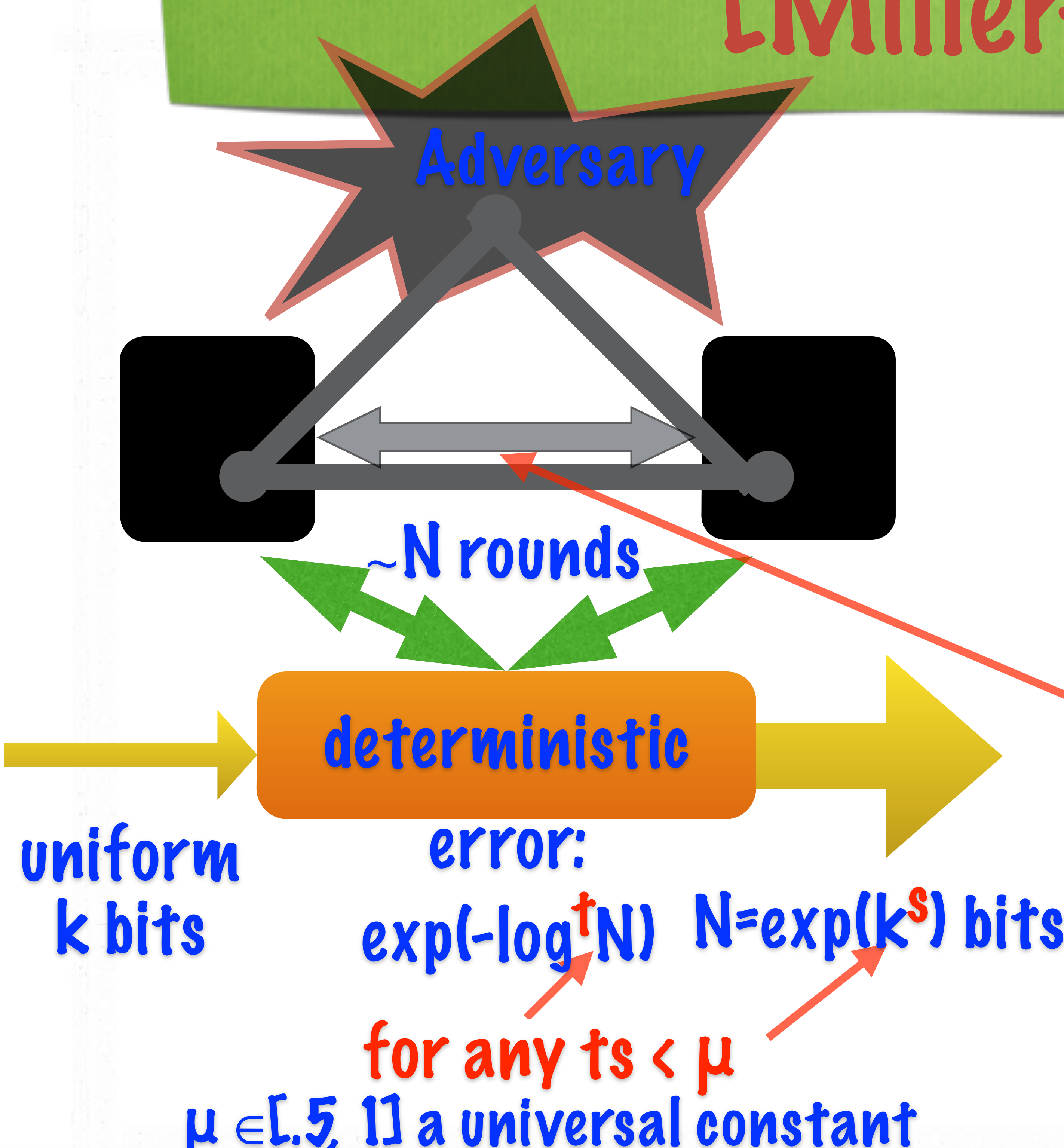
Model and Results::seeded extraction

Result: seeded extraction [Miller-Shi]



- 2 devices, exponential expanding, quantum security (match VV'12)
- Cryptographic security: errors = negligible in running time
- Robustness: constant level of noise
- Unit size quantum memory: allow in-between-rounds of communication
- Flexibility in building-blocks

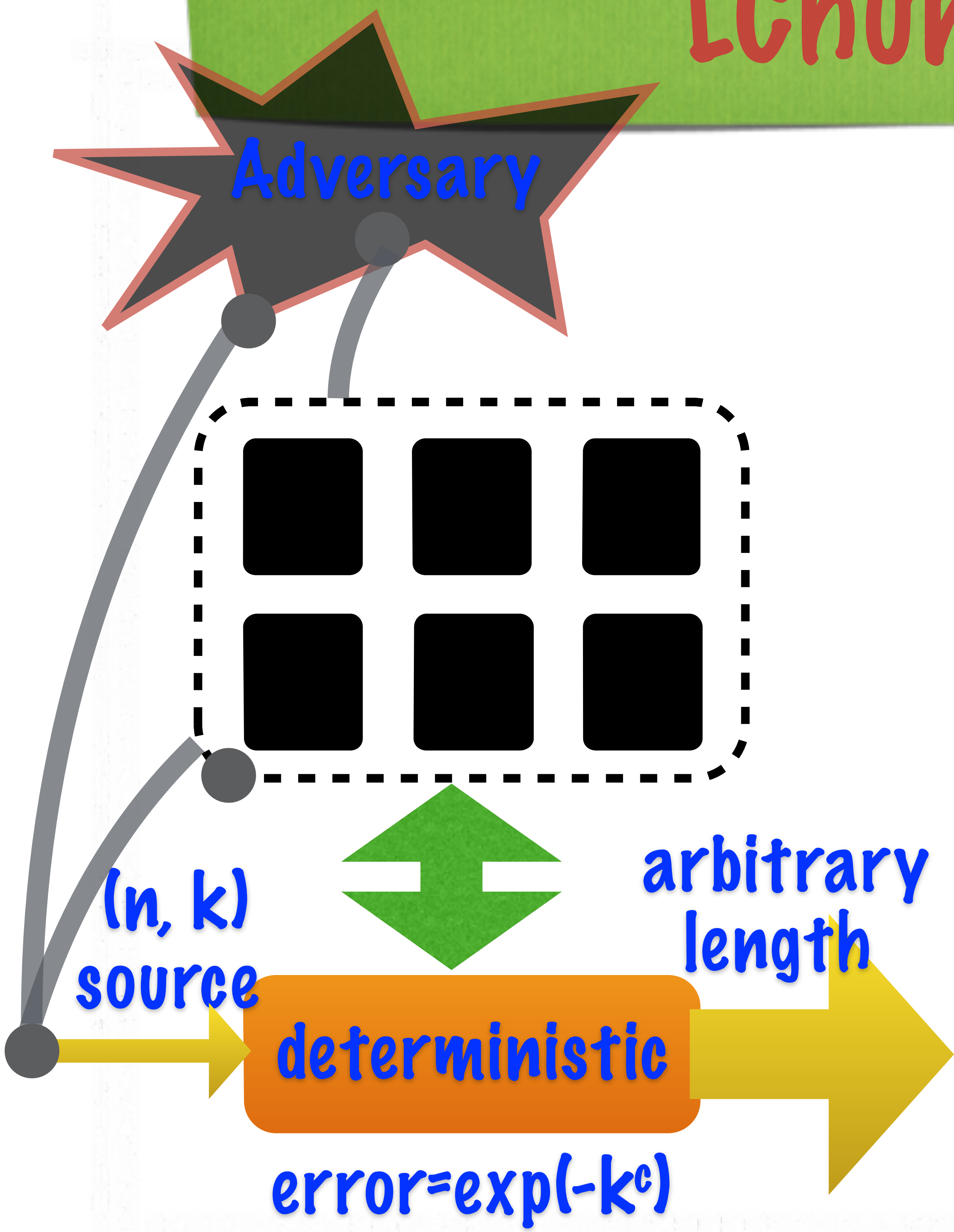
Result: seeded extraction [Miller-Shi]



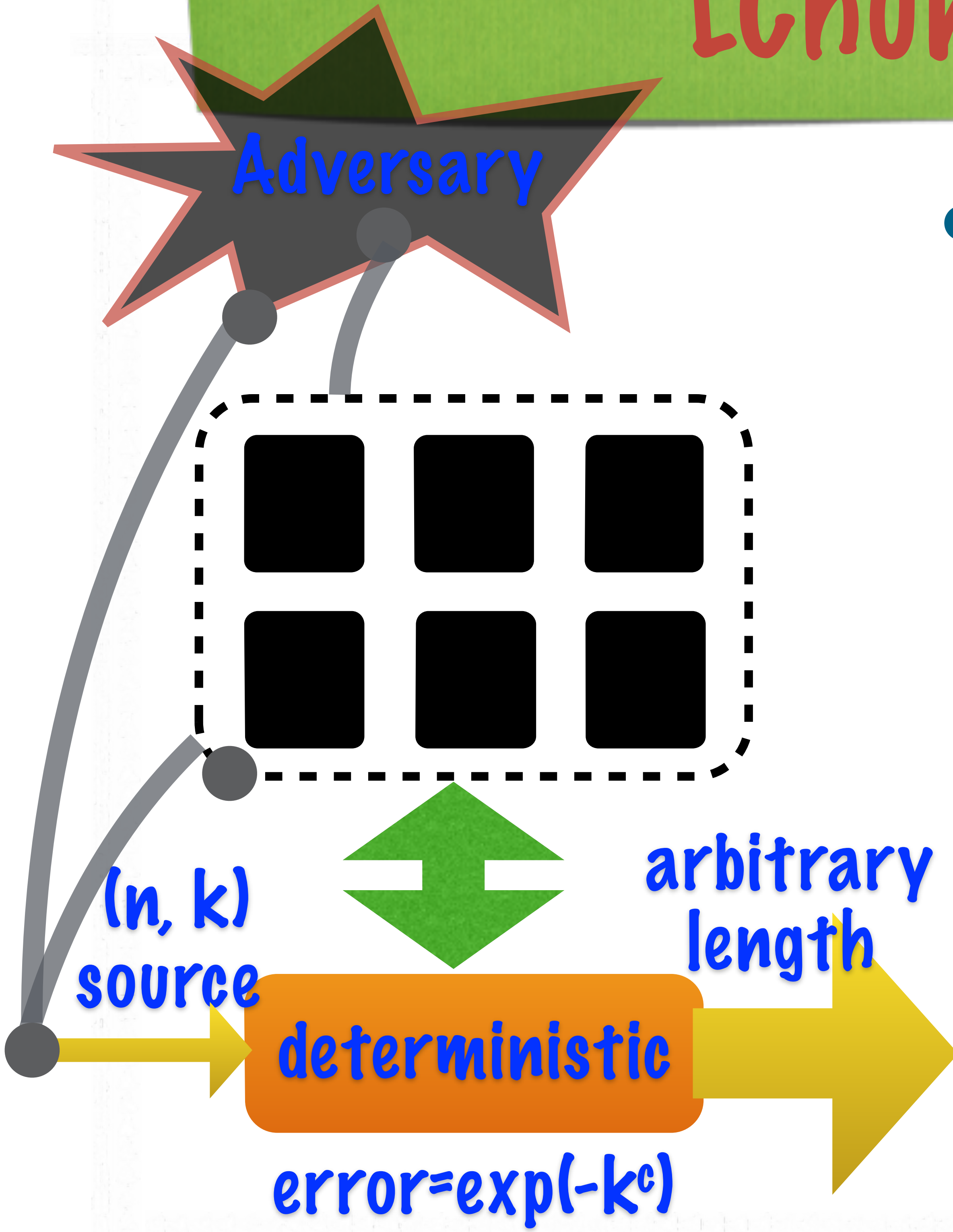
- 2 devices, exponential expanding, quantum security (match VV'12)
- Cryptographic security: errors = negligible in running time
- Robustness: constant level of noise
- Unit size quantum memory: allow in-between-rounds of communication
- Flexibility in building-blocks
- New proof techniques

Model and Results::seeded extraction

Result: seedless extraction [Chung-Shi-Wu]

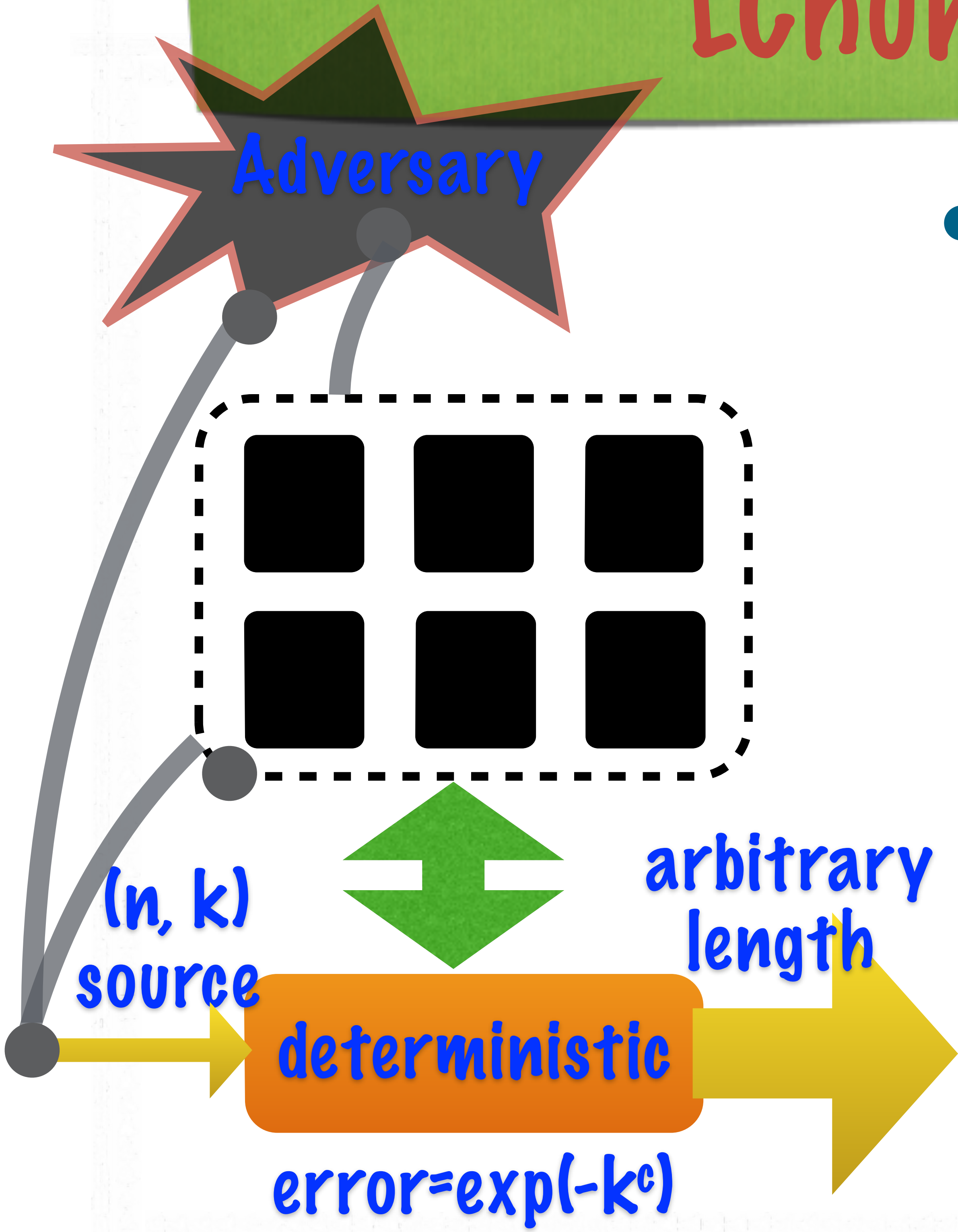


Result: seedless extraction [Chung-Shi-Wu]



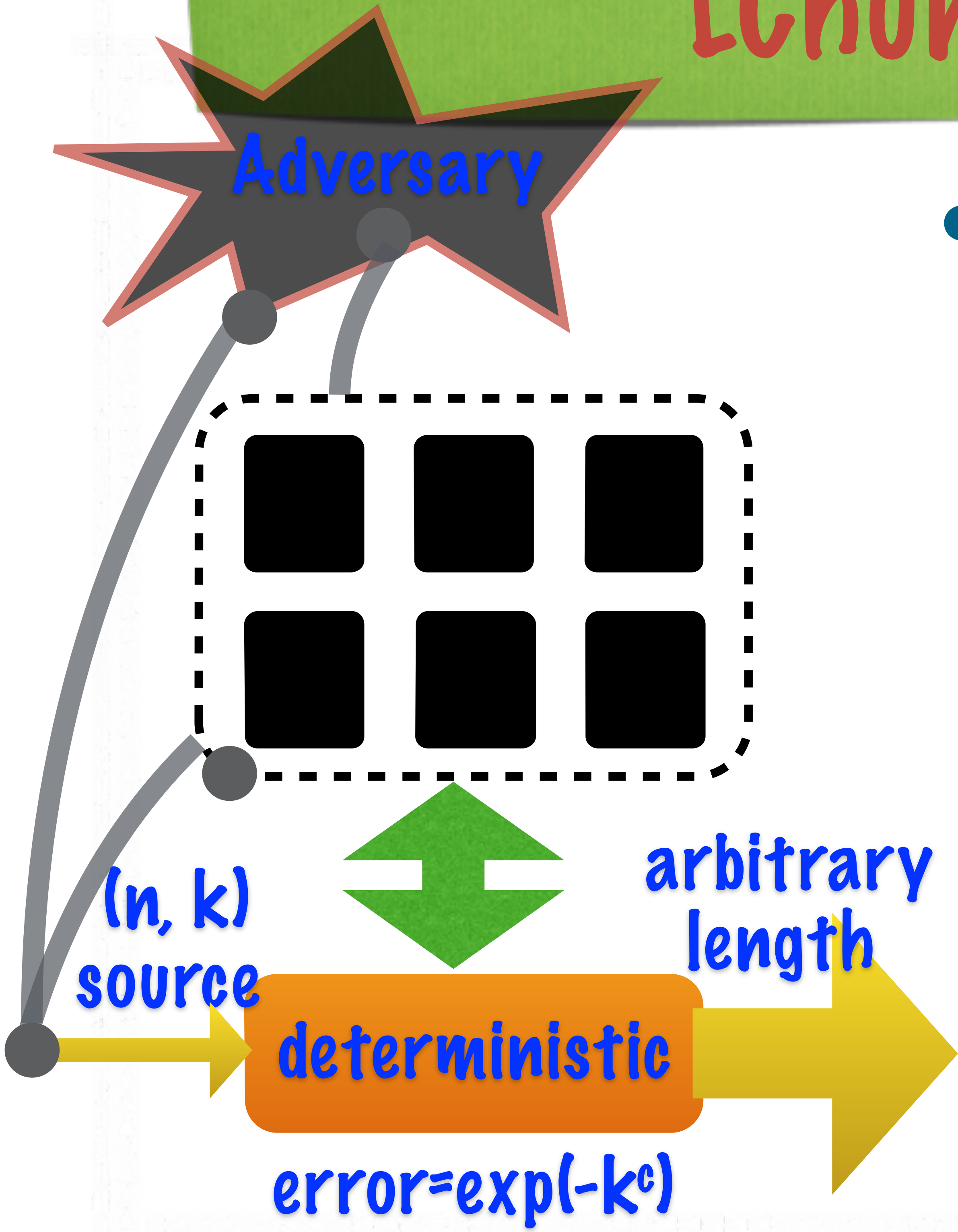
- Use just one min-entropy source

Result: seedless extraction [Chung-Shi-Wu]



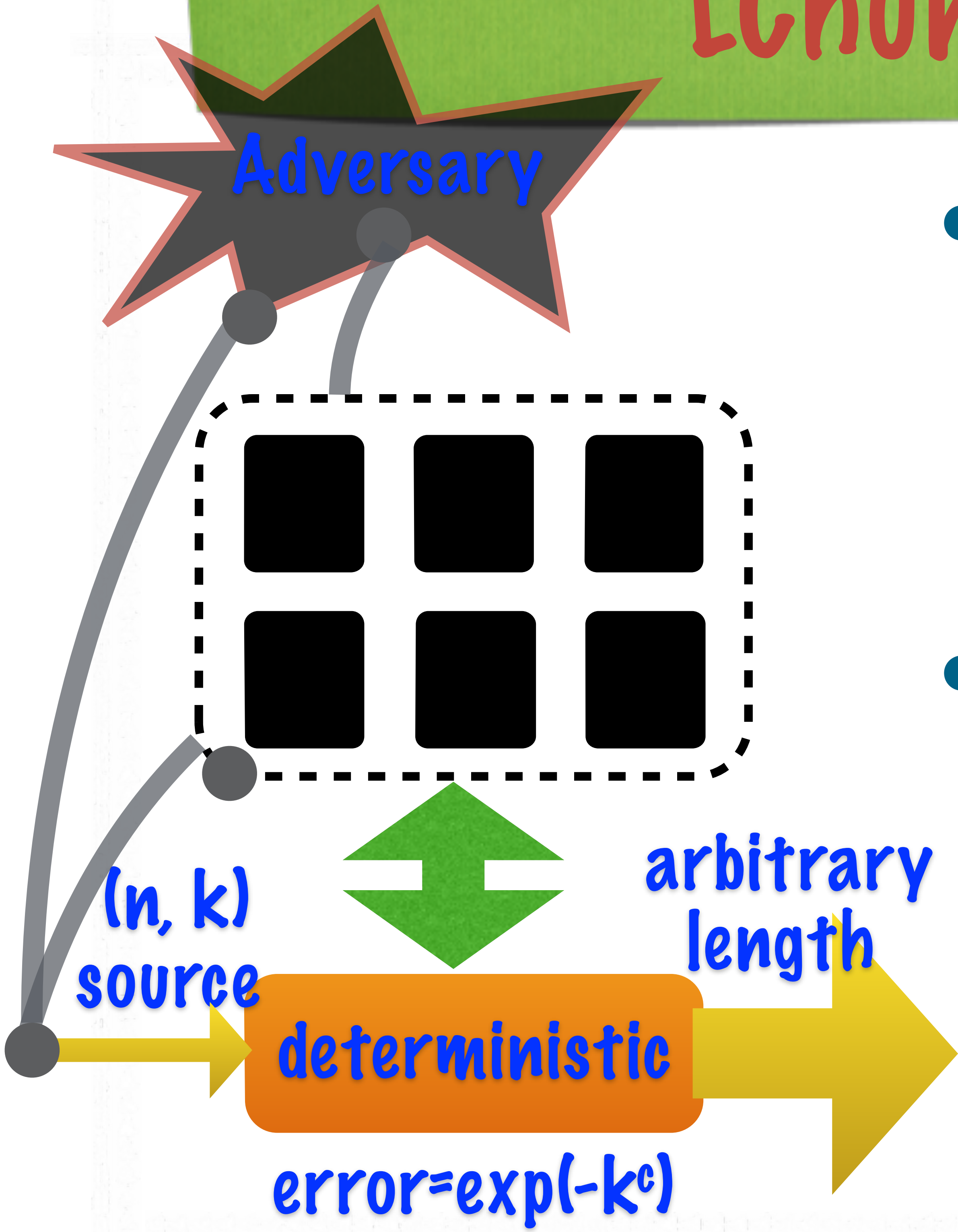
- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices

Result: seedless extraction [Chung-Shi-Wu]



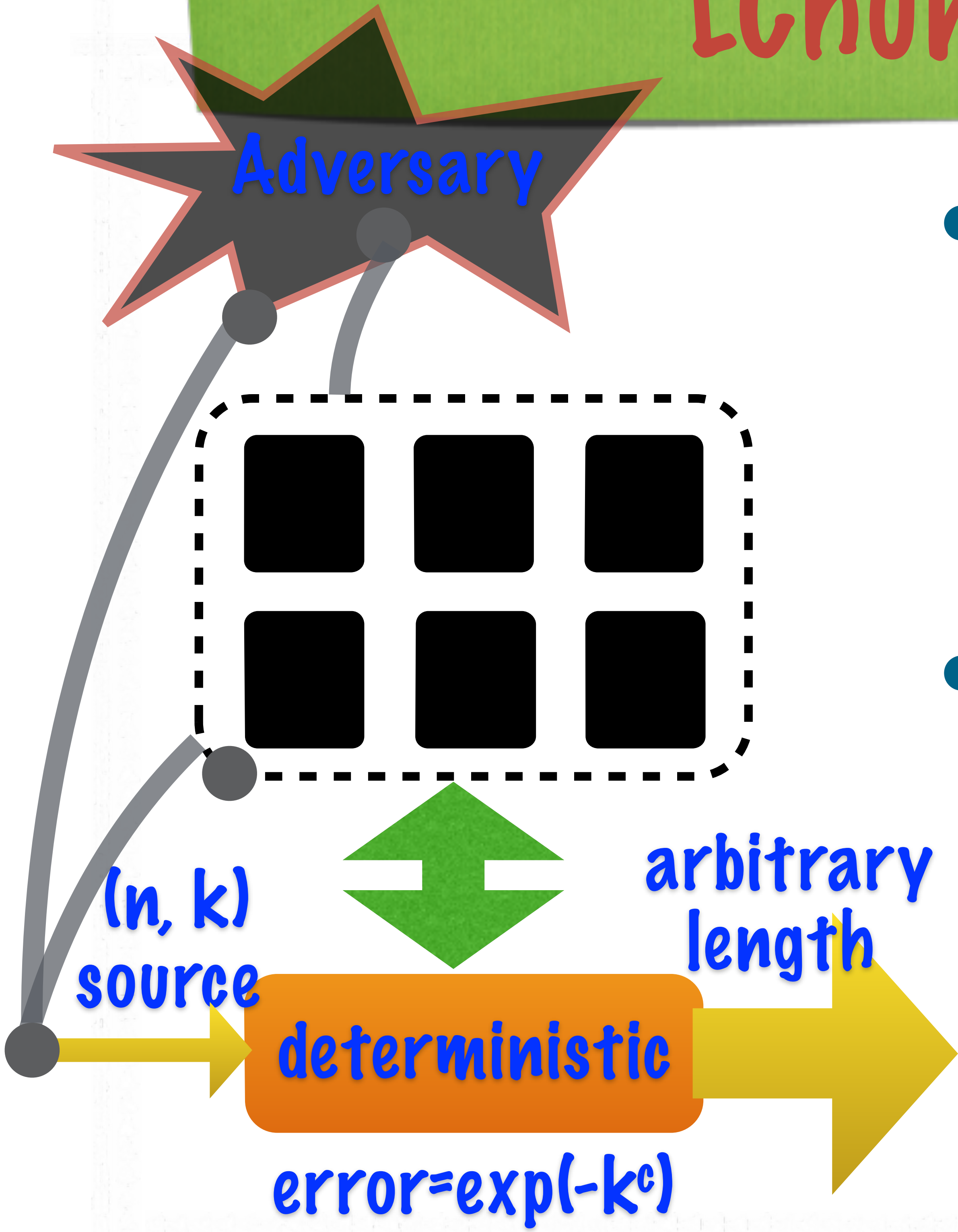
- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices
  - k can be arbitrarily small, e.g. a constant

Result: seedless extraction [Chung-Shi-Wu]



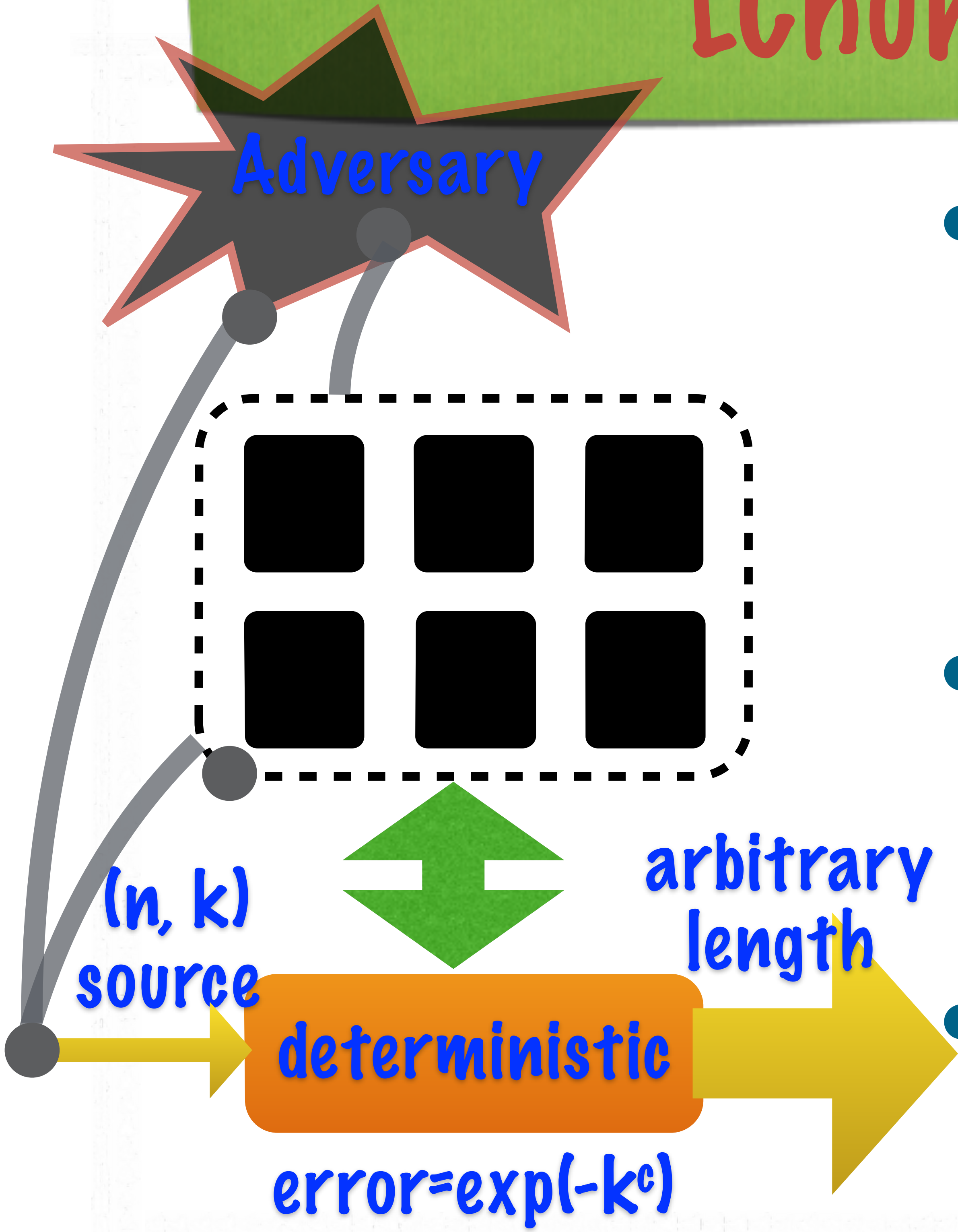
- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices
  - k can be arbitrarily small, e.g. a constant
- A reduction of seedless extraction to seeded extraction

Result: seedless extraction [Chung-Shi-Wu]



