Infinite Randomness Expansion and Amplification with a Constant Number of Devices

Matthew Coudron, Henry Yuen

MIT EECS

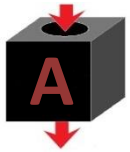
arXiv 1310.6755

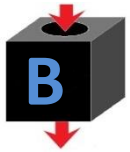
Randomness Expansion

- Roger Colbeck – PhD Thesis, 2006

S = Input Seed

Randomness Expansion

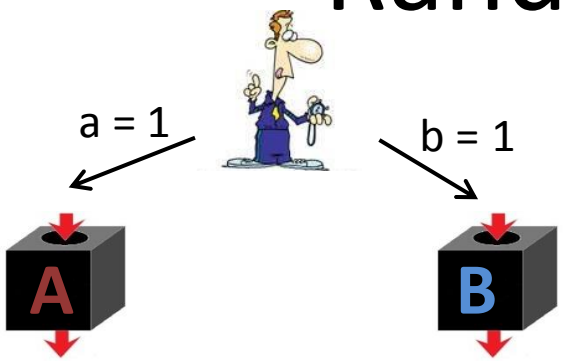




- Roger Colbeck – PhD Thesis, 2006

S = Input Seed

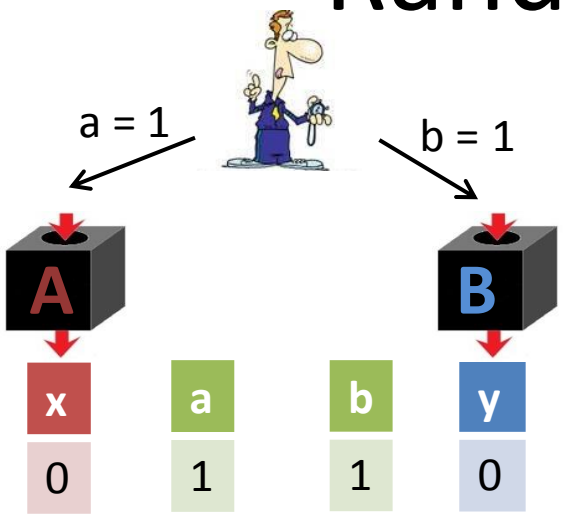
Randomness Expansion



- Roger Colbeck – PhD Thesis, 2006

S = Input Seed

Randomness Expansion

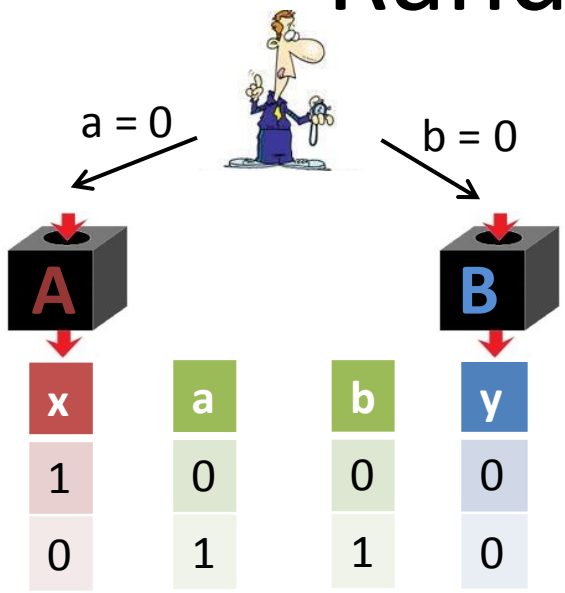


- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

S = Input Seed

Randomness Expansion

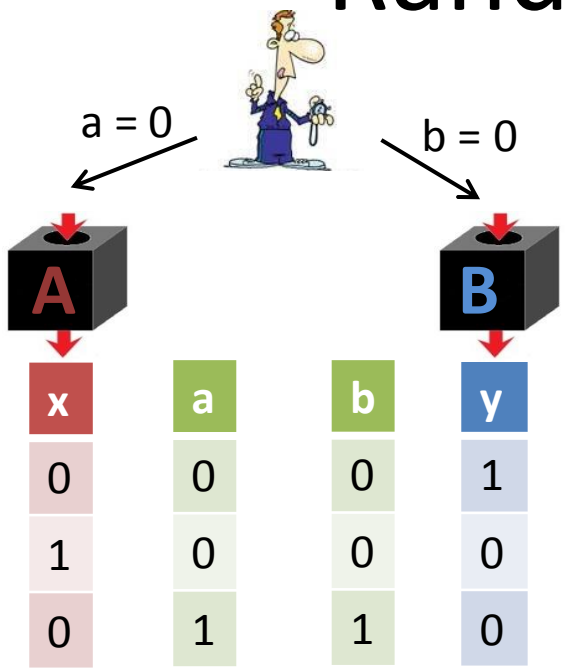


- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

S = Input Seed

Randomness Expansion

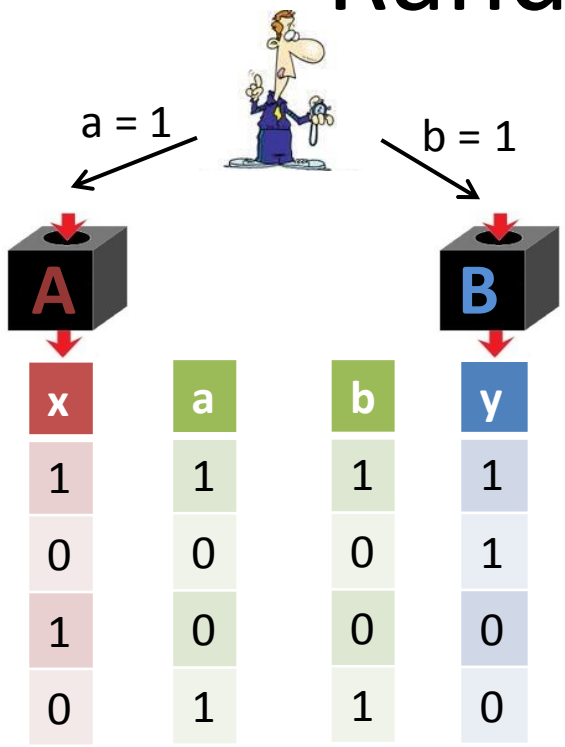


- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

S = Input Seed

Randomness Expansion



- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

Randomness Expansion

S = Input Seed

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

Test

O = Output

- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

Test

Pass

O = Output

- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

O has high Min-Entropy
(high “randomness”)

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

Test

Fail

Abort Protocol

Pass

O = Output

- Roger Colbeck – PhD Thesis, 2006
- Serial rounds

  “Query and Response”

O has high Min-Entropy
(high “randomness”)

S = Input Seed

Randomness Expansion

VV Protocol [Vazirani, Vidick '11]

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

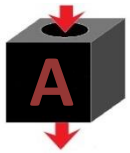
S = Input Seed

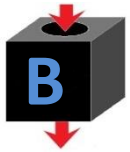
Randomness Expansion

VV Protocol [Vazirani, Vidick '11]

a = 1

b = 0





x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

- Exponential expansion

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

VV Protocol [Vazirani, Vidick '11]

- Exponential expansion

n bit seed -> O has $2^{\sqrt[3]{n}}$ Min Entropy

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

VV Protocol [Vazirani, Vidick '11]

- Exponential expansion

n bit seed -> O has $2^{\sqrt[3]{n}}$ Min Entropy

- Secure against quantum eavesdropper

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

VV Protocol [Vazirani, Vidick '11]

- Exponential expansion

n bit seed -> O has $2^{\sqrt[3]{n}}$ Min Entropy

- Secure against quantum eavesdropper

S = Input Seed

Randomness Expansion

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O = Output

VV Protocol [Vazirani, Vidick '11]

- Exponential expansion

n bit seed -> O has $2^{\sqrt[3]{n}}$ Min Entropy

- Secure against quantum eavesdropper

$$\rho_{SDE} \approx \rho_U \otimes \rho_{DE} \Rightarrow \rho_{OE} \approx \rho_U \otimes \rho_E$$

Questions

1) What is the greatest possible rate of randomness expansion? Exponential? Higher?

Questions

1) What is the greatest possible rate of randomness expansion? Exponential? Higher?
2) How does the expansion rate depend on # of devices used?

Questions

1) What is the greatest possible rate of randomness expansion? Exponential? Higher?
2) How does the expansion rate depend on # of devices used?

Our Result:

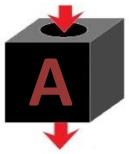
Infinite randomness expansion with 8 devices.
(We can also do 6)

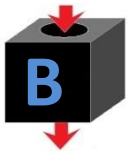
Input Seed

Compose?

a = 1

b = 0





x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O

Input Seed

Compose?

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O

Input Seed

Compose?

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O

a = 1

b = 0

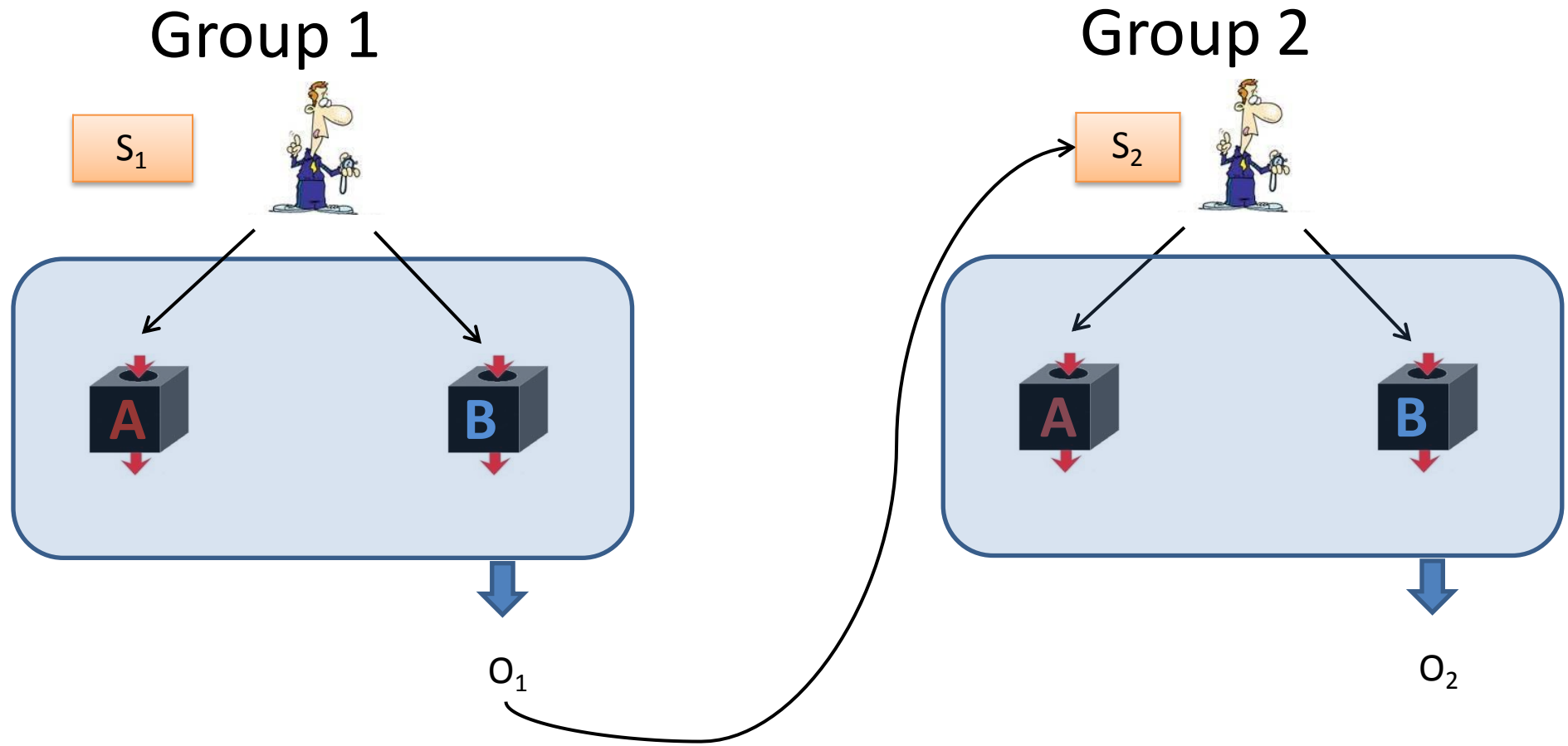
A

B

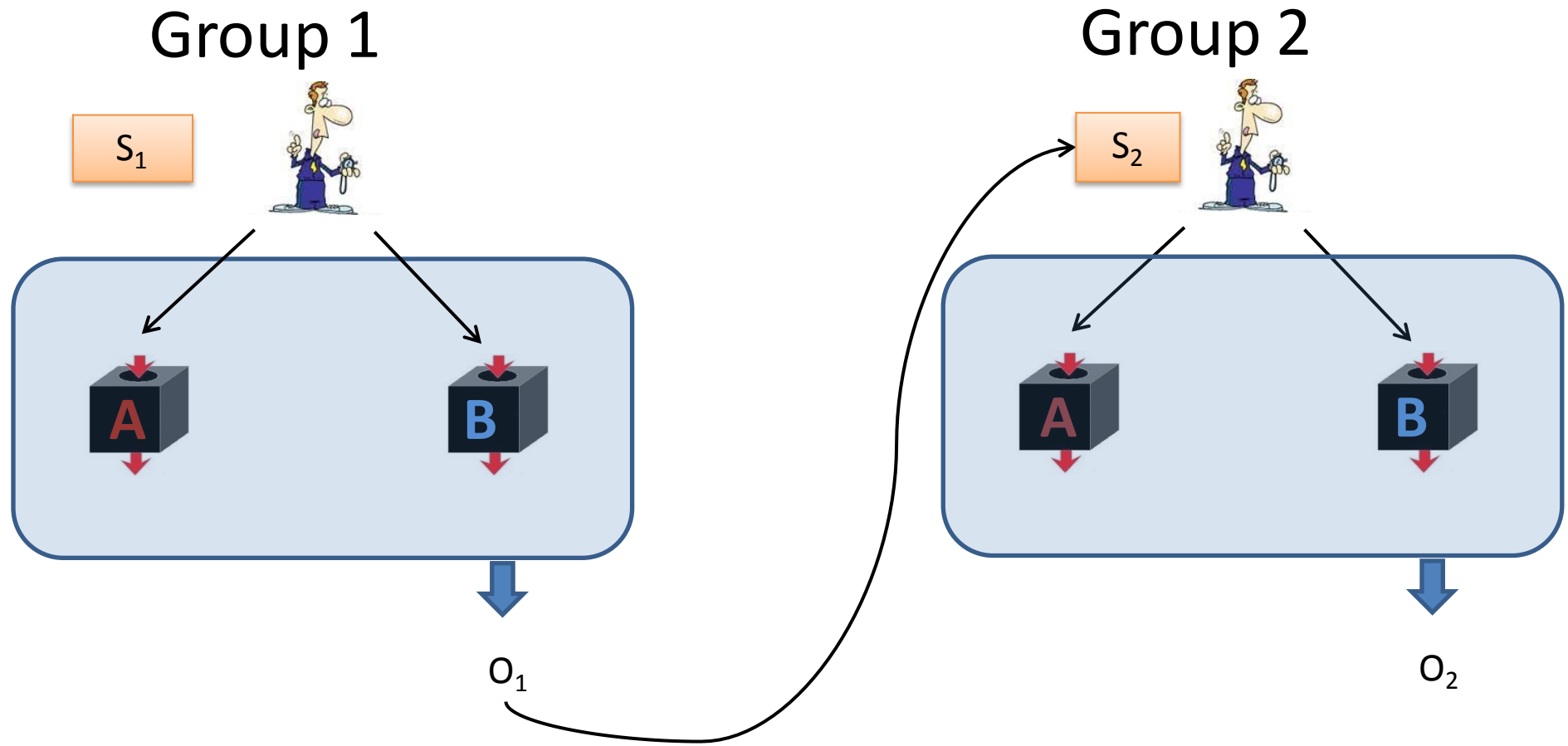
x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

O

Compose?

