Title: Device-independent quantum key distribution

Date: Oct 25, 2010 04:00 PM

URL: http://pirsa.org/10100055

Abstract: Even though the security of quantum key distribution has been rigorously proven, most practical schemes can be attacked and broken. These attacks make use of imperfections of the physical devices used for their implementation. Since current security proofs assume that the physical devices' exact and complete specification is known, they do not hold for this scenario. The goal of device-independent quantum key distribution is to show security without making any assumptions about the internal working of the devices. In this talk, I will first explain the assumptions 'traditional' security proofs make and why they are problematic. Then, I will discuss how the violation of Bell inequalities can be used to show security even when a large part of the physical devices is untrusted.

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Qi.ethz.ch

Device-Independent Quantum Key Distribution

Esther Hänggi
ETH Zürich

Perimeter Institute
25th October 2010

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

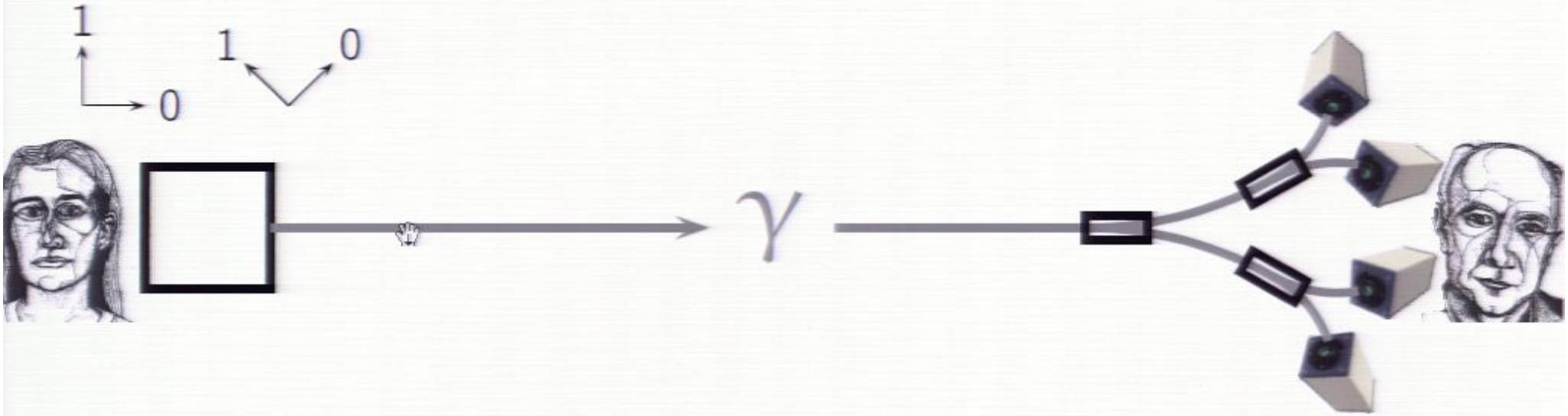
Qi .ethz.ch

Device-Independent Quantum Key Distribution

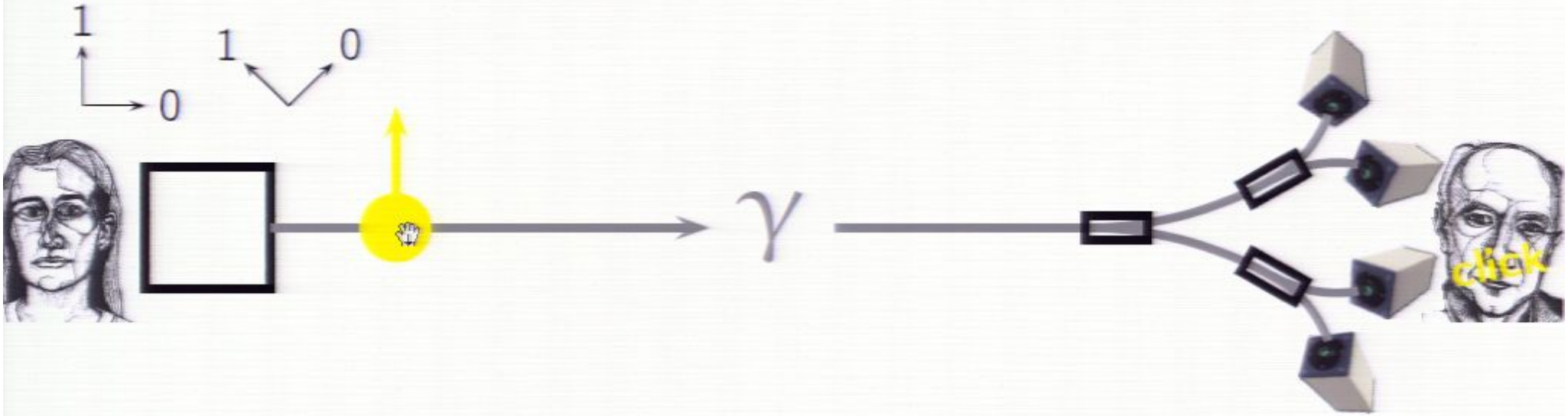
Esther Hänggi
ETH Zürich

Perimeter Institute
25th October 2010

Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]



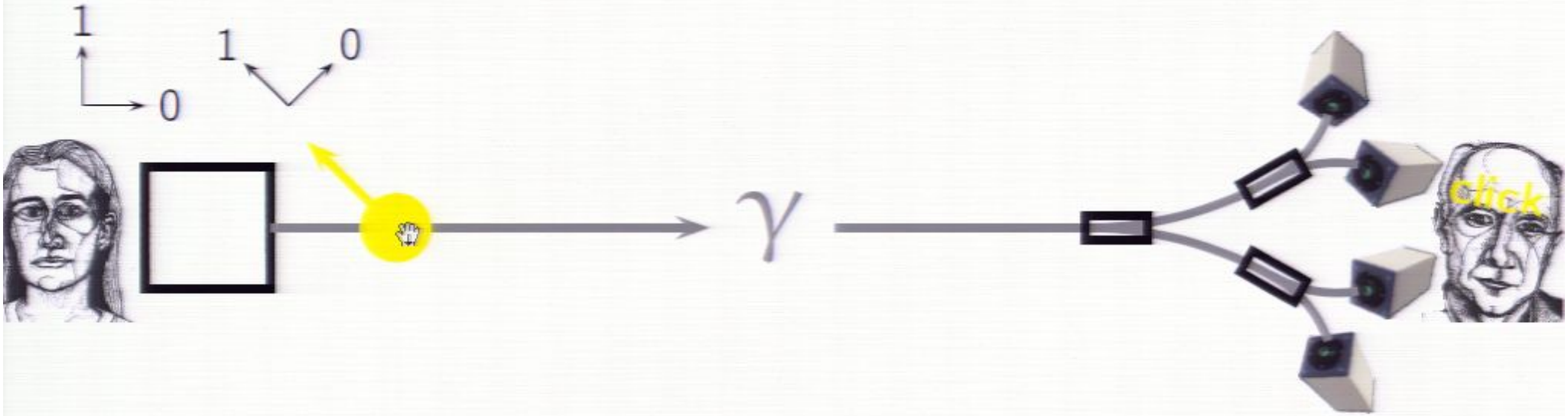
Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]



basis	+					
bit	1					

basis	×					
result	0					

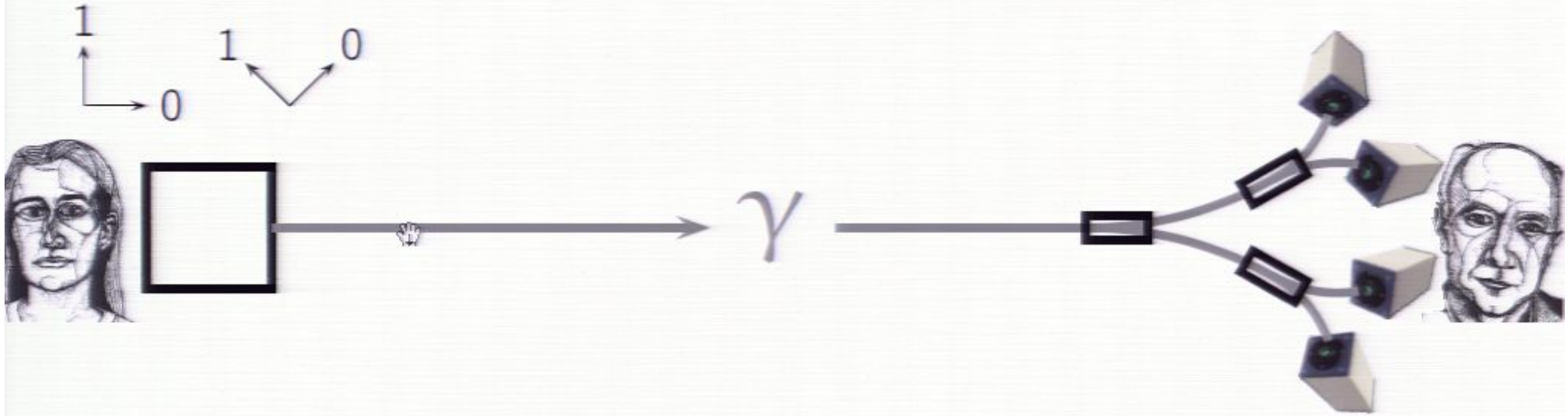
Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]