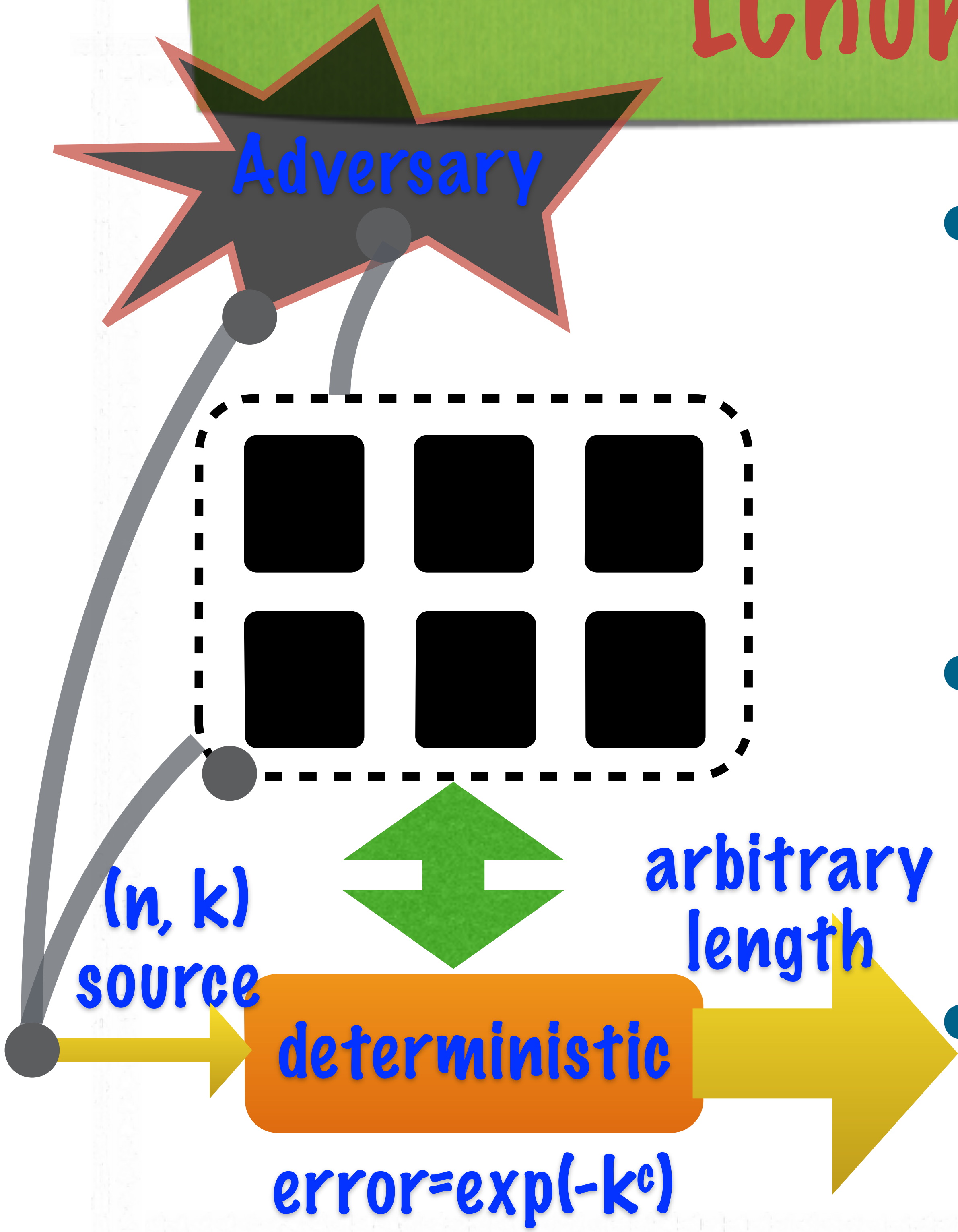
- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices
  - k can be arbitrarily small, e.g. a constant
- A reduction of seedless extraction to seeded extraction
  - Tolerate constant noise by using Miller-Shi or Vazirani-Vidick (qkd)

Result: seedless extraction [Chung-Shi-Wu]



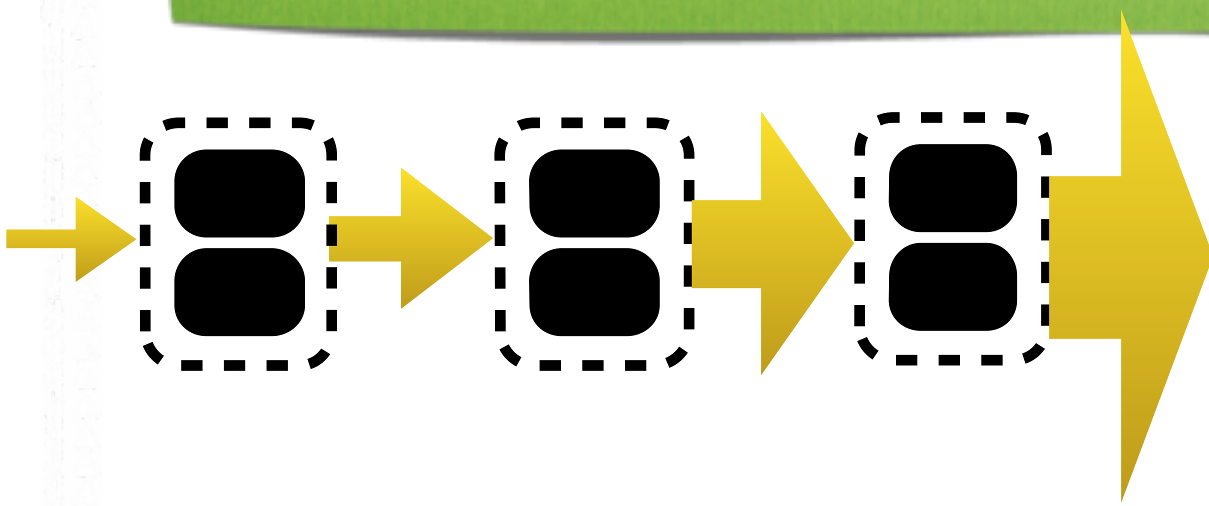
- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices
  - k can be arbitrarily small, e.g. a constant
- A reduction of seedless extraction to seeded extraction
  - Tolerate constant noise by using Miller-Shi or Vazirani-Vidick (qkd)
- Tradeoff between error and #devices

Result: seedless extraction [Chung-Shi-Wu]

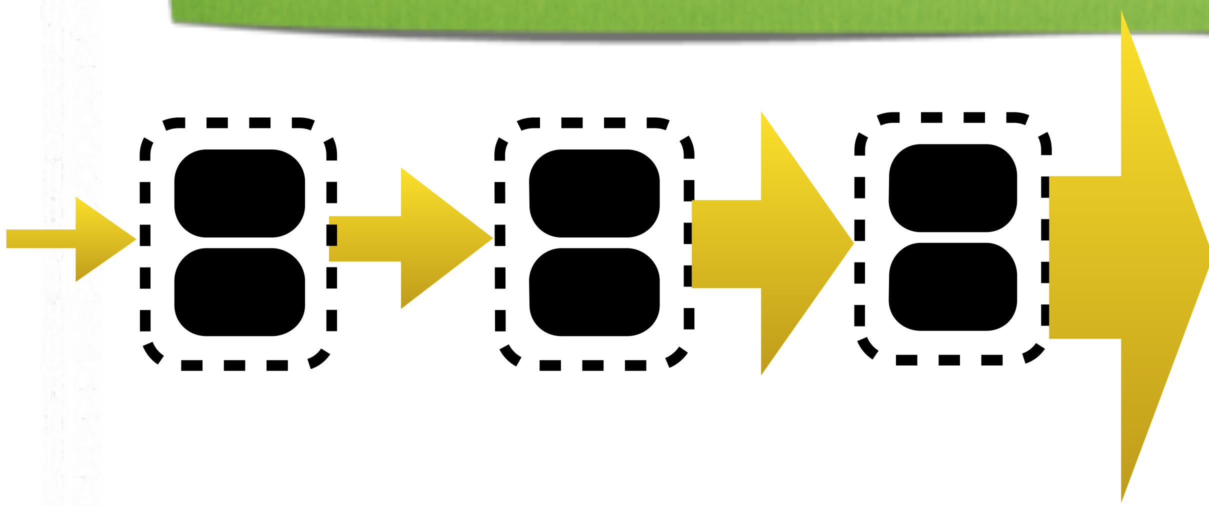


- Use just one min-entropy source
  - can be known to Adversary: min-entropy w.r.t. devices
  - k can be arbitrarily small, e.g. a constant
- A reduction of seedless extraction to seeded extraction
  - Tolerate constant noise by using Miller-Shi or Vazirani-Vidick (qkd)
- Tradeoff between error and #devices
  - Error can be made close to optimal: $\exp(-k^c)$ (lower bound: 2^{-k})

Application: robust unbounded expansion [CSW+MS]

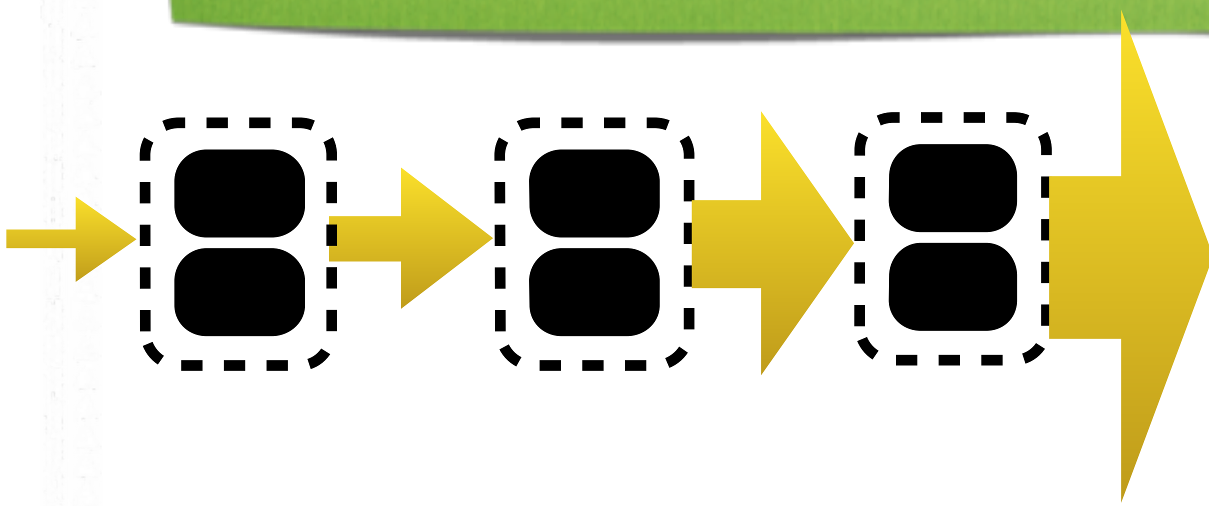


Application: robust unbounded expansion [CSW+MS]



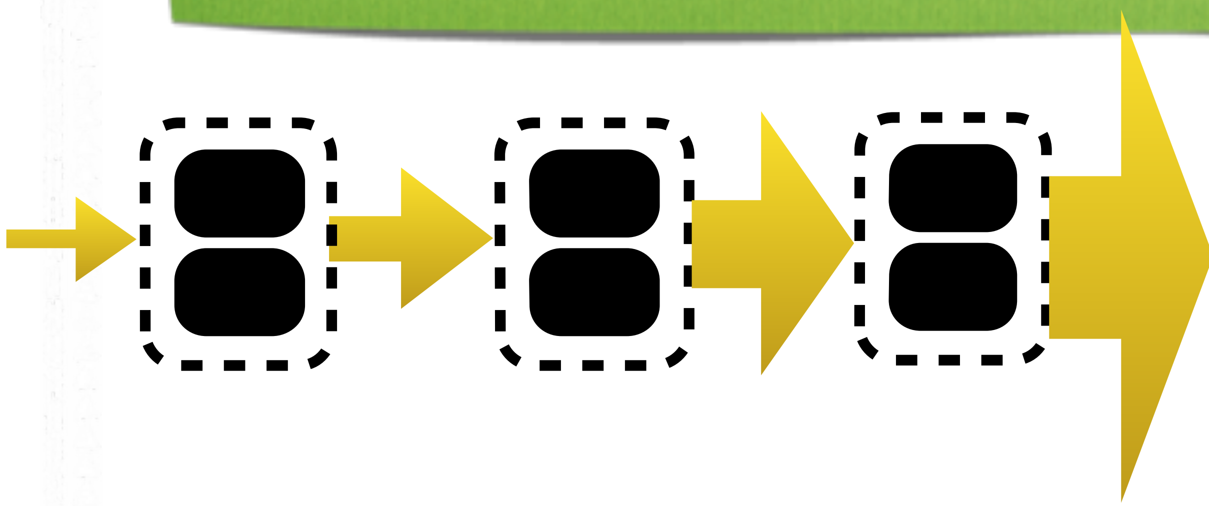
- Goal: k bits -> arbitrarily N-bits

Application: robust unbounded expansion [CSW+MS]



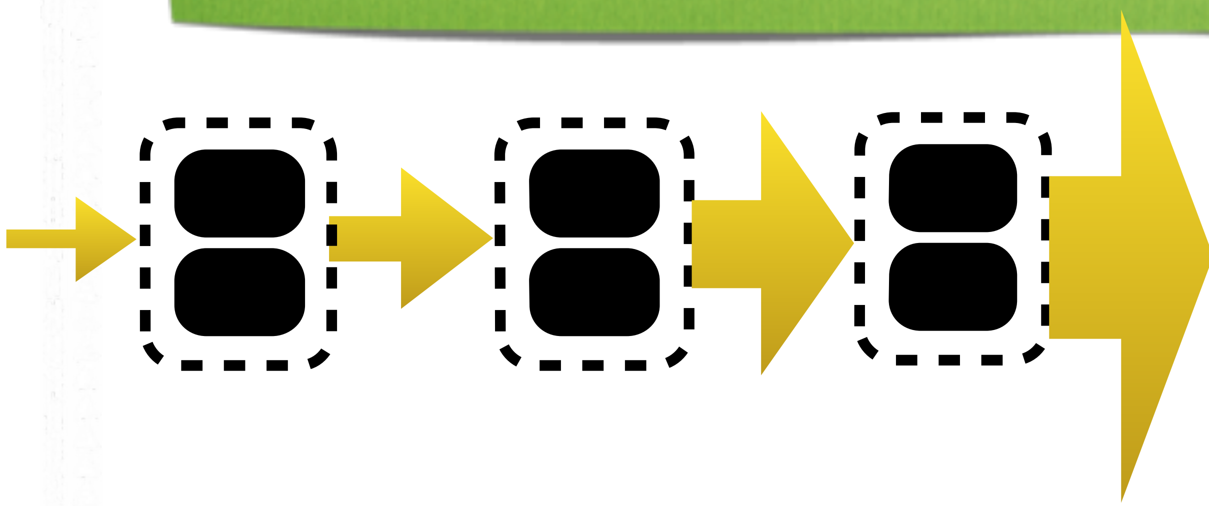
- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices

Application: robust unbounded expansion [CSW+MS]



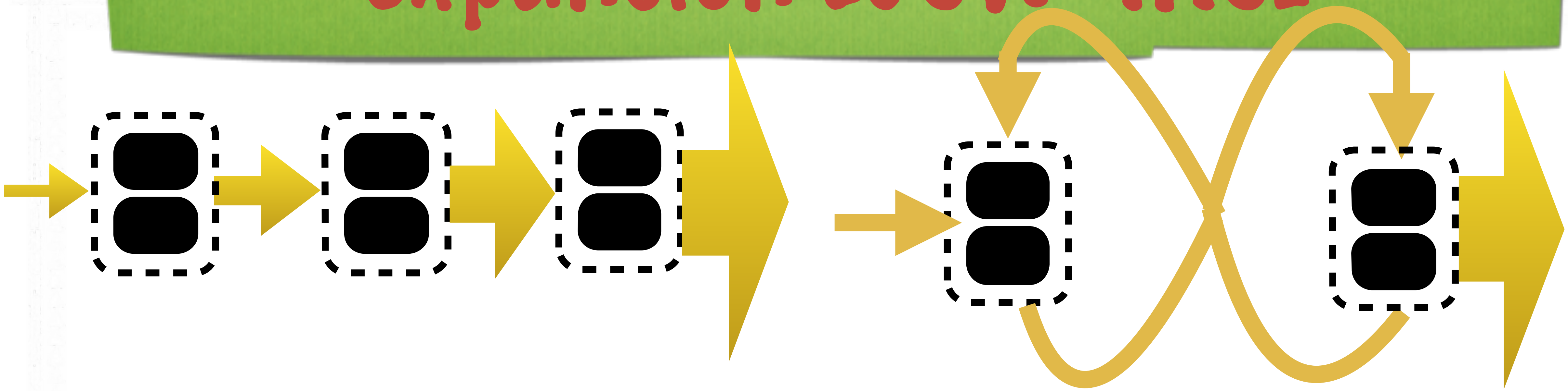
- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices
    - Robust by using Miller-Shi

Application: robust unbounded expansion [CSW+MS]



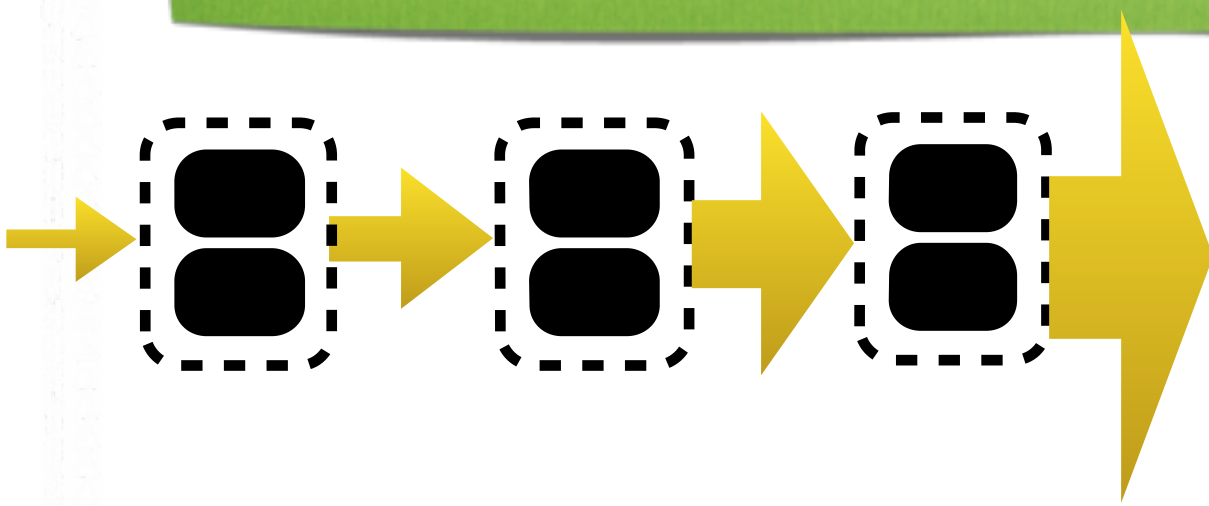
- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices
  - Robust by using Miller-Shi
  - error dominated by the first term

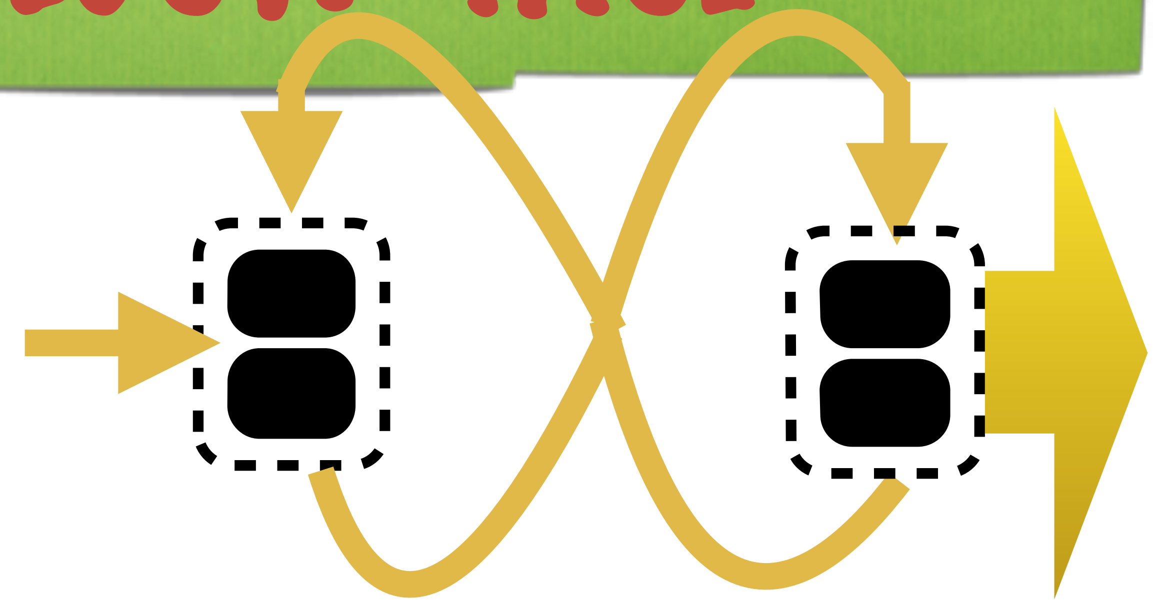
Application: robust unbounded expansion [CSW+MS]



- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices
  - Robust by using Miller-Shi
  - error dominated by the first term
- Constant number of devices through cross-feeding two expansion protocols [Fehr+'13]?

Application: robust unbounded expansion [CSW+MS]

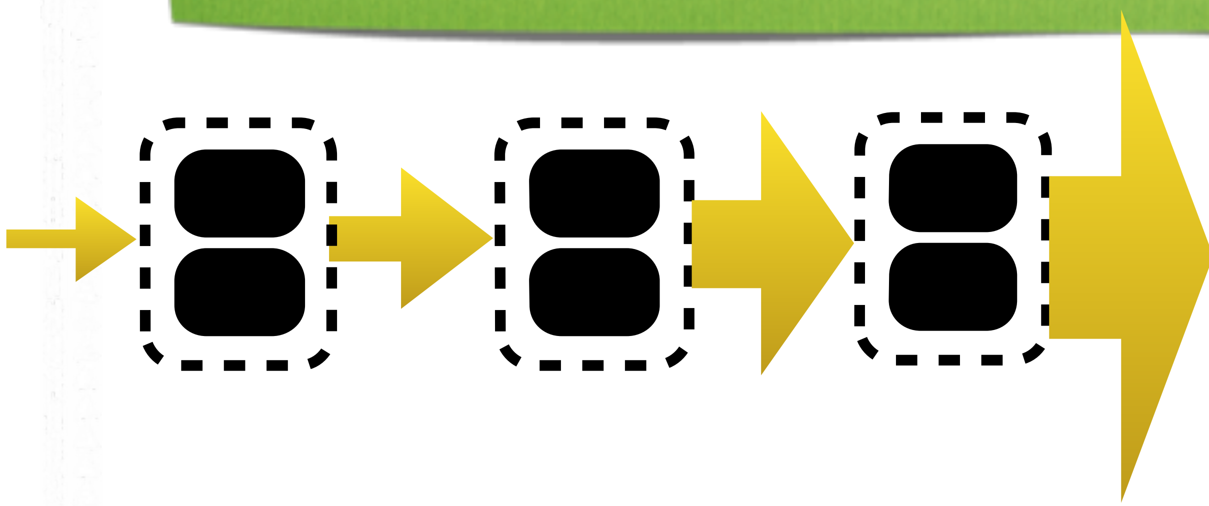


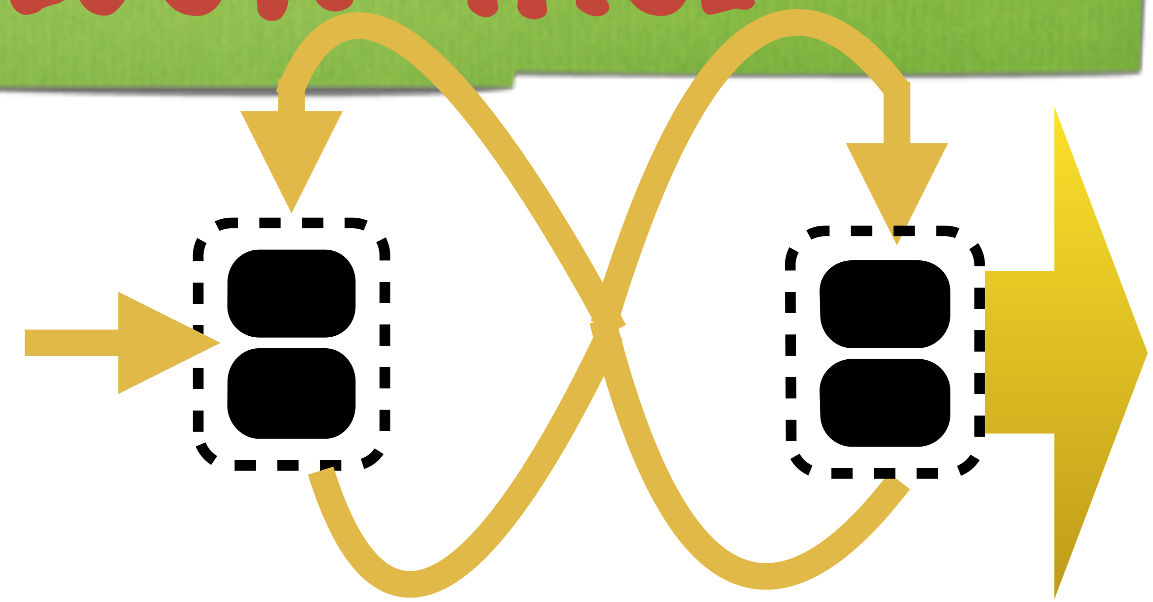


- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices
  - Robust by using Miller-Shi
  - error dominated by the first term
- Constant number of devices through cross-feeding two expansion protocols [Fehr+'13]?

- Yes: [Coudron-Yuen'13] based on VV'12+Reichardt-Unger-Vazirani'13: 8 devices, non-robust

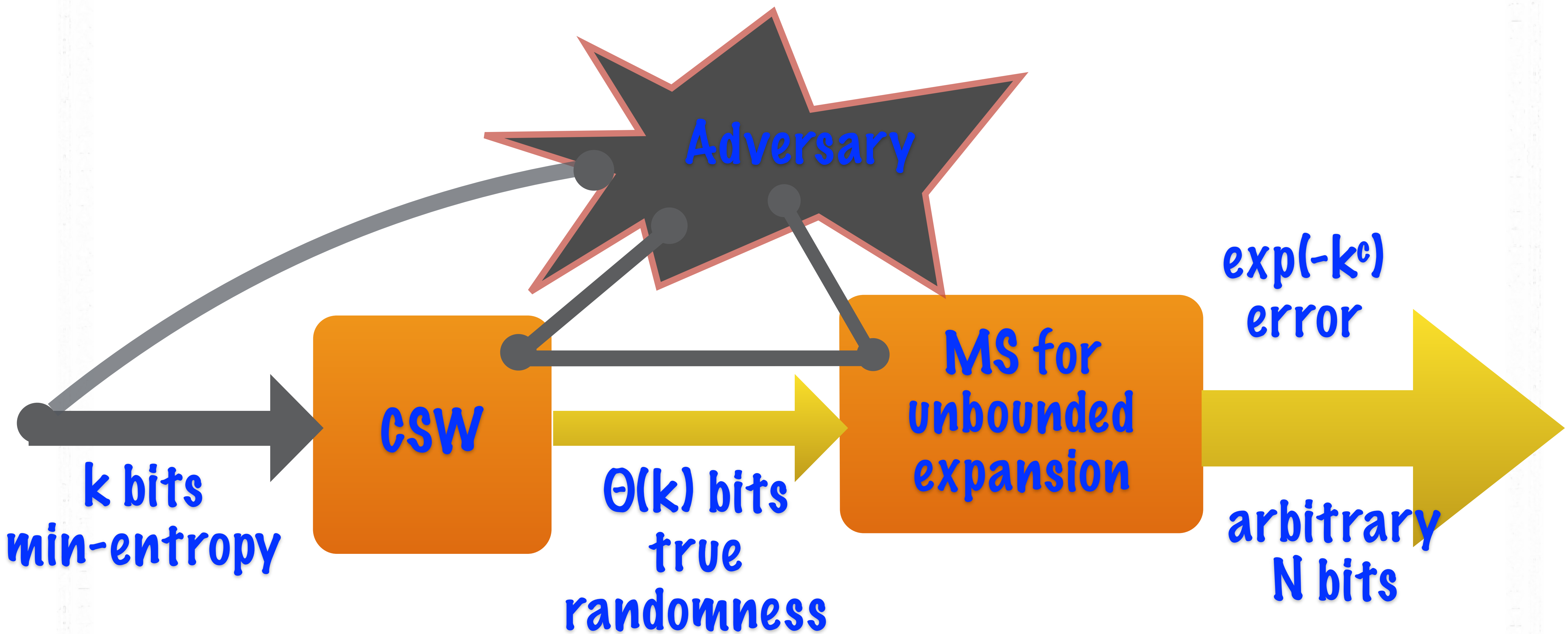
Application: robust unbounded expansion [CSW+MS]