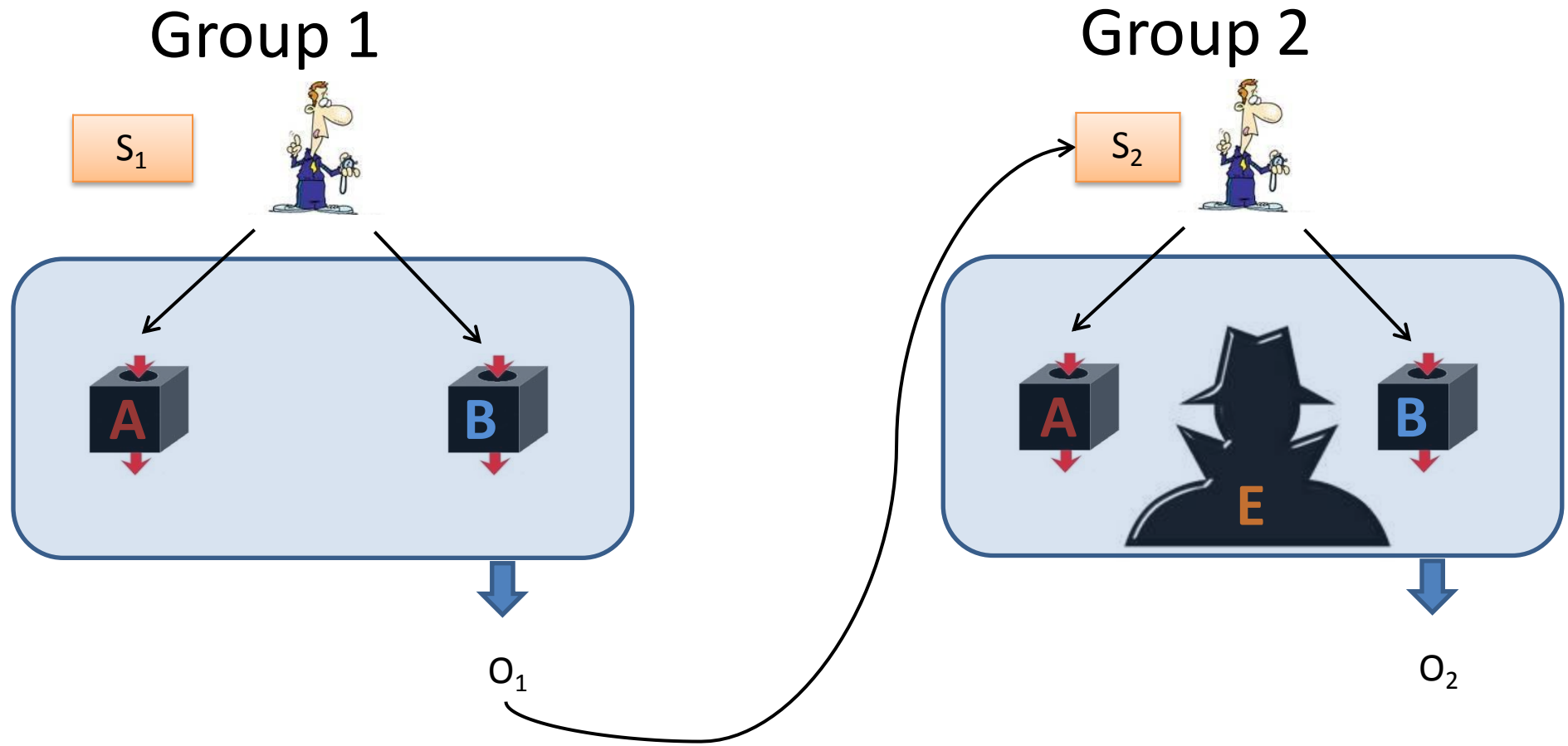


Compose?



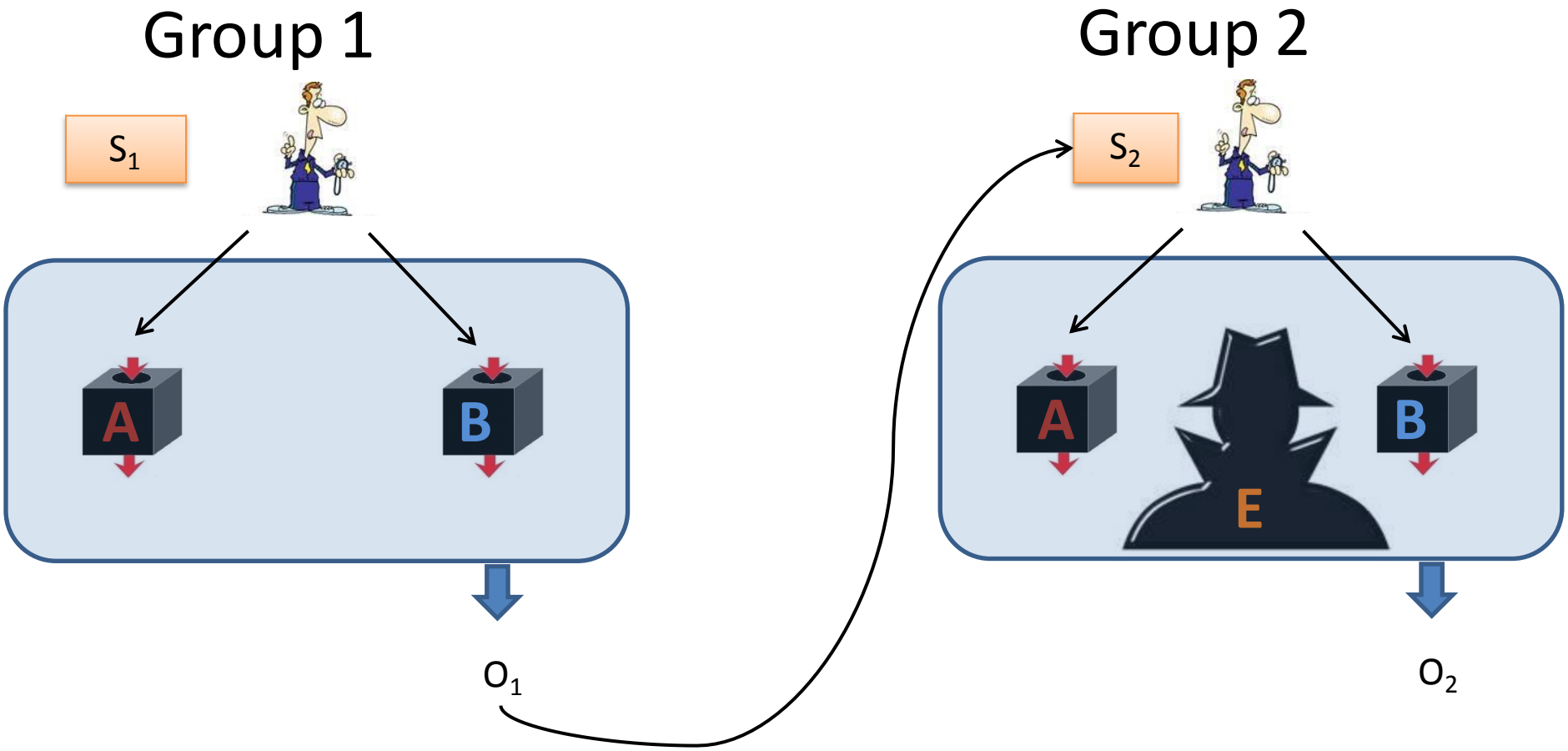
Secure Against Eavesdropper

Compose?



Secure Against Eavesdropper

Compose?

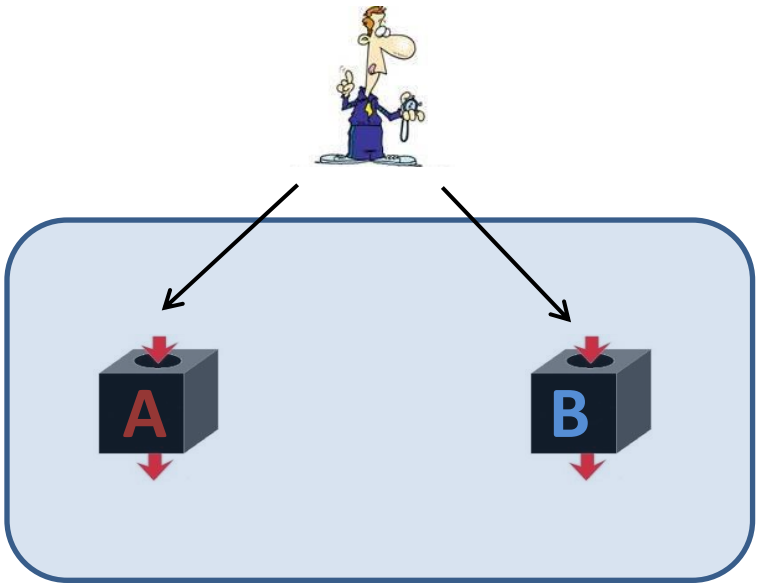


Secure Against Eavesdropper

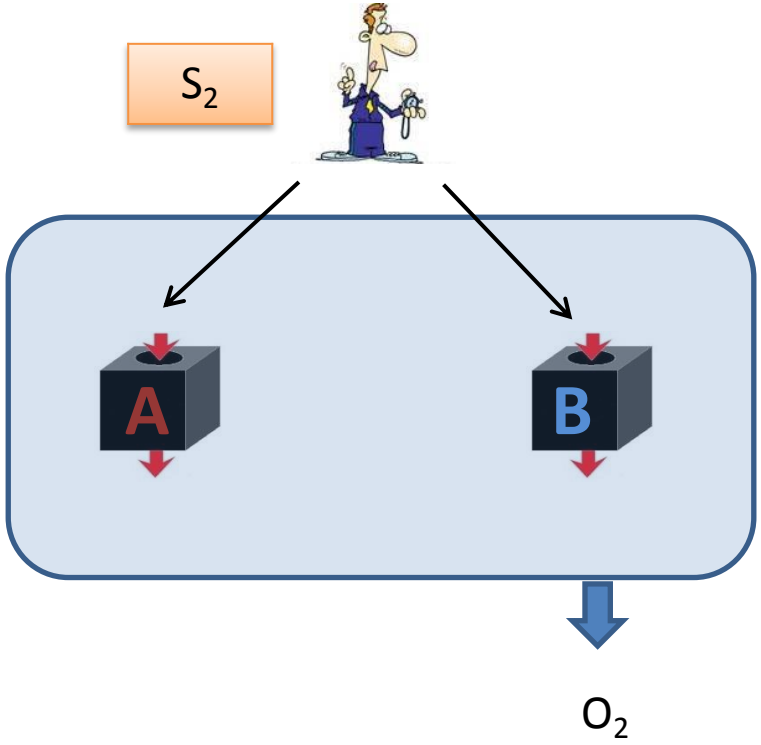
$$\rho_{S_1 G_1 G_2} \approx \rho_U \otimes \rho_{G_1 G_2} \Rightarrow \rho_{O_1 G_2} \approx \rho_U \otimes \rho_{G_2}$$

Alternate?