basis	+	+	×	+	×	
bit	1	0	0	0	1	

basis	×	+	×	+	+	
result	0	0	1	0	1	

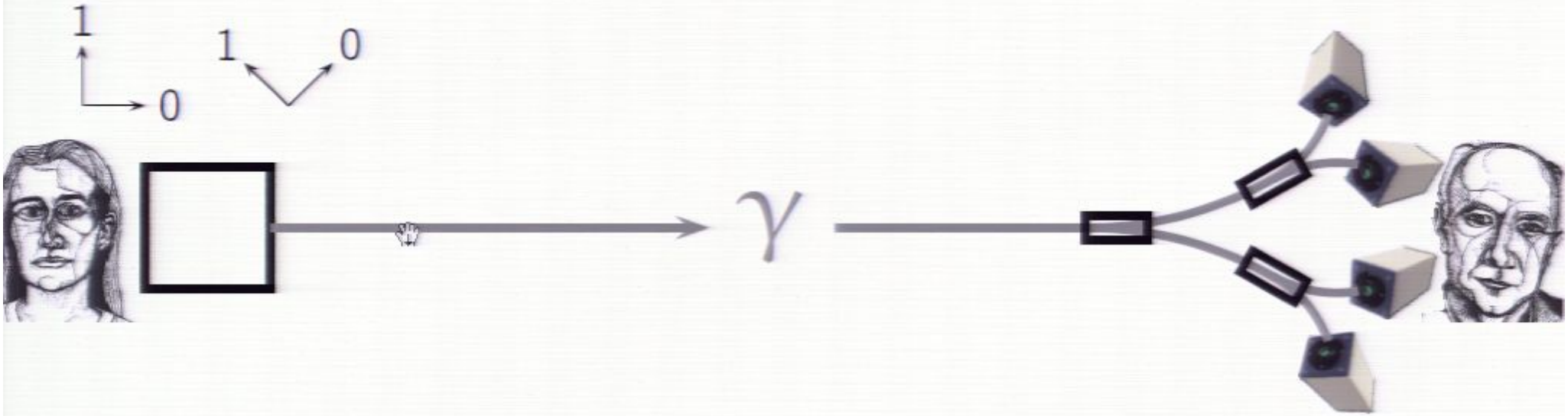
Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]



basis	+	+	×	+	×	×
bit	1	0	0	0	1	1

basis	×	+	×	+	+	×
result	0	0	1	0	1	1

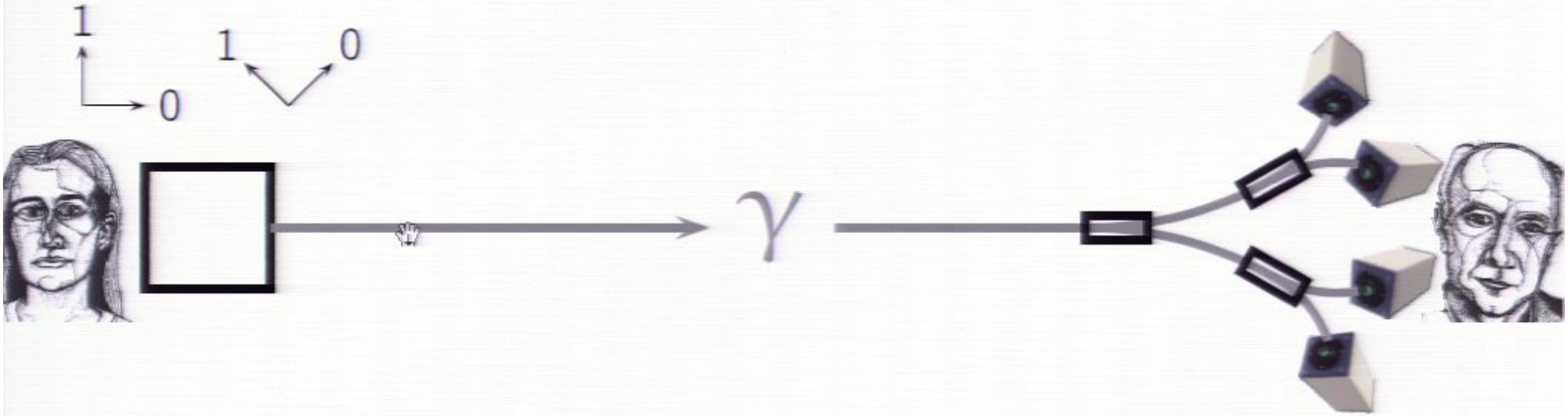
Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]



basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	✗	✓	✓	✓	✗	✓

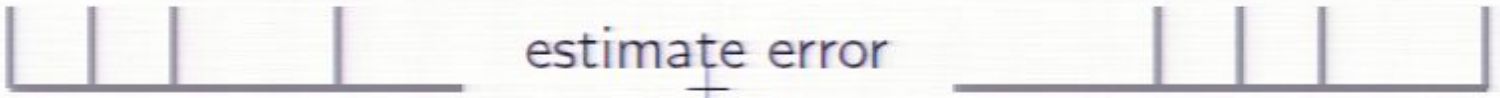
basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	✗	✓	✓	✓	✗	✓

Quantum Key Distribution [Bennet,Brassard 84,Ekert 91]

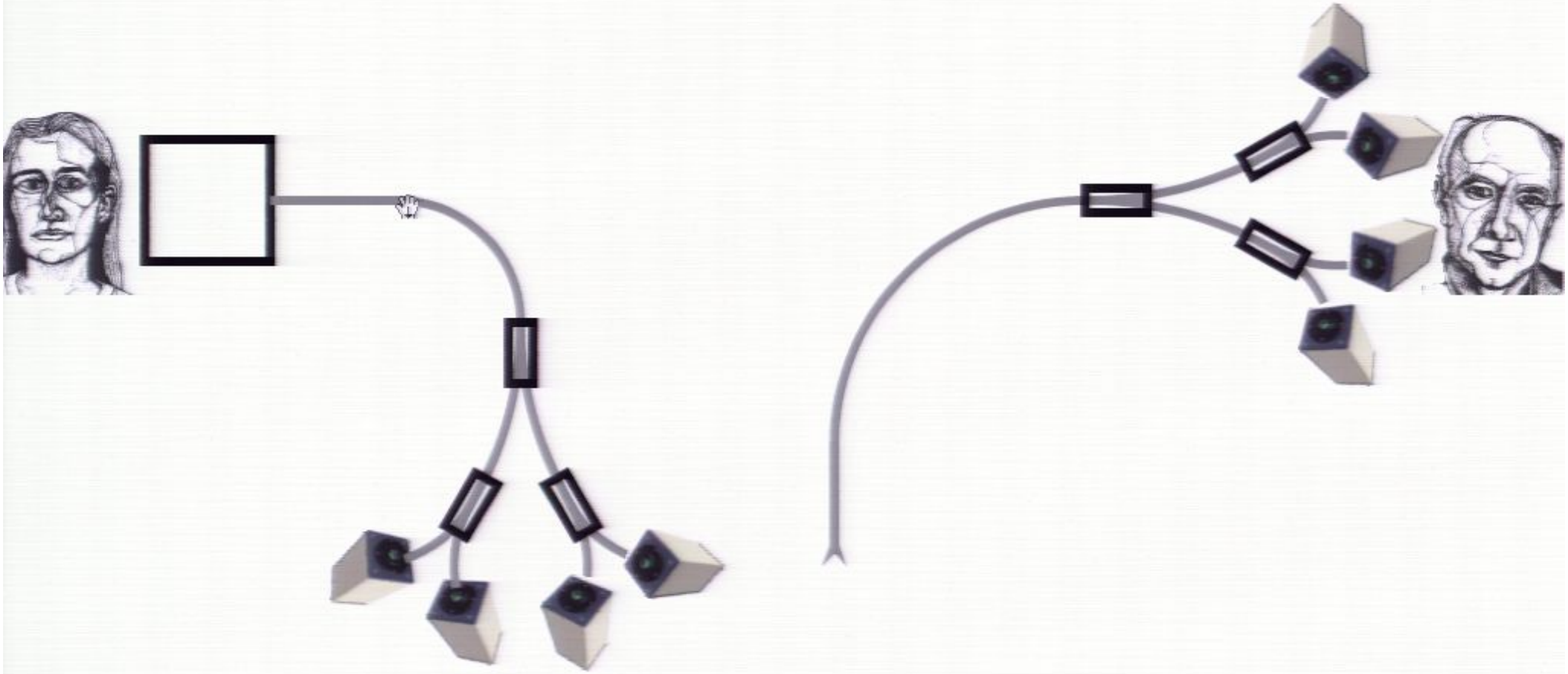


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	✗	✓	✓	✓	✗	✓

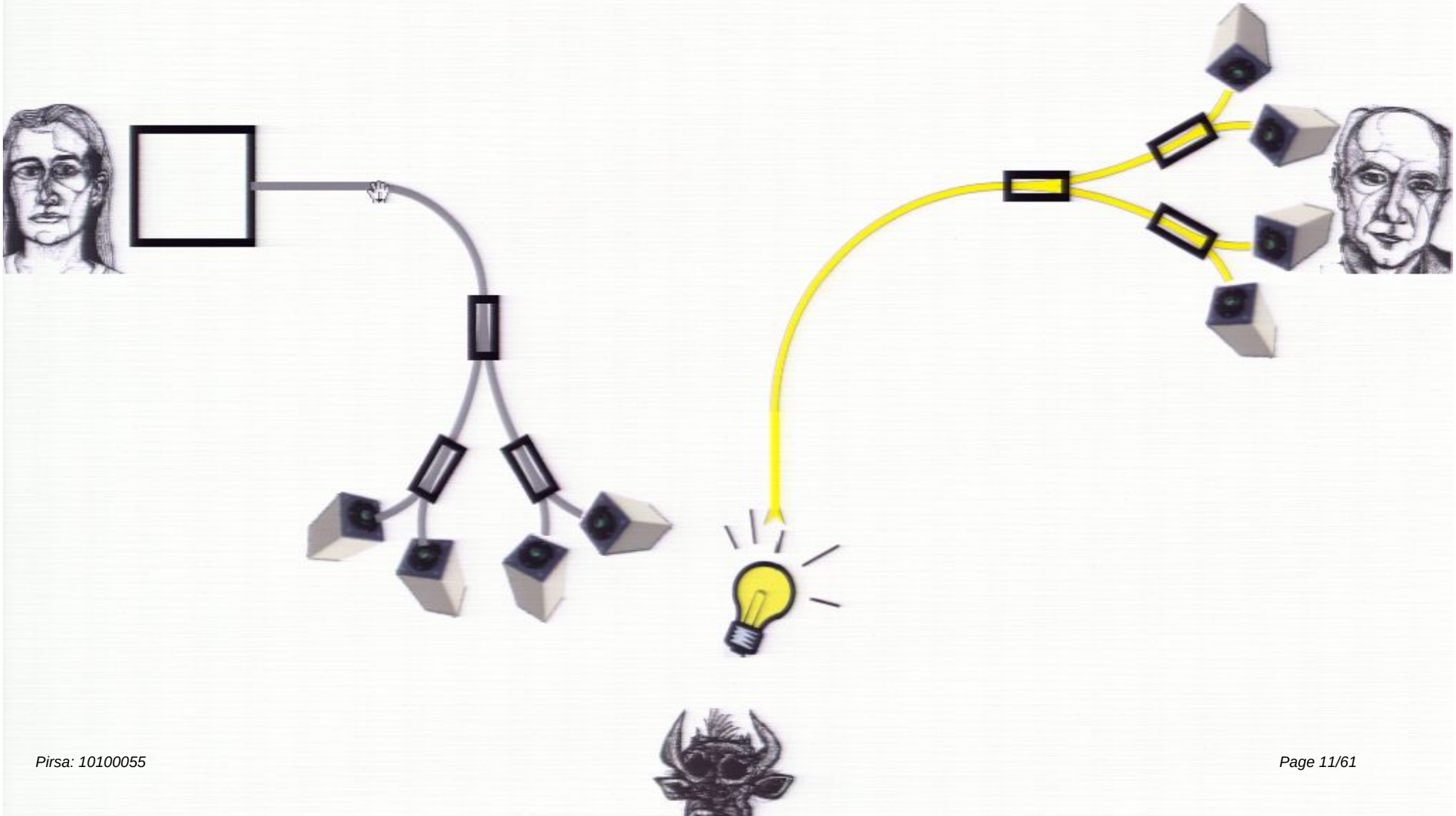
basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	✗	✓	✓	✓	✗	✓