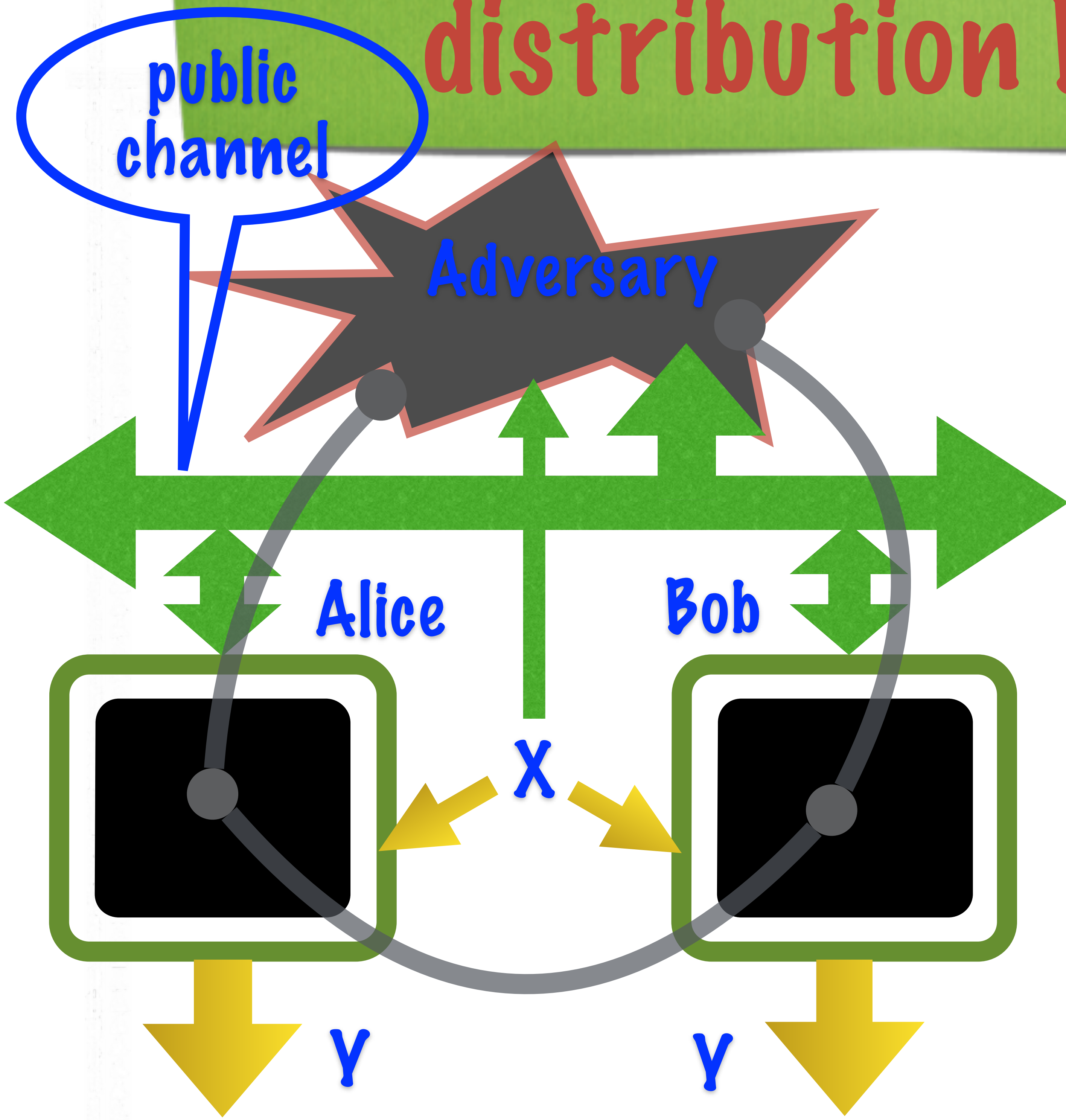
- Goal: k bits -> arbitrarily N-bits
- Trivial by using log*N devices
  - Robust by using Miller-Shi
  - error dominated by the first term
- Constant number of devices through cross-feeding two expansion protocols [Fehr+'13]?
- Yes: [Coudron-Yuen'13] based on VV'12+Reichardt-Unger-Vazirani'13: 8 devices, non-robust
- CSW+MS: any expanding protocol safe for cross-feeding with doubled number of devices and about the same error
  - Using Miller-Shi: robust, 4-devices

CSW+MS: robust unbounded expansion from just one and arbitrary min-entropy source and almost optimal error



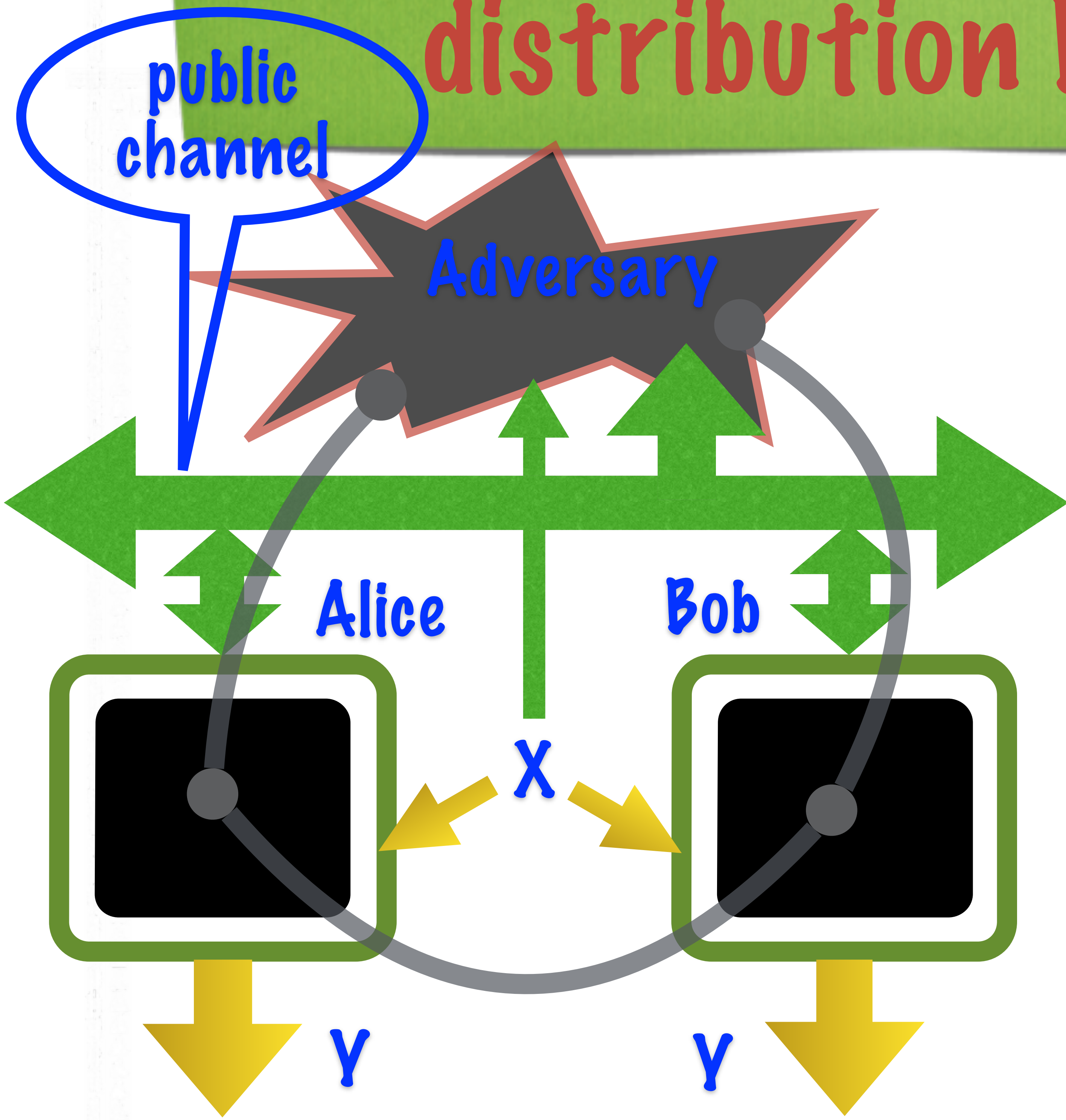
Application: expanding key distribution [Miller-Shi]

Application: expanding key distribution [Miller-Shi]



- Robust untrusted device qkd first proved by Vazirani-Vidick'13

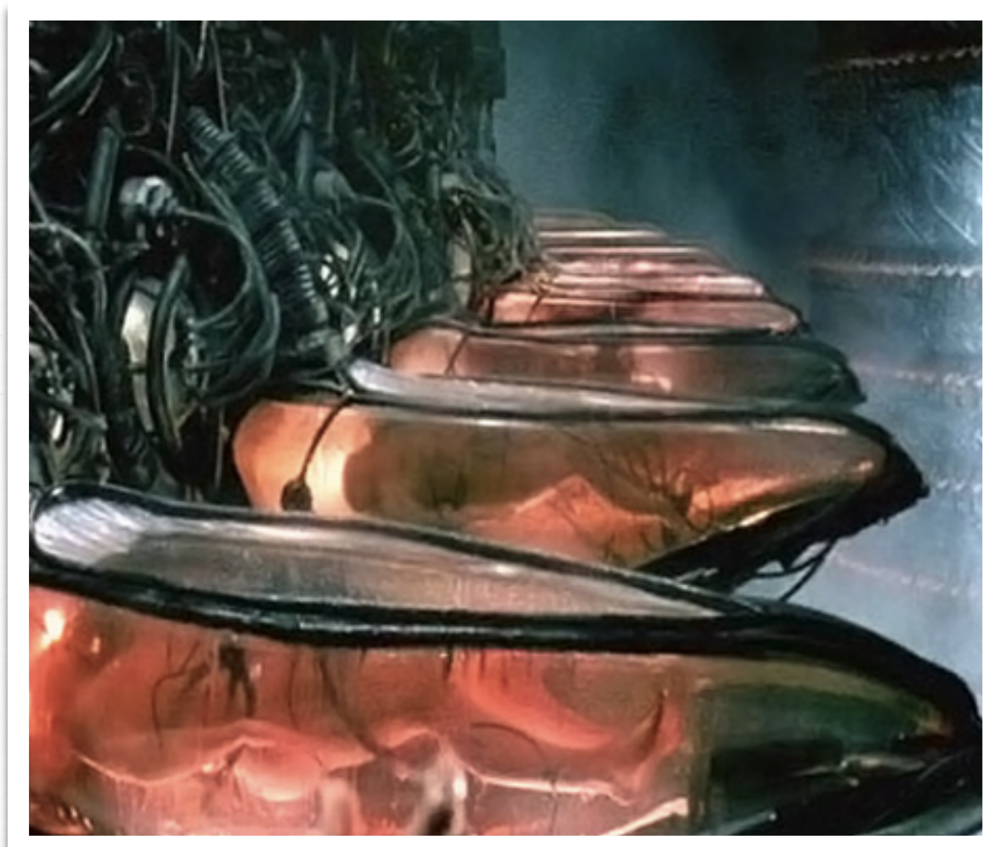
Application: expanding key distribution [Miller-Shi]



- Robust untrusted device qkd first proved by Vazirani-Vidick'13
- New in the adapted Miller-Shi: exponentially expanding key with 2 devices (unbounded with 4)

Dichotomy between deterministic and fundamentally random world

[Colbeck-Renner'12, Gallego+'13, CSW'14]

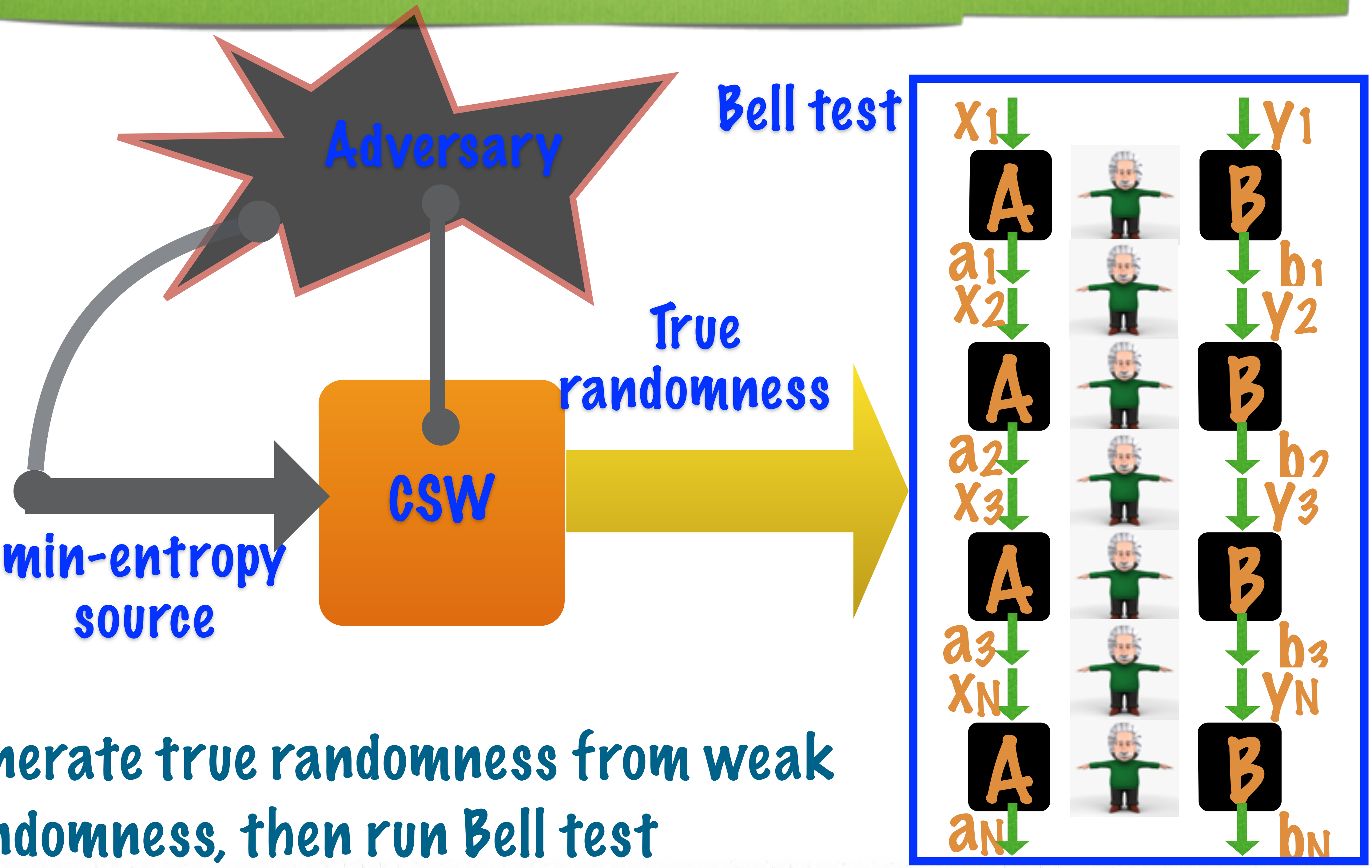


V.S.

True randomness in Nature either does not exist or exist in almost perfect quality and unbounded quantity

Untrusted-device protocols

Mitigating freedom-of-choice loophole



Generate true randomness from weak randomness, then run Bell test

3. Protocols and Proof Method

Foundation: Classical Test of a Quantum Duck

Foundation: Classical Test of a Quantum Duck

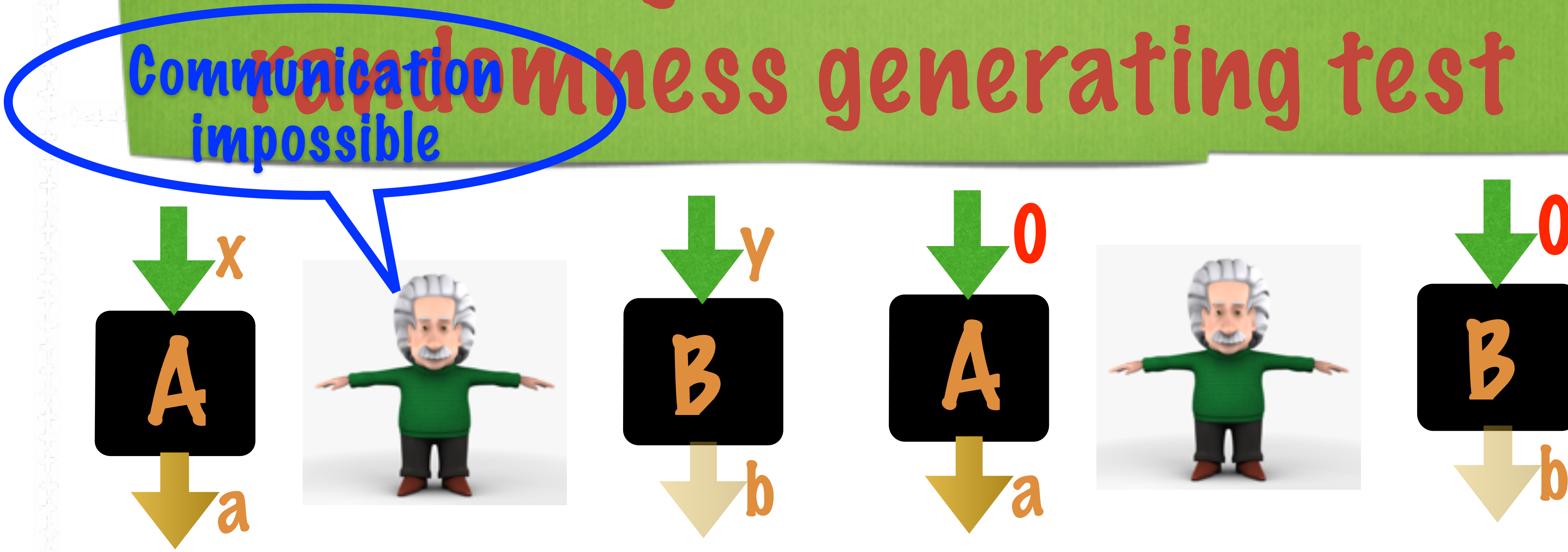
Foundation: Classical Test of a Quantum Duck

- Test if the devices behave like the ideal devices

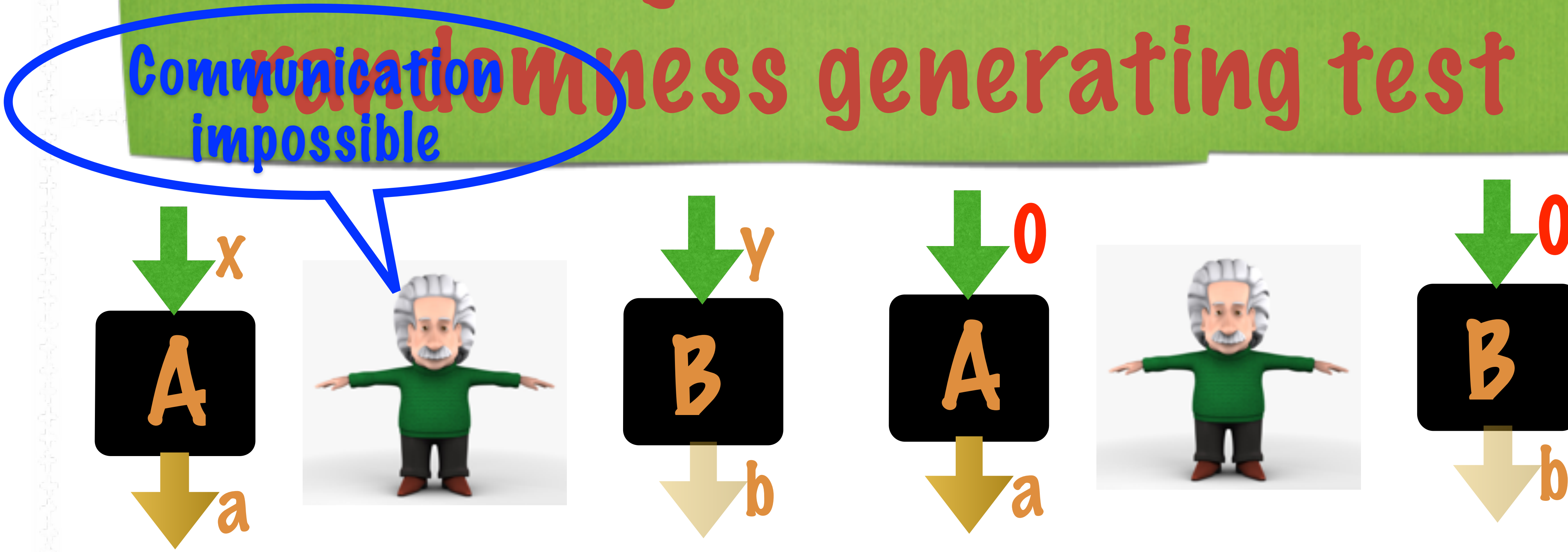
Foundation: Classical Test of a Quantum Duck

- Test if the devices behave like the ideal devices
- Idea devices generate randomness

CHSH game: a robust & randomness generating test

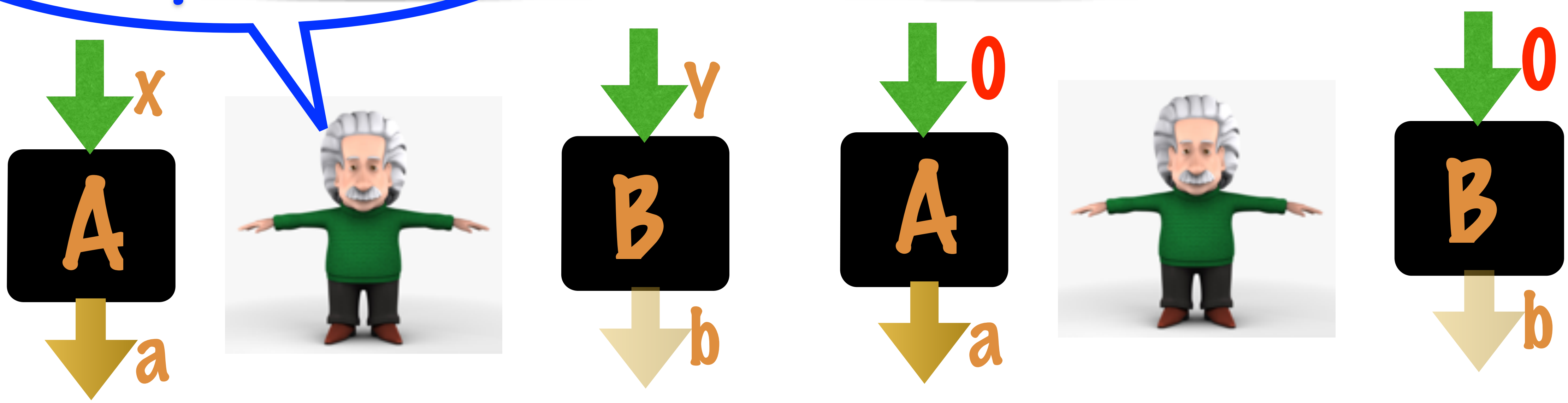


CHSH game: a robust & randomness generating test



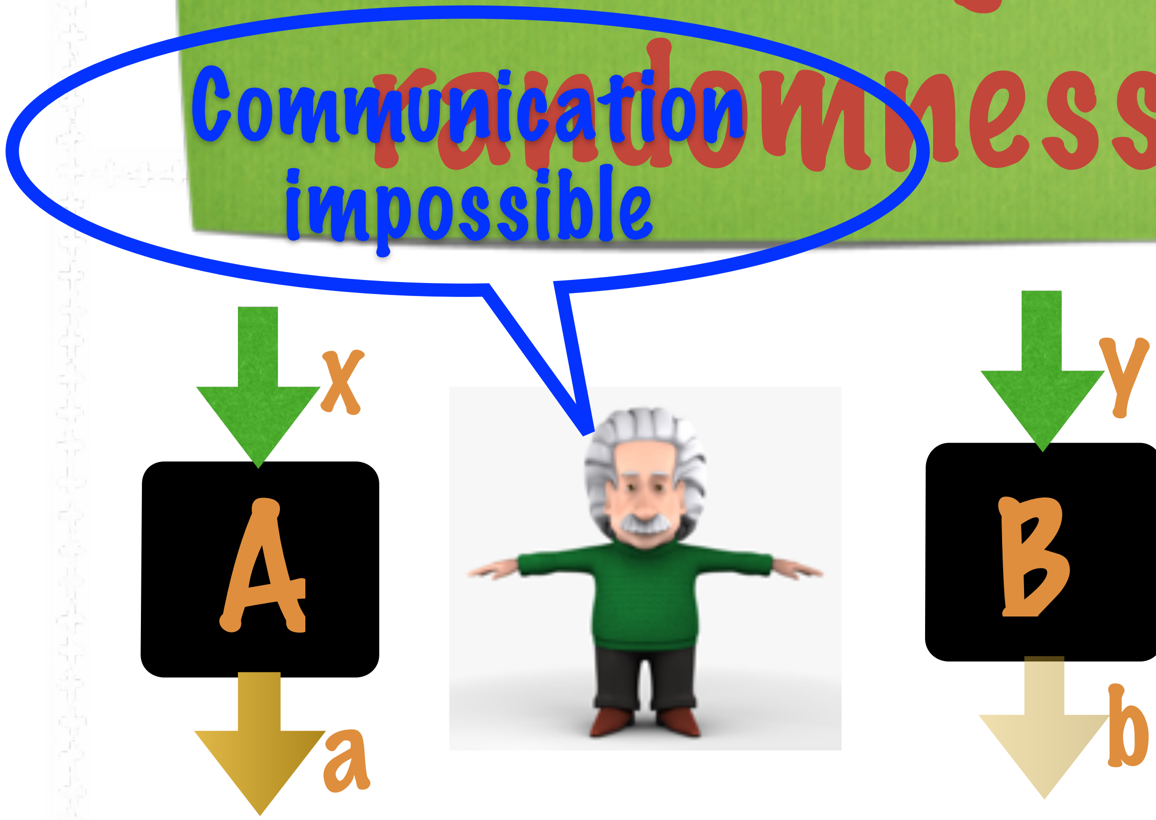
- No communication allowed during game
- Each device receives a bit, outputs a bit

CHSH game: a robust & randomness generating test



- No communication allowed during game
- Each device receives a bit, outputs a bit
- Device wins if $a \oplus b = x \wedge y$

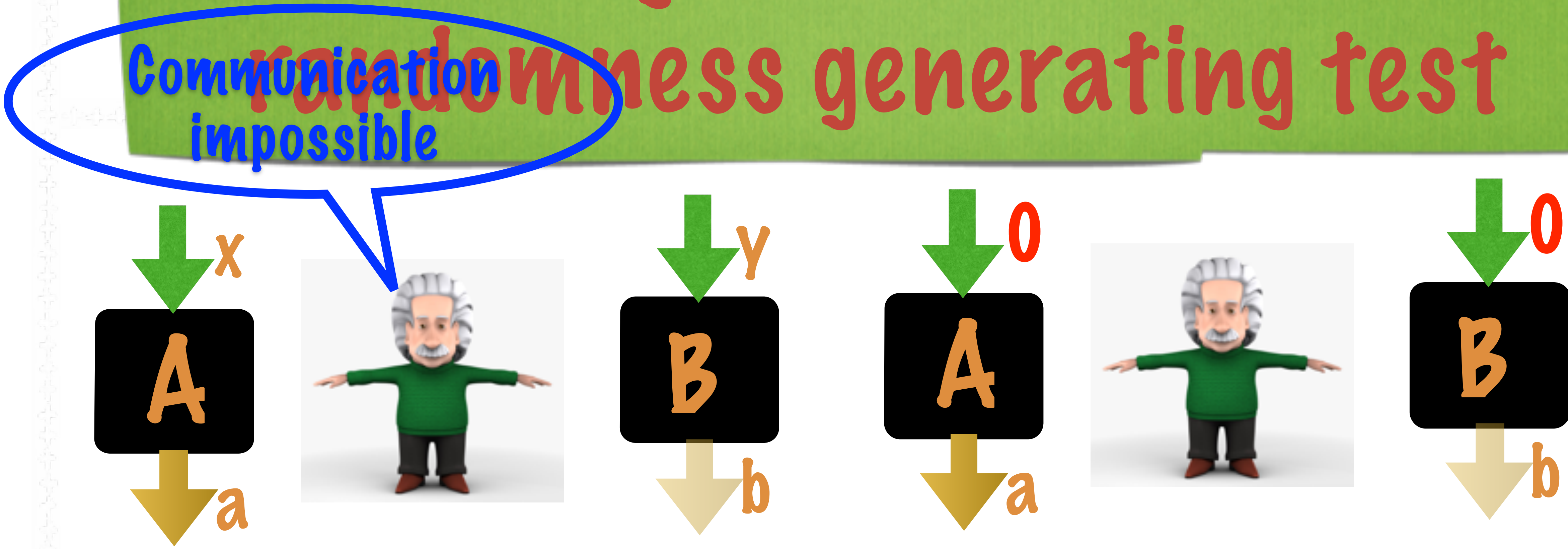
CHSH game: a robust & randomness generating test



- No communication allowed during game
- Each device receives a bit, outputs a bit
- Device wins if $a \oplus b = x \wedge y$

- On uniformly random input, OPT quantum wins prob = .85 > OPT classical = .75

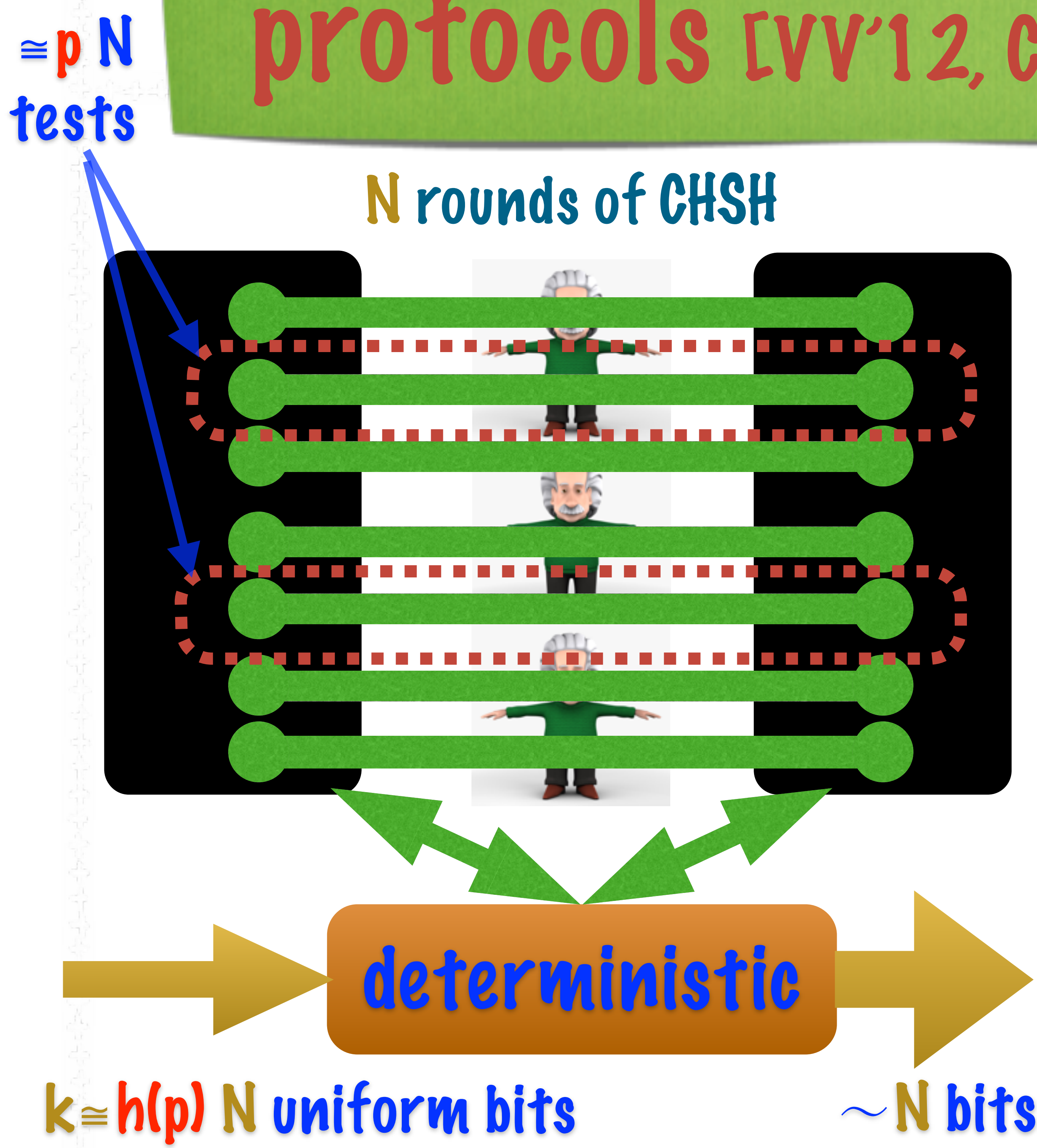
CHSH game: a robust & randomness generating test