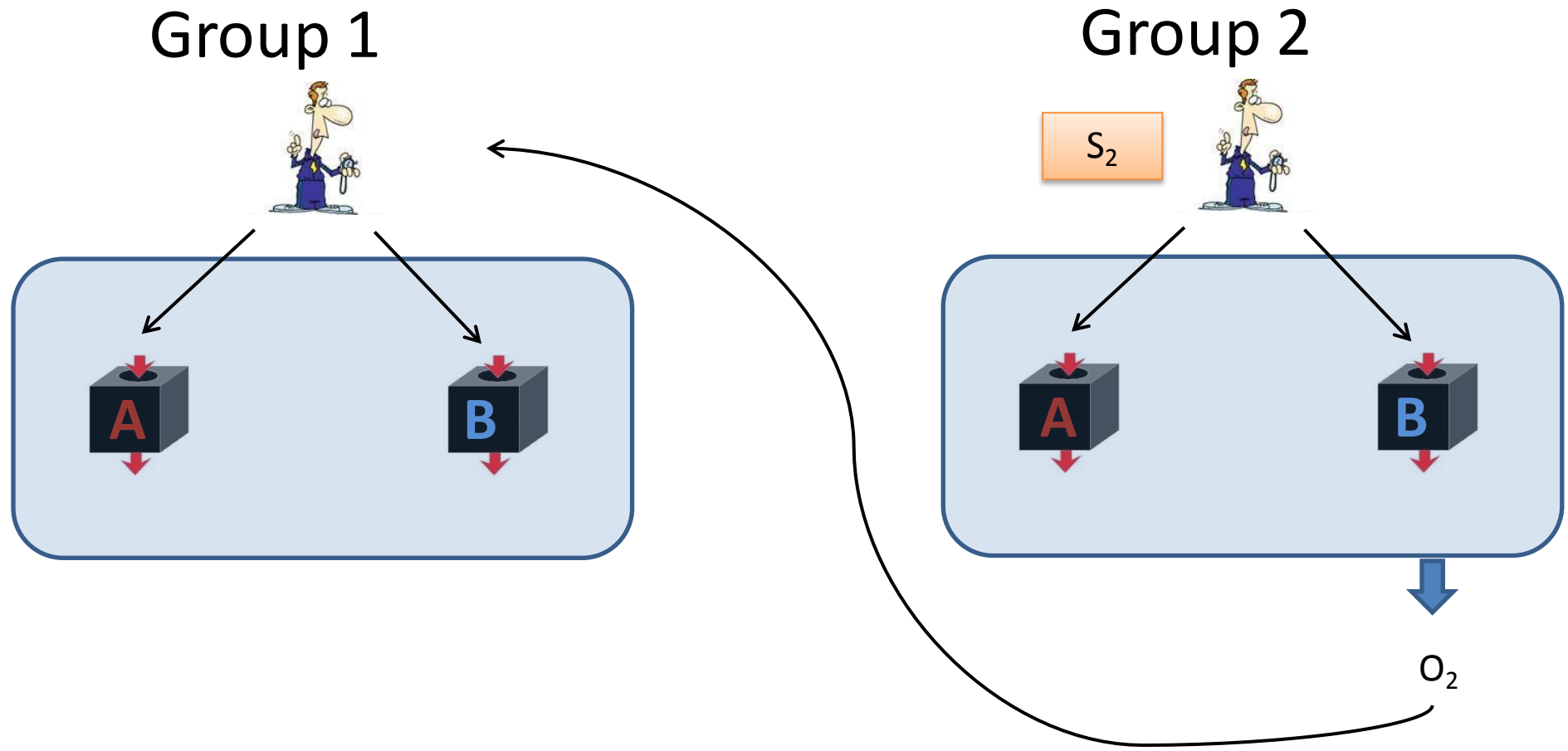
Group 1



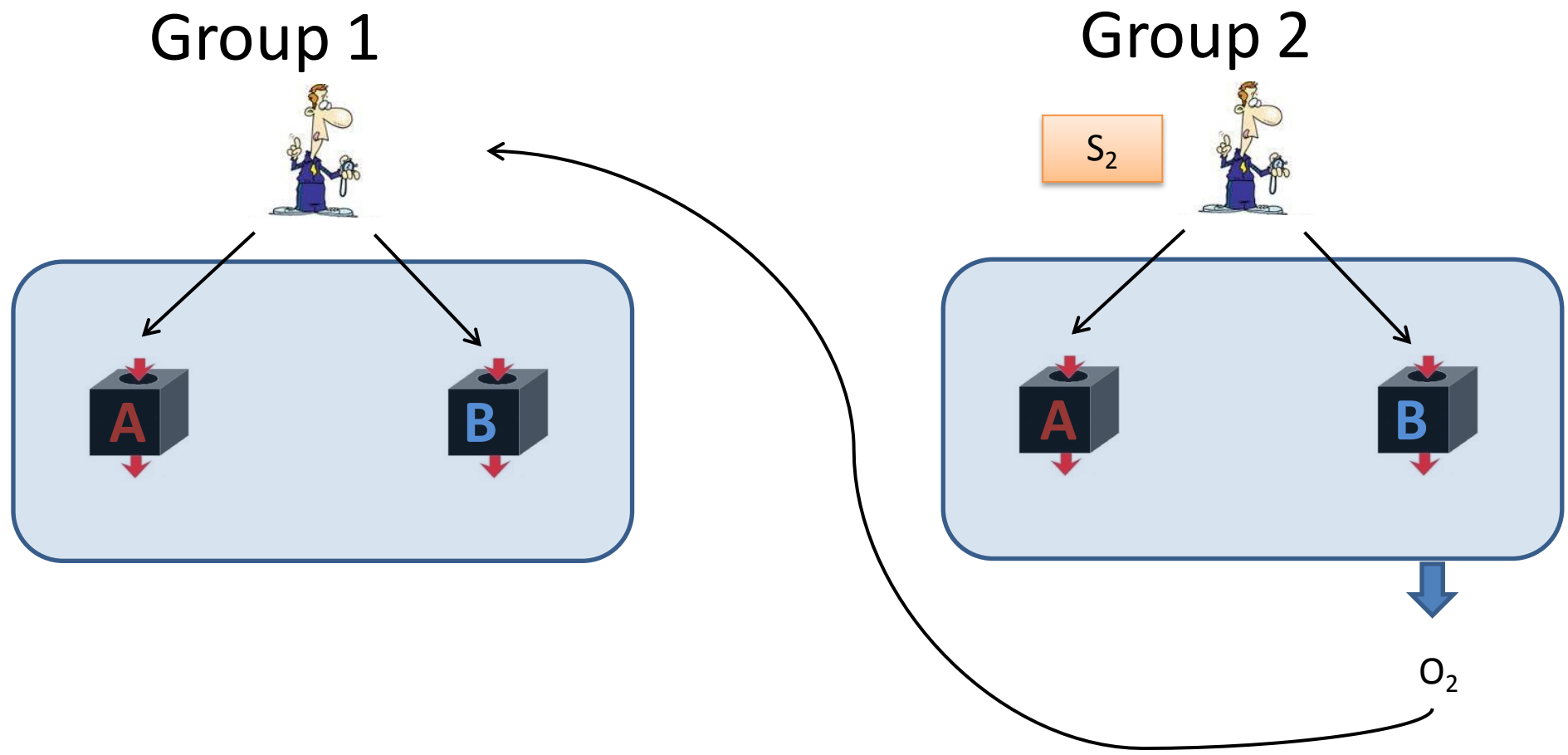
Group 2



Alternate?

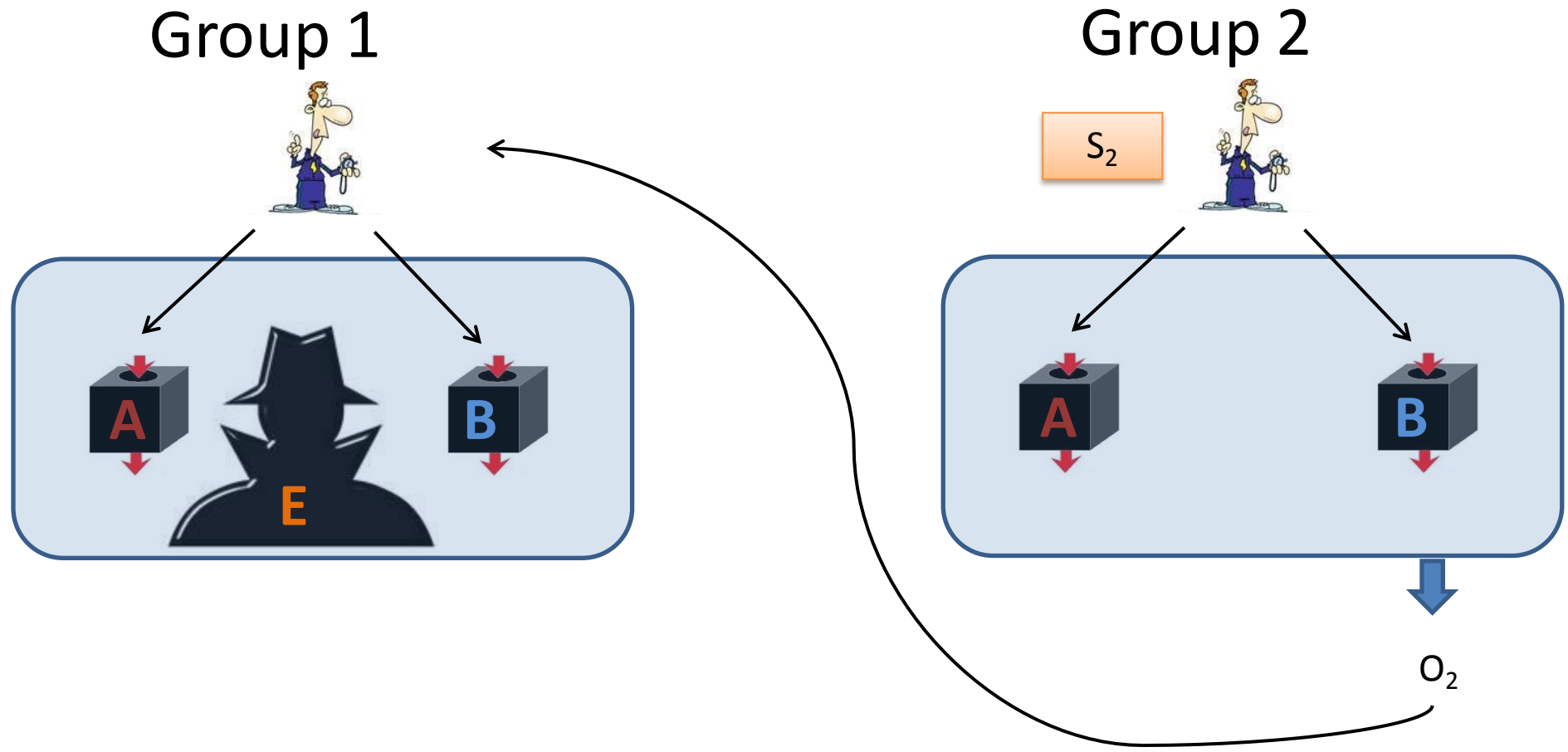


Alternate?



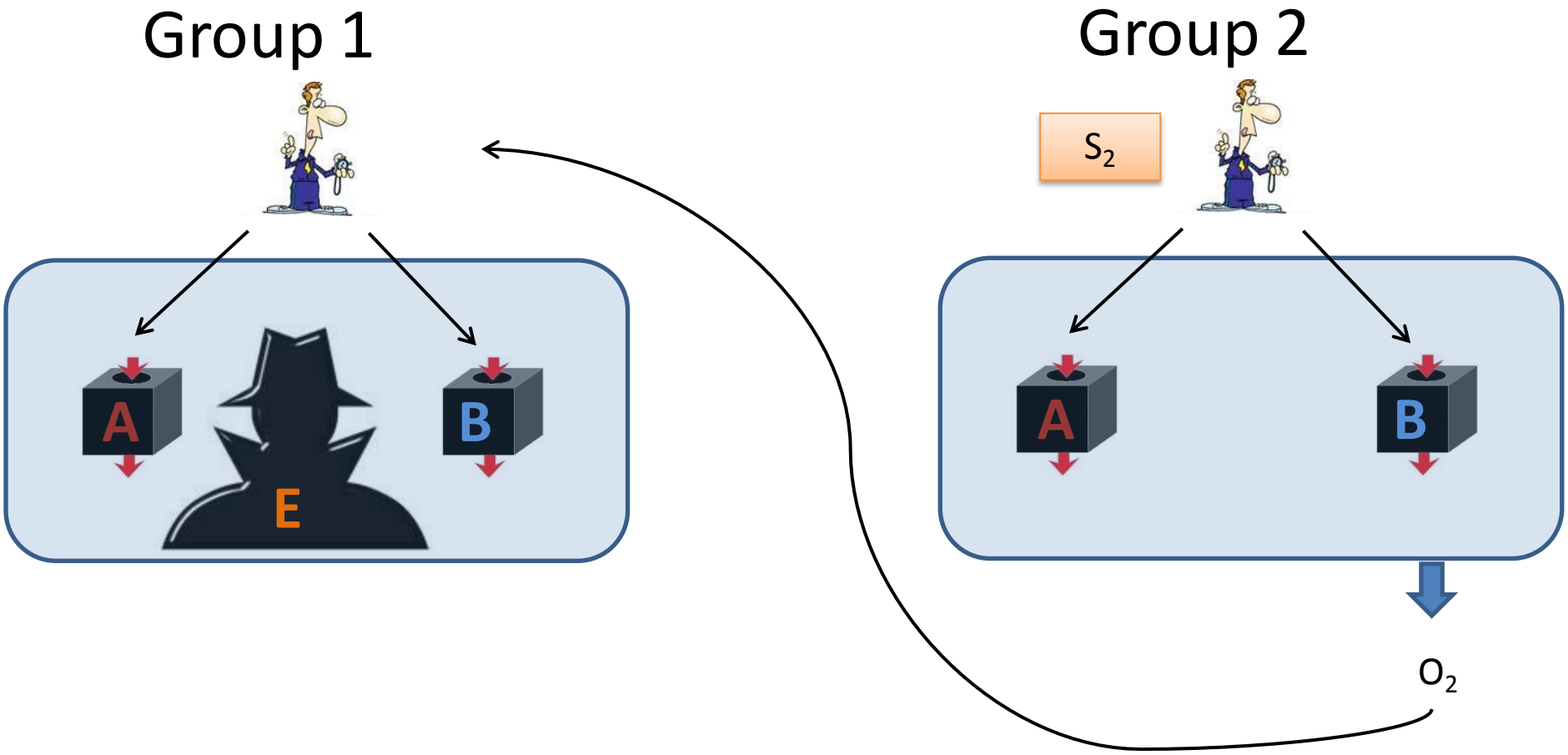
Secure Against Eavesdropper

Alternate?



Secure Against Eavesdropper

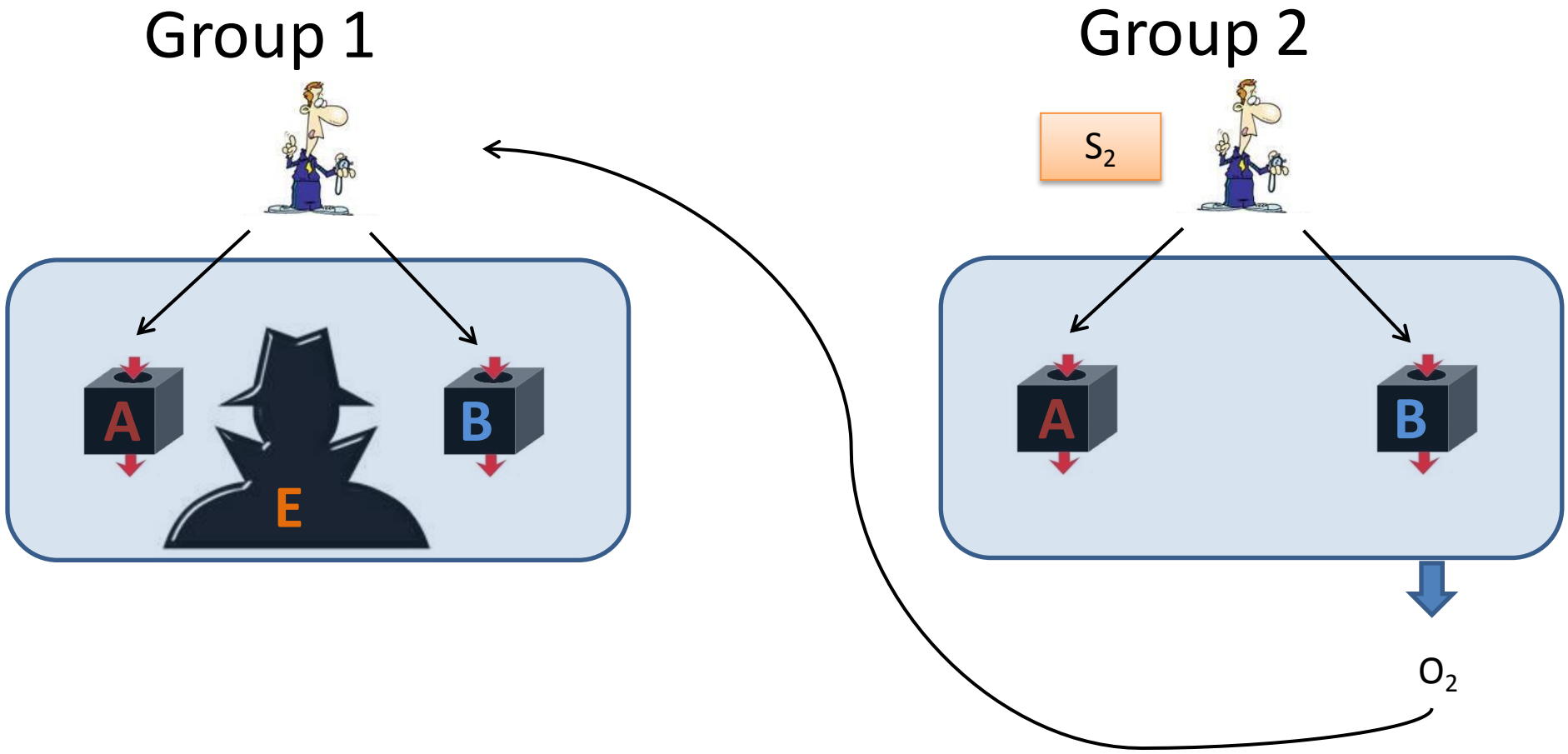
Alternate?