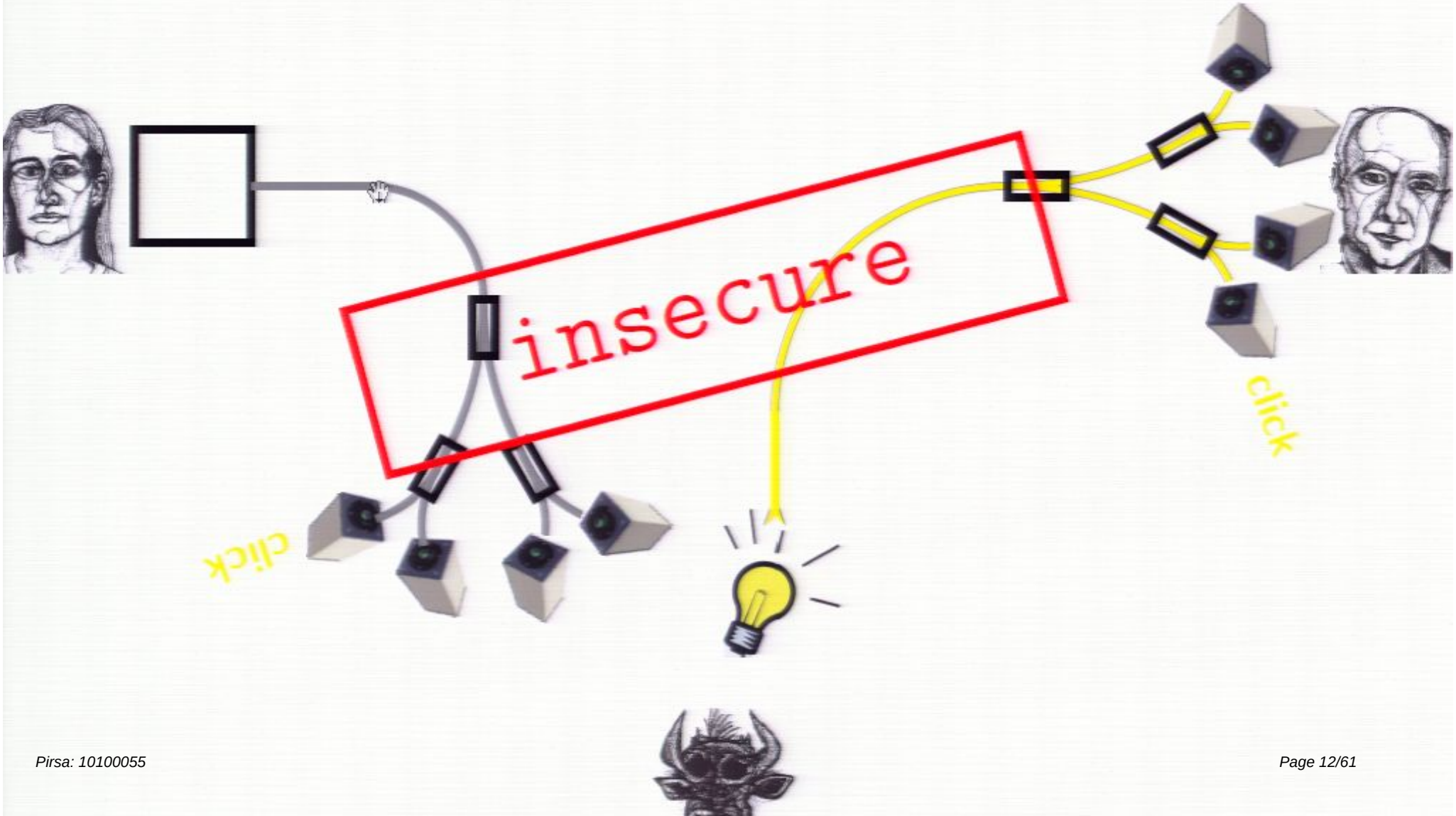
Possibility to Attack [Makarov 09]



Possibility to Attack [Makarov 09]



Possibility to Attack [Makarov 09]



Oh ...

comments on this story

Stories by subject
- Physics
- Technology

Stories by keywords
- Quantum cryptography
- Hacking
- Security

This article elsewhere
Blogs linking to this article
Add to Connotea

Published online 20 May 2010 | Nature | doi:10.1038/news.2010.256

News

Quantum crack in cryptographic armour

A commercial quantum encryption system has been fully hacked for the first time.

Zeeya Merali

Quantum cryptography isn't as invincible as many researchers thought: a commercial quantum key has been fully hacked for the first time.

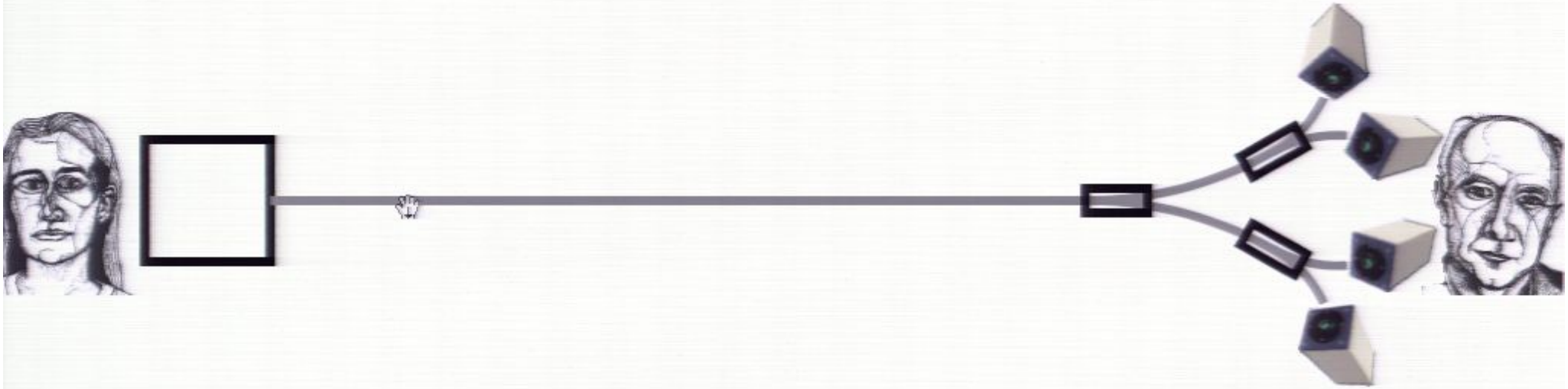
In theory, quantum cryptography — the use of quantum systems to encrypt information

most recent | commented

- Clever coupling catalysts lauded by chemistry Nobel
  06 October 2010
- Plan for addiction institute splits NIH
  06 October 2010
- Scientists need a shorter path to research freedom
  06 October 2010
- Racehorses came from European stock
  05 October 2010
- Food agency denies conflict-of-interest claim
  05 October 2010

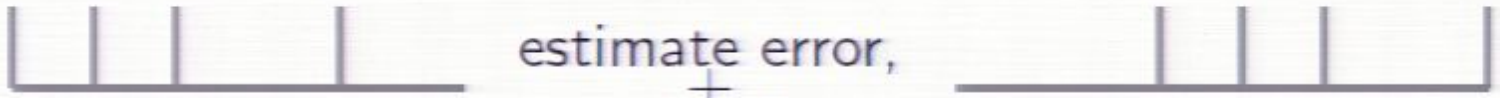
Related stories
- Nano-antennas could help keep quantum