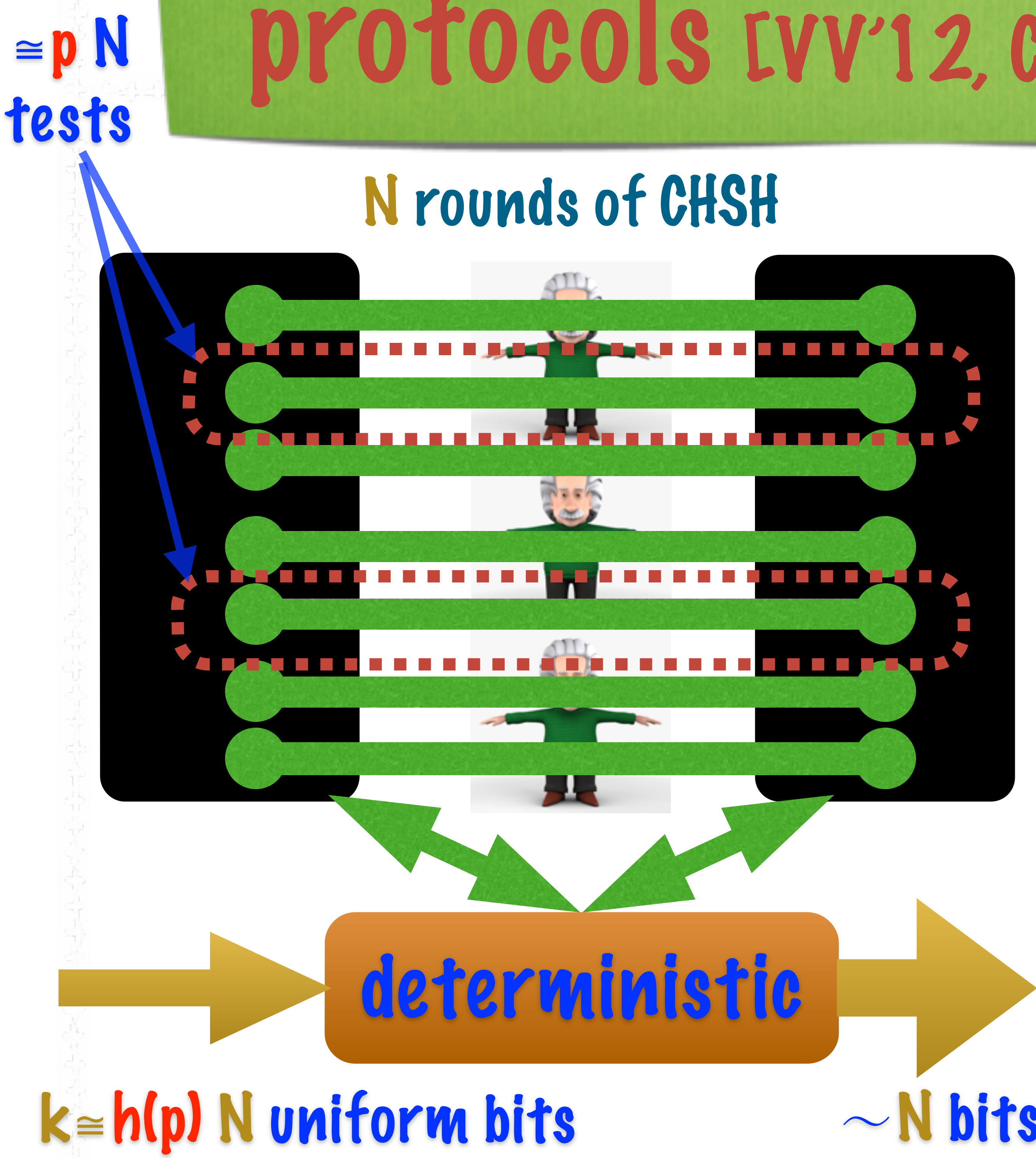
- No communication allowed during game
- Each device receives a bit, outputs a bit
- Device wins if $a \oplus b = x \wedge y$

- On uniformly random input, OPT quantum wins prob = .85 > OPT classical = .75
- Bit a in OPT quantum uniform to the input+Adversary, on all inputs, including (0,0)

Seeded extraction: Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]

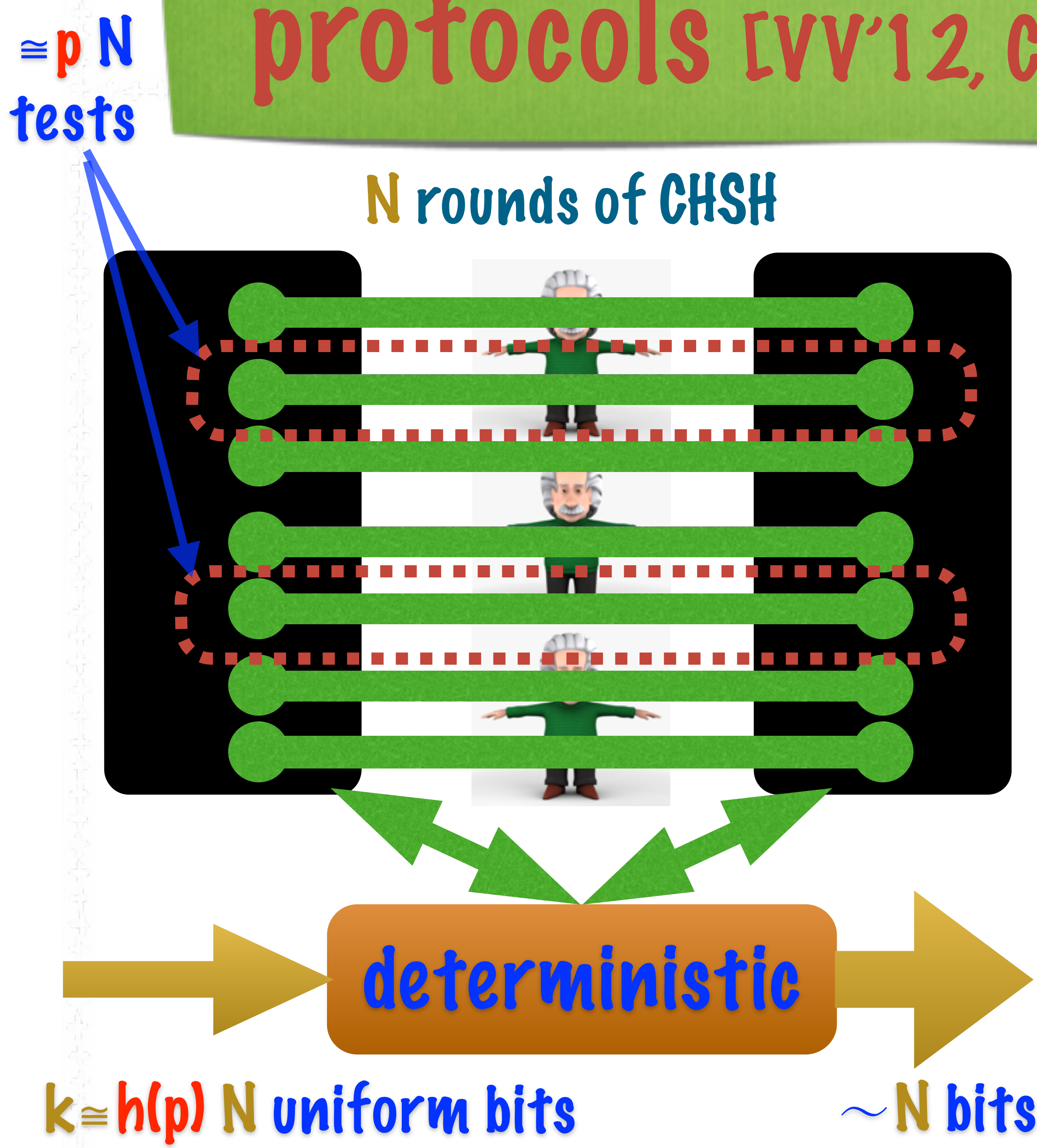


Seeded extraction: Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]



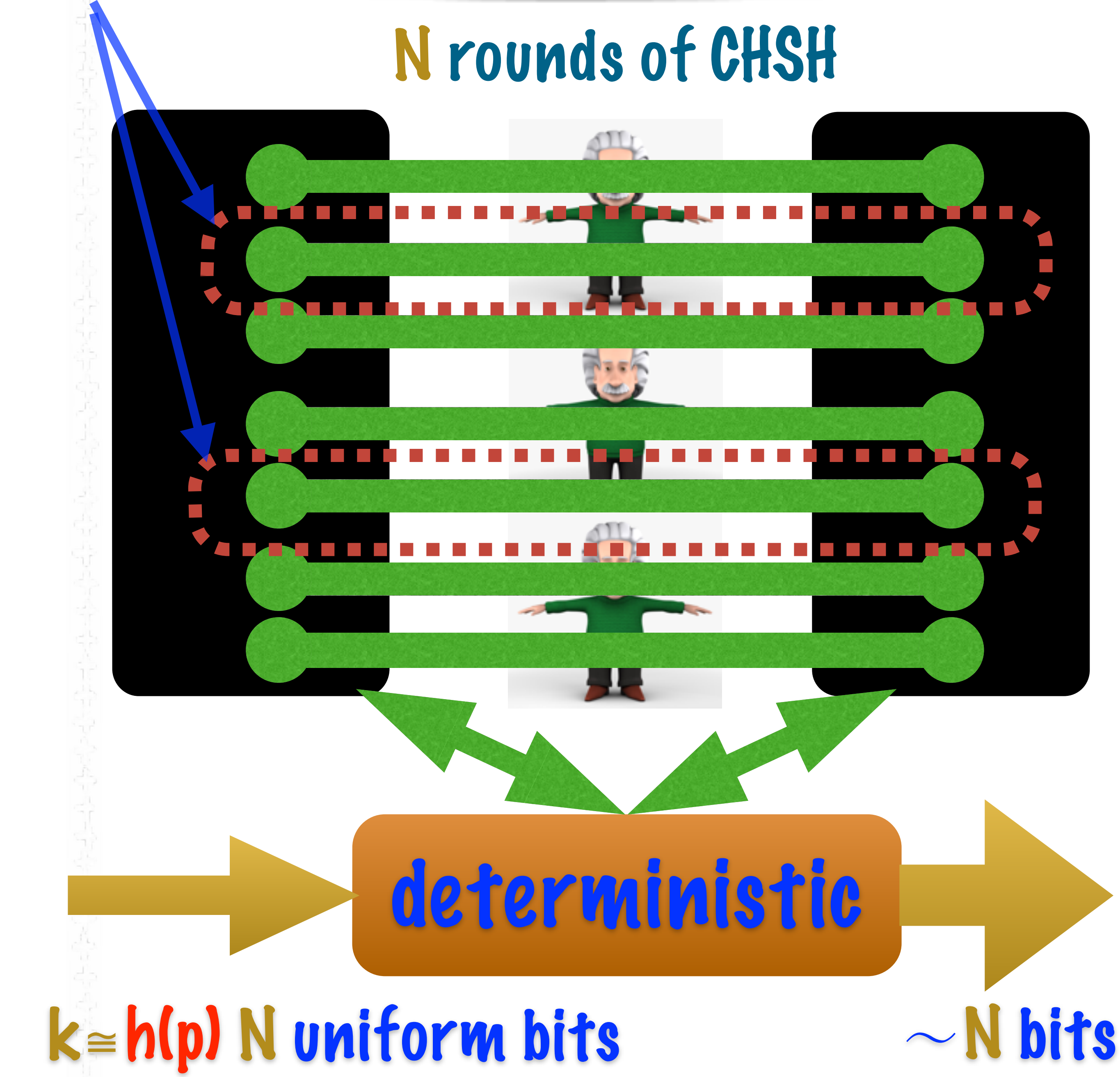
- Play N sequential CHSH

Seeded extraction: Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]



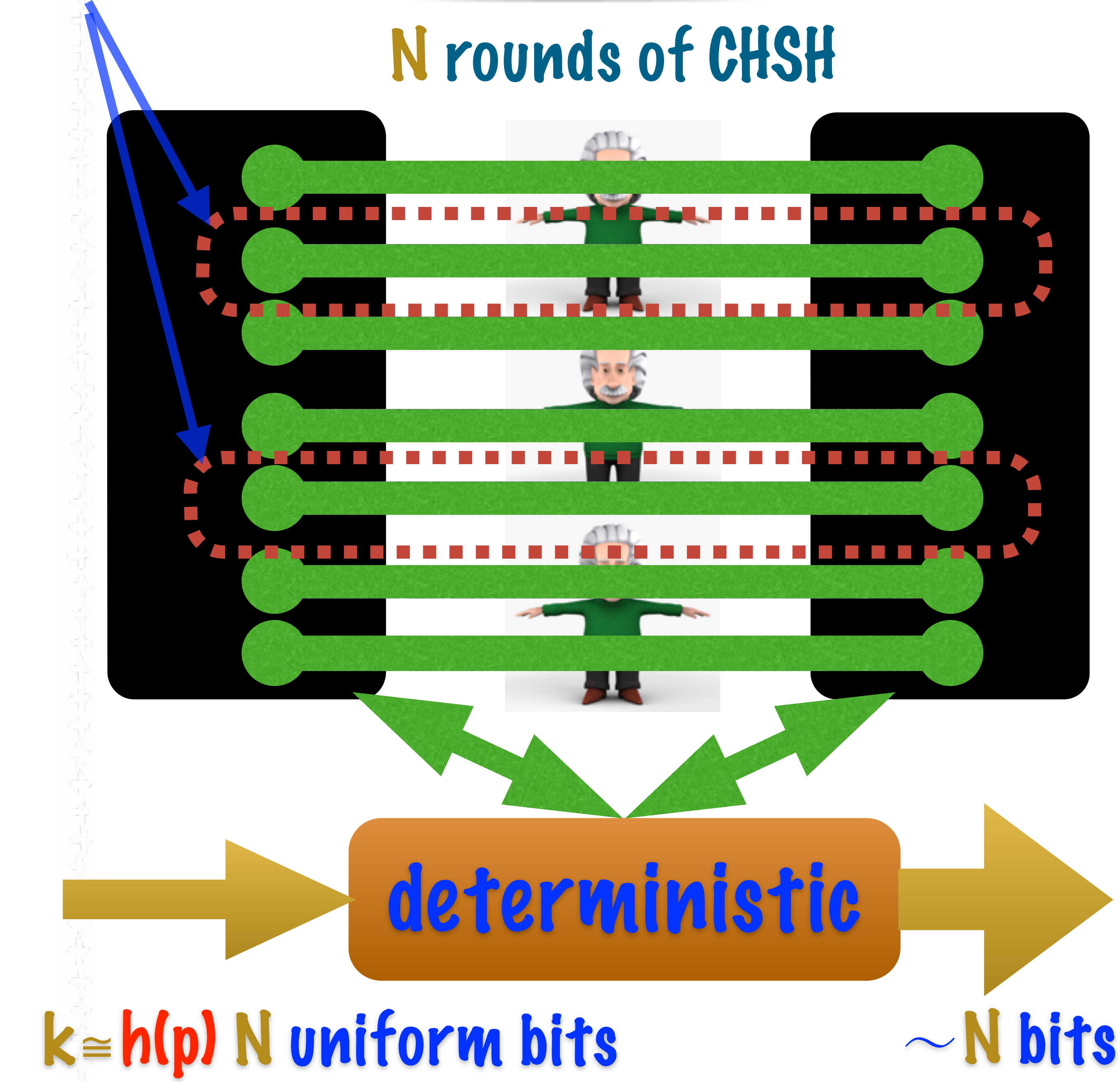
- Play N sequential CHSH
- Choose a small number of games for testing; others for randomness generation

Seeded extraction: Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]



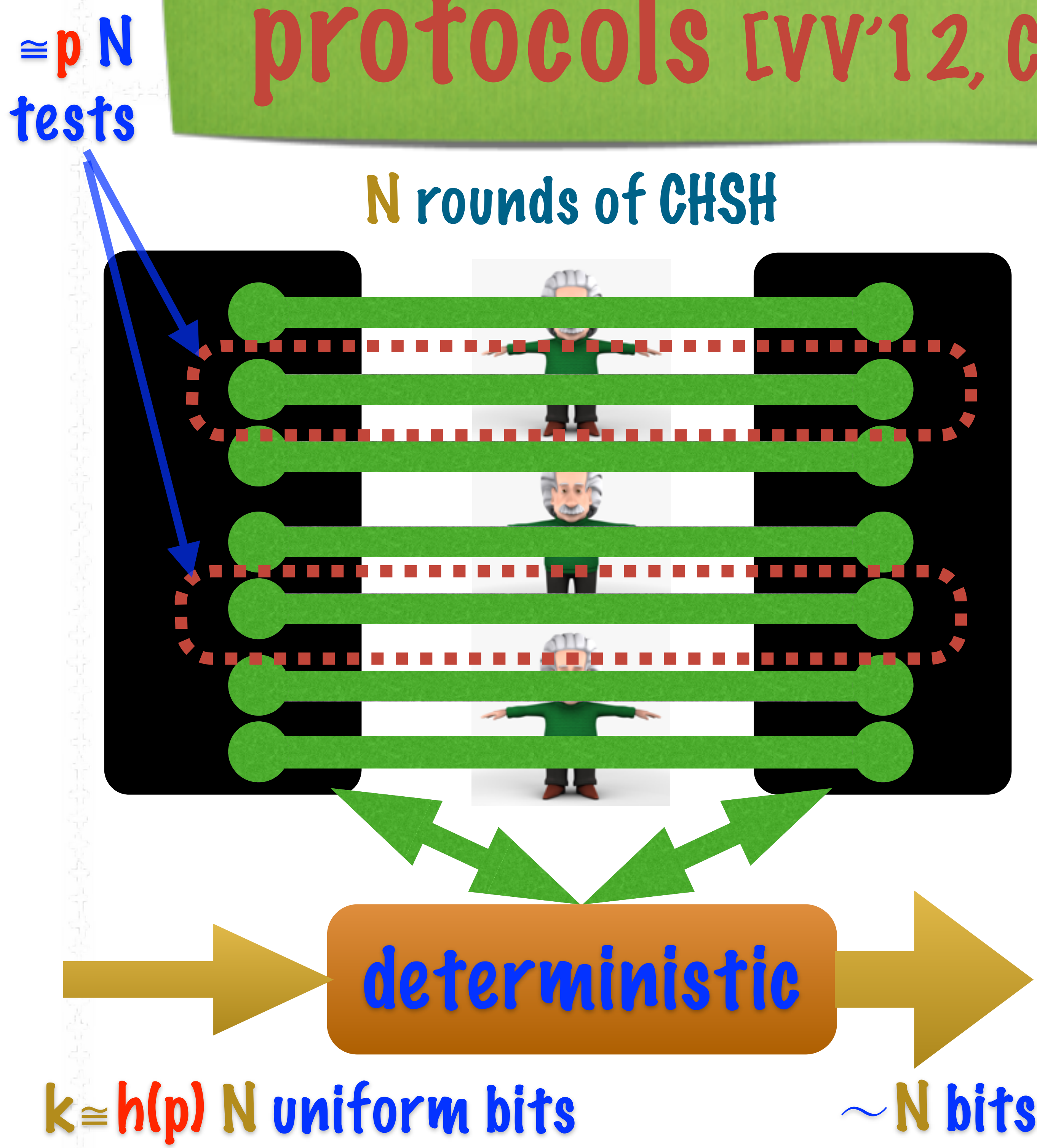
- Play N sequential CHSH
- Choose a small number of games for testing; others for randomness generation
    - CYV'13: test independently with a small probability p

Seeded extraction: Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]



- Play N sequential CHSH
- Choose a small number of games for testing; others for randomness generation
  - CYV'13: test independently with a small probability p
- Reject when losing too much in test rounds

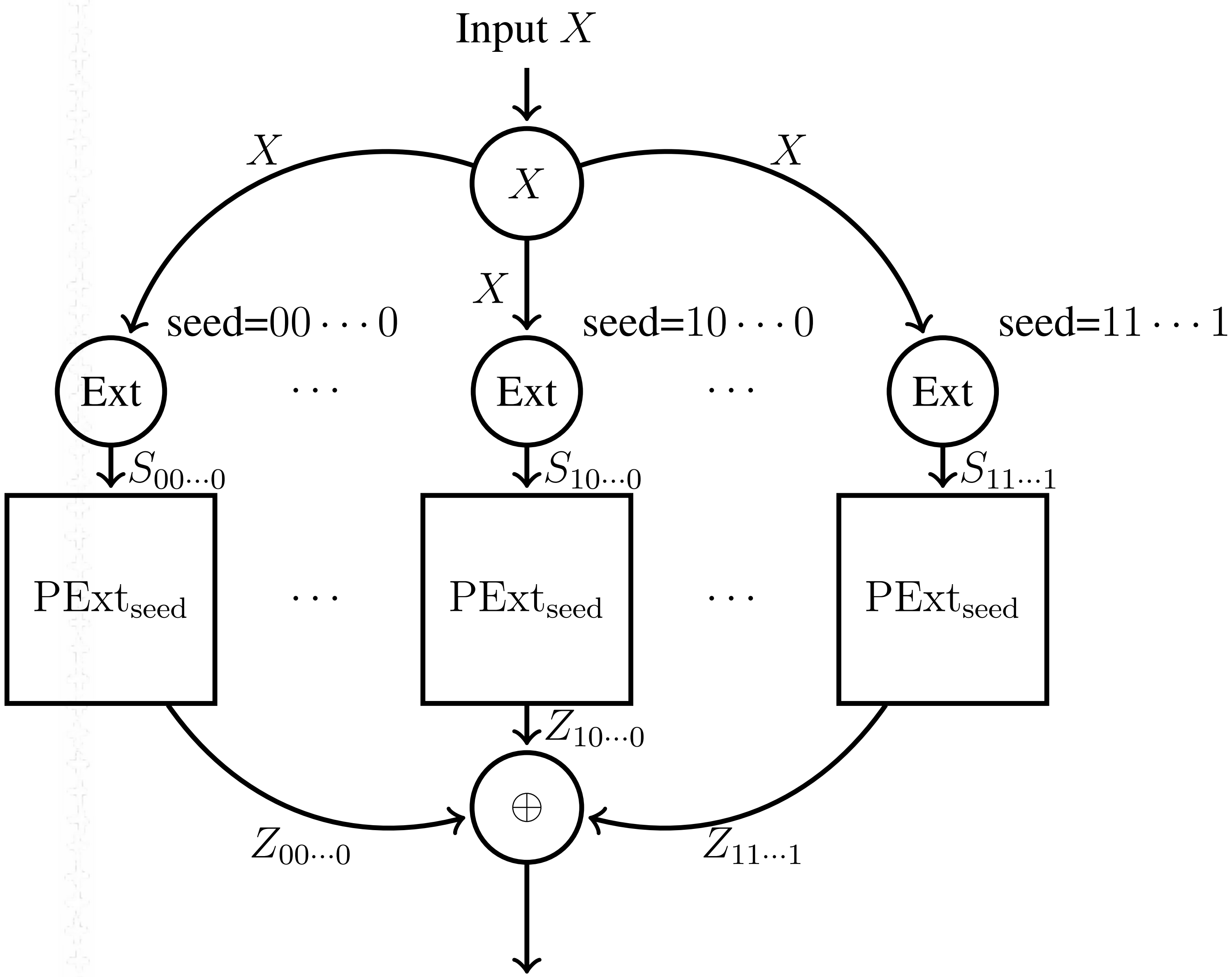
Seeded extraction:Spot-checking protocols [VV'12, Coudron-Yuen-Vidick'13]



- Play N sequential CHSH
- Choose a small number of games for testing; others for randomness generation
  - CYV'13: test independently with a small probability p
- Reject when losing too much in test rounds
- Input length h(p) N << N for tiny p

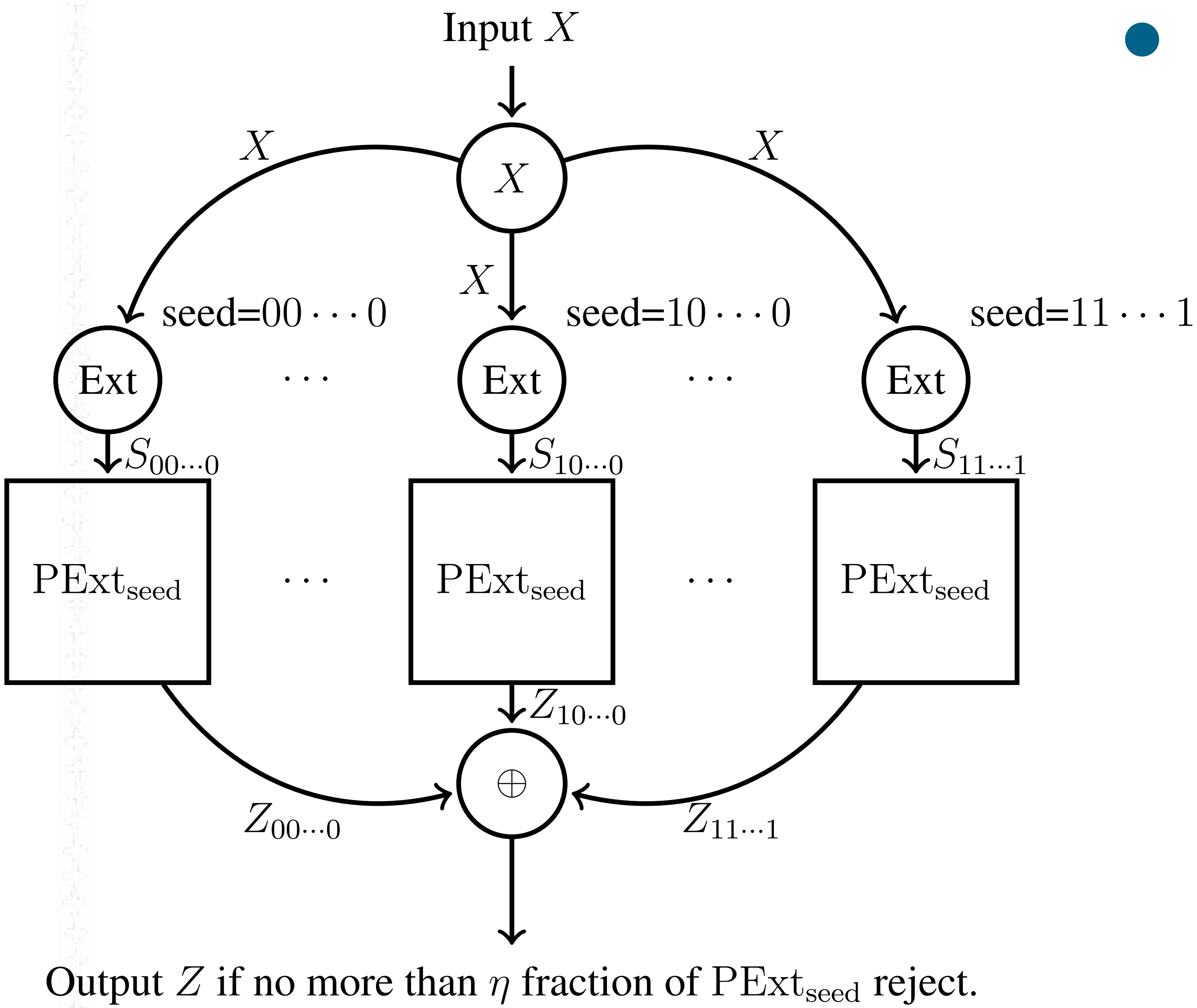
Seedless extraction: Master protocol [Chung-Shi-Wu]

Seedless extraction: Master protocol [Chung-Shi-Wu]



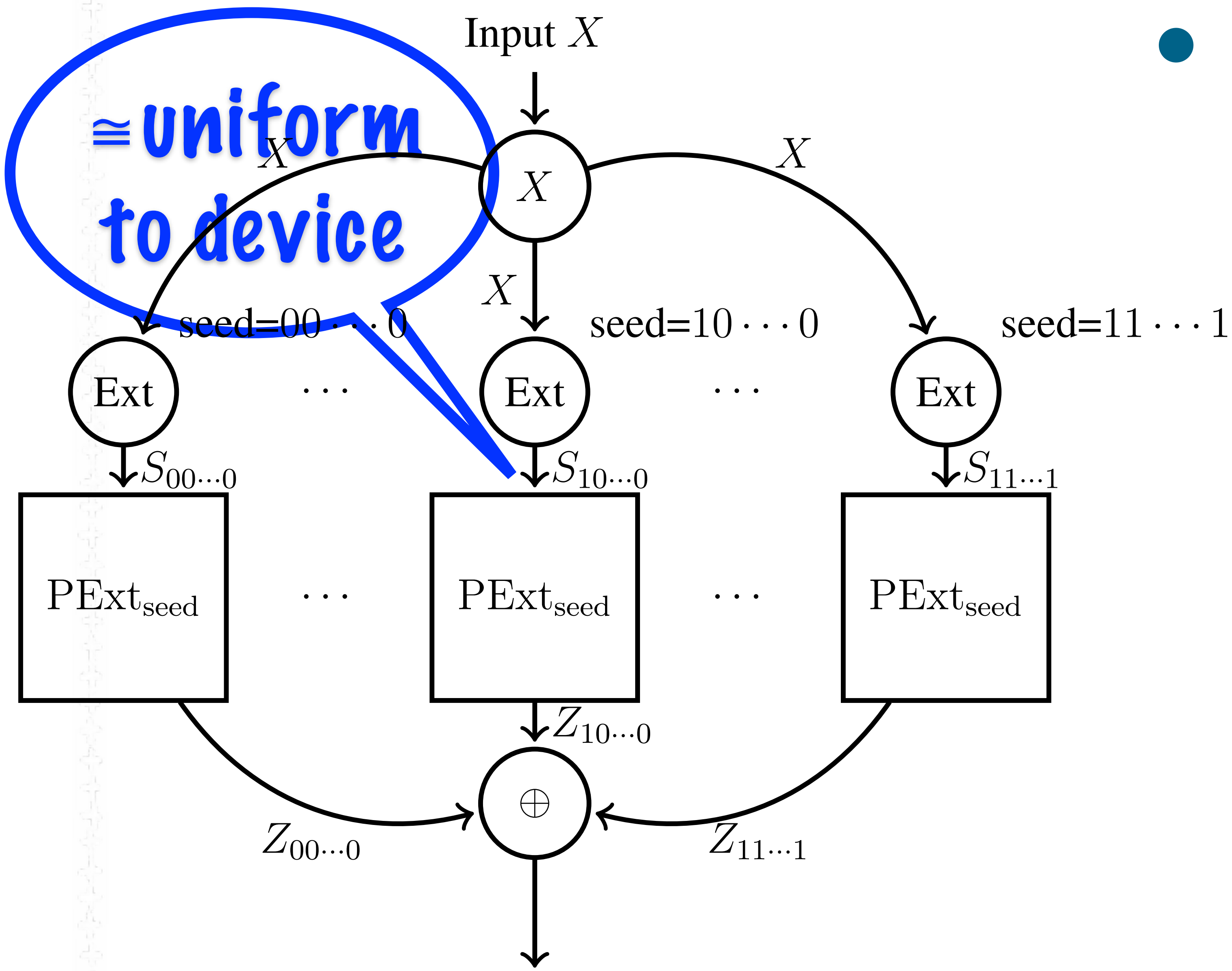
Output Z if no more than η fraction of $\mathrm{PExt}_{\mathrm{seed}}$ reject.