Secure Against Eavesdropper

$$\rho_{S_2 G_2 G_1} \approx \rho_U \otimes \rho_{G_2 G_1} \Rightarrow \rho_{O_2 G_1} \approx \rho_U \otimes \rho_{G_1}$$

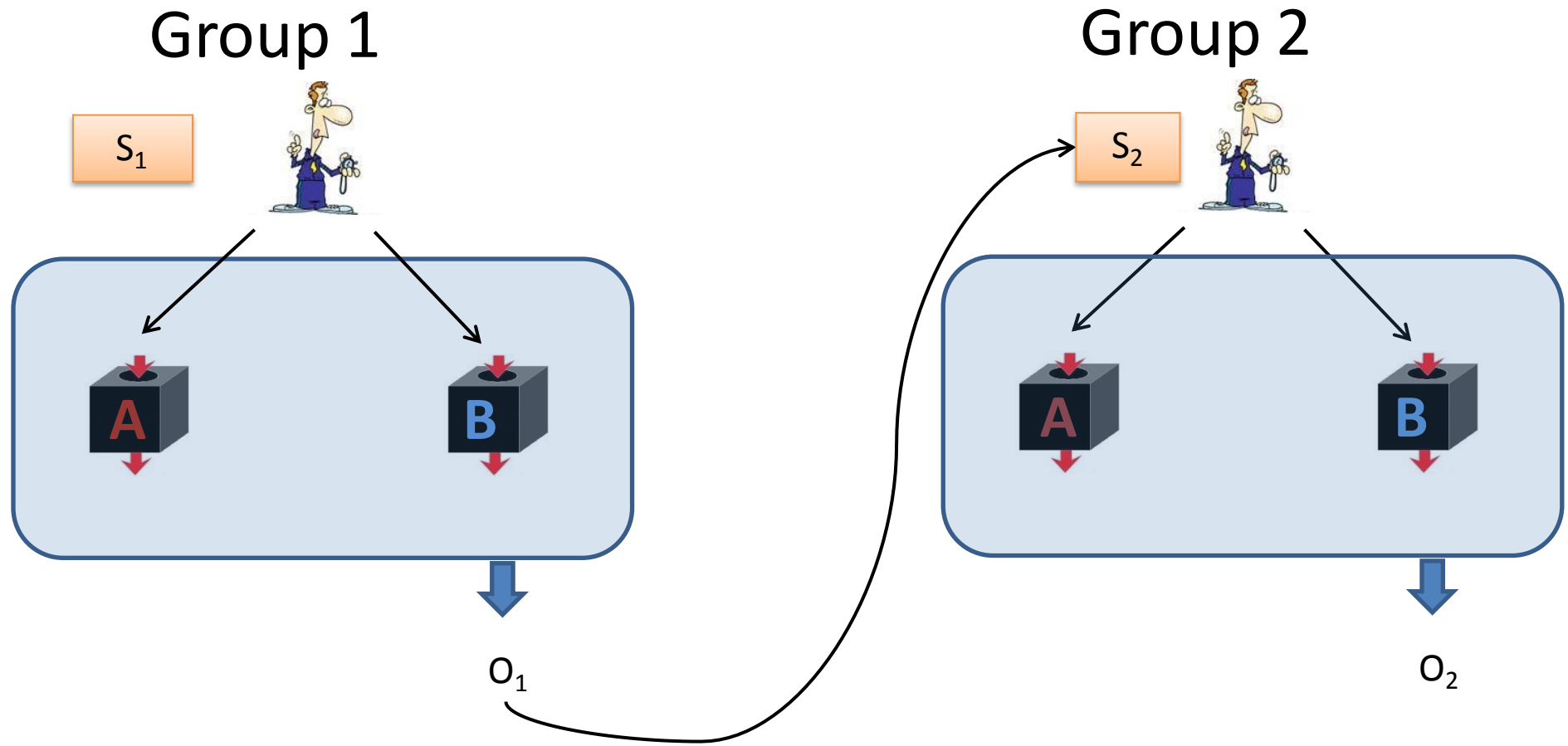
Alternate?



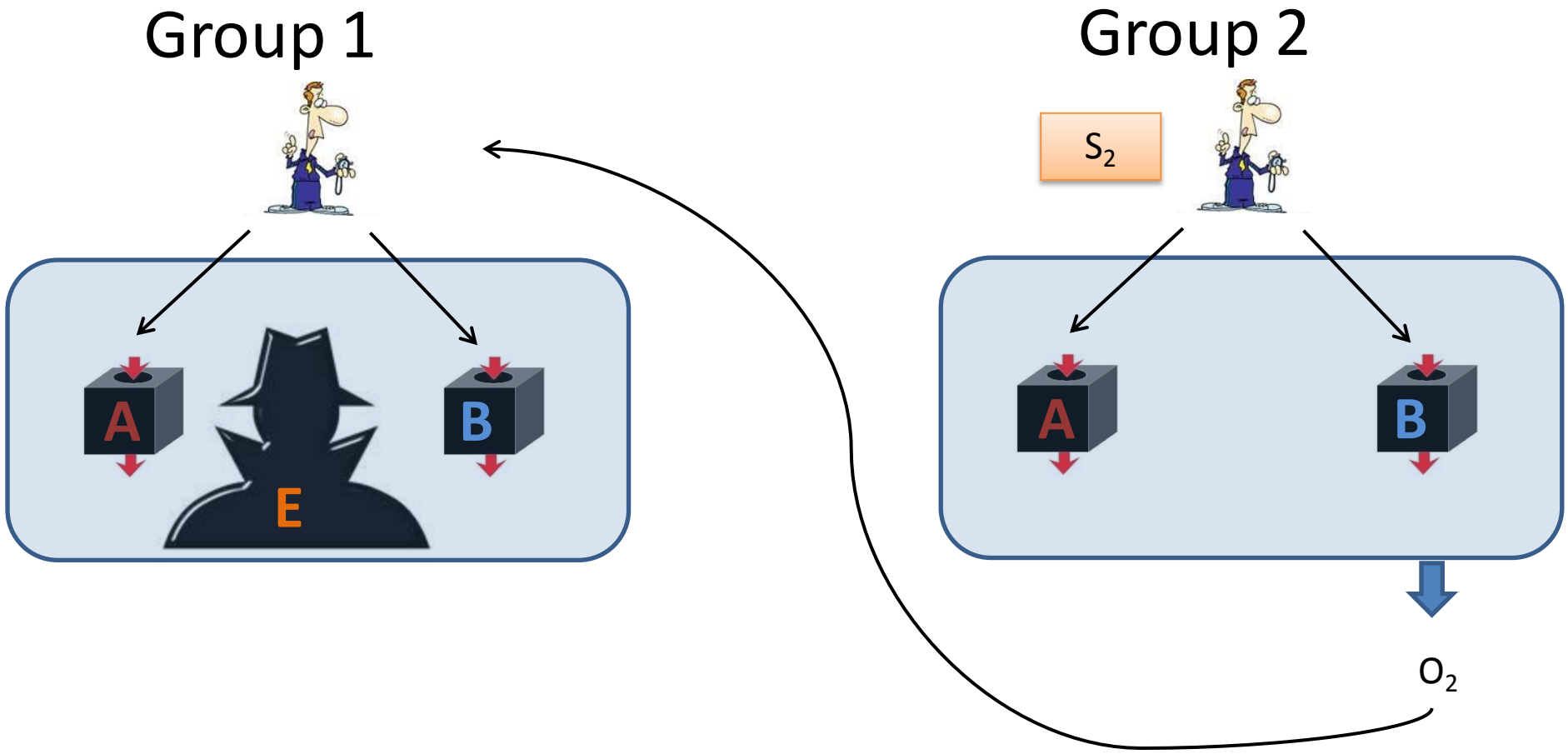
Secure Against Eavesdropper

$$\rho_{S_2 G_2 G_1} \approx \rho_U \otimes \rho_{G_2 G_1} \Rightarrow \rho_{O_2 G_1} \approx \rho_U \otimes \rho_{G_1}$$

Compose?



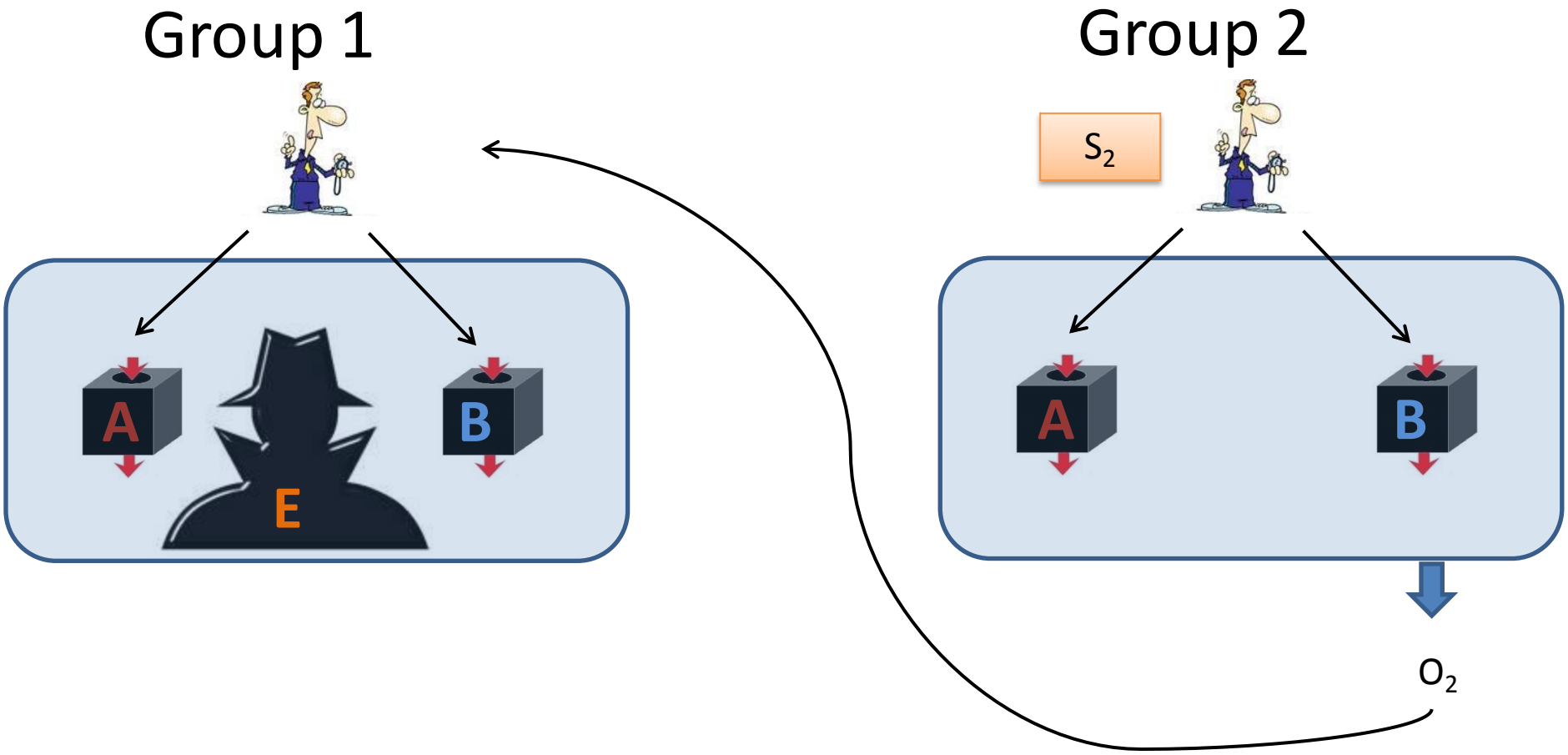
Alternate?



Secure Against Eavesdropper

$$\rho_{S_2 G_2 G_1} \approx \rho_U \otimes \rho_{G_2 G_1} \Rightarrow \rho_{O_2 G_1} \approx \rho_U \otimes \rho_{G_1}$$

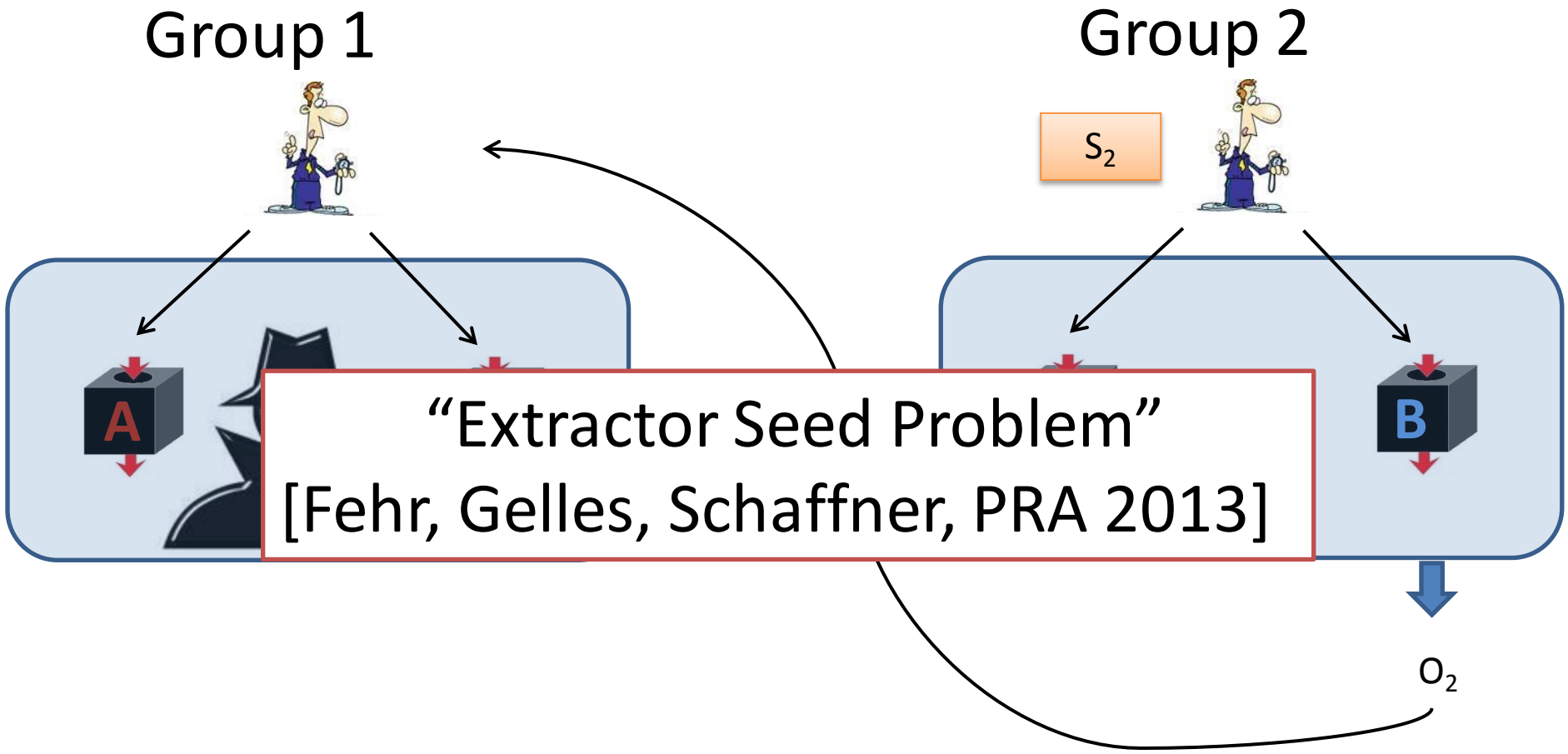
Alternate?