Assumptions in Quantum Key Distribution

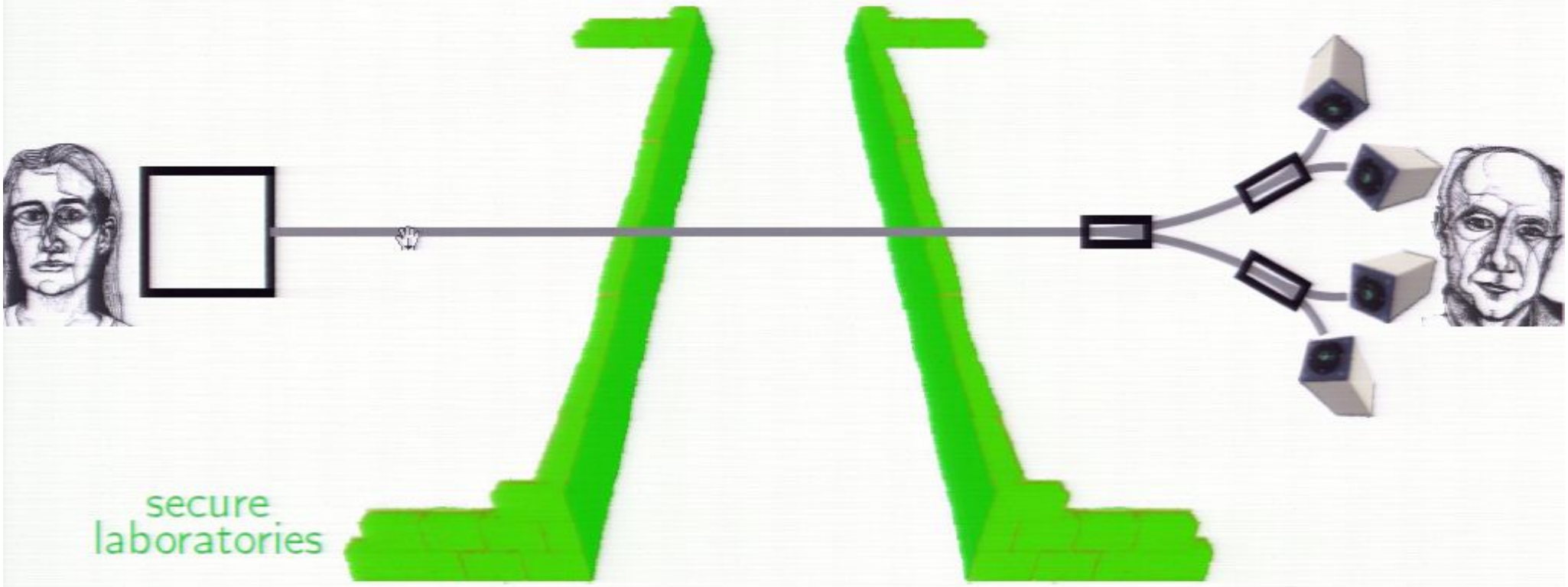


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓



Assumptions in Quantum Key Distribution

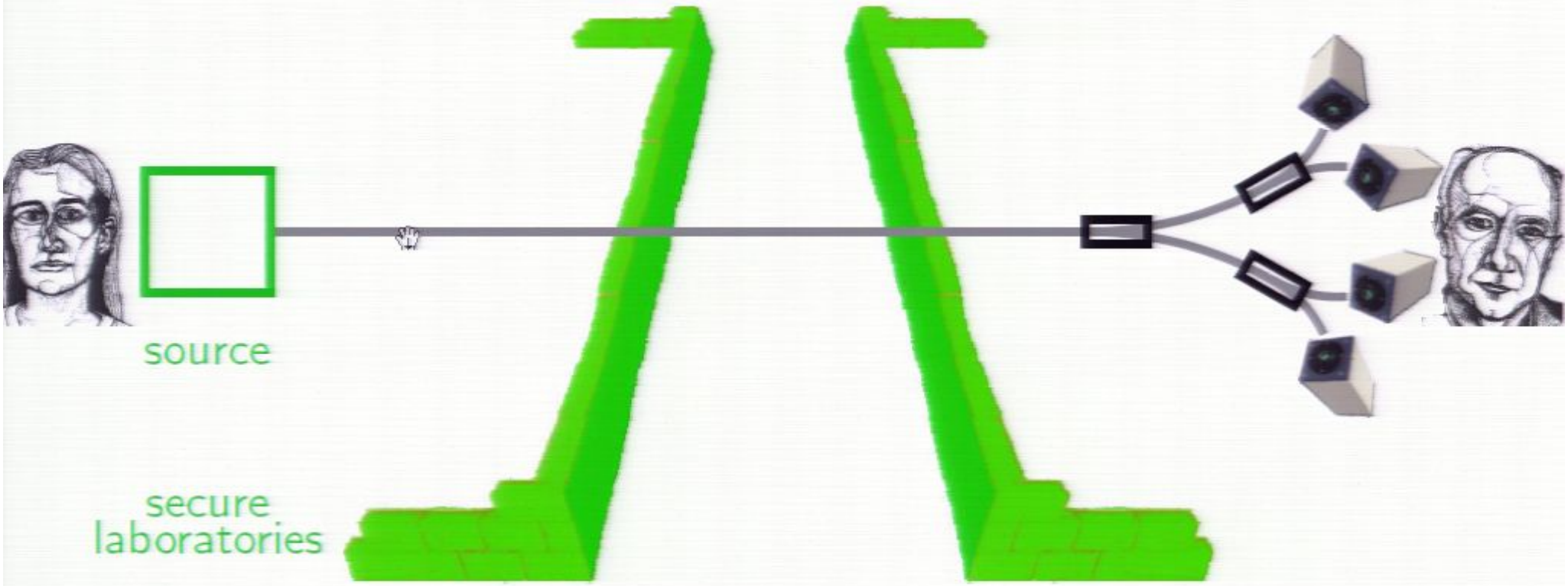


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

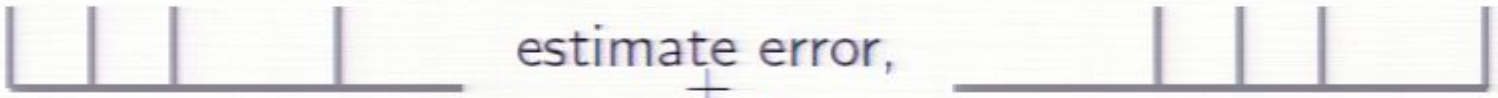
estimate error,

Assumptions in Quantum Key Distribution

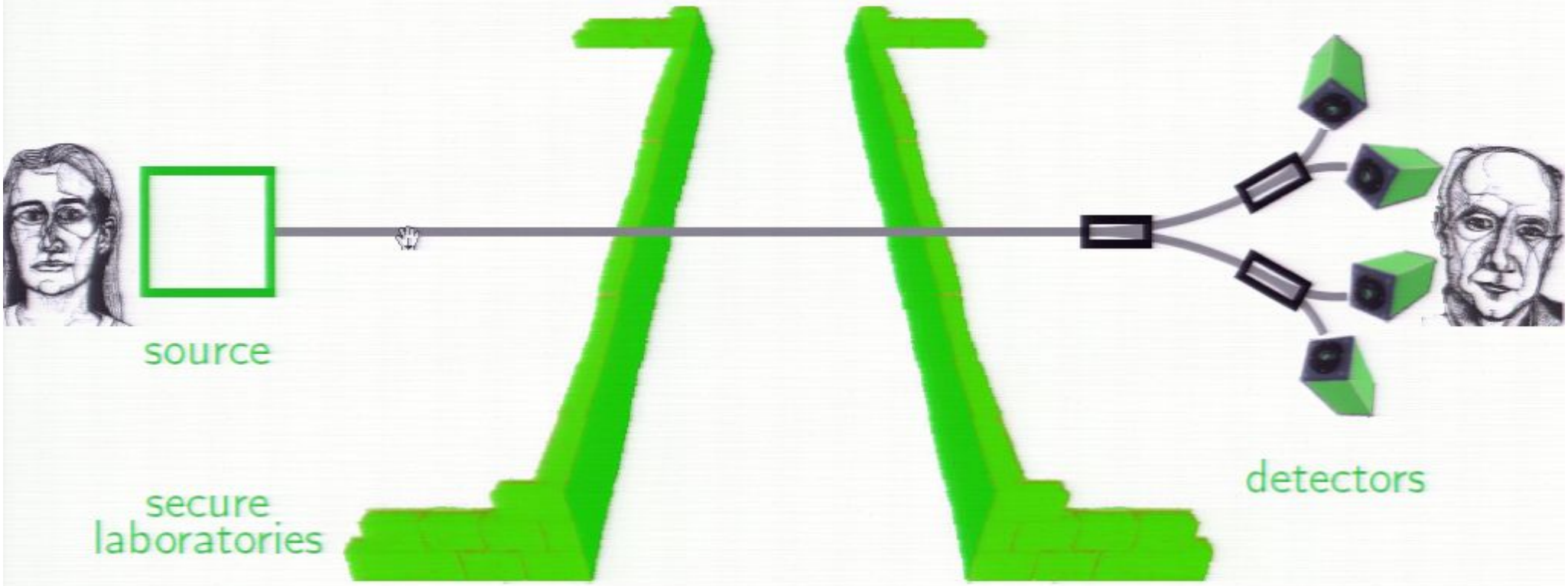


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓



Assumptions in Quantum Key Distribution