Seedless extraction: Master protocol [Chung-Shi-Wu]



- Create "quantum somewhere randomness",

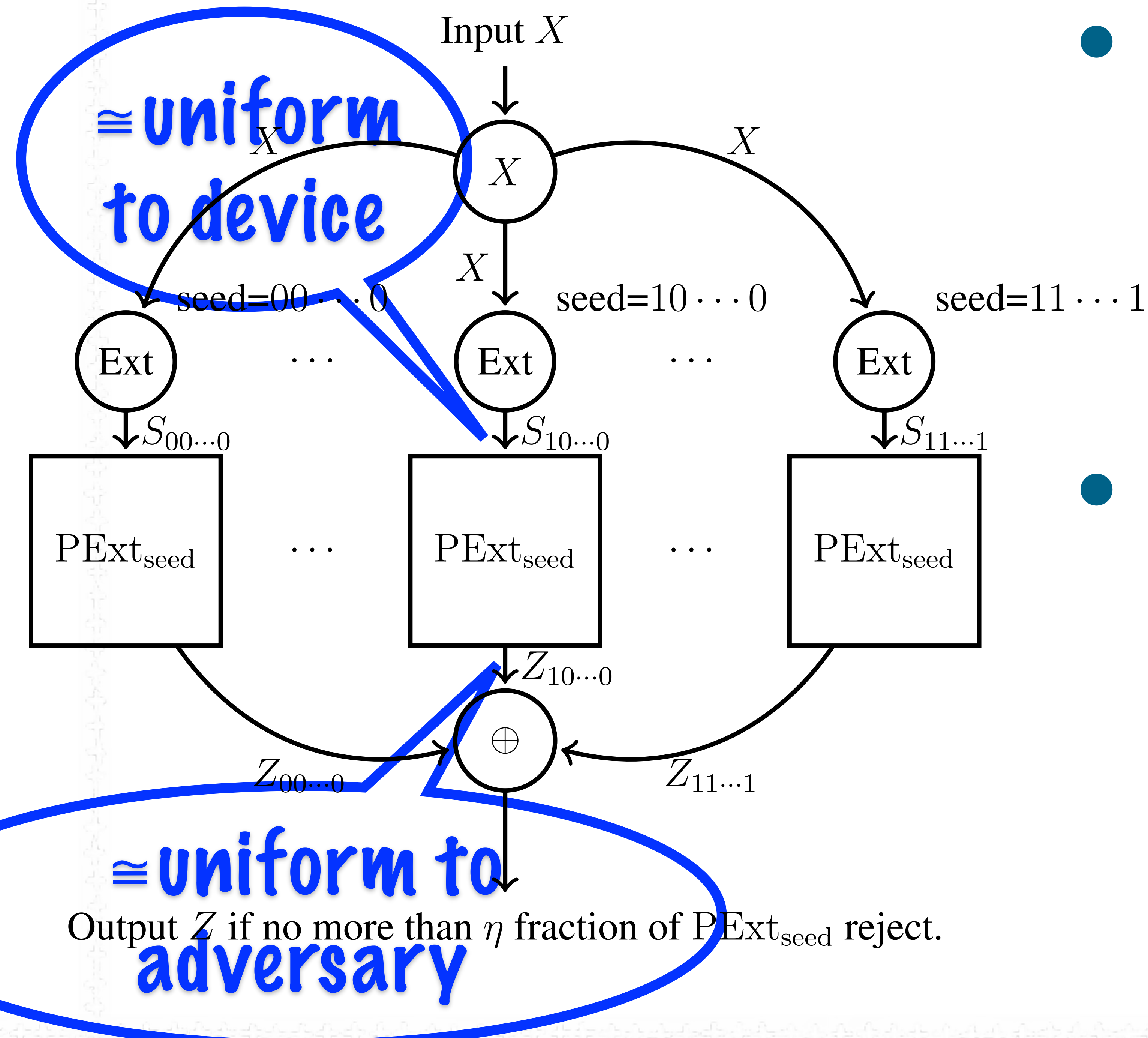
Seedless extraction: Master protocol [Chung-Shi-Wu]



Output Z if no more than η fraction of $\mathrm{PExt}_{\mathrm{seed}}$ reject.

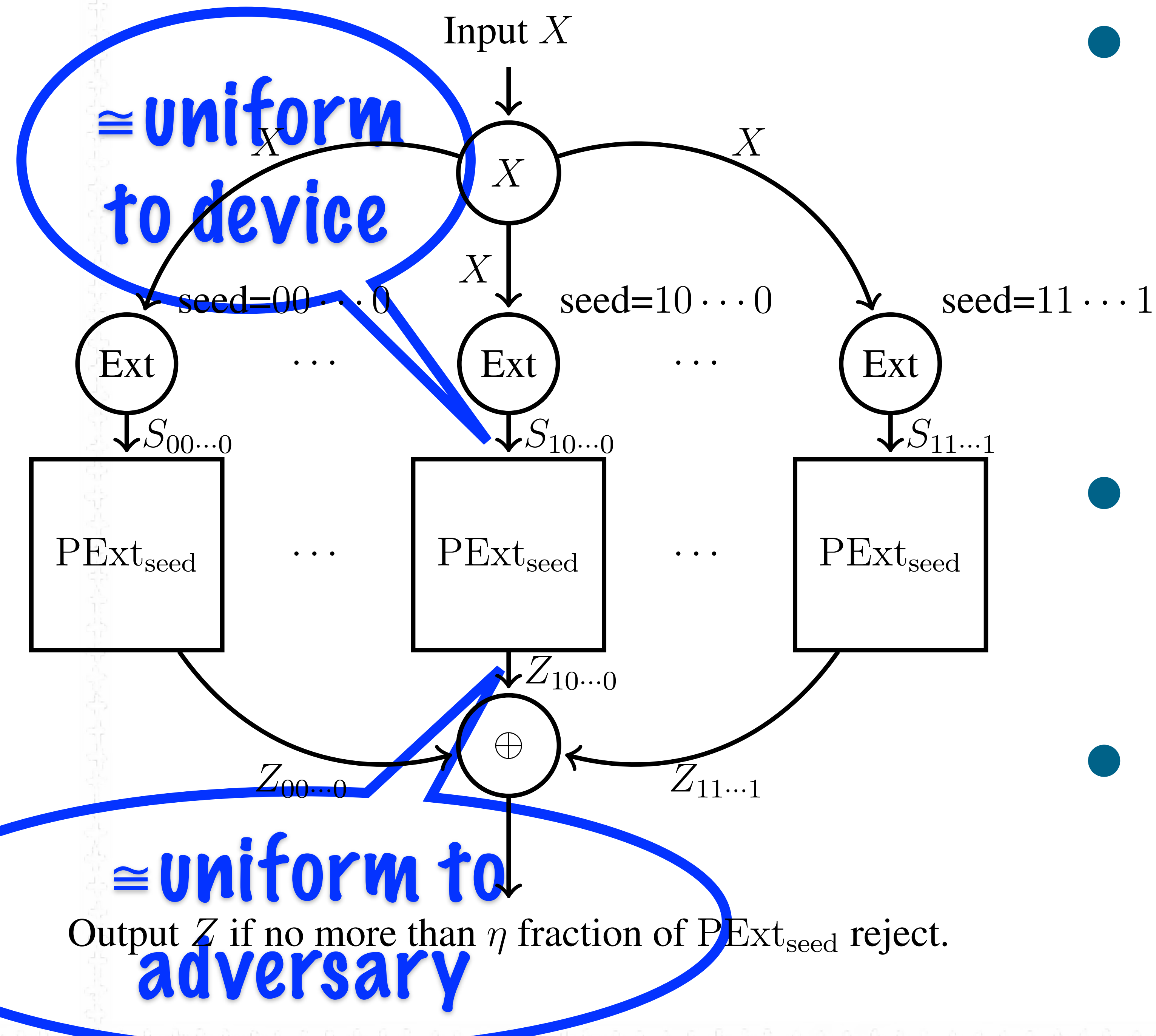
- Create "quantum somewhere randomness"
  - Most blocks are "good" (almost uniform to device)

Seedless extraction: Master protocol [Chung-Shi-Wu]



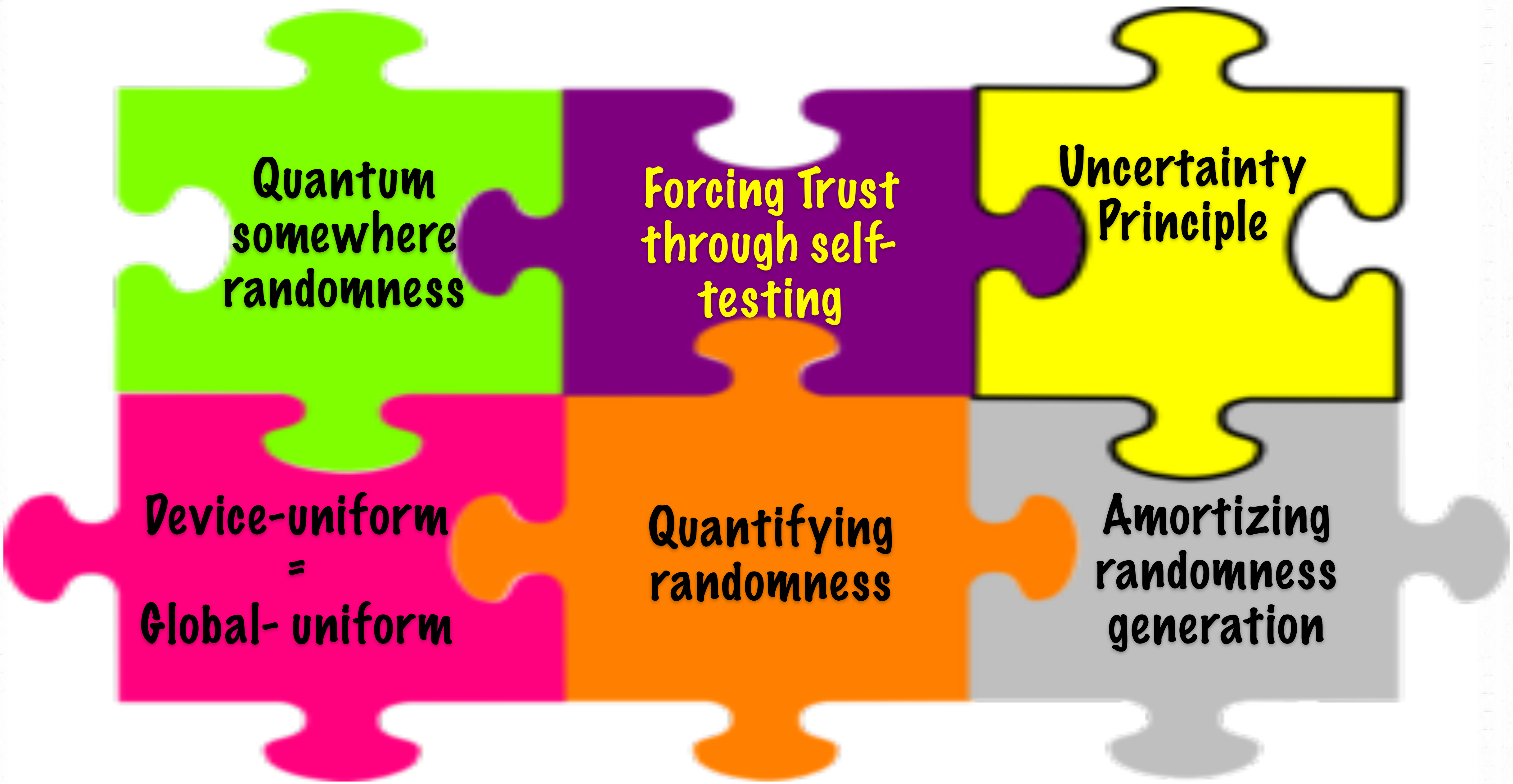
- Create "quantum somewhere randomness"
  - Most blocks are "good" (almost uniform to device)
- Transform each good block to adversary-uniform through Decoupling

Seedless extraction: Master protocol [Chung-Shi-Wu]



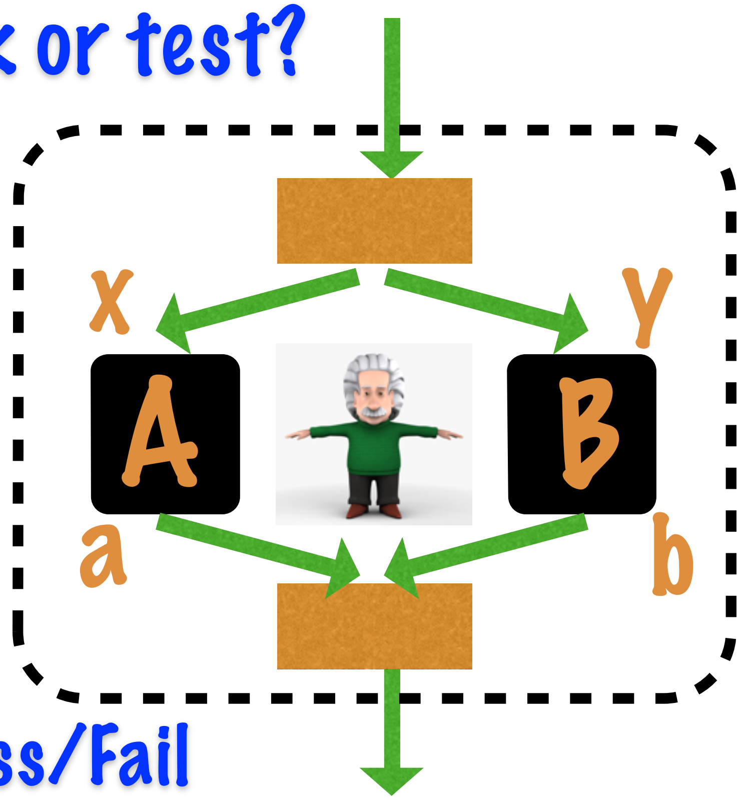
- Create "quantum somewhere randomness"
    - Most blocks are "good" (almost uniform to device)
- Transform each good block to adversary-uniform through Decoupling
- Accept if the number of acceptance exceeds a threshold. XOR accepted outputs close to adversary random

Our techniques: many pieces to the puzzle...



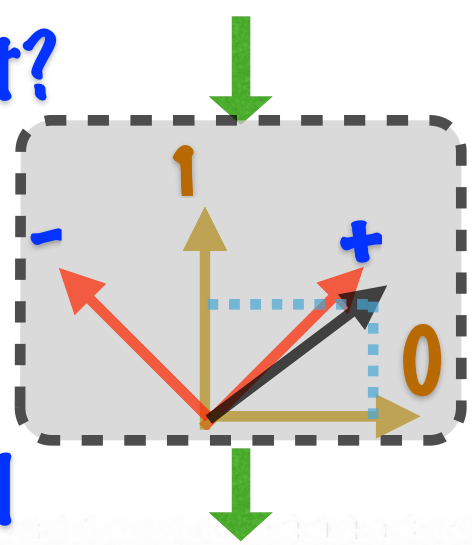
Forcing trust on adversarial devices

work or test?



0/1 or Pass/Fail

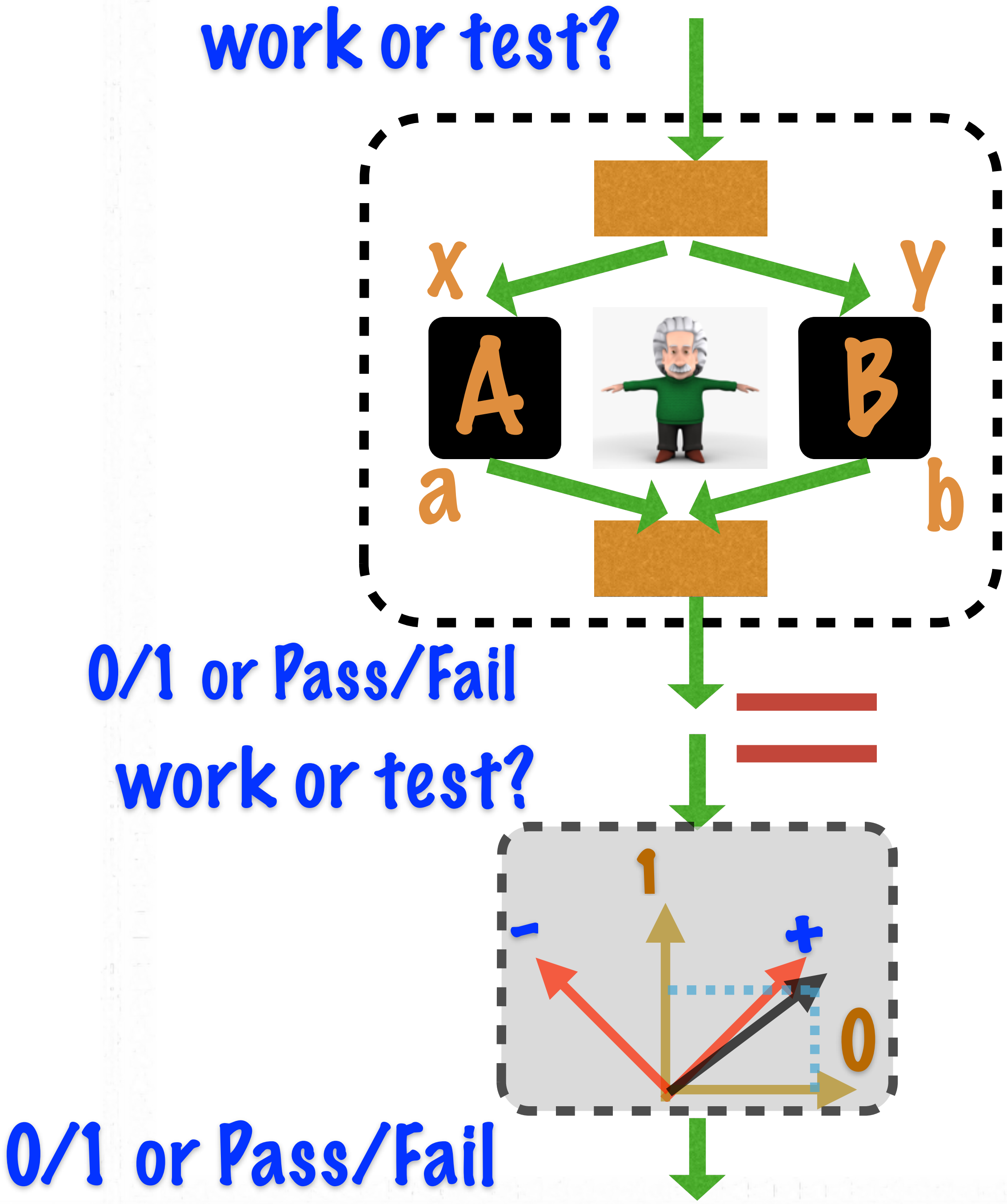
work or test?



0/1 or Pass/Fail

Method::seeded extraction

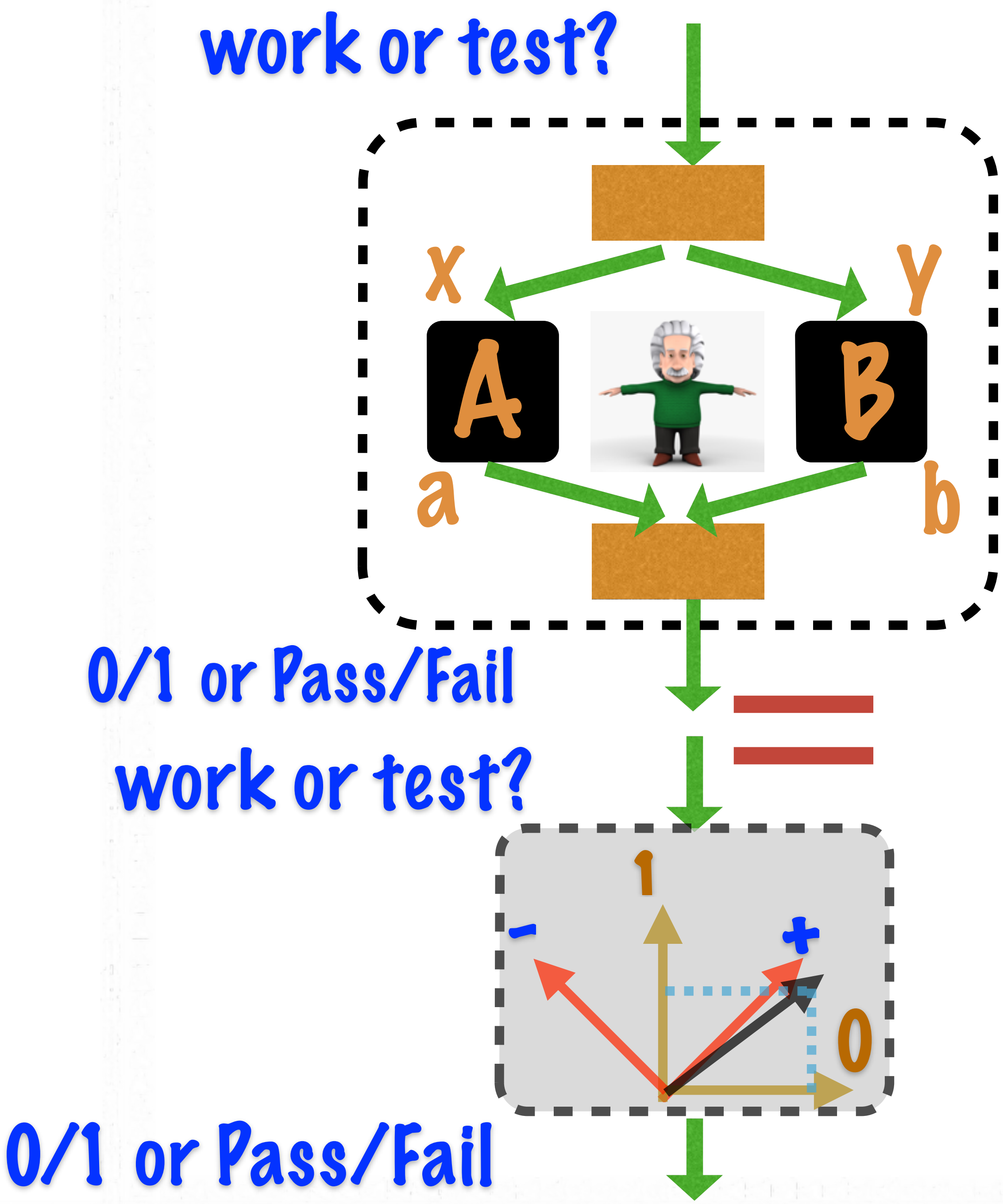
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device

Method::seeded extraction

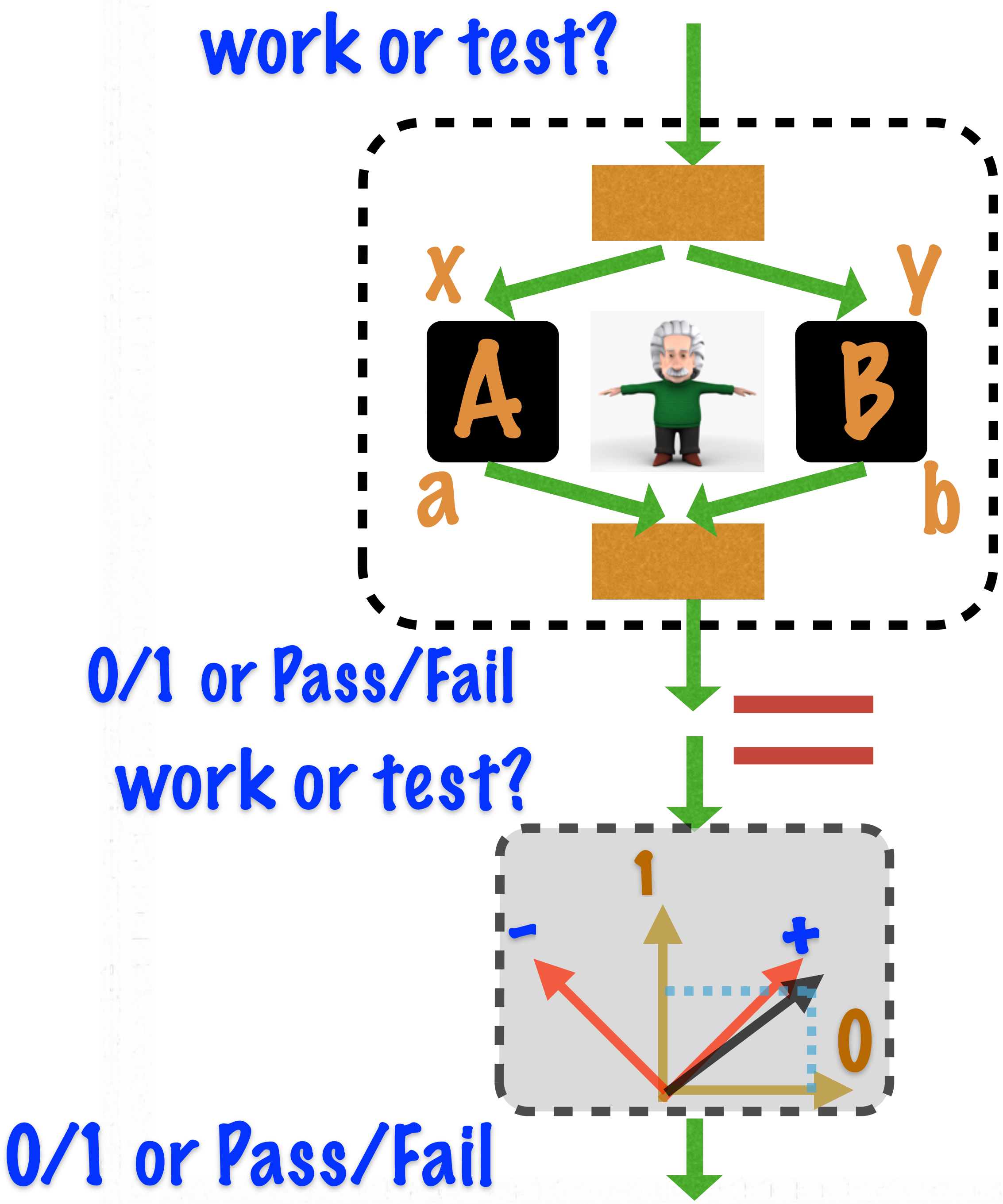
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.