Secure Against Eavesdropper

$$\rho_{S_2 G_2 G_1} \approx \rho_U \otimes \rho_{G_2 G_1} \Rightarrow \rho_{O_2 G_1} \approx \rho_U \otimes \rho_{G_1}$$

Alternate?



Secure Against Eavesdropper

$$\rho_{S_2 G_2 G_1} \approx \rho_U \otimes \rho_{G_2 G_1} \Rightarrow \rho_{O_2 G_1} \approx \rho_U \otimes \rho_{G_1}$$

Input Security

Secure Against Q. Eavesdropper

$$\rho_{SDE} \approx \rho_U \otimes \rho_{DE}$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

Input Security

Secure Against Q. Eavesdropper

$$\rho_{SDE} \approx \rho_U \otimes \rho_{DE}$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

- Provably input secure randomness expansion protocol ⟶ Infinite randomness expansion.

Input Security

Secure Against Q. Eavesdropper

$$\rho_{SDE} \approx \rho_U \otimes \rho_{DE}$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

- Provably input secure randomness expansion protocol ⟶ Infinite randomness expansion.
- Can we obtain input security in a randomness expansion protocol?

Input Security

Secure Against Q. Eavesdropper

$$\rho_{SDE} \approx \rho_U \otimes \rho_{DE}$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

- Provably input secure randomness expansion protocol ⟶ Infinite randomness expansion.
- Can we obtain input security in a randomness expansion protocol?
- Randomness Extractors are provably not input secure.

S = Input Seed

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

A New Tool

[Reichardt, Unger, Vazirani 2012]

S = Input Seed

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

A New Tool

[Reichardt, Unger, Vazirani 2012]

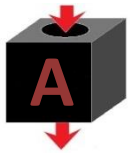
"RUV" Protocol

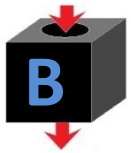
- Device Independent protocol

S = Input Seed

a = 1

b = 0





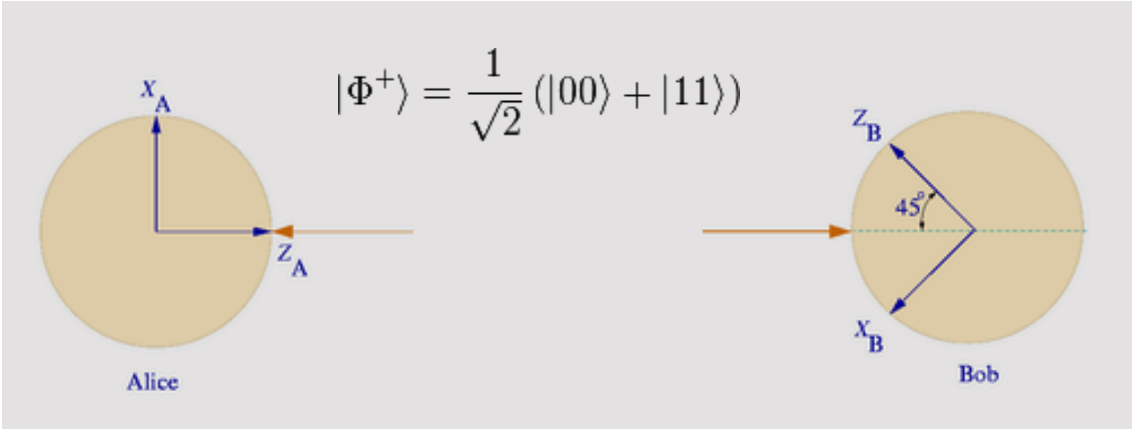
x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

A New Tool

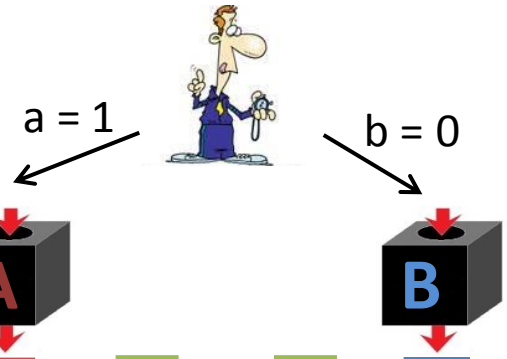
[Reichardt, Unger, Vazirani 2012]

"RUV" Protocol

- Device Independent protocol
- Certifies that devices are measuring an EPR pair in certain rounds.



S = Input Seed



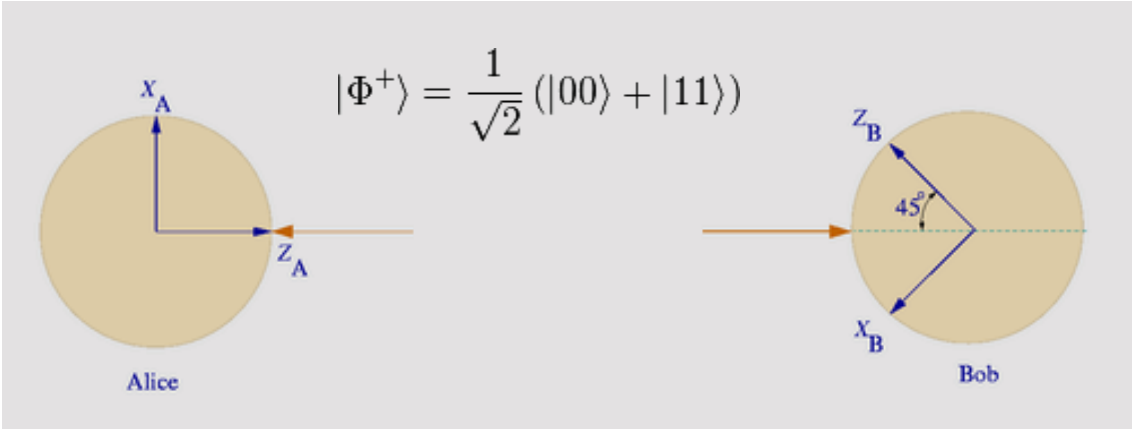
x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

A New Tool

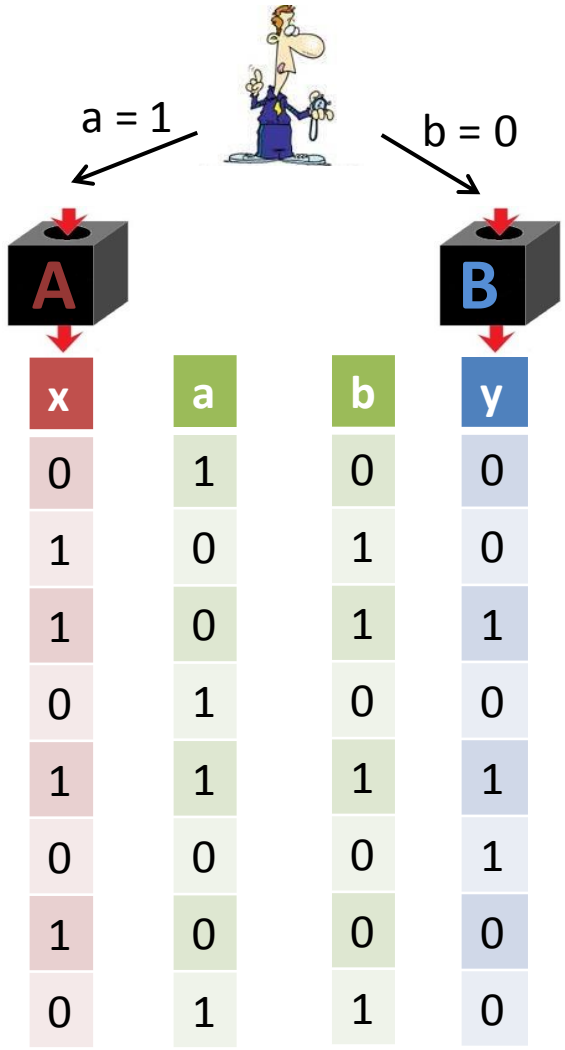
[Reichardt, Unger, Vazirani 2012]

"RUV" Protocol

- Device Independent protocol
- Certifies that devices are measuring an EPR pair in certain rounds.
- Employs CHSH Rigidity



Input Secure?

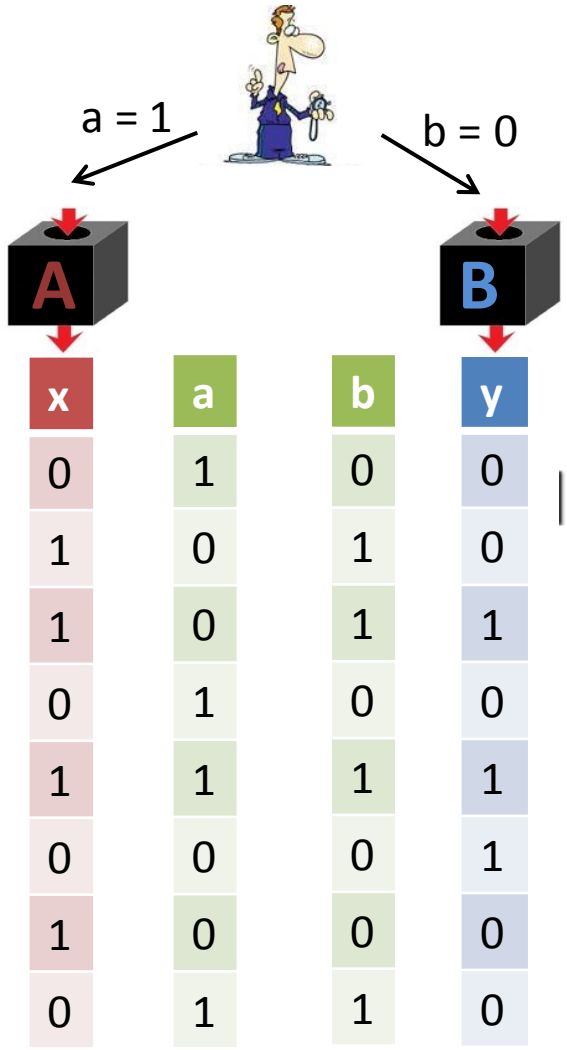


x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

The RUV protocol seems Input Secure!

.

Input Secure?



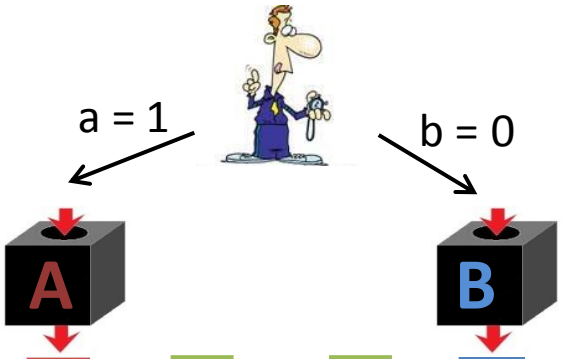
x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

The RUV protocol seems Input Secure!

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

.

Input Secure?



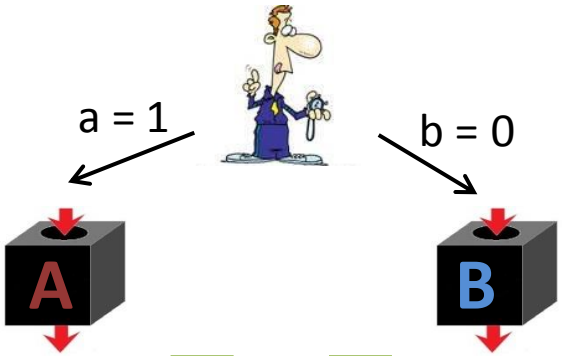
The RUV protocol seems Input Secure!

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

.

Input Secure?



x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

The RUV protocol seems Input Secure!

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

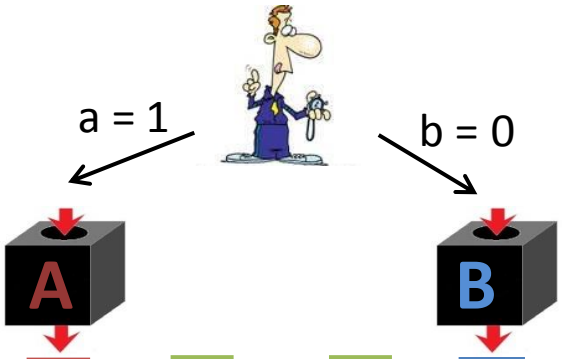
.

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

Input Secure?



x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

The RUV protocol seems Input Secure!