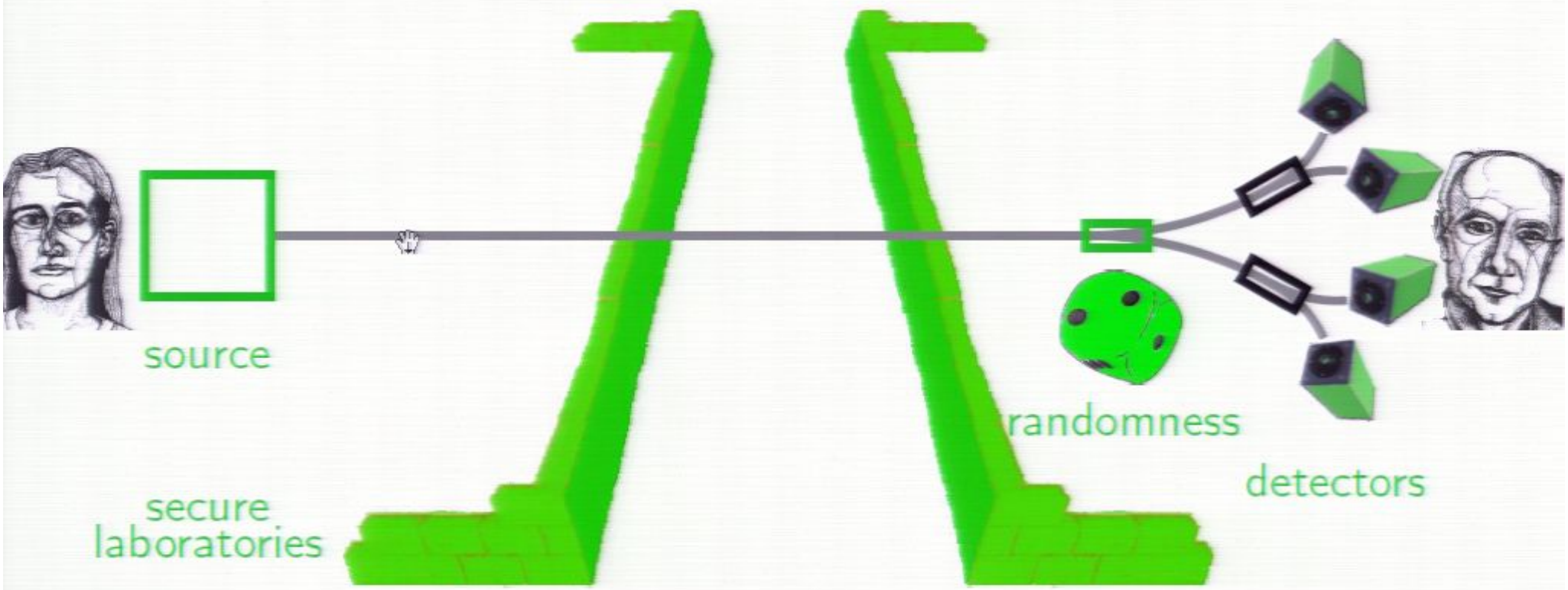


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

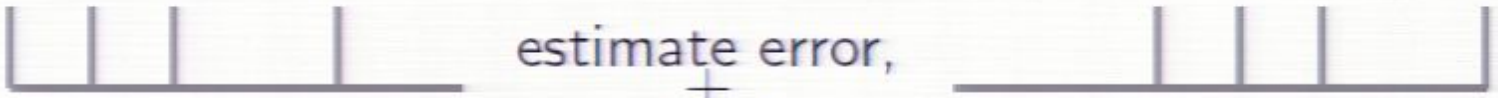
estimate error,

Assumptions in Quantum Key Distribution

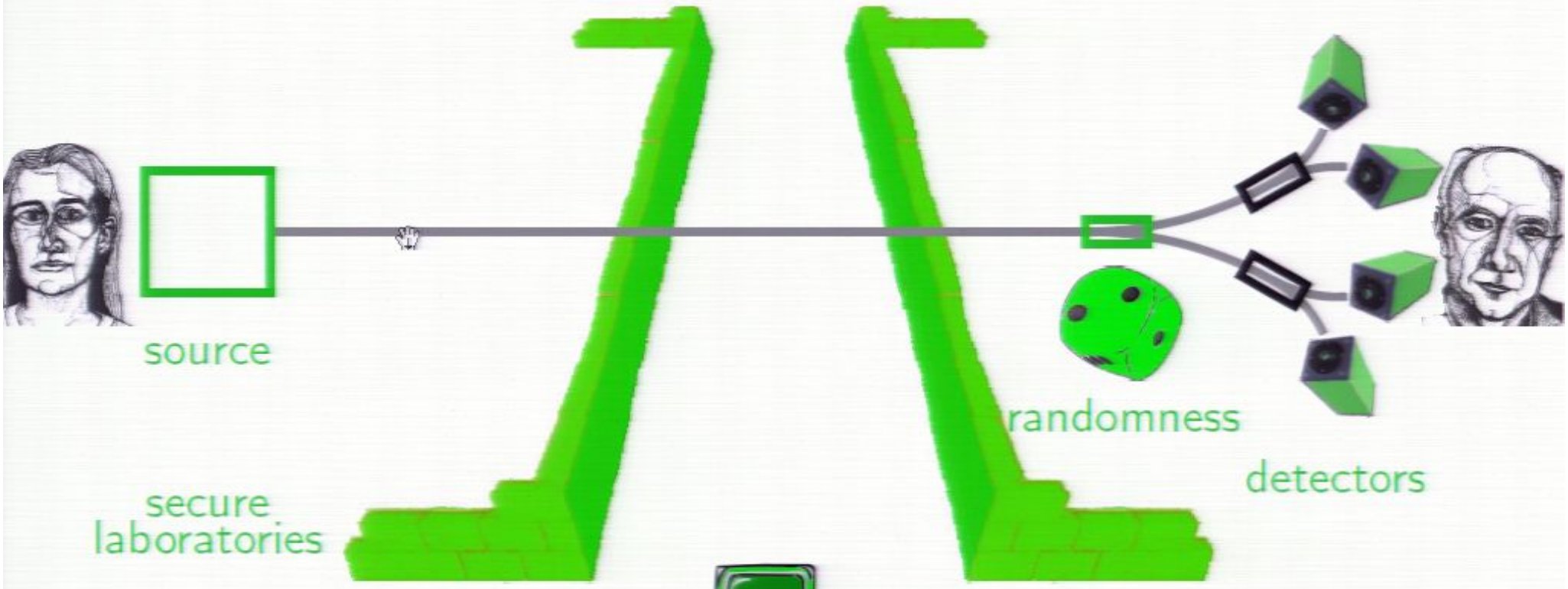


basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓



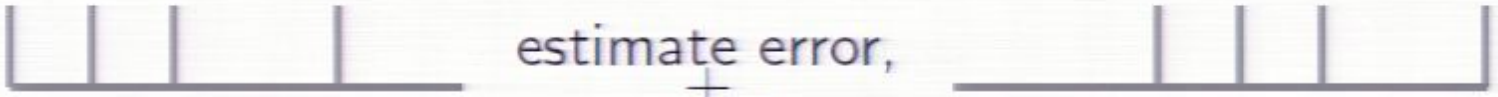
Assumptions in Quantum Key Distribution



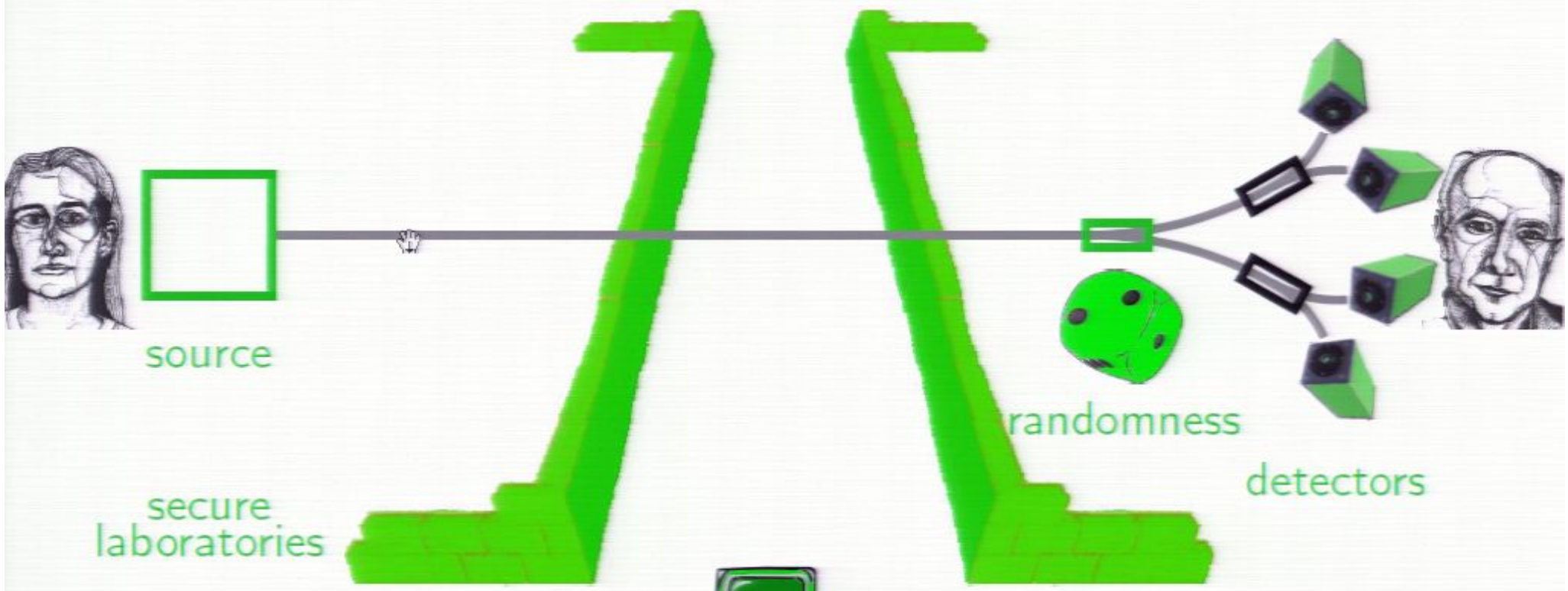
basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