Method::seeded extraction

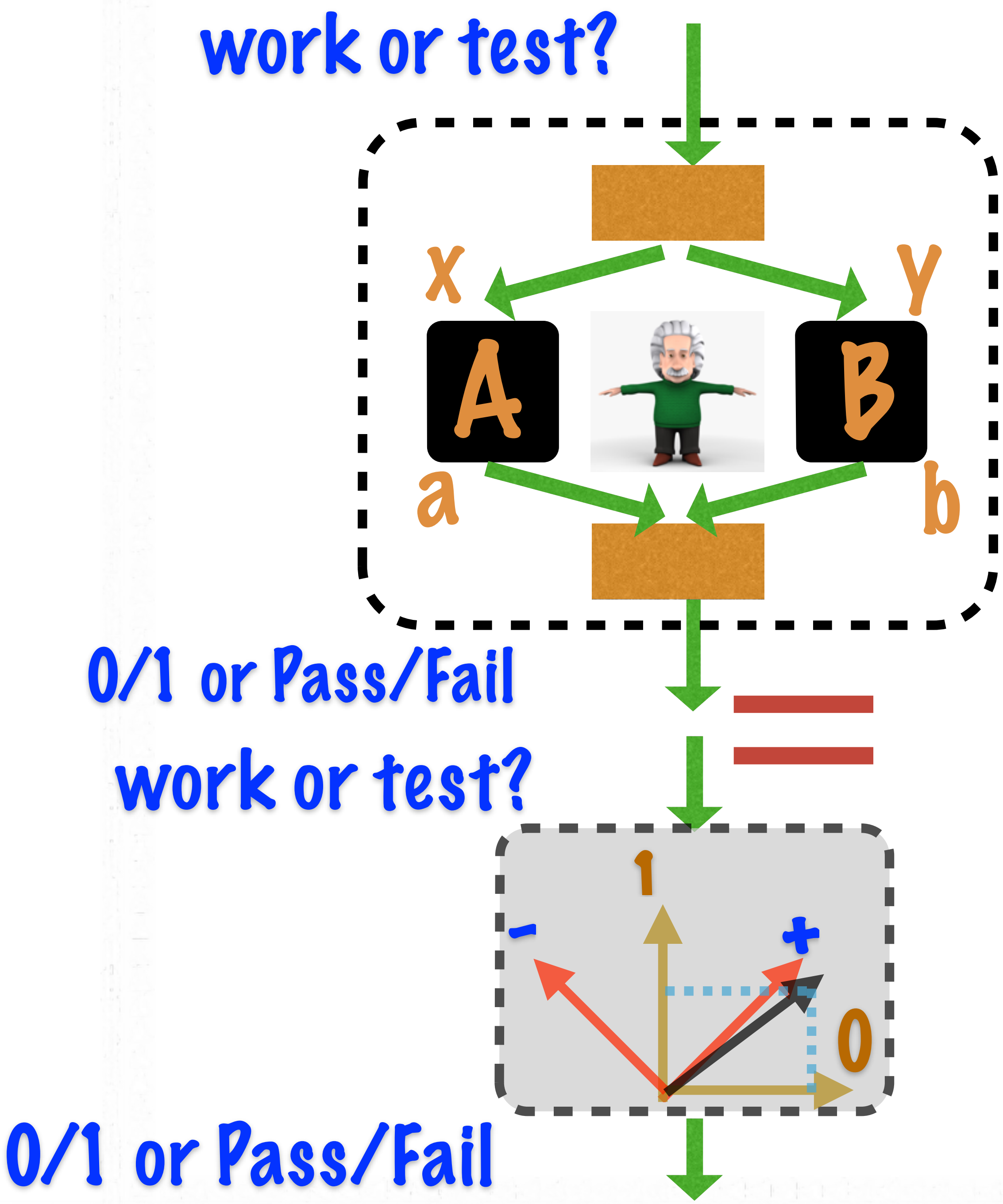
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.
- Trusted measurement device selects from anti-commuting measurements

Method::seeded extraction

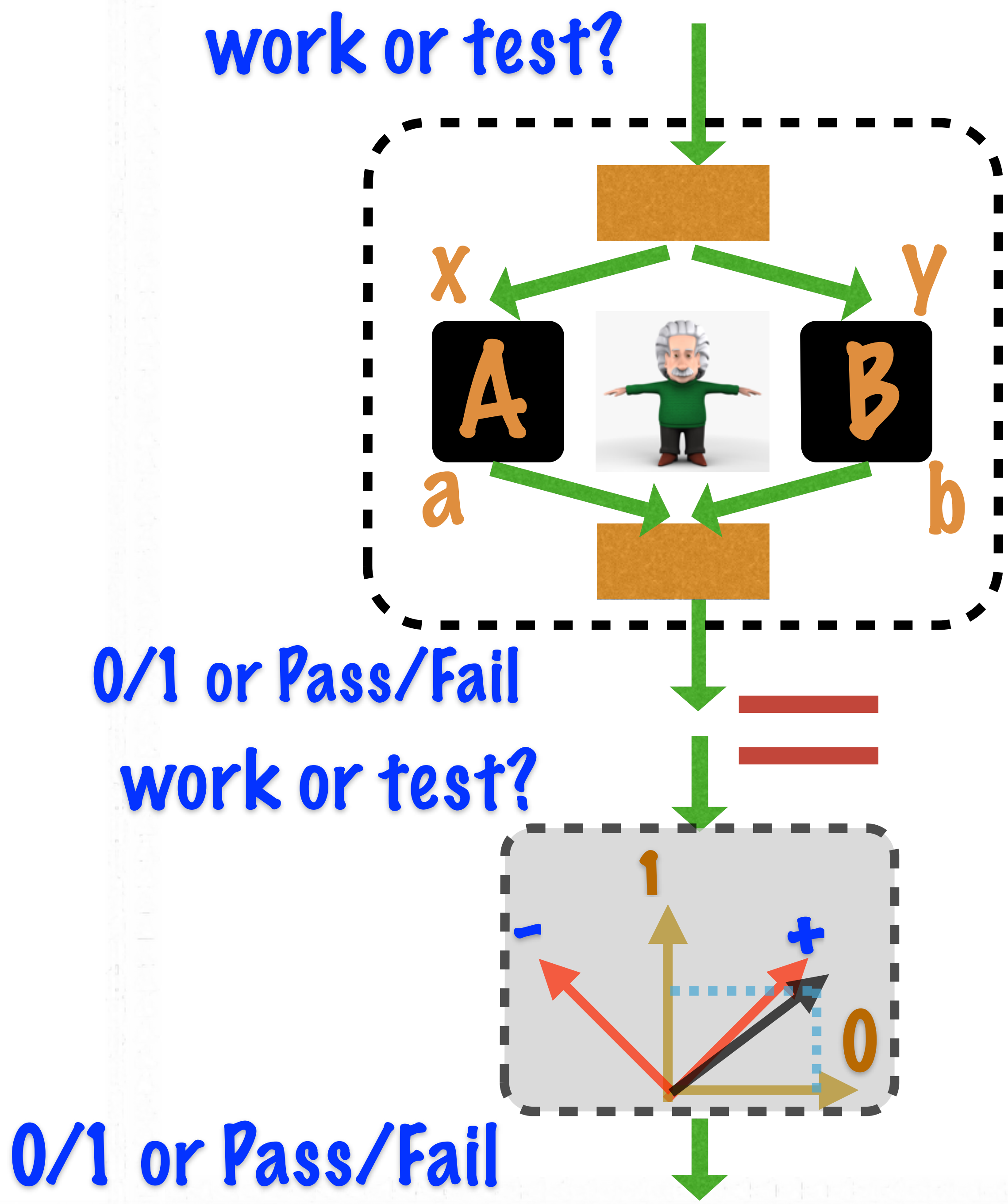
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.
- Trusted measurement device selects from anti-commuting measurements
  - work: measures 0/1

Method::seeded extraction

Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.
- Trusted measurement device selects from anti-commuting measurements
  - work: measures 0/1
  - test: measures +/- (pass/fail)

Method::seeded extraction

Challenges and solutions

Challenges and solutions

- Adversarial devices:
  "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component

Challenges and solutions

- **Adversarial devices:**
  "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component

- **Uneven rate of randomness:**
  "Amortized" analysis of randomness generation

Challenges and solutions

- **Adversarial devices:**
  "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component

- **Uneven rate of randomness:**
  "Amortized" analysis of randomness generation

- **Quantify randomness** generated at each step:
  Schatten norm

Method::seeded extraction

Challenges and solutions

- **Adversarial devices:** "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component
- **Uneven rate of randomness:** "Amortized" analysis of randomness generation
- **Quantify randomness** generated at each step: Schatten norm
- **Bounding randomness** generated at each step: A new uncertainty principle

Method::seeded extraction

Challenges and solutions

- **Adversarial devices:** "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component
- **Uneven rate of randomness:** "Amortized" analysis of randomness generation
- **Quantify randomness** generated at each step: Schatten norm
- **Bounding randomness** generated at each step: A new uncertainty principle
- **Creating uniform input** for seeded extractor: somewhere randomness from quantum-proof extractor

Method::seeded extraction

Challenges and solutions

- Adversarial devices: "Forcing Trust", the pre- and post-processing's force all devices to have a "trusted" component
- Uneven rate of randomness: "Amortized" analysis of randomness generation
- Quantify randomness generated at each step: Schatten norm
- Bounding randomness generated at each step: A new uncertainty principle
- Creating uniform input for seeded extractor: somewhere randomness from quantum-proof extractor
- Security in composing seeded protocols: Equivalence Lemma

Method::seeded extraction

4. Open Problems

“Randomness capacity” of untrusted-devices

- What quantifies the maximum amount of extractible randomness from (non-communicating) untrusted devices?
  - All published proofs require linear amount of entanglement
  - Is entanglement really needed?!

Maximum noise tolerable: the boundaries between quantum-classical-no security

- What is the maximum level of imperfection allowed for ensuring quantum security?
  - Trivial upper bound: quantum-classical gap
  - Another trivial but better (?) bound: quantum - OPT when output is deterministic
- Is there a range of noise values that provide classical security but not quantum security?

Maximum output bit rate under noise

- A more quantitative version of the previous question; important for practical use
- Two ways to improve the rate under noise based on Miller-Shi
  - Improve the trust coefficient
    - Method for computing the optimal trust coefficient?
  - Improve the Schatten norm uncertainty principle

Open problems

What are the most general class of games allowed?

- Anything having a quantum-classical gap?
  - Kochen-Specker games?

Minimum device number for unbounded expansion

- What is the minimum number of devices required for unbounded expansion?
  - MS+CSW: <= 4
  - 3?
  - 2?
  - 3 for constant noise, 2 for almost perfect devices?

Minimum device number for seedless extraction

- What is the minimum number of devices that can be used to extract from all (n, k) sources with a desired ϵ error?
  - CSW's upper bound >= poly(n/ϵ)
  - Could it be polylog(n/ϵ) or even constant?
  - Possibly no...
- For condensors (increasing min-entropy/length)?

Minimum device number for seedless extraction

- What is the minimum number of devices that can be used to extract from all (n, k) sources with a desired ϵ error?
  - CSW's upper bound >= poly(n/ϵ)
  - Could it be polylog(n/ϵ) or even constant?
  - Possibly no...

Optimal quantum-proof classical extractors

- What is the shortest seed length allowed for a quantum-proof classical extractor?
  - As a function of the source, output, and error parameters
  - Trevisan's extractor [De et. al.'12]: $\log^2(n/\epsilon)\log(m)$
  - Just $O(\log(n/\epsilon))$?

Open problems

Perfect Physical Extractor?

- A perfect physical extractor?
  - Optimizing all parameters simultaneously or necessary tradeoffs?

A general principle translating classical security to quantum security?

Open problems

A general principle translating classical security to quantum security?

Thanks!

Open problems

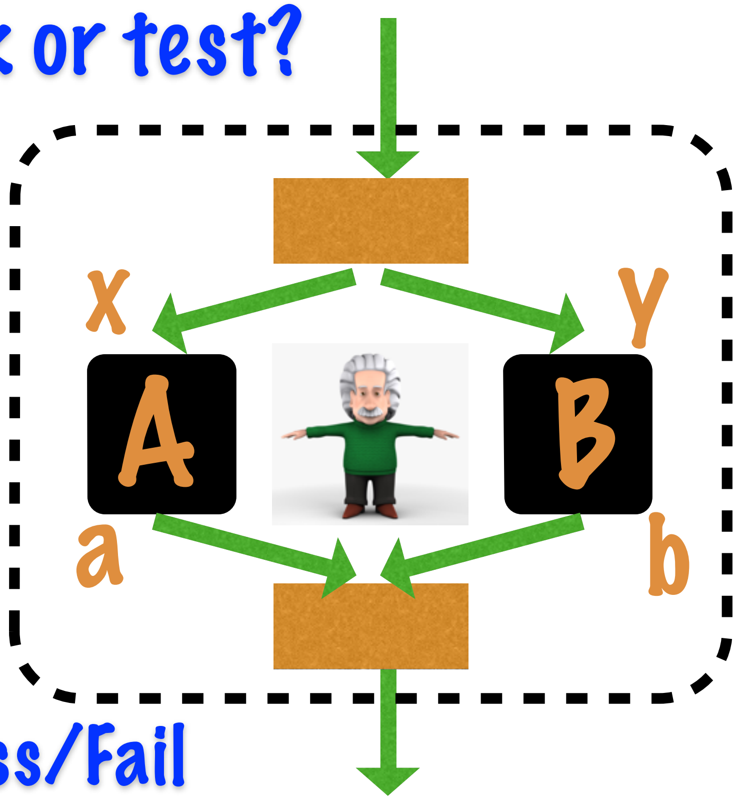
A general principle translating classical security to quantum security?

Thanks!

Questions?

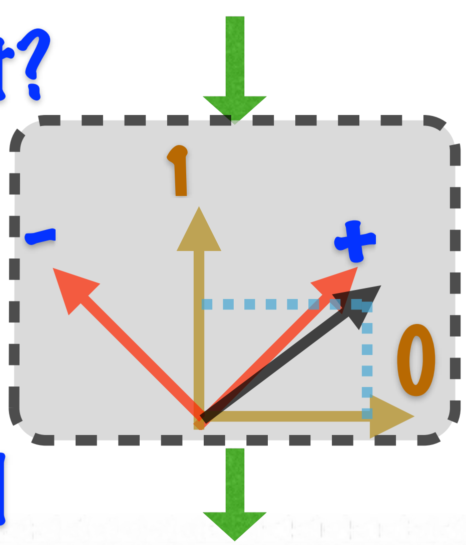
Forcing trust on adversarial devices

work or test?



0/1 or Pass/Fail

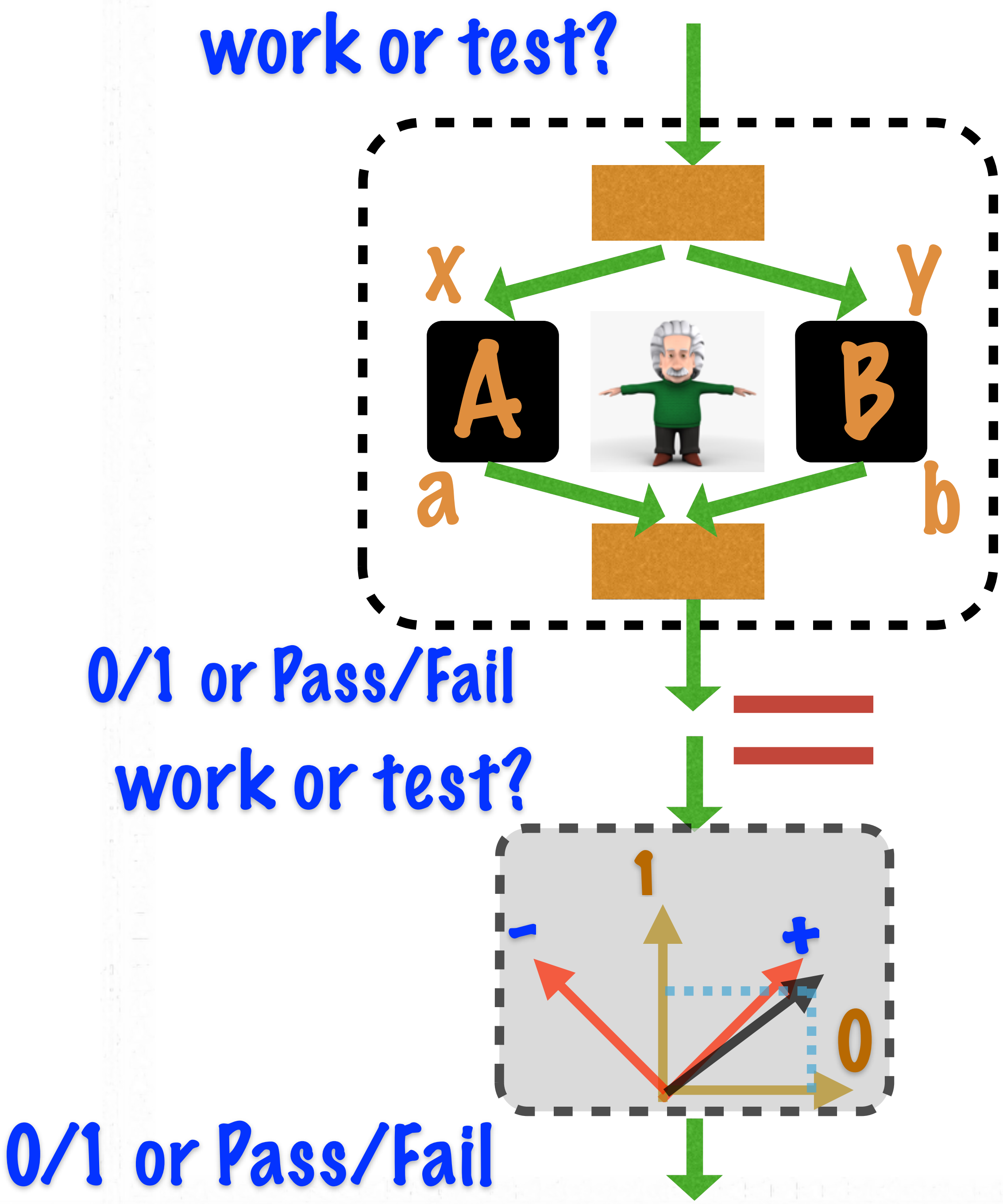
work or test?



0/1 or Pass/Fail

Method::seeded extraction

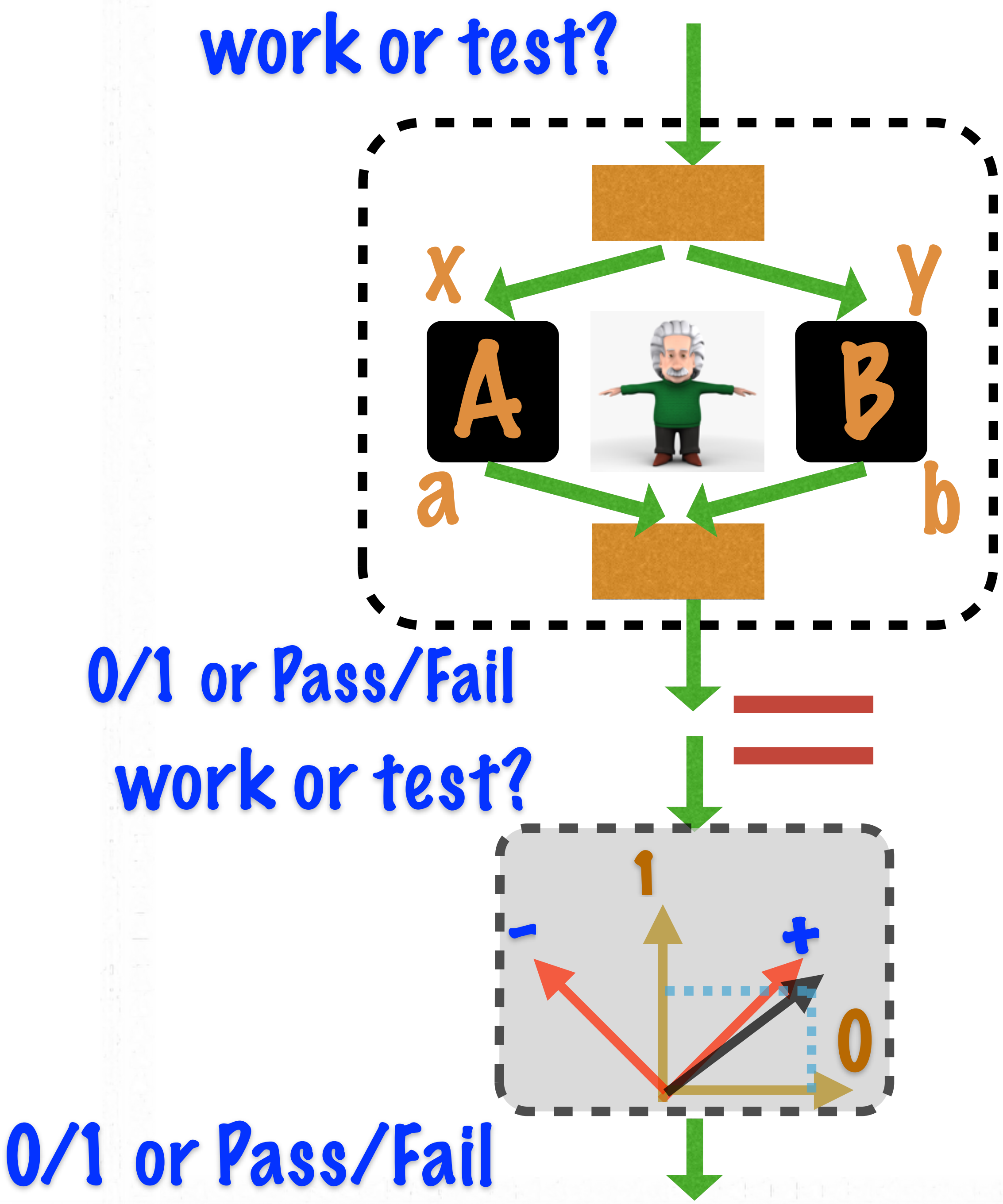
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device

Method::seeded extraction

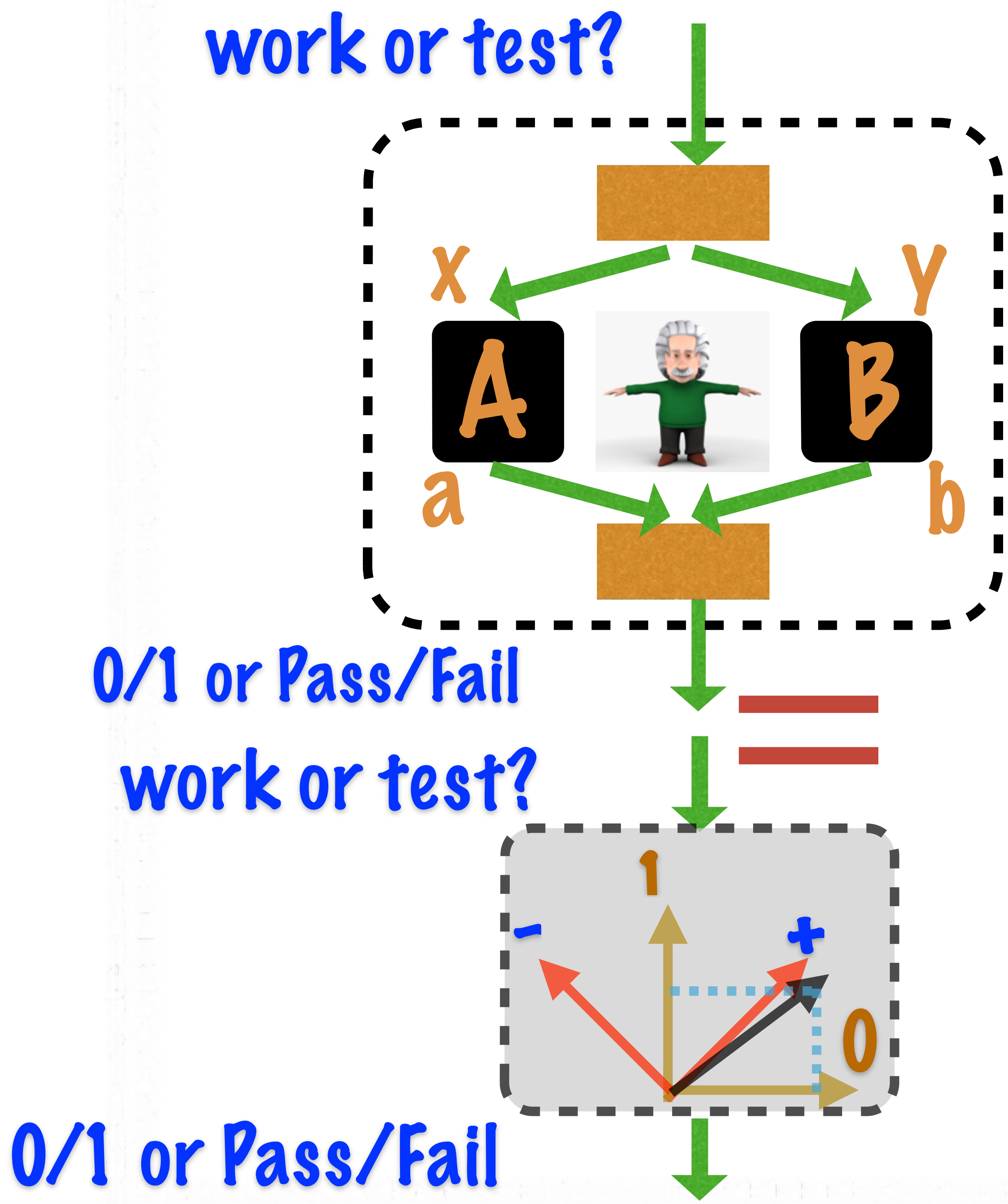
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.

Method::seeded extraction

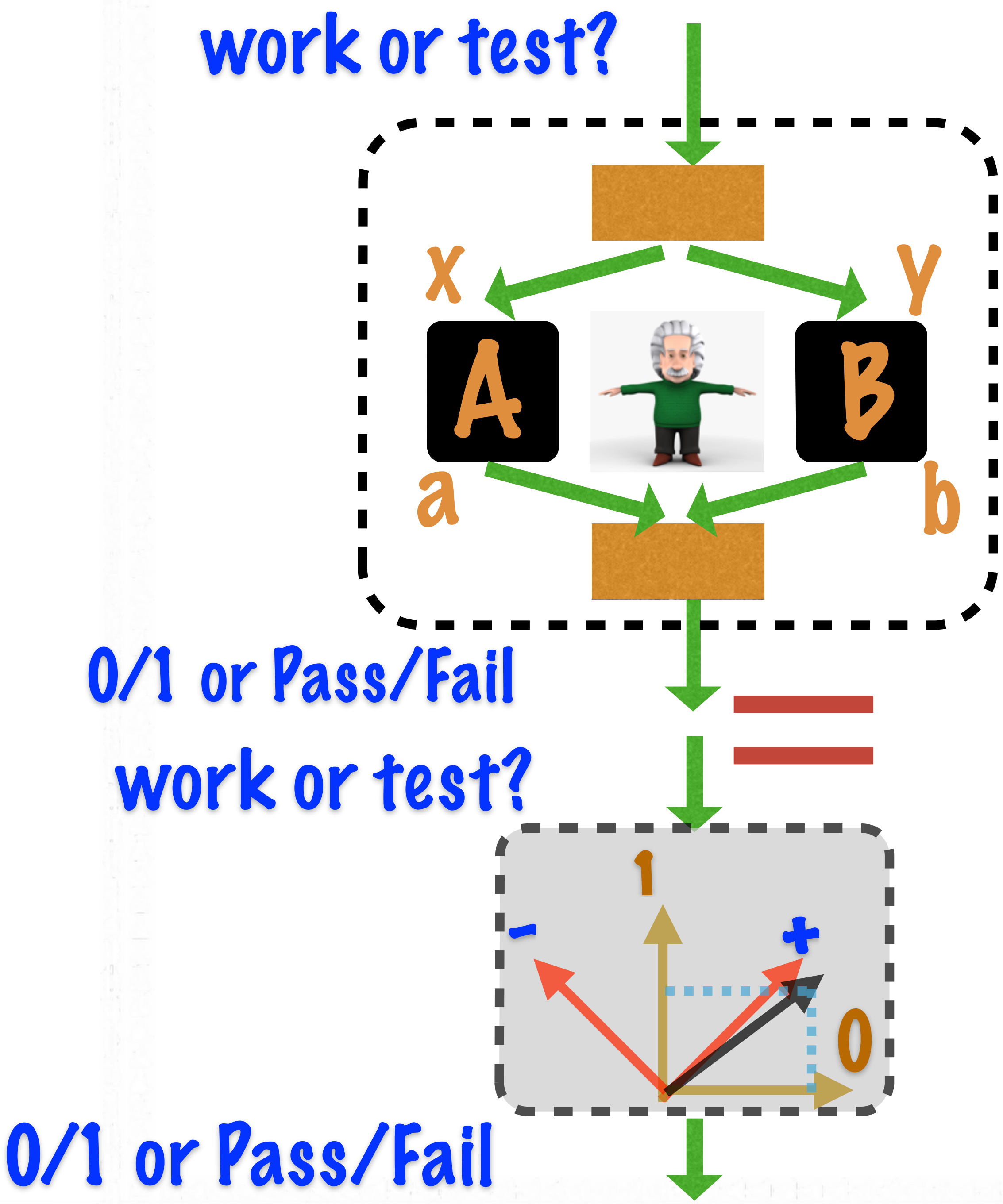
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.
- Trusted measurement device selects from anti-commuting measurements

Method::seeded extraction

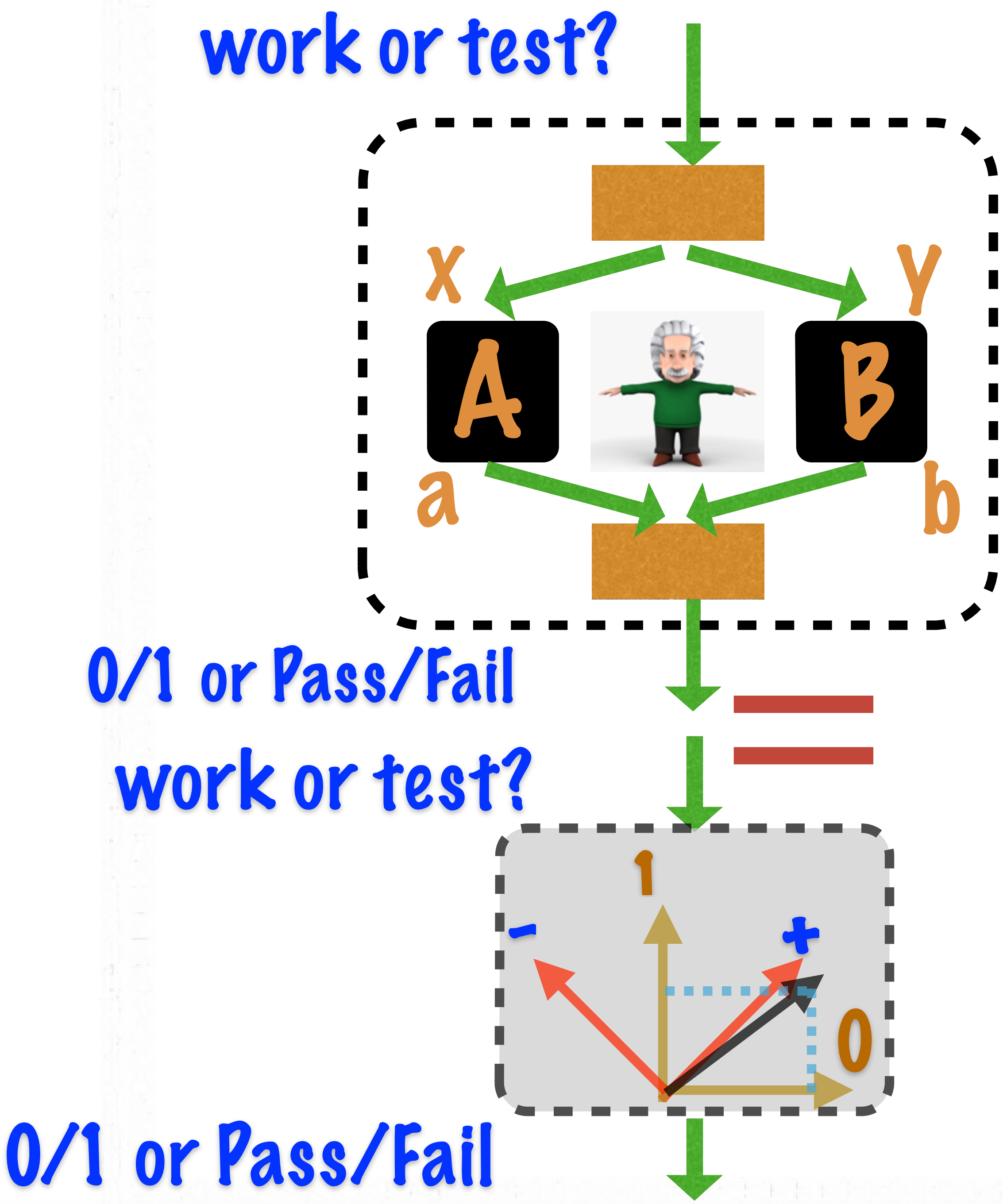
Forcing trust on adversarial devices



- Composed with the classical pre- and post-processing, each round is a single binary input/output device
- Proposition. The combined device always has a constant "trusted" measurement component.
- Trusted measurement device selects from anti-commuting measurements
  - work: measures 0/1

Method::seeded extraction

Forcing trust on adversarial devices

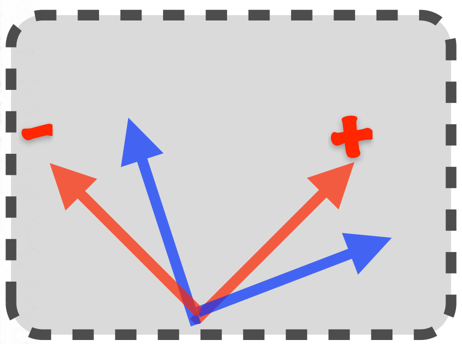


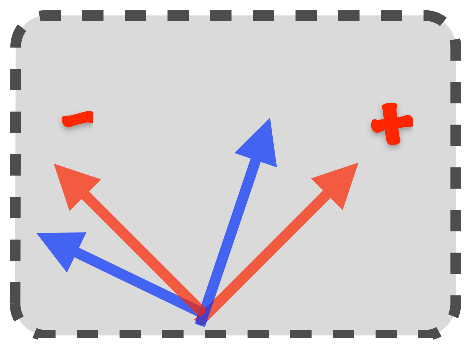
- Composed with the classical pre- and post-processing, each round is a **single binary input/output device**
- **Proposition.** The combined device always has a **constant "trusted" measurement component.**
- Trusted measurement device selects from **anti-commuting measurements**
  - work: measures 0/1
  - test: measures +/- (pass/fail)