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

"Input Secure"

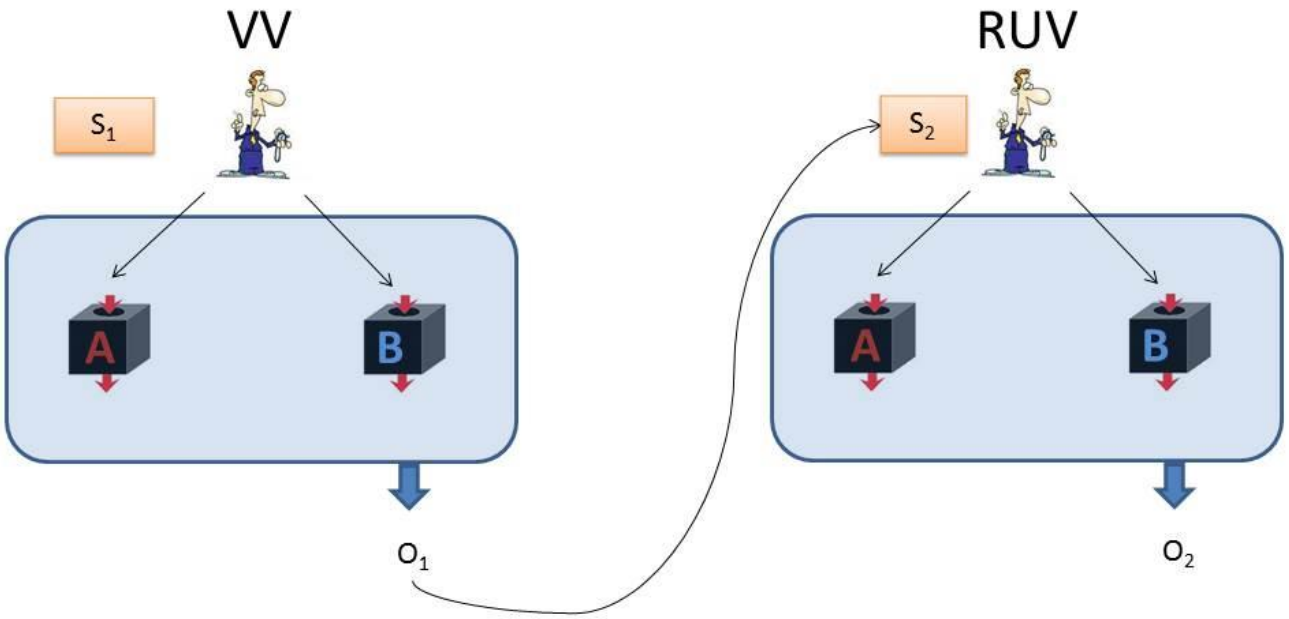
$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

However:

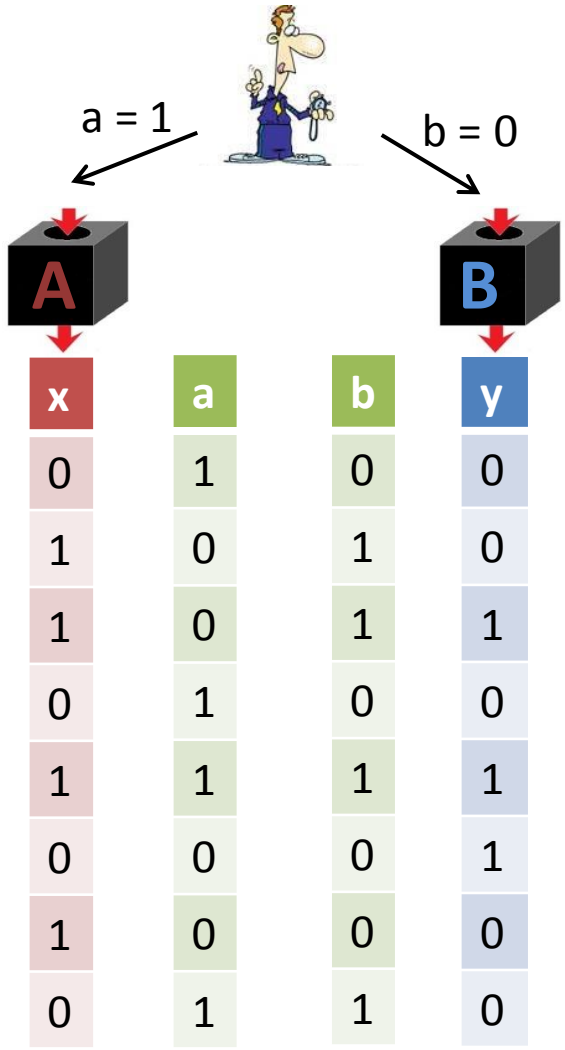
1) Not randomness *expanding*.

Obtaining Expansion



- VV
  - Exponential Expansion
  - Q. Secure
- RUV:
  - Polynomial Contraction
- Net:
  - Exponential Expansion

Input Secure?



This RUV protocol seems Input Secure!

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

"Input Secure"

$$\rho_{SD} \approx \rho_U \otimes \rho_D$$

However:

$$\rho_{OE} \approx \rho_U \otimes \rho_E$$

1) Not randomness *expanding.*
2) Not input secure *conditioned on passing*.

Input Security revisited

a = 1

b = 0

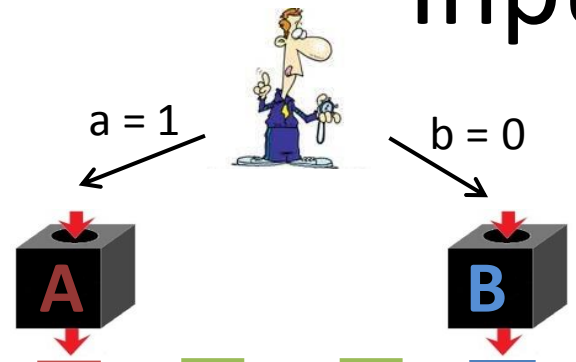
A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

- We only use the output of RUV in the event that the protocol passes

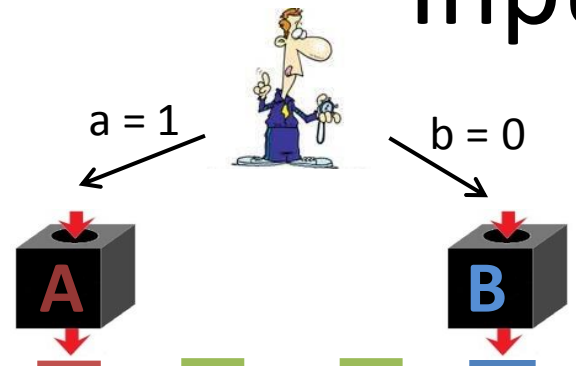
Input Security revisited



x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

- We only use the output of RUV in the event that the protocol passes
- In general conditioning on this event can reveal output information to the eavesdropper

Input Security revisited



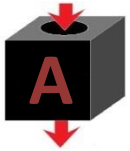
x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

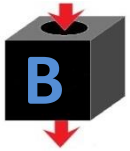
- We only use the output of RUV in the event that the protocol passes
- In general conditioning on this event can reveal output information to the eavesdropper
- This would invalidate the Input Security gained from RUV

Input Security: The Solution

a = 1

b = 0





x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

X_1

X_2

X_3

X

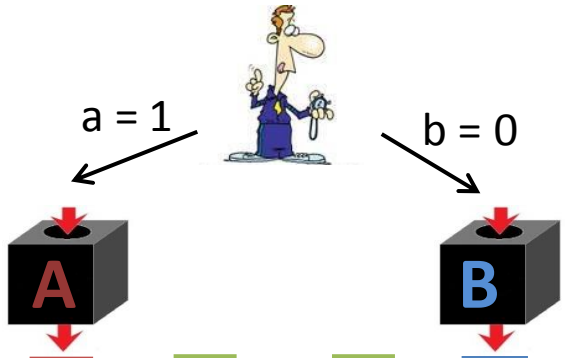
F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

- Divide the output X into blocks



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

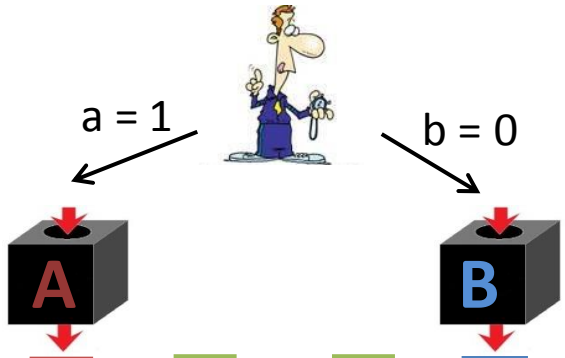
X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution



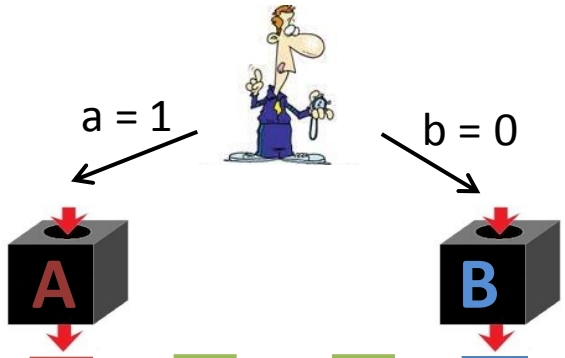
x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

- Divide the output X into blocks
- On average each block will be nearly unentangled with the combined system FE

X F E

Pass	Fail
F = 1	F = 0

Input Security: The Solution



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

- Divide the output X into blocks
- On average each block will be nearly unentangled with the combined system FE
- Output a random block

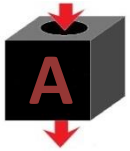
X F E

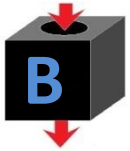
Pass	Fail
F = 1	F = 0

Input Security: The Solution

a = 1

b = 0





x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

X_1

X_2

X_3

X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

$$I(X:E) \approx 0$$

a = 1

b = 0

A

B

x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

$$I(X:E) \approx 0$$

$$I(X:FE) \leq 2\,H(F) \leq 2$$

a = 1

b = 0

A

B

x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

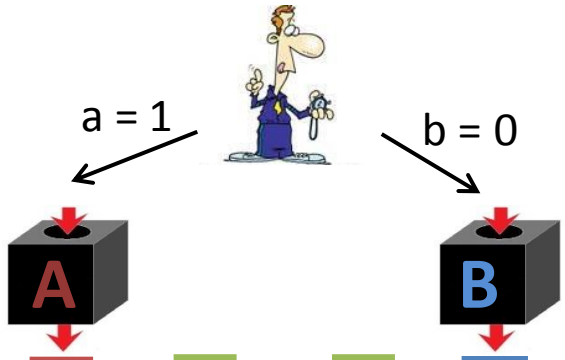
X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

$$I(X:E) \approx 0$$

$$I(X:FE) \leq 2\,H(F) \leq 2$$

$$2 \geq I(X:FE) = \sum_i I(X_i:FE|X_{<i})$$

$$\geq \sum_i I(X_i:FE)$$

F

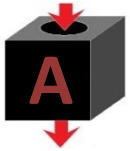
Pass	Fail
F = 1	F = 0

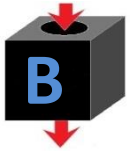
E

Input Security: The Solution

a = 1

b = 0





x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

X_1

X_2

X_3

X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

$$\frac{1}{N}\sum_i I(X_i : FE) \le \frac{1}{N} I(X : FE) \le \frac{2}{N}$$

a = 1

b = 0

A

B

x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

$$\frac{1}{N}\sum_i I(X_i : FE) \le \frac{1}{N} I(X : FE) \le \frac{2}{N}$$

Pinsker's Inequality

a = 1

b = 0

A

B

x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

X_1

X_2

X_3

X

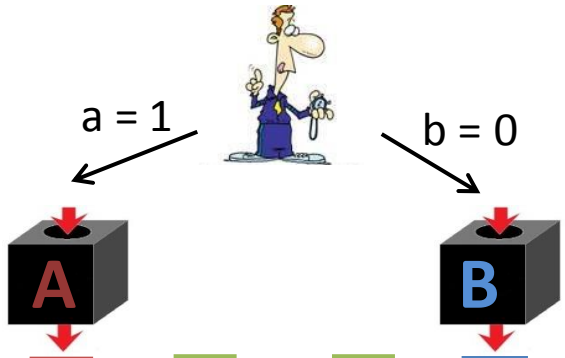
F

Pass	Fail
F = 1	F = 0

E

Input Security: The Solution

$$\frac{1}{N}\sum_i I(X_i : FE) \le \frac{1}{N} I(X : FE) \le \frac{2}{N}$$



x	a	b	y
0	1	0	0
1	0	1	0
1	0	1	1
0	1	0	0
1	1	1	1
0	0	0	1
1	0	0	0
0	1	1	0

X_1 X_2 X_3 X

Pinsker's Inequality

$$\frac{1}{N}\sum_i || \rho_{X_i FE} - \rho_{X_i} \otimes \rho_{FE} ||^2$$

$$\le \frac{1}{N}\sum_i I(X_i : FE) \le \frac{2}{N}$$

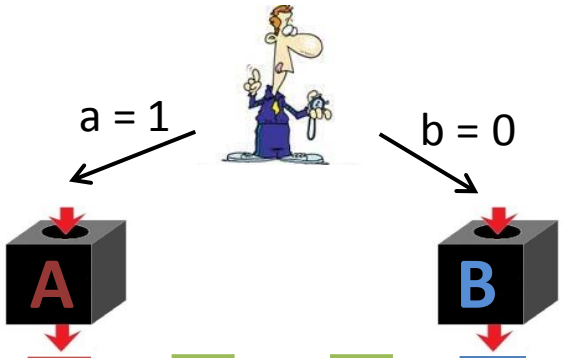
F

Pass	Fail
F = 1	F = 0

E

Selecting Random Blocks

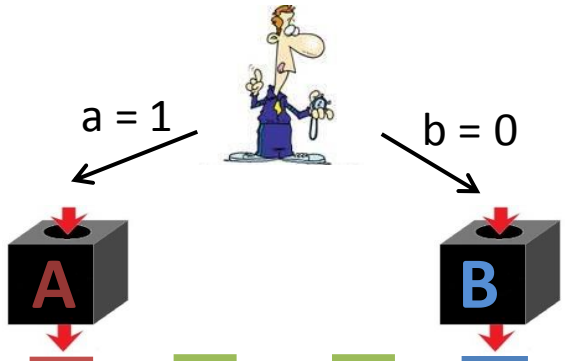
- Our solution selects output blocks at random….



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

Selecting Random Blocks



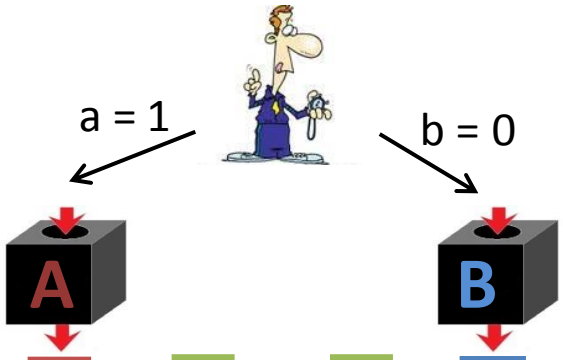
x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

- Our solution selects output blocks at random….

  ….using an input seed unknown to the devices

Selecting Random Blocks



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

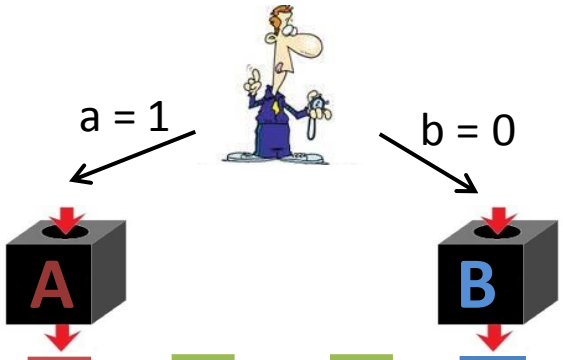
X

- Our solution selects output blocks at random….