classical computation

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓



Countermeasures



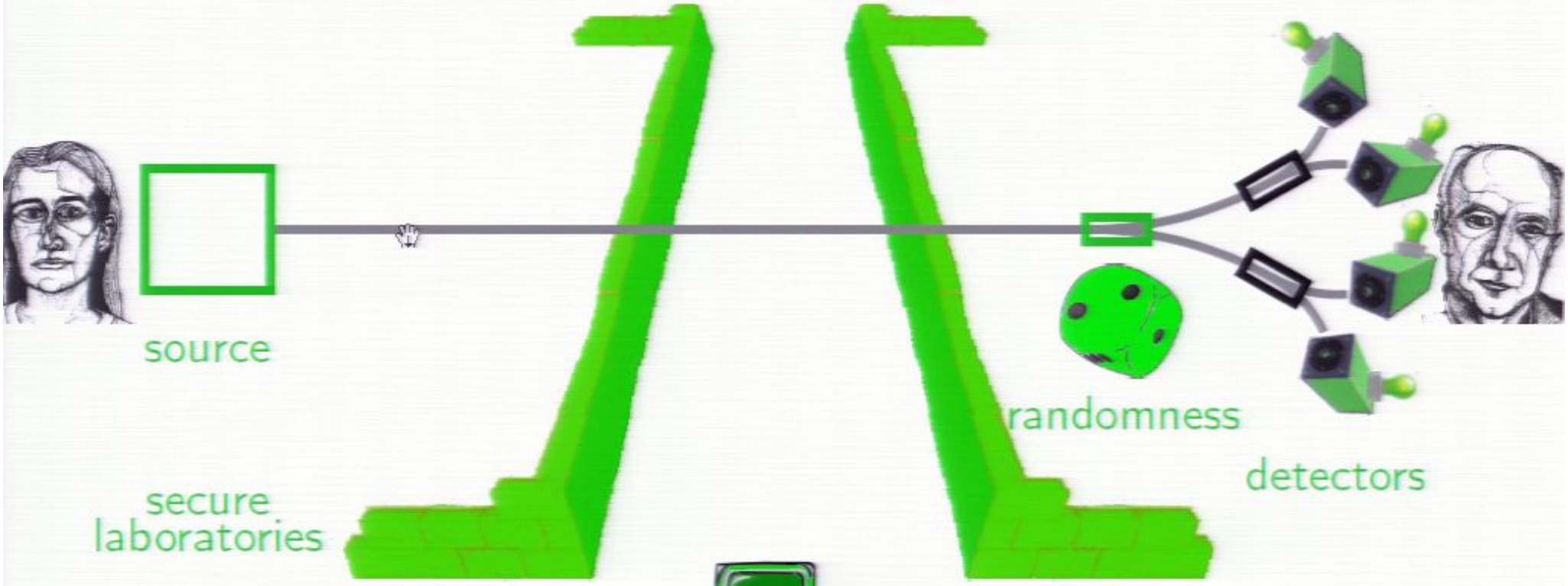
basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

classical computation

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

estimate error,

Countermeasures



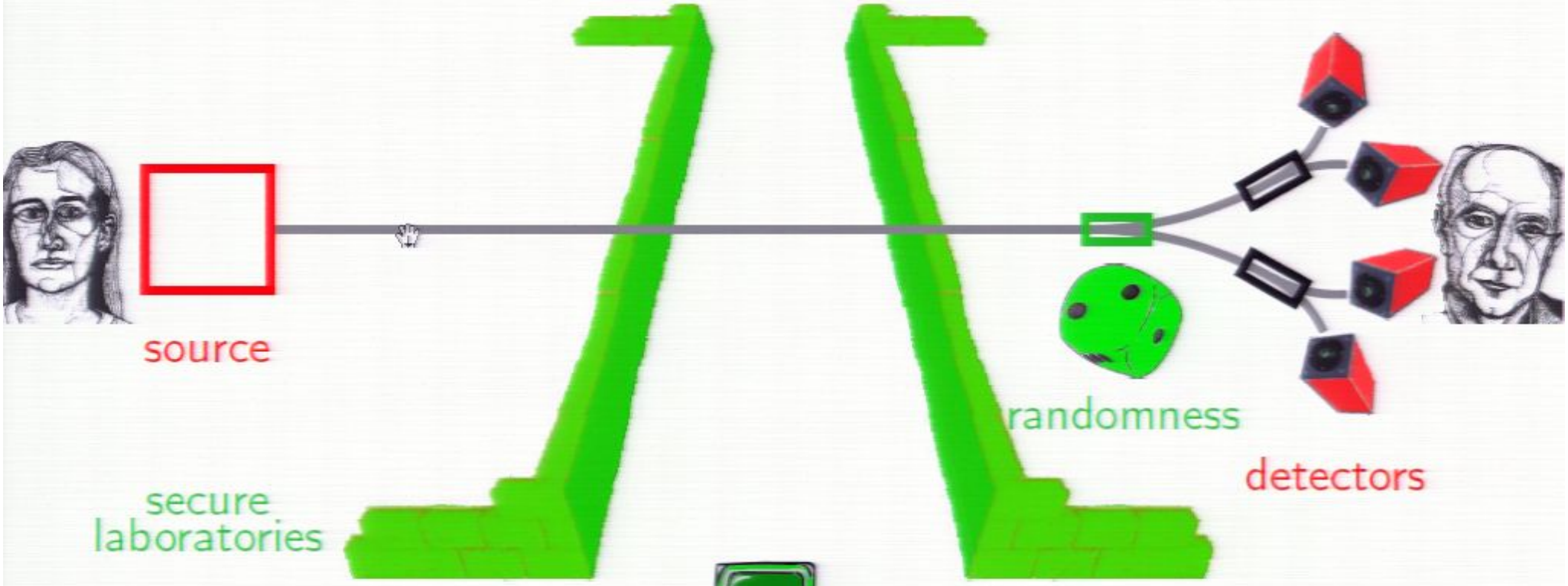
basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

classical computation

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

estimate error,

Countermeasures: Device-Independent QKD



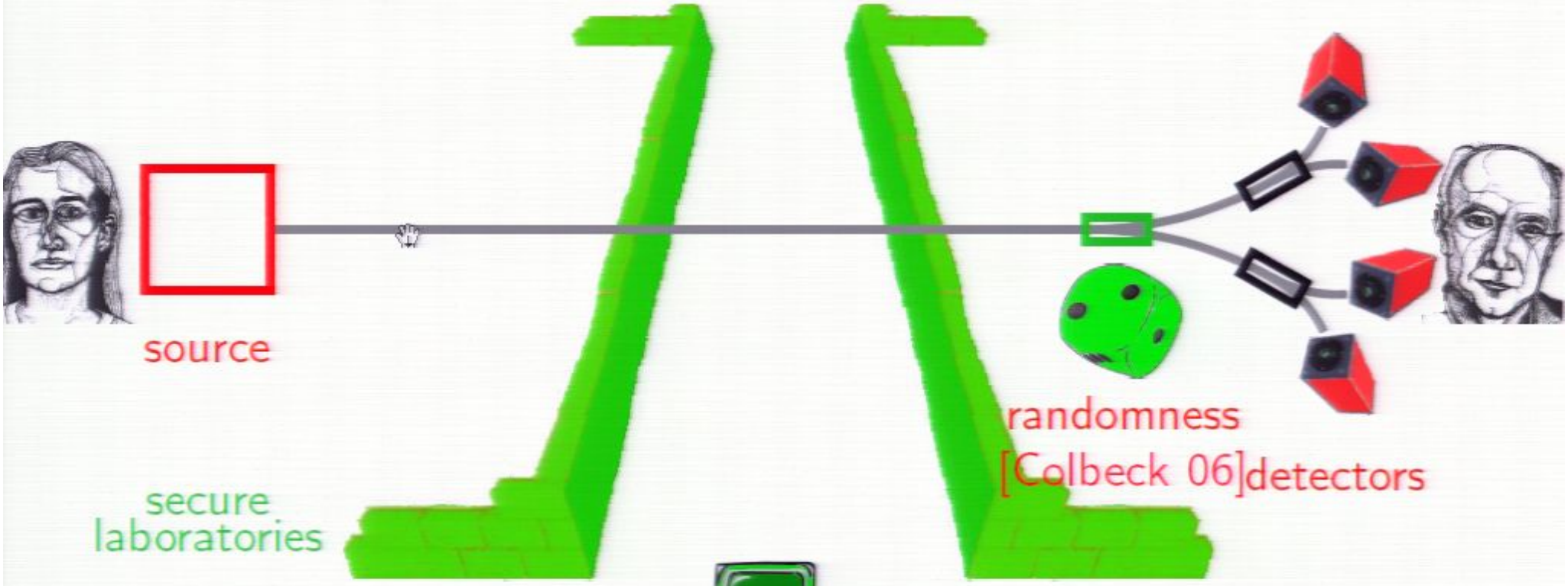
basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

classical computation

basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

estimate error,

Countermeasures: Device-Independent QKD



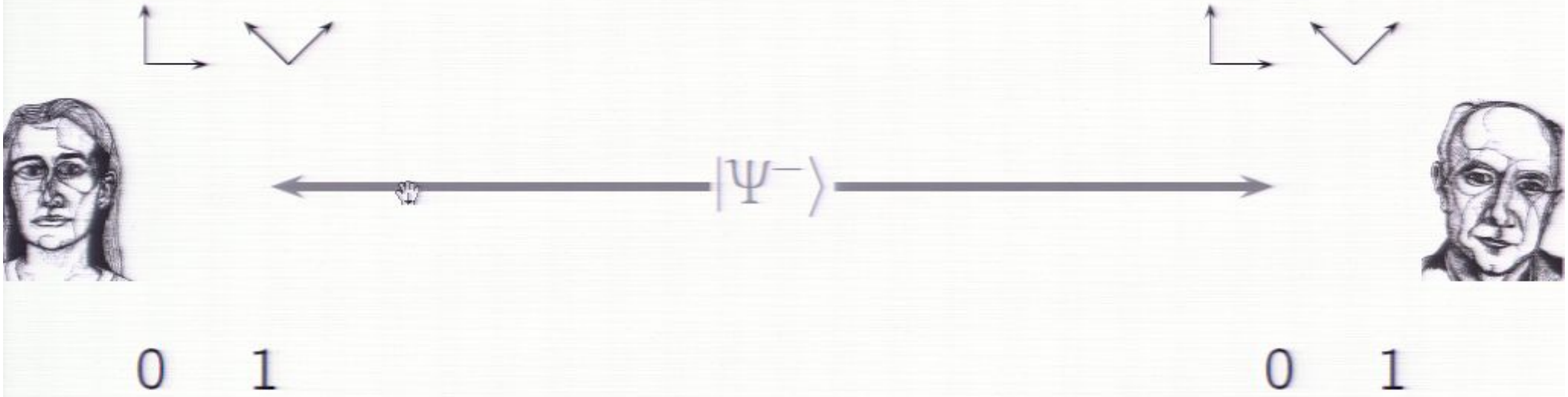
basis	+	+	×	+	×	×
bit	1	0	0	0	1	1
	×	✓	✓	✓	×	✓