Method::seeded extraction

Forcing trust: the case of CSHS

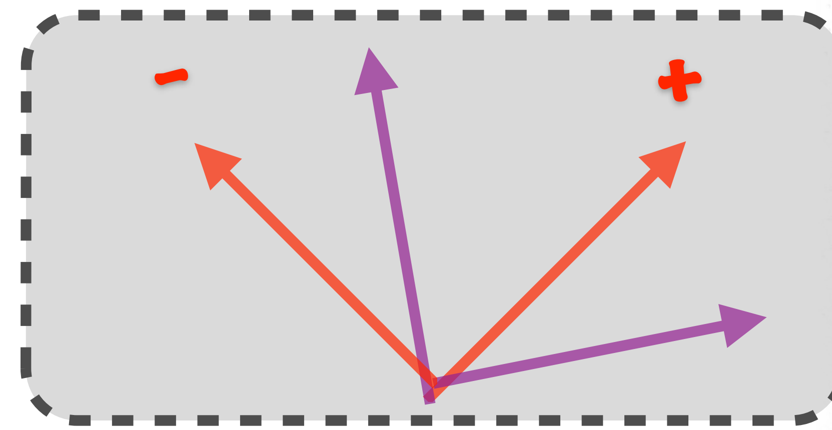
- On 0 measure M, on 1 measure N
- Simplify and normalize





$$M_A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad M_B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$N_A = \begin{pmatrix} 0 & x \\ \bar{x} & 0 \end{pmatrix} \qquad N_B = \begin{pmatrix} 0 & y \\ \bar{y} & 0 \end{pmatrix}$$



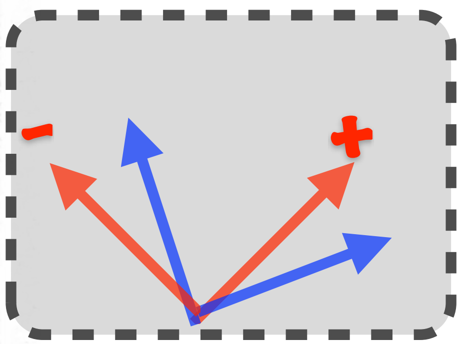
$$M_A \otimes I_B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

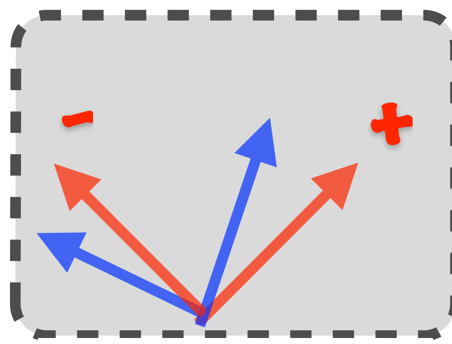
$$N_{AB} = \frac{1}{4} \begin{pmatrix} 0 & 0 & 0 & 1 + x + y - xy \\ 0 & 0 & 1 + x + \bar{y} - x\bar{y} & 0 \\ 0 & 1 + \bar{x} + y - \bar{x}y & 0 & 0 \\ 1 + \bar{x} + \bar{y} - \bar{x}\bar{y} & 0 & 0 & 0 \end{pmatrix}$$

Method::seeded extraction

Forcing trust: the case of CSHS

- On 0 measure M, on 1 measure N



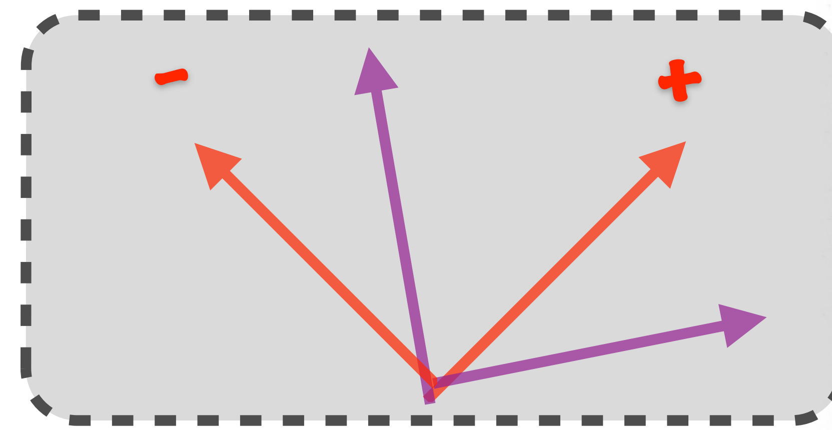


$$M_A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad M_B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$N_A = \begin{pmatrix} 0 & x \\ \bar{x} & 0 \end{pmatrix} \qquad N_B = \begin{pmatrix} 0 & y \\ \bar{y} & 0 \end{pmatrix}$$

- Simplify and normalize

=



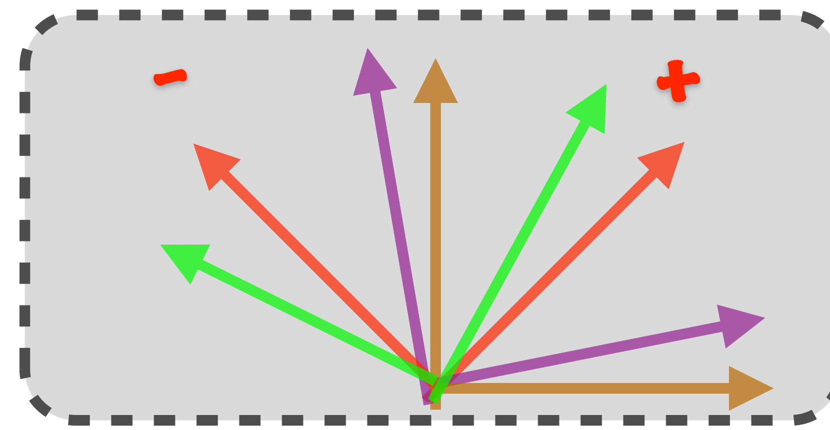
$$M_A \otimes I_B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$N_{AB} = \frac{1}{4} \begin{pmatrix} 0 & 0 & 0 & 1 + x + y - xy \\ 0 & 0 & 1 + x + \bar{y} - x\bar{y} & 0 \\ 0 & 1 + \bar{x} + y - \bar{x}y & 0 & 0 \\ 1 + \bar{x} + \bar{y} - \bar{x}\bar{y} & 0 & 0 & 0 \end{pmatrix}$$

Method::seeded extraction

Forcing trust: the case of CSHS

- **Proposition.** There exists a constant v, $0<v<1/\sqrt{2}$, s.t. for any N_{AB}, there exist T, N,
  - $N_{AB} = v\,T + (1/\sqrt{2}-v)\,N'$
  - $TM_A+M_AT=0$, $\|N'\|$, $\|T\|\leqq 1$ and
- Largest v: trust coefficient
  - $v \geqq .15$
- $1-1/\sqrt{2}$: coefficient for random coin flipping



$$M_A \otimes I_B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$N_{AB} = \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 & 1+x+y-xy \\ 0 & 0 & 1+x+\bar{y}-x\bar{y} & 0 \\ 0 & 1+\bar{x}+y-\bar{x}y & 0 & 0 \\ 1+\bar{x}+\bar{y}-\bar{x}\bar{y} & 0 & 0 & 0 \end{pmatrix}$$

Method::seeded extraction

Quantifying randomness

Method::seeded extraction

Quantifying randomness

- Smooth guessing probability $G_\epsilon(\rho_{YE})$: characterizes extractible bits in a C-Q state ρ_{YE}

  $G_\epsilon(\rho_{YE})$ = min {OPT prob. of guessing Y from E in ρ'_{YE} : $\|\rho'_{YE}-\rho_{YE}\|\leq\epsilon$}

Quantifying randomness

- Smooth guessing probability $G_\epsilon(\rho_{YE})$: characterizes extractible bits in a C-Q state ρ_{YE}

  $G_\epsilon(\rho_{YE})$ = min {OPT prob. of guessing Y from E in ρ'_{YE} : $\|\rho'_{YE}-\rho_{YE}\| \leq \epsilon$}

  - Difficult to bound $G_\epsilon(\rho_{YE})$ directly

Quantifying randomness

- Smooth guessing probability $G_\epsilon(\varrho_{YE})$: characterizes extractible bits in a C-Q state ϱ_{YE}

  $G_\epsilon(\varrho_{YE})$ = min {OPT prob. of guessing Y from E in ϱ'_{YE} : $\|\varrho'_{YE}-\varrho_{YE}\|\leq\epsilon$}

  - Difficult to bound $G_\epsilon(\varrho_{YE})$ directly

- Collision entropy $\mathrm{Tr}[\varrho^2]$: [DFW'14, TCR'09]

  $G_\epsilon(\varrho_{YE}) \leq (2/\epsilon^2)\, \mathrm{Tr}[\varrho'^2]$

Quantifying randomness

- Smooth guessing probability $G_\epsilon(\rho_{YE})$: characterizes extractible bits in a C-Q state ρ_{YE}

  $G_\epsilon(\rho_{YE})$ = min {OPT prob. of guessing Y from E in ρ'_{YE} : $\|\rho'_{YE}-\rho_{YE}\| \leqq \epsilon$}

  - Difficult to bound $G_\epsilon(\rho_{YE})$ directly

- Collision entropy $Tr[\rho^2]$: [DFW'14, TCR'09]

  $G_\epsilon(\rho_{YE}) \leqq (2/\epsilon^2)\, Tr[\rho'^2]$

  - No sensitive enough to detect generated randomness for small q.

Method::seeded extraction

Quantifying randomness

- Smooth guessing probability $G_\epsilon(\rho_{YE})$: characterizes extractible bits in a C-Q state ρ_{YE}

  $G_\epsilon(\rho_{YE})$ = min {OPT prob. of guessing Y from E in ρ'_{YE} : $\|\rho'_{YE}-\rho_{YE}\|\leqq\epsilon$}

  - Difficult to bound $G_\epsilon(\rho_{YE})$ directly

- Collision entropy $\mathrm{Tr}[\rho^2]$: [DFW'14, TCR'09]

  $G_\epsilon(\rho_{YE}) \leqq (2/\epsilon^2)\,\mathrm{Tr}[\rho'^2]$

  - No sensitive enough to detect generated randomness for small q.

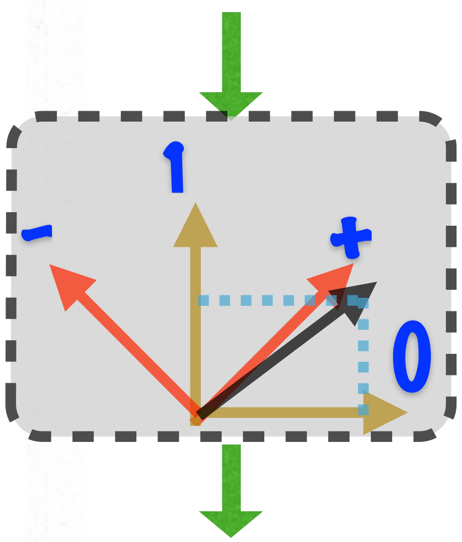
- Schatten norm $\mathrm{Tr}(\rho^{1+q})$: turns out to be appropriate

  $G_\epsilon(\rho_{YE})^q \leqq (2/\epsilon^2)\,\mathrm{Tr}[\rho'^{1+q}]$

Method::seeded extraction

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?

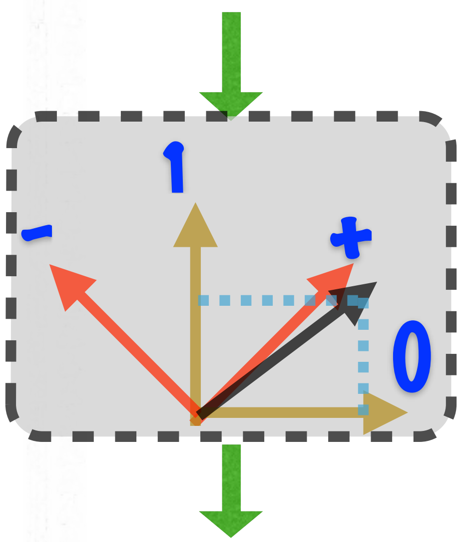


0/1 or Pass/Fail

Method::seeded extraction

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?

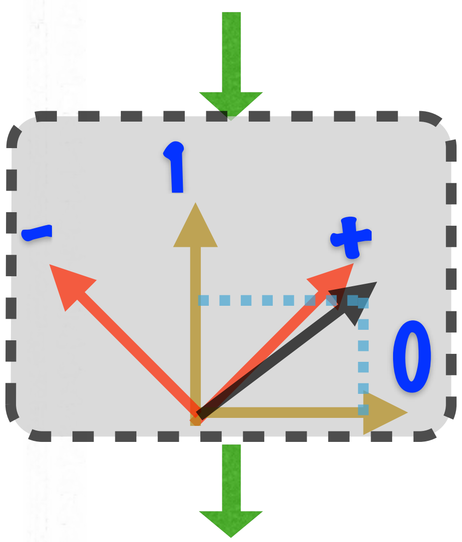


0/1 or Pass/Fail

- If the chance of passing is high, then the bit generated tends to be random

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?

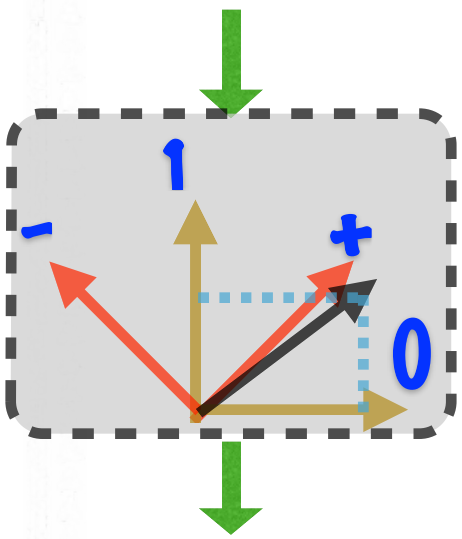


0/1 or Pass/Fail

- If the chance of passing is high, then the bit generated tends to be random
- Uncertainty Principle: the two measurement outcomes cannot be close to deterministic at the same time

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?



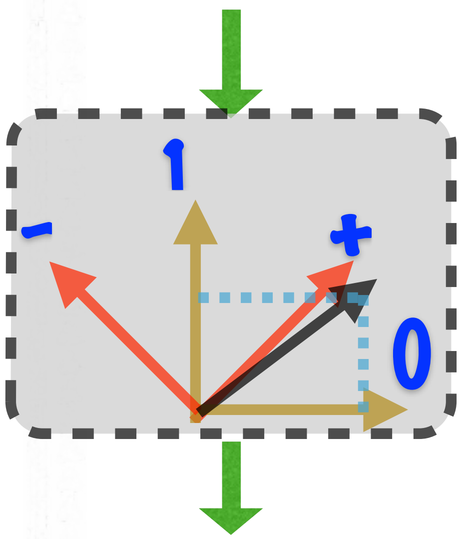
0/1 or Pass/Fail

- If the chance of passing is high, then the bit generated tends to be random
- Uncertainty Principle: the two measurement outcomes cannot be close to deterministic at the same time

Theorem. Let ρ_0, ρ_1, ρ_P, ρ_F, be the adversary's "states" from measuring 0/1 and +/-, respectively. For sufficiently small δ and q,

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?



0/1 or Pass/Fail

- If the chance of passing is high, then the bit generated tends to be random
- Uncertainty Principle: the two measurement outcomes cannot be close to deterministic at the same time

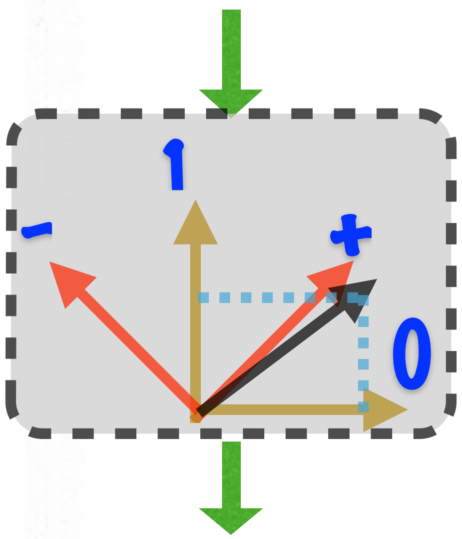
Theorem. Let ρ_0, ρ_1, ρ_P, ρ_F, be the adversary's "states" from measuring 0/1 and +/-, respectively. For sufficiently small δ and q,

$$\text{if } \mathrm{Tr}(\rho_F^{1+q}) \leq \delta\, \mathrm{Tr}(\rho^{1+q}), \qquad \mathrm{Tr}(\rho_0^{1+q}) + \mathrm{Tr}(\rho_1^{1+q}) \leq (1/2)^{q\pi(q,\delta)}\, \mathrm{Tr}(\rho^{1+q})$$

Method::seeded extraction

Why anti-commuting measurements are good? —A Schatten norm Uncertainty Principle

work or test?



0/1 or Pass/Fail

- If the chance of passing is high, then the bit generated tends to be random

- Uncertainty Principle: the two measurement outcomes cannot be close to deterministic at the same time

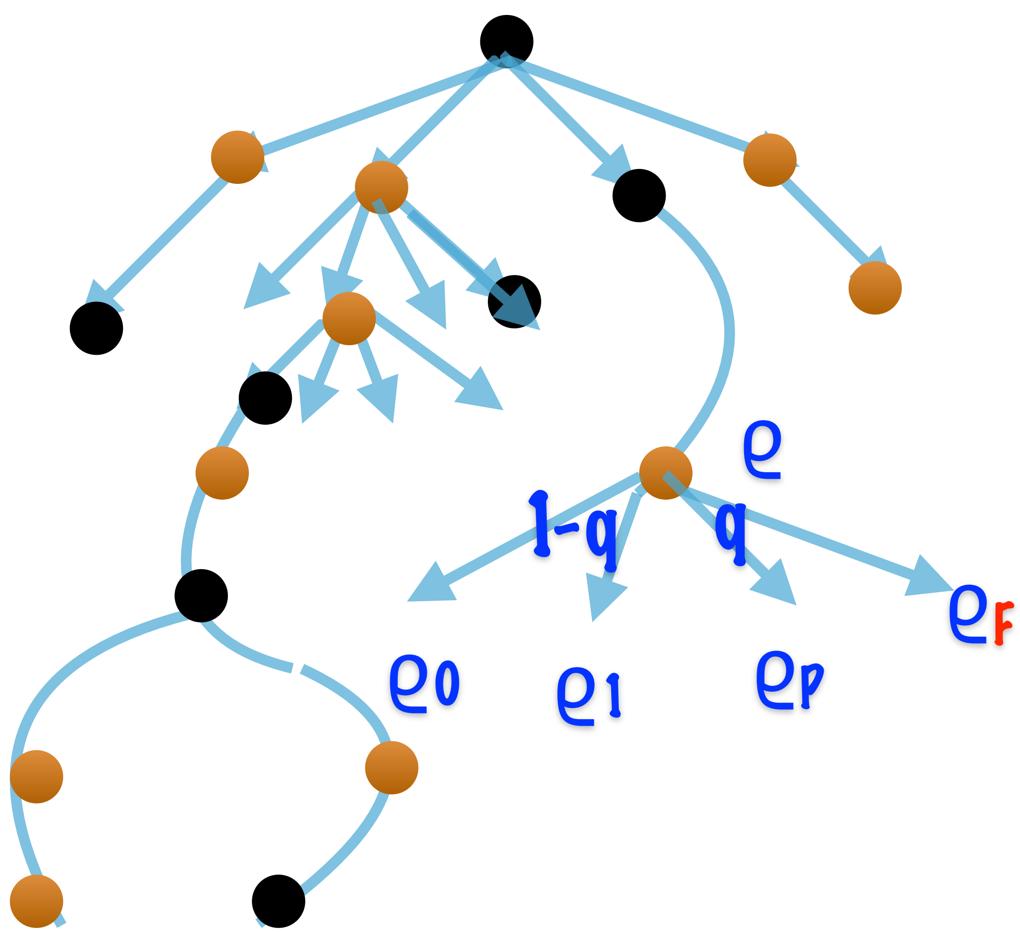
Theorem. Let ρ_0, ρ_1, ρ_P, ρ_F, be the adversary's "states" from measuring 0/1 and +/-, respectively. For sufficiently small δ and q,

if $\mathrm{Tr}(\rho_F^{1+q}) \leq \delta\, \mathrm{Tr}(\rho^{1+q})$, $\quad \mathrm{Tr}(\rho_0^{1+q}) + \mathrm{Tr}(\rho_1^{1+q}) \leq (1/2)^{q\pi(q,\delta)}\, \mathrm{Tr}(\rho^{1+q})$

$\pi(q,\delta) \to$ 1, when q, $\delta \to 0$

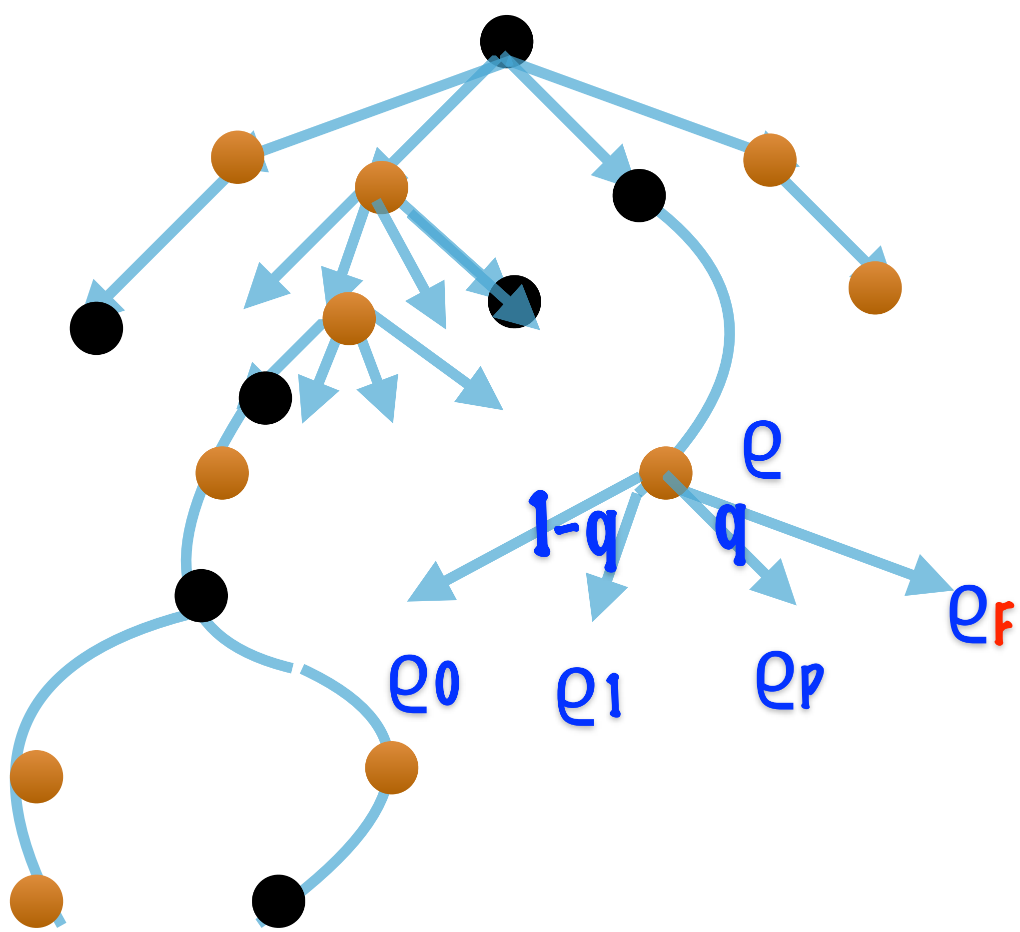
Method::seeded extraction

Amortized randomness generation



Method::seeded extraction

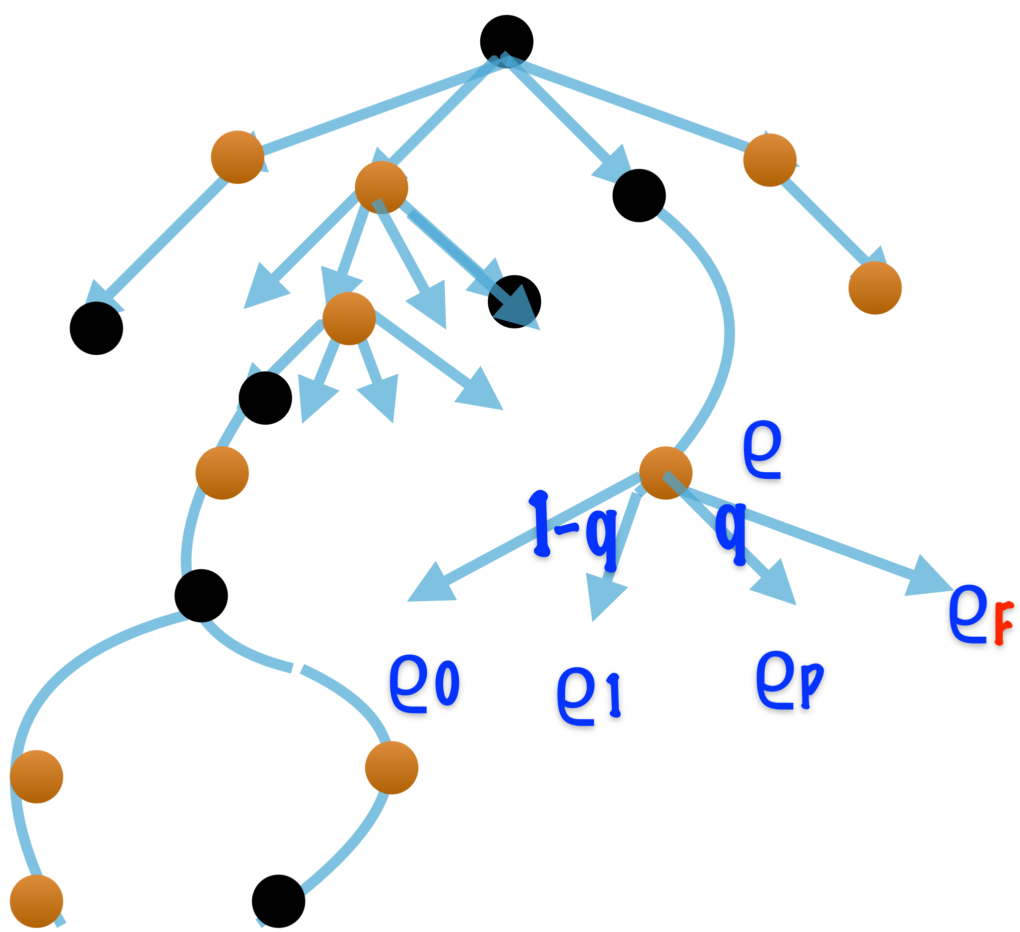
Amortized randomness generation



- The behavior at each round depends on the history

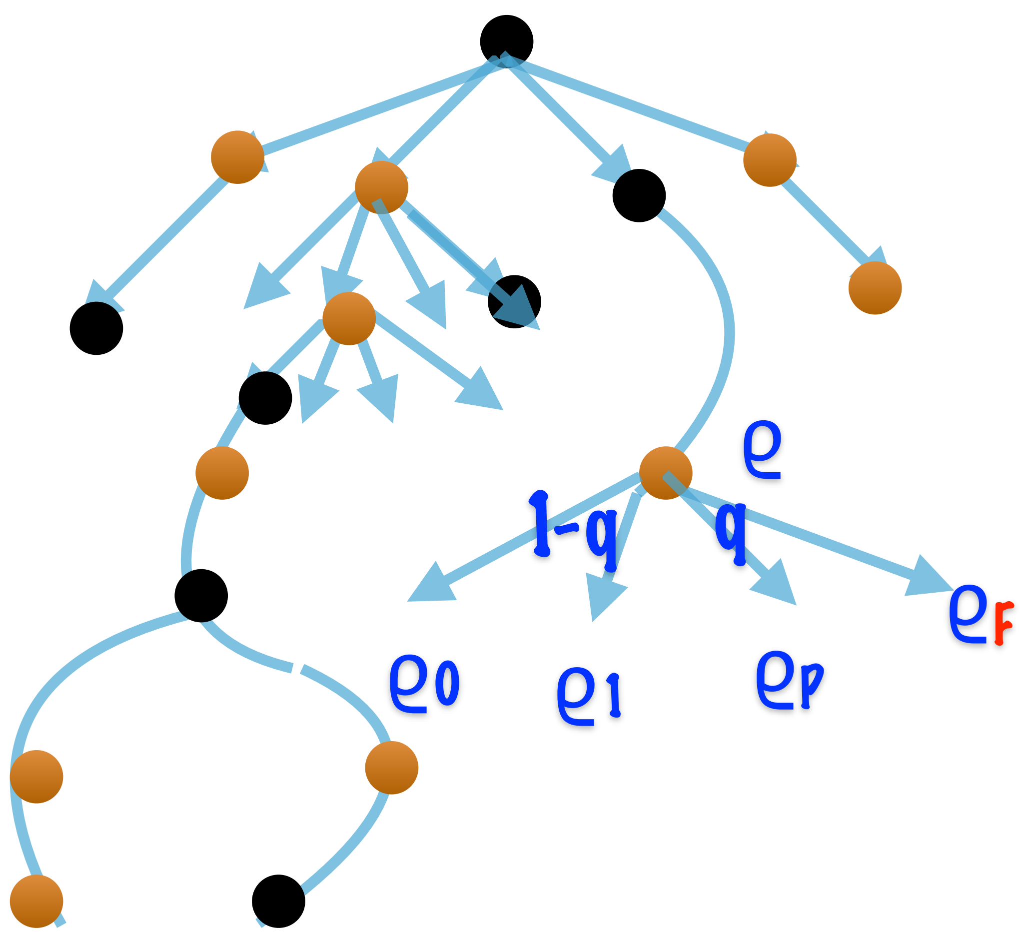
Method::seeded extraction

Amortized randomness generation



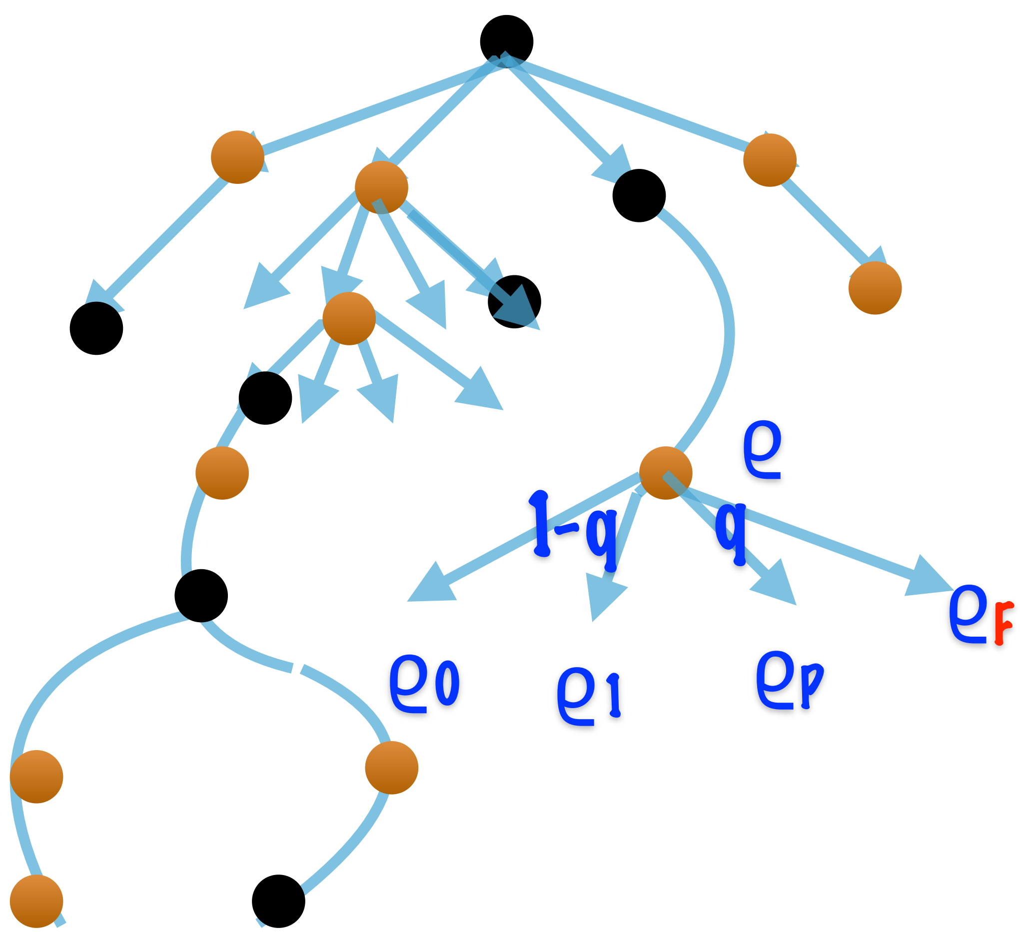
- The behavior at each round depends on the history
- If failing test, "toss a coin" and "loan" some randomness to the protocol