  ….using an input seed unknown to the devices

- But could the seed be correlated with the position of "bad" blocks?

Selecting Random Blocks

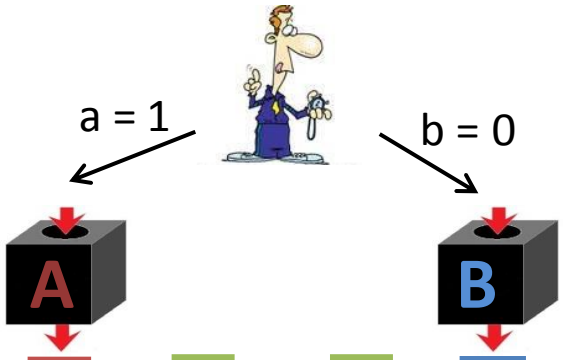


- Such adversarial correlations can be ruled out using a purification and simulation argument.

x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

X

Selecting Random Blocks



x	a	b	y	
0	1	0	0	X_1
1	0	1	0	
1	0	1	1	
0	1	0	0	X_2
1	1	1	1	
0	0	0	1	
1	0	0	0	X_3
0	1	1	0	

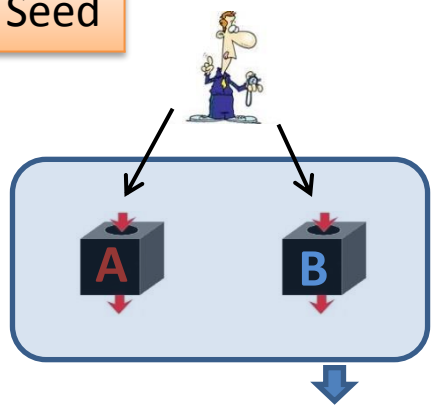
X

- Such adversarial correlations can be ruled out using a purification and simulation argument.
- This implies full input security for this composition of VV and RUV.