classical computation

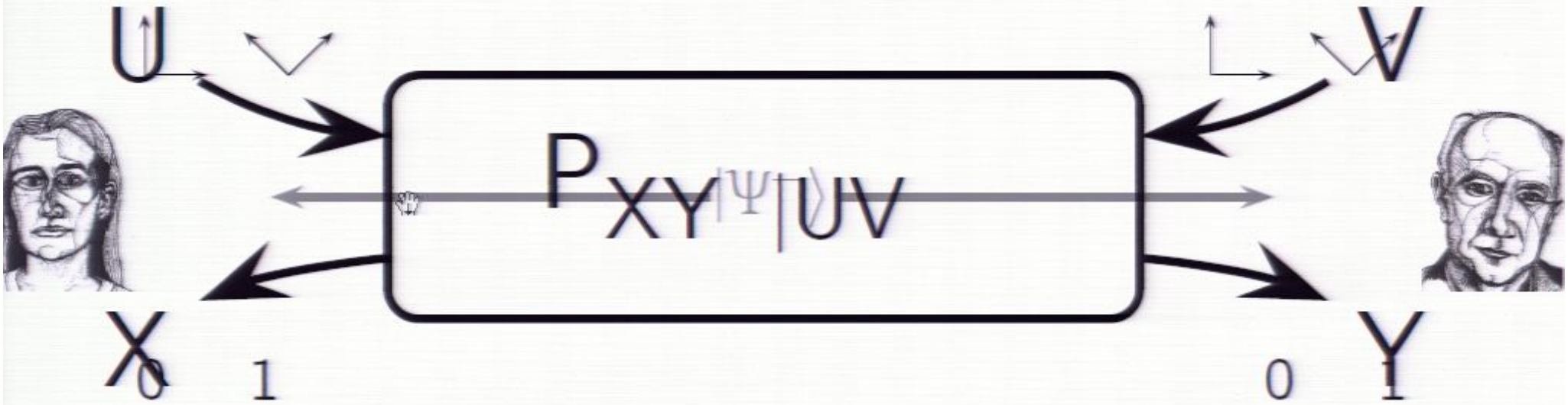
basis	×	+	×	+	+	×
result	0	0	1	0	1	1
	×	✓	✓	✓	×	✓

estimate error,

Device-Independent Quantum Key Distribution

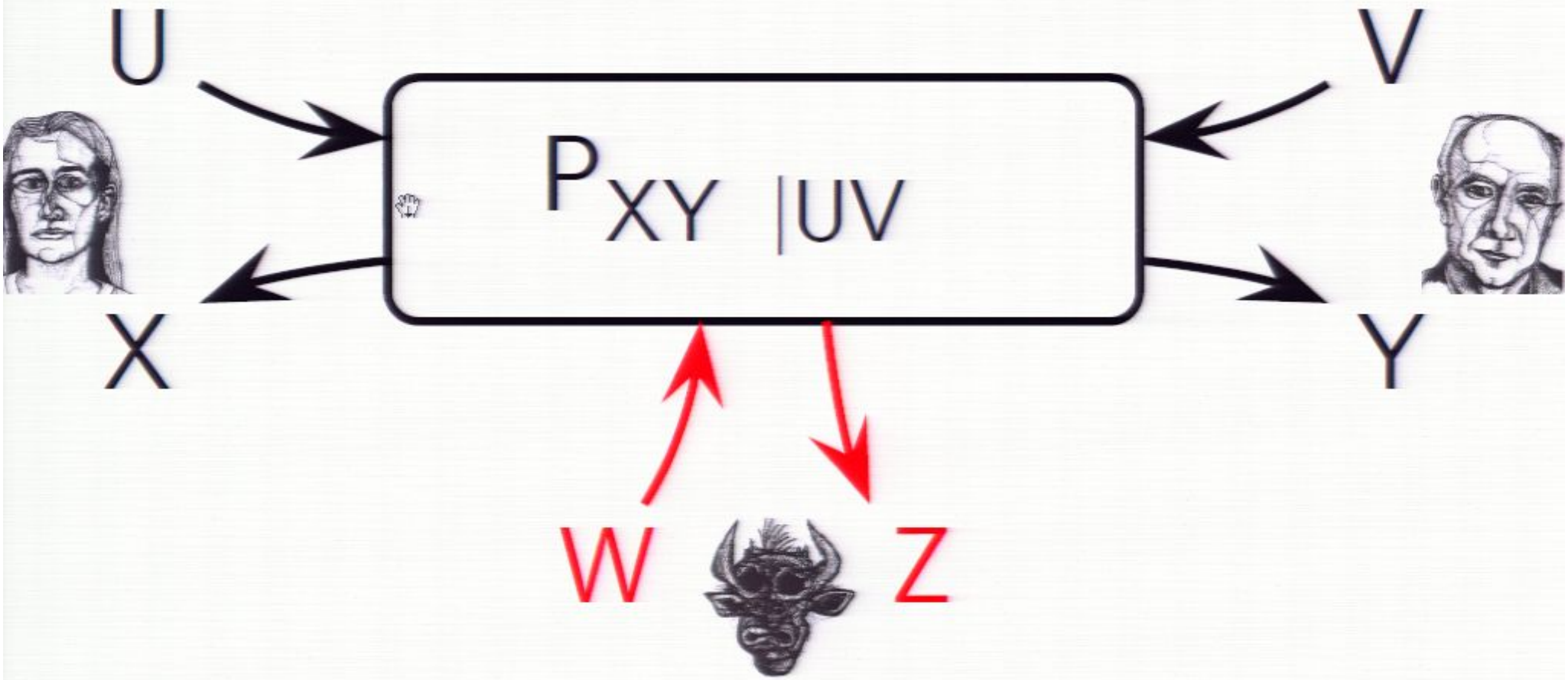


Device-Independent Quantum Key Distribution

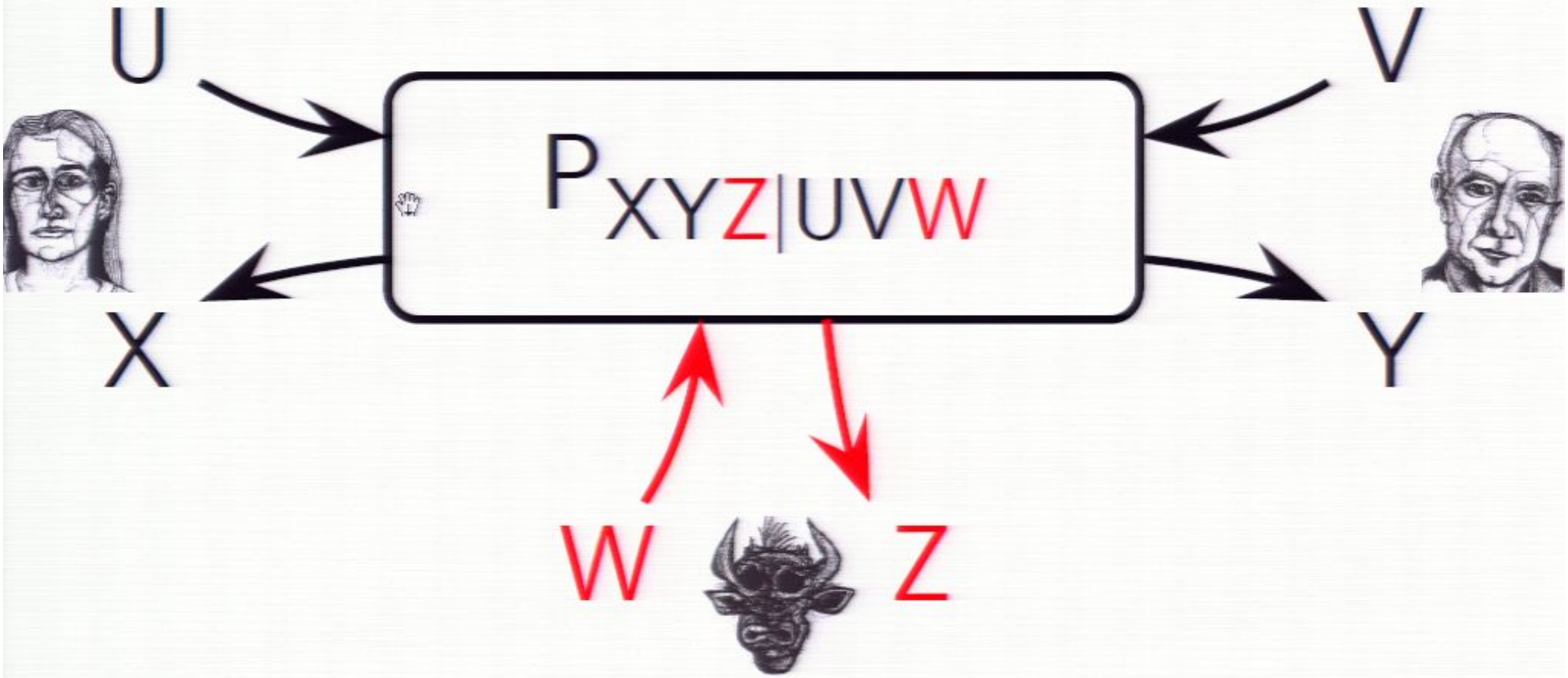


Device-Independent Quantum Key Distribution

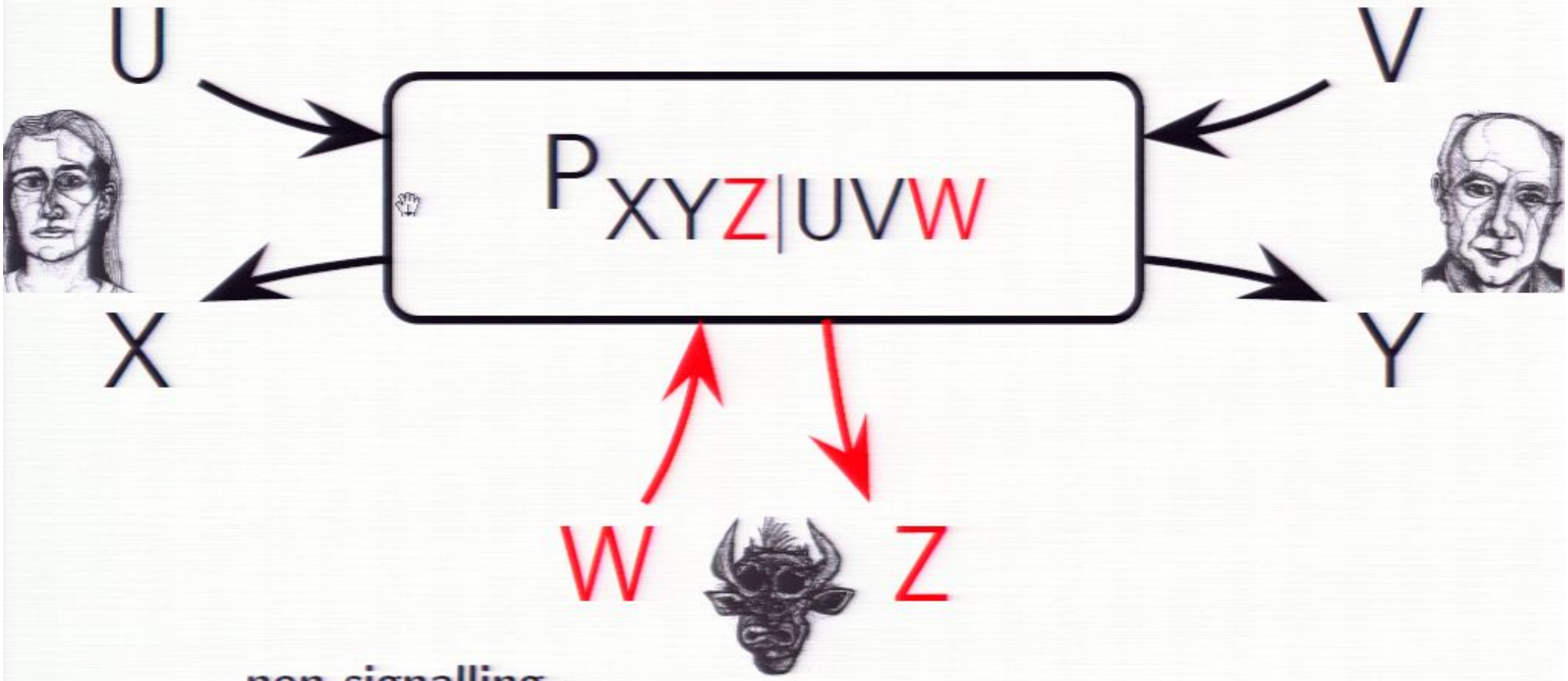
Device-Independent Quantum Key Distribution



Device-Independent Quantum Key Distribution



Device-Independent Quantum Key Distribution



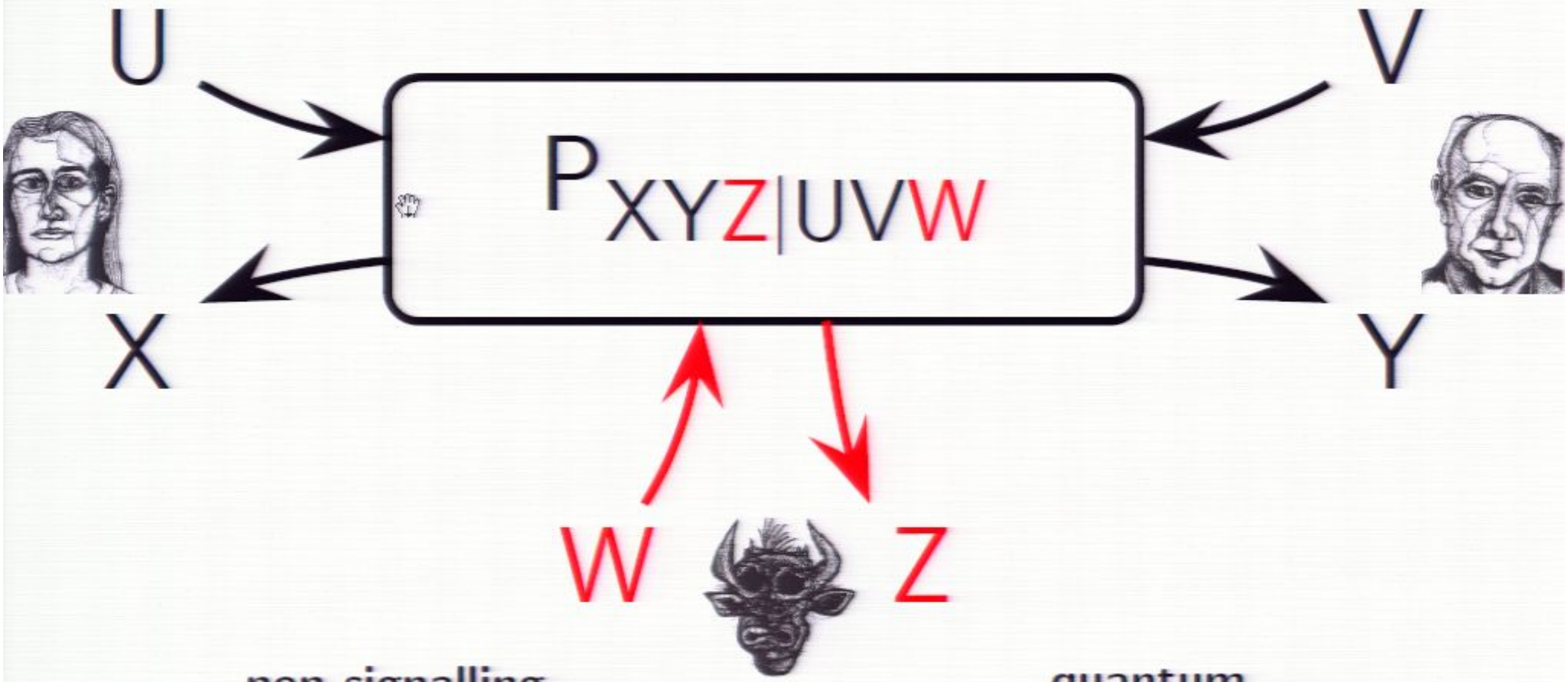
non-signalling

no message transmission

via physical device

[Barrett Hardy Kent 05]

Device-Independent Quantum Key Distribution



non-signalling

no message transmission via physical device

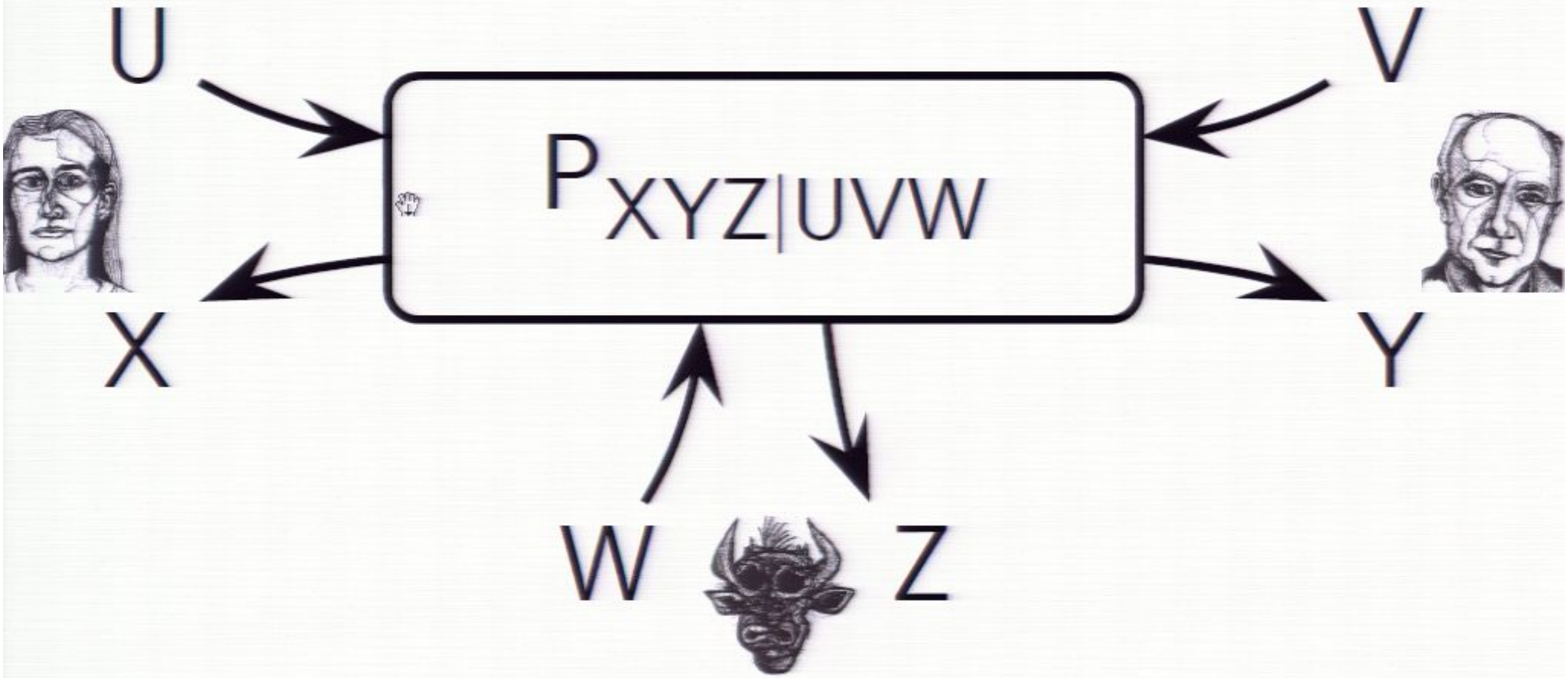
[Barrett Hardy Kent 05]

quantum