Amortized randomness generation



- The behavior at each round depends on the history
- If failing test, "toss a coin" and "loan" some randomness to the protocol
  - Ensuring each step increase randomness

Amortized randomness generation



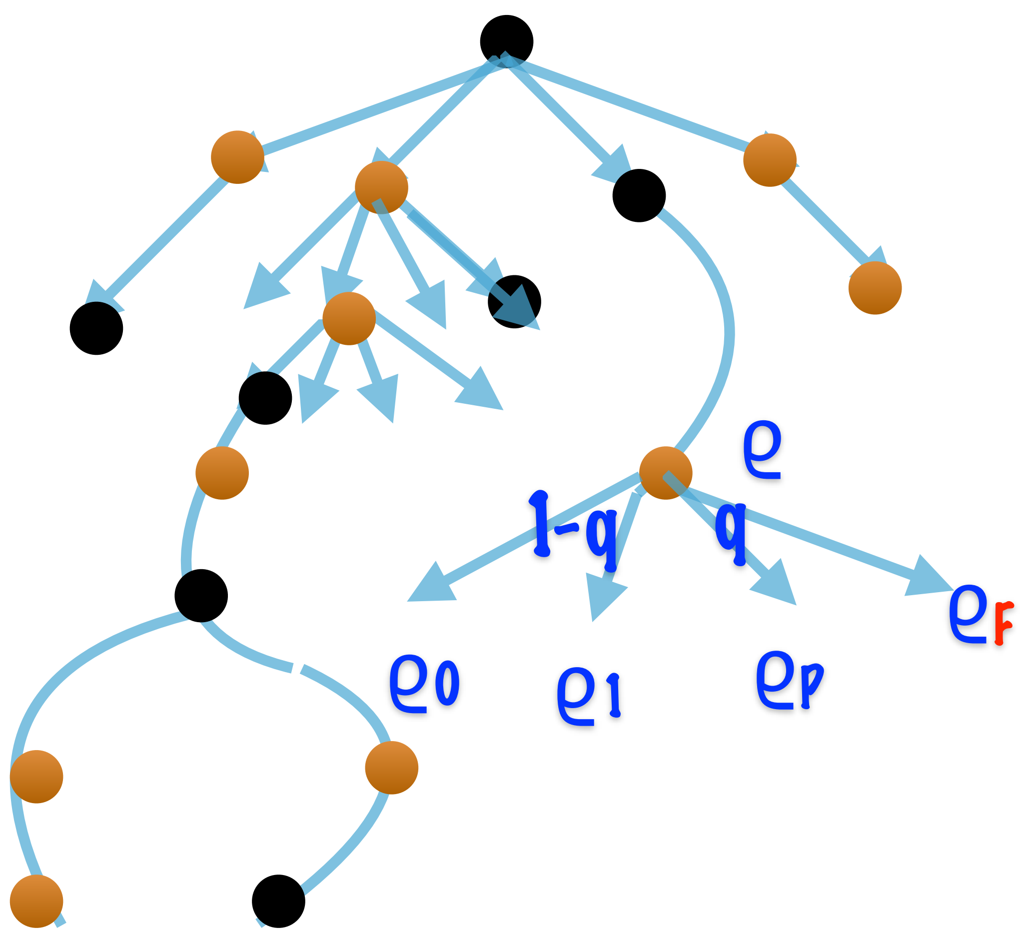
- The behavior at each round depends on the history
- If failing test, "toss a coin" and "loan" some randomness to the protocol
  - Ensuring each step increase randomness

Geometrically decreasing:

$$\mathrm{Tr}[(1-q)\rho_0^{1+q} + (1-q)\rho_1^{1+q} + q\rho_P^{1+q} + (1/2)q\rho_F^{1+q}]$$

Method::seeded extraction

Amortized randomness generation



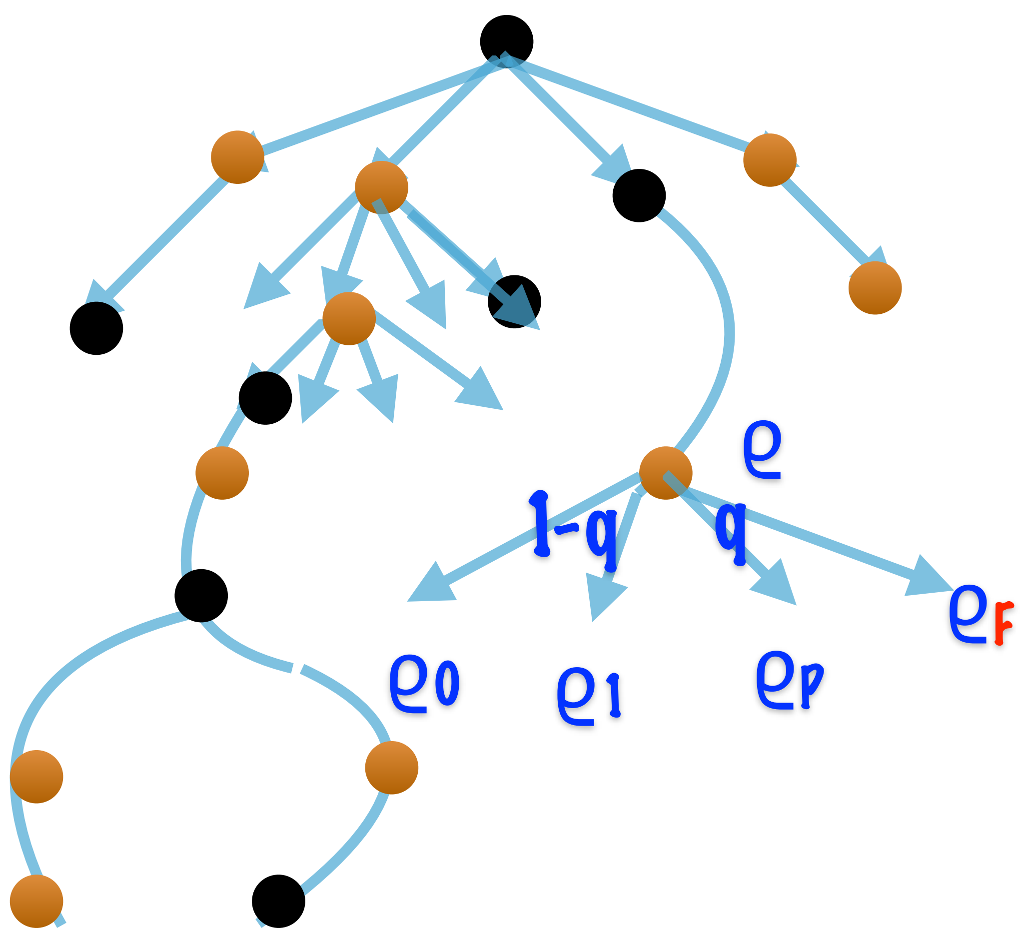
- The behavior at each round depends on the history
- If failing test, "toss a coin" and "loan" some randomness to the protocol
  - Ensuring each step increase randomness
- Total amount of loans is small (few testing rounds)

Geometrically decreasing:

$$\mathrm{Tr}[(1-q)\rho_0^{1+q} + (1-q)\rho_1^{1+q} + q\rho_P^{1+q} + (1/2)q\rho_F^{1+q}]$$

Method::seeded extraction

Amortized randomness generation

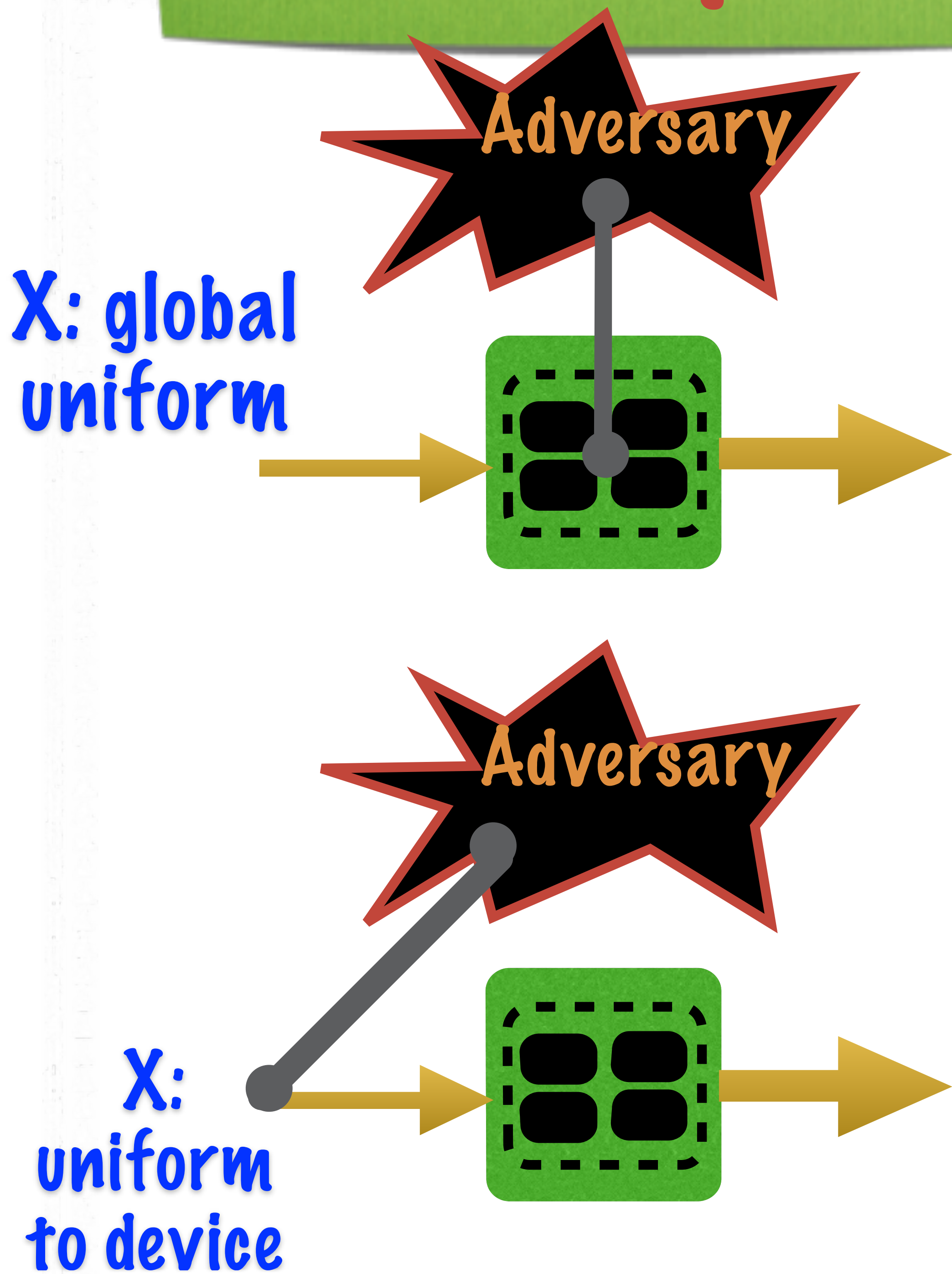


- The behavior at each round depends on the history
- If failing test, "toss a coin" and "loan" some randomness to the protocol
    - Ensuring each step increase randomness
- Total amount of loans is small (few testing rounds)
    - Fresh randomness still a lot

Geometrically decreasing:

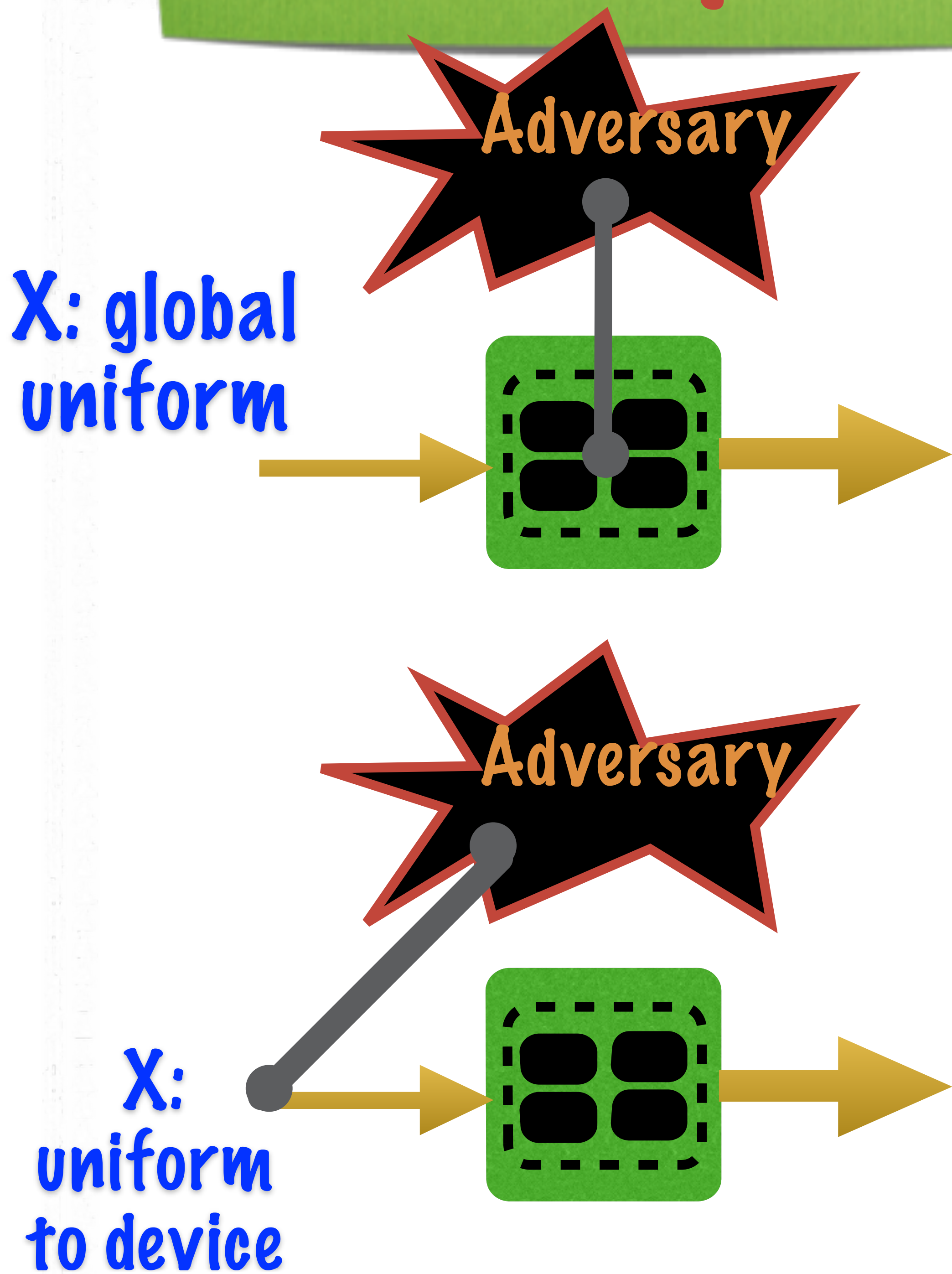
$$\mathrm{Tr}[(1-q)\rho_0^{1+q} + (1-q)\rho_1^{1+q} + q\rho_P^{1+q} + (1/2)q\rho_F^{1+q}]$$

Security under composition: Equivalence Lemma



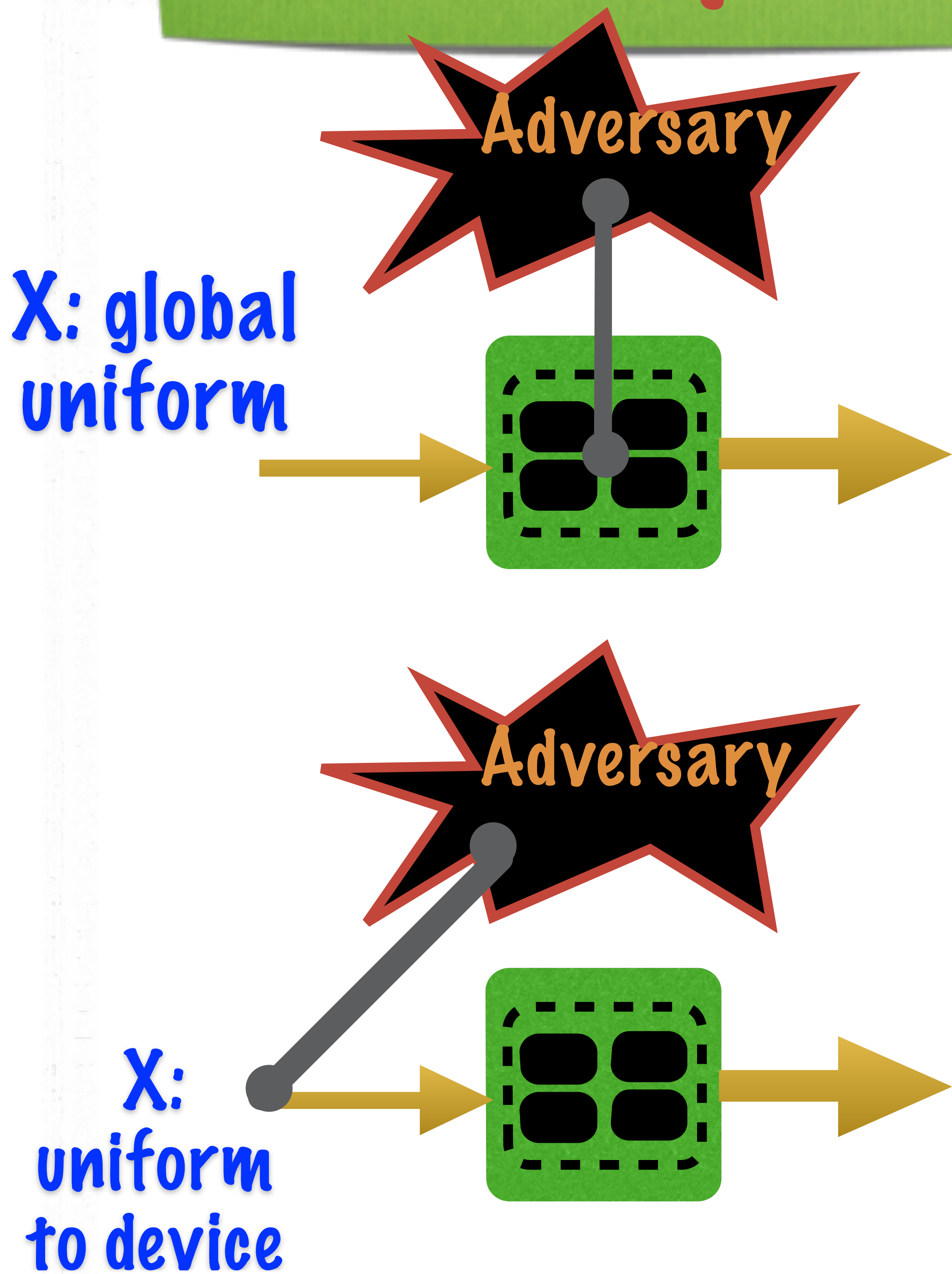
Method::seedless extraction

Security under composition: Equivalence Lemma



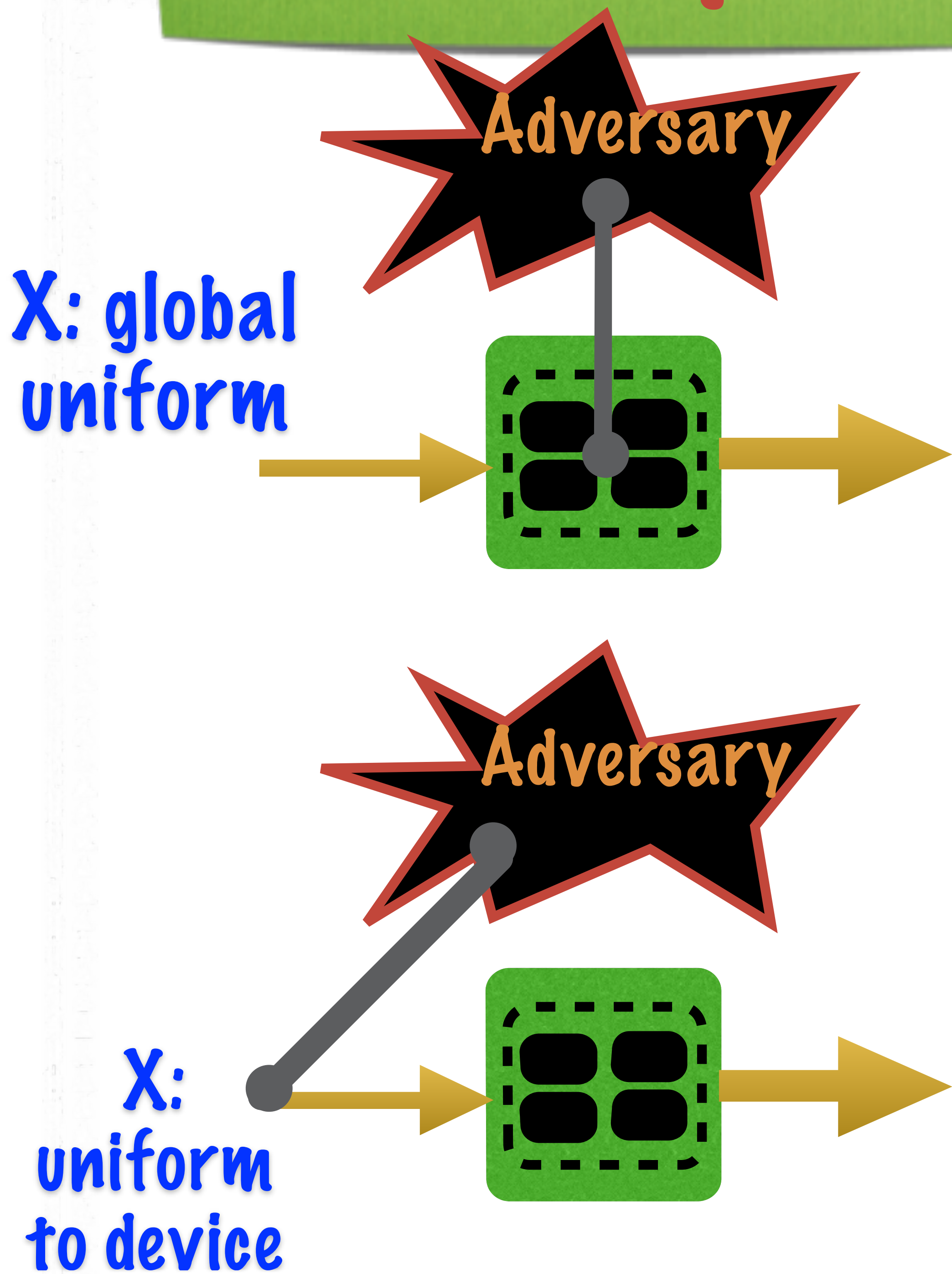
- All known expansion protocols were proved assuming globally uniform input

Security under composition: Equivalence Lemma



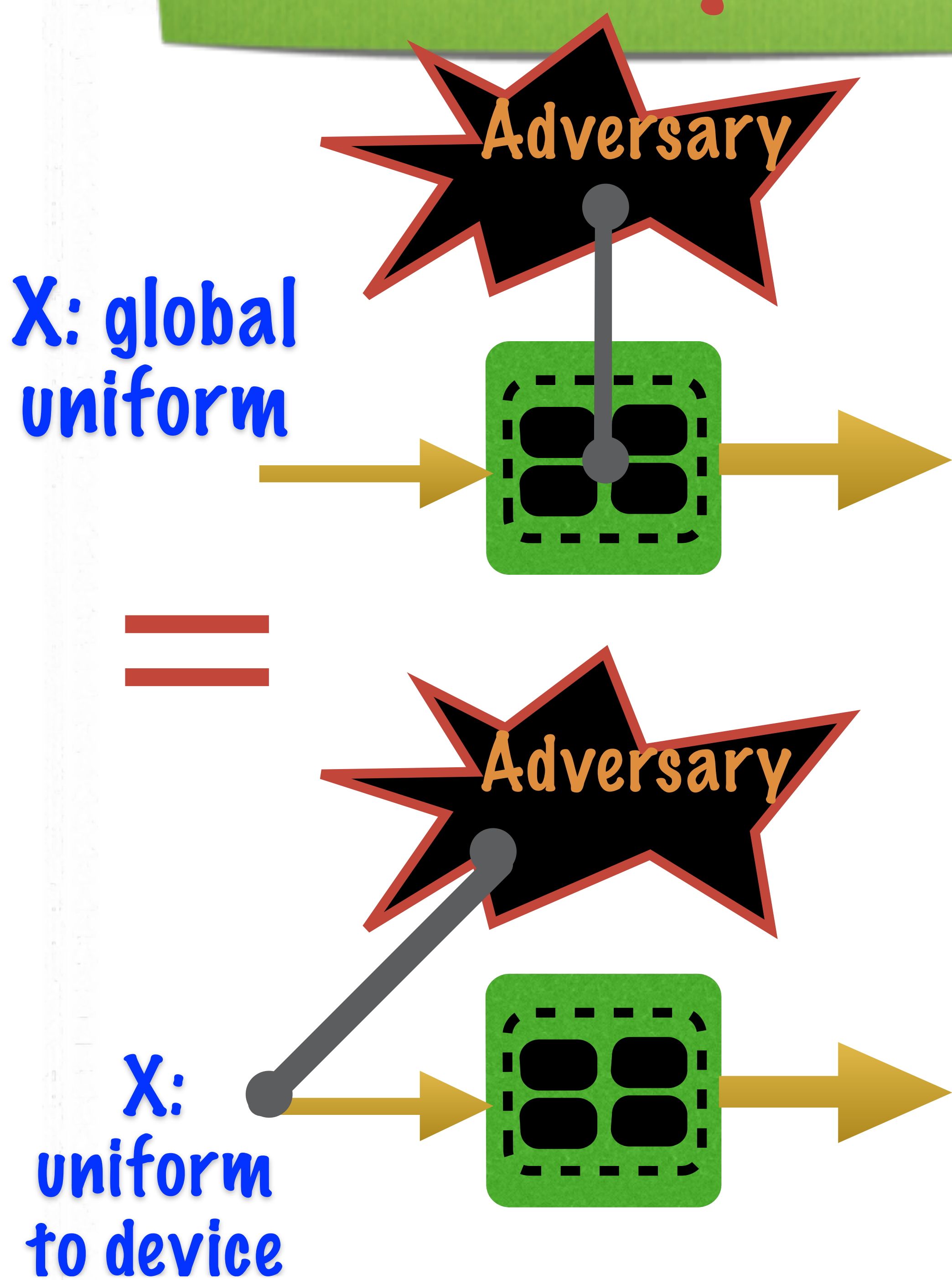
- All known expansion protocols were proved assuming globally uniform input
- Equivalence Lemma: same performance using uniform-to-device input

Security under composition: Equivalence Lemma



- All known expansion protocols were proved assuming globally uniform input
- Equivalence Lemma: same performance using uniform-to-device input
  - All correlations with Adversary can be produced from global uniform input by an operator OP commuting with protocol

Security under composition: Equivalence Lemma



- All known expansion protocols were proved assuming globally uniform input
- Equivalence Lemma: same performance using uniform-to-device input
  - All correlations with Adversary can be produced from global uniform input by an operator OP commuting with protocol
  - OP does not change performance

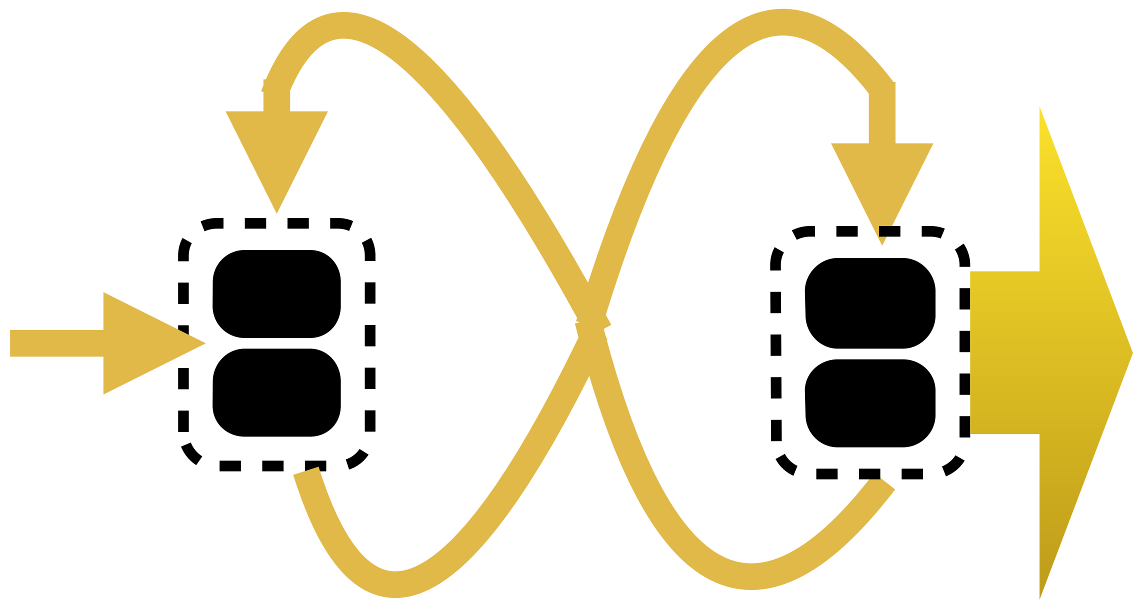
Method::seedless extraction

E.L. implies unbounded expansion from cross-feeding any protocol

Invariant: each device's output is (close to) uniform to the other device

Method::Equivalence Lemma

E.L. implies unbounded expansion from cross-feeding any protocol



Invariant: each device's output is (close to) uniform to the other device

Method::Equivalence Lemma