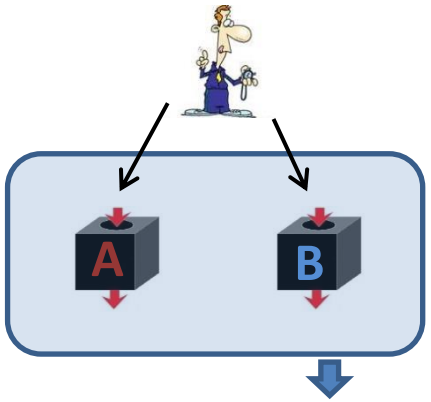
Our Protocol

S = Input Seed

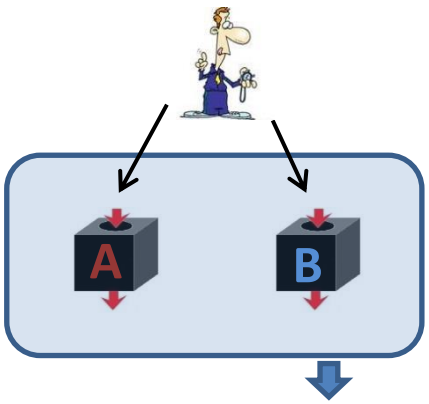
VV



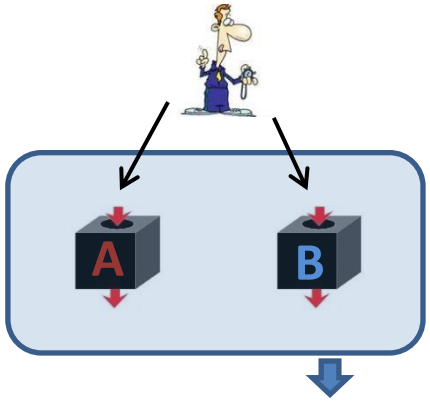
VV



RUV

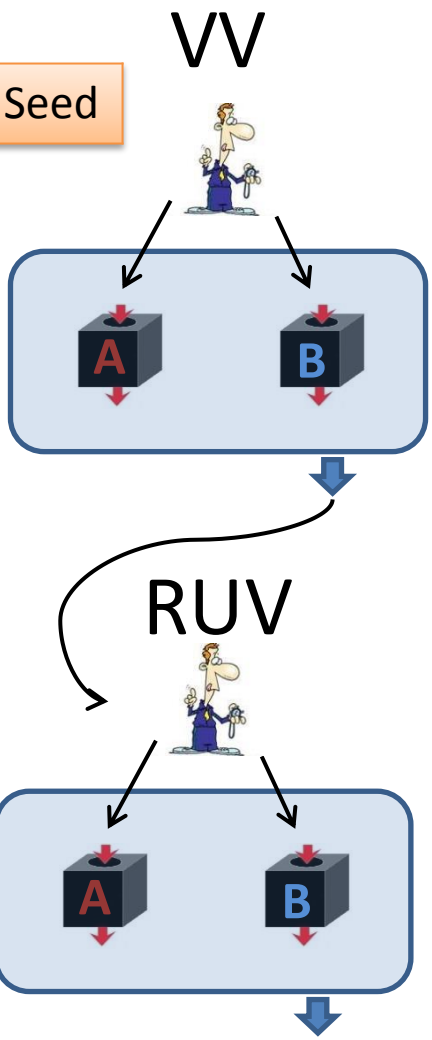


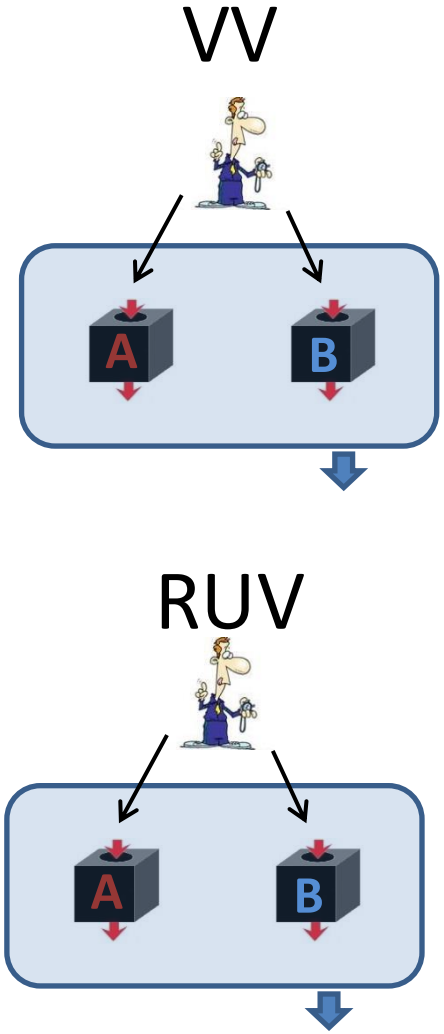
RUV



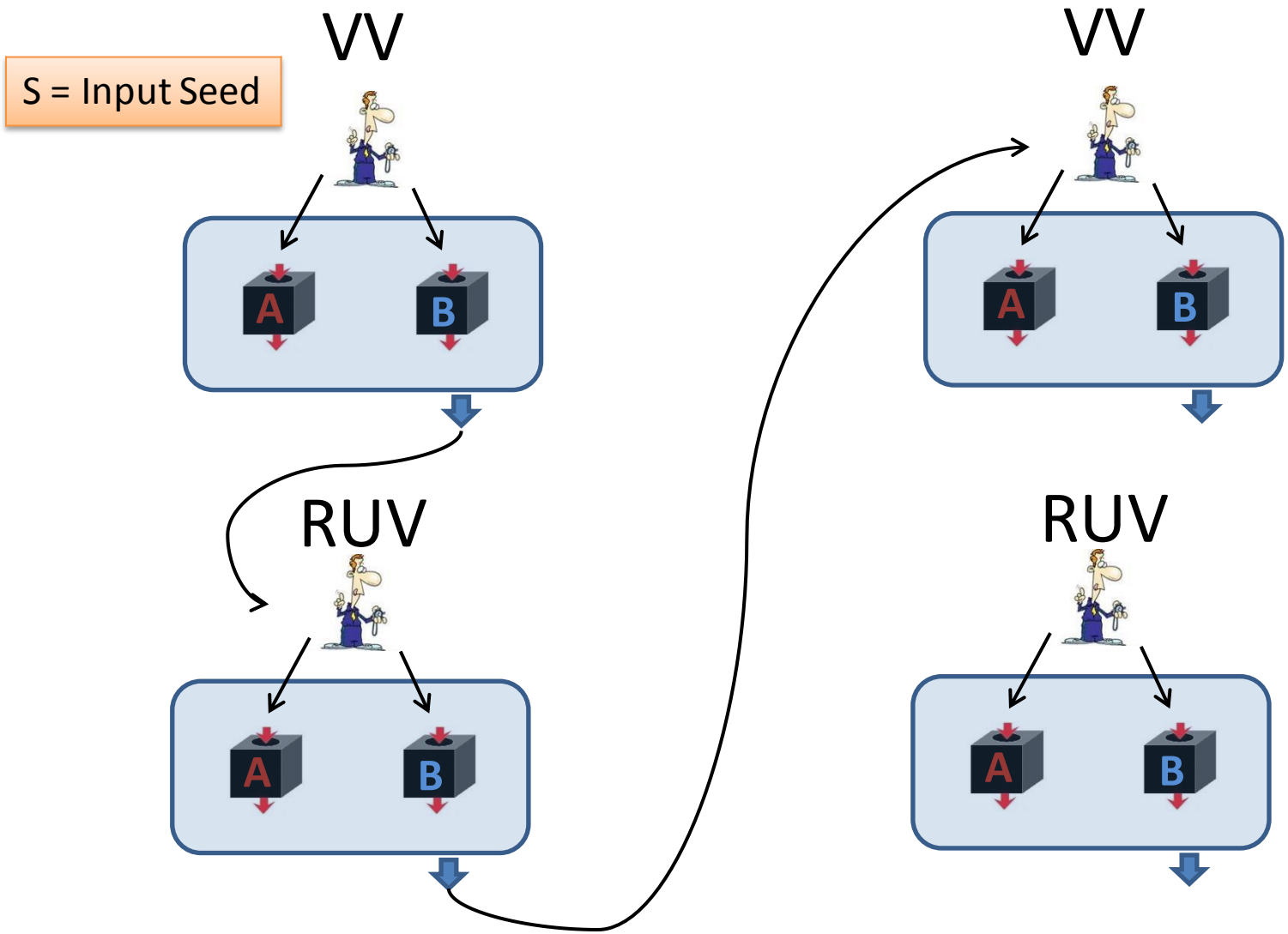
Our Protocol

S = Input Seed

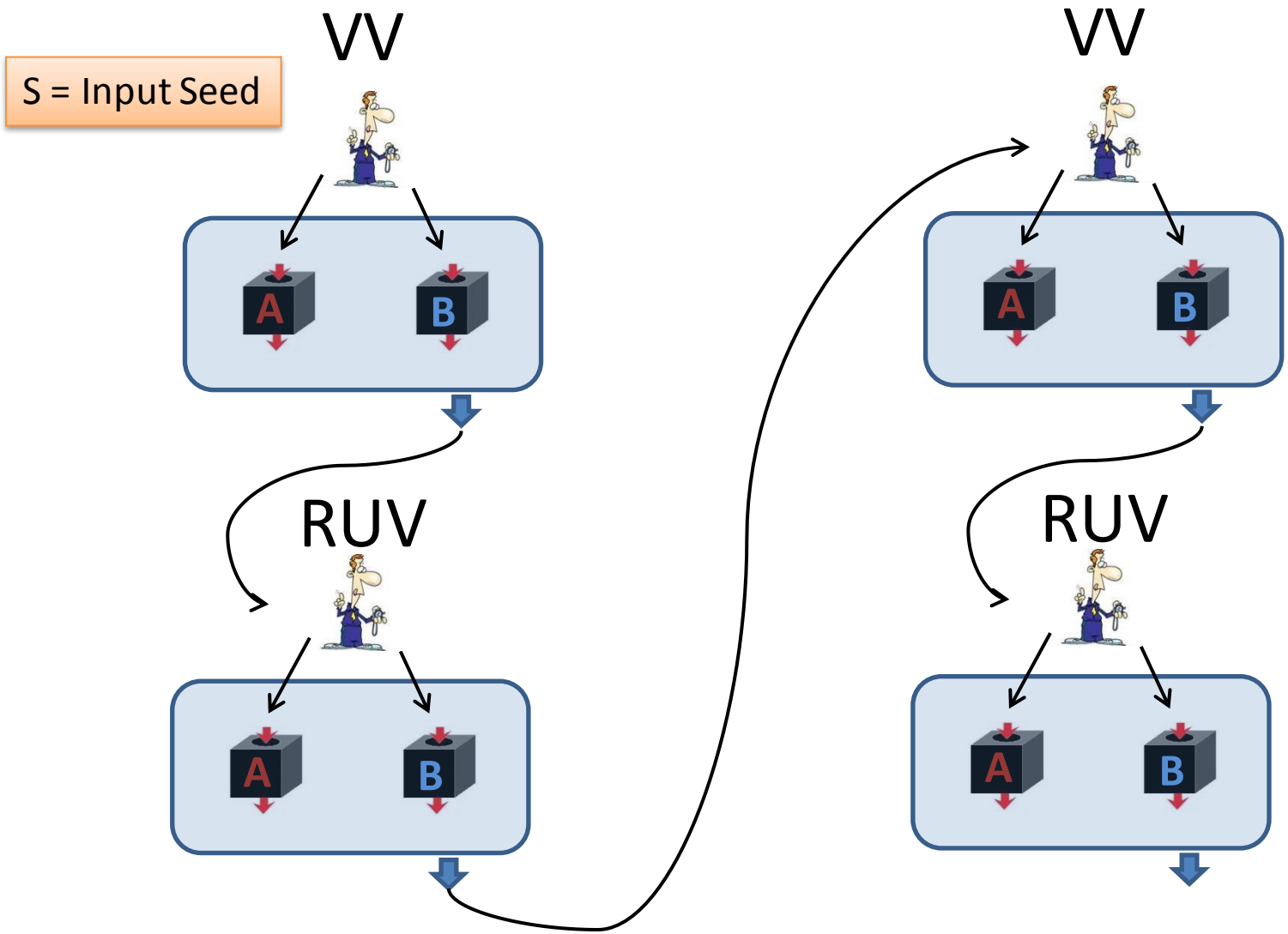




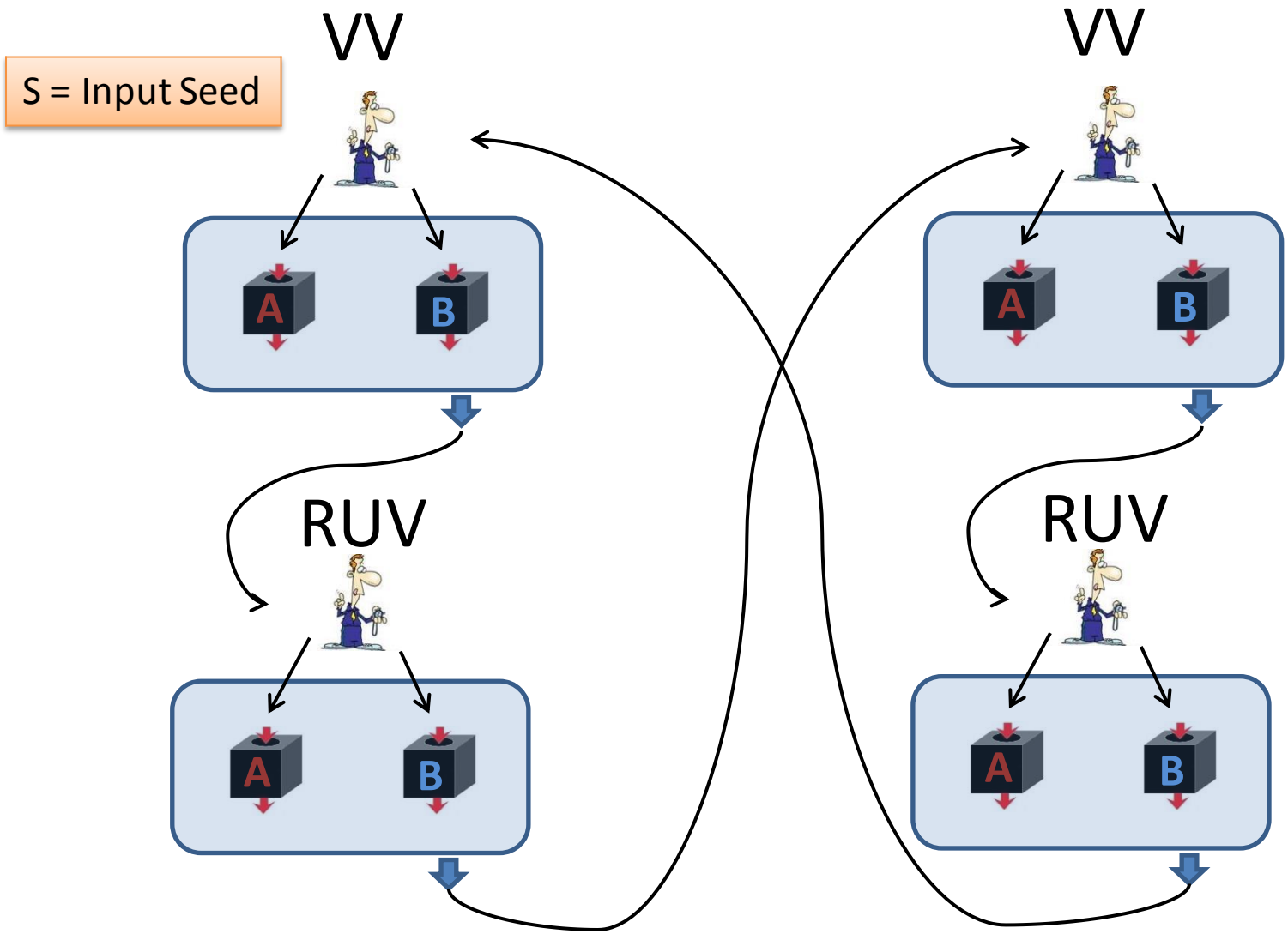
Our Protocol



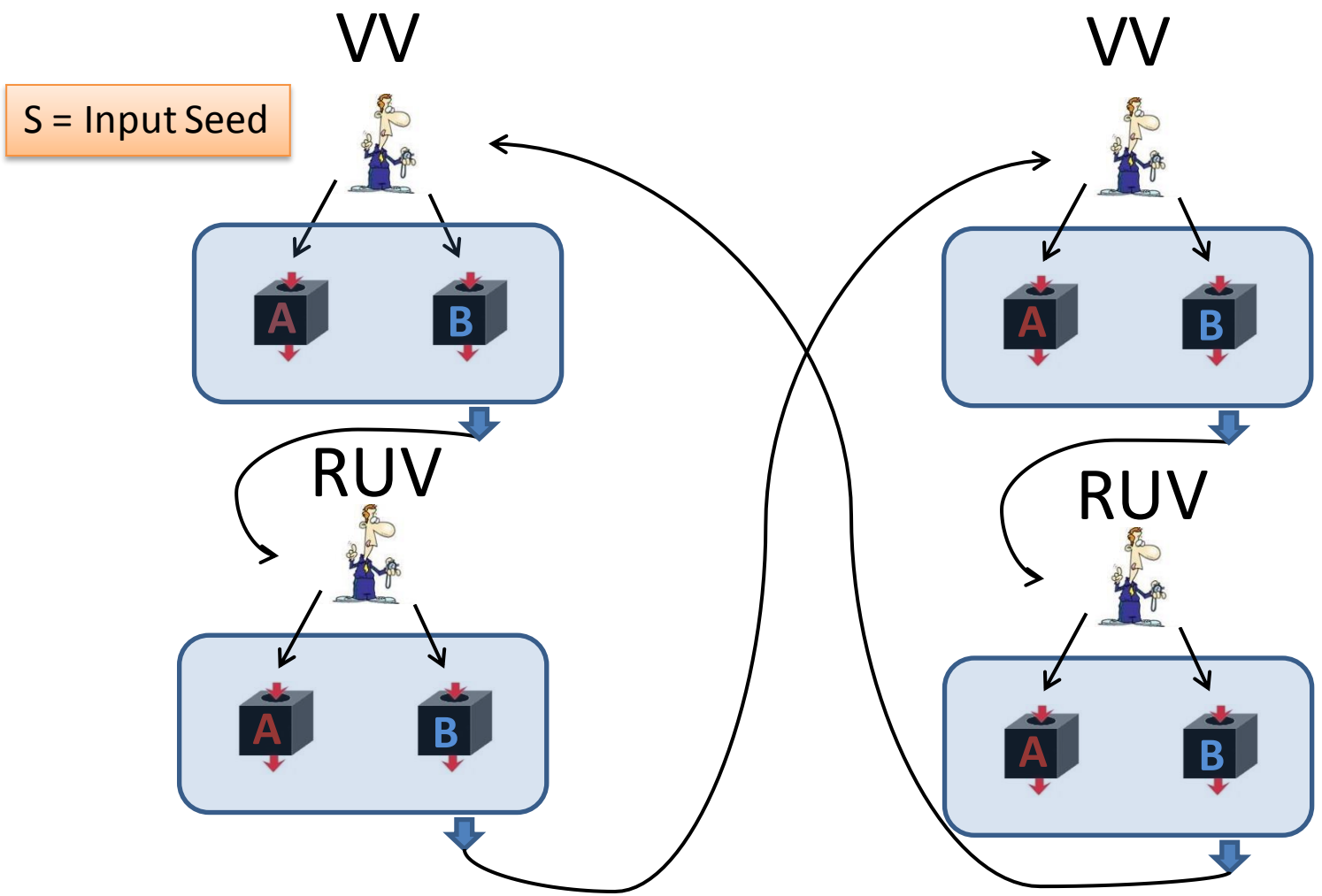
Our Protocol



Our Protocol

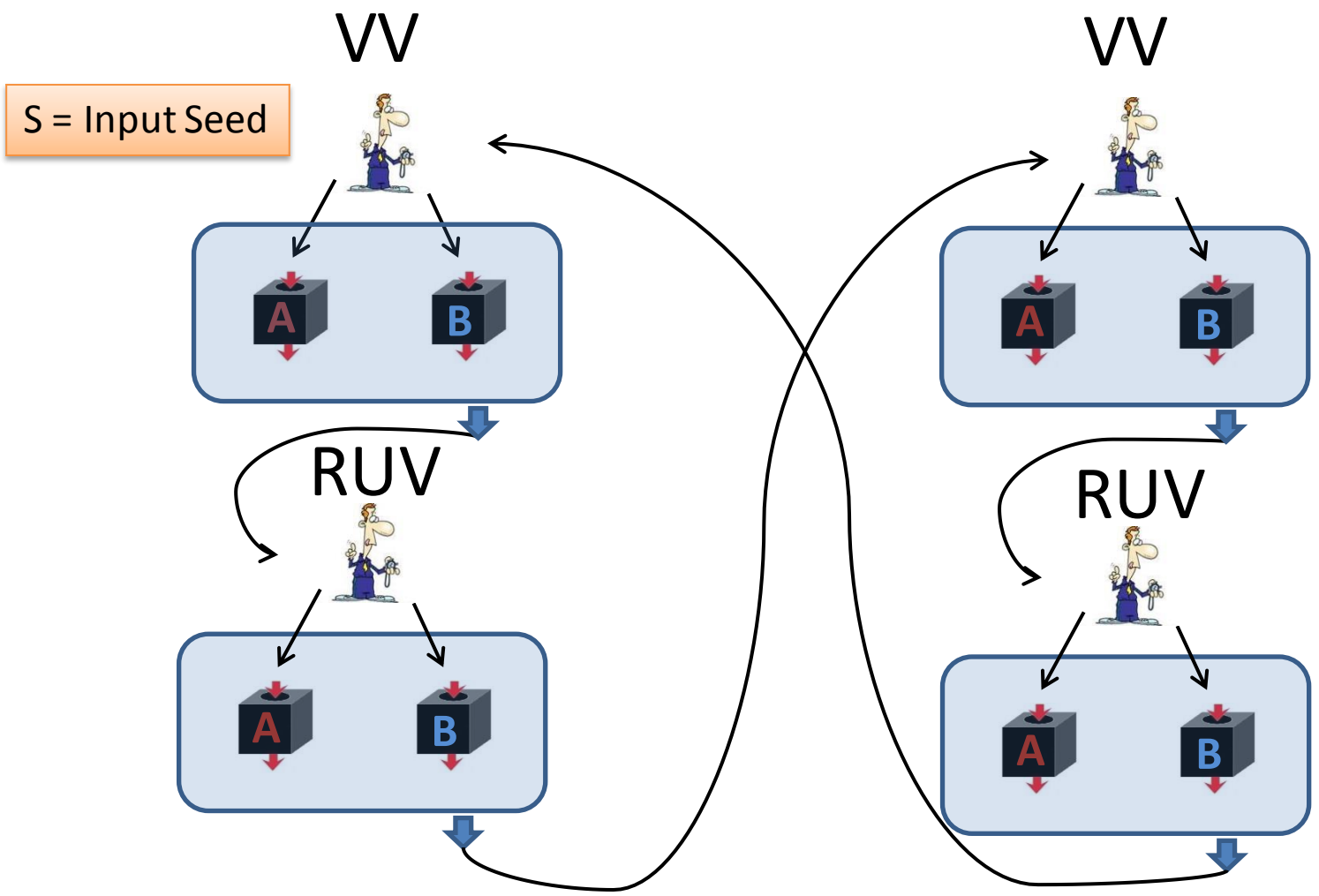


Infinite Randomness Expansion

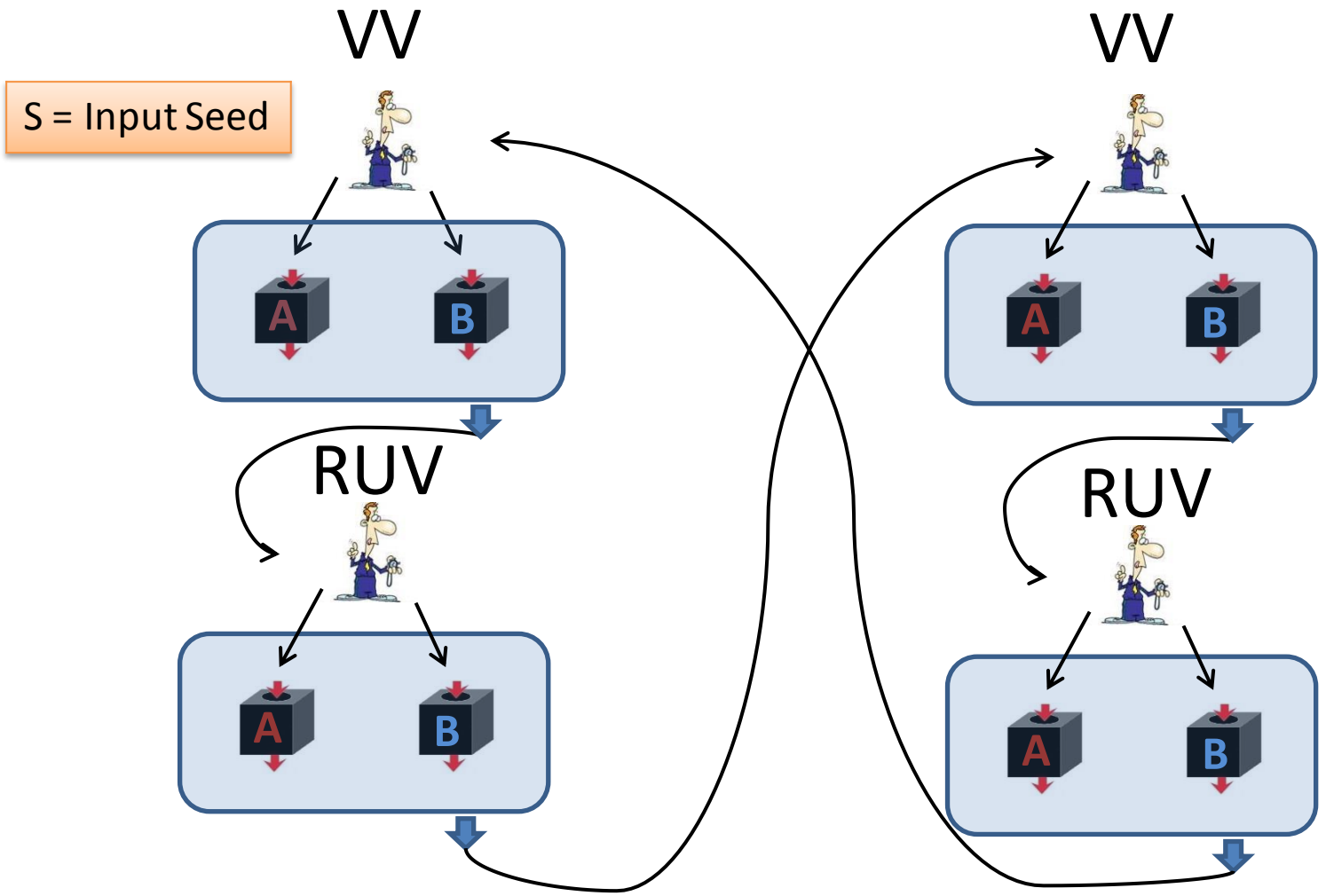


- Approximately Input Secure steps (composable)
- Exponential Expansion at each step

Infinite Randomness Expansion



- Accumulated error converges
- Output is $\frac{1}{exp(|S|)}$ -close to uniform and secure against quantum eavesdropper.



Open Questions

- Robust protocols [Miller, Shi], [Chung, Shi, Wu]
- Optimal Parameters?
- Protocols other than Randomness Expansion [Reichardt, Unger, Vazirani 2012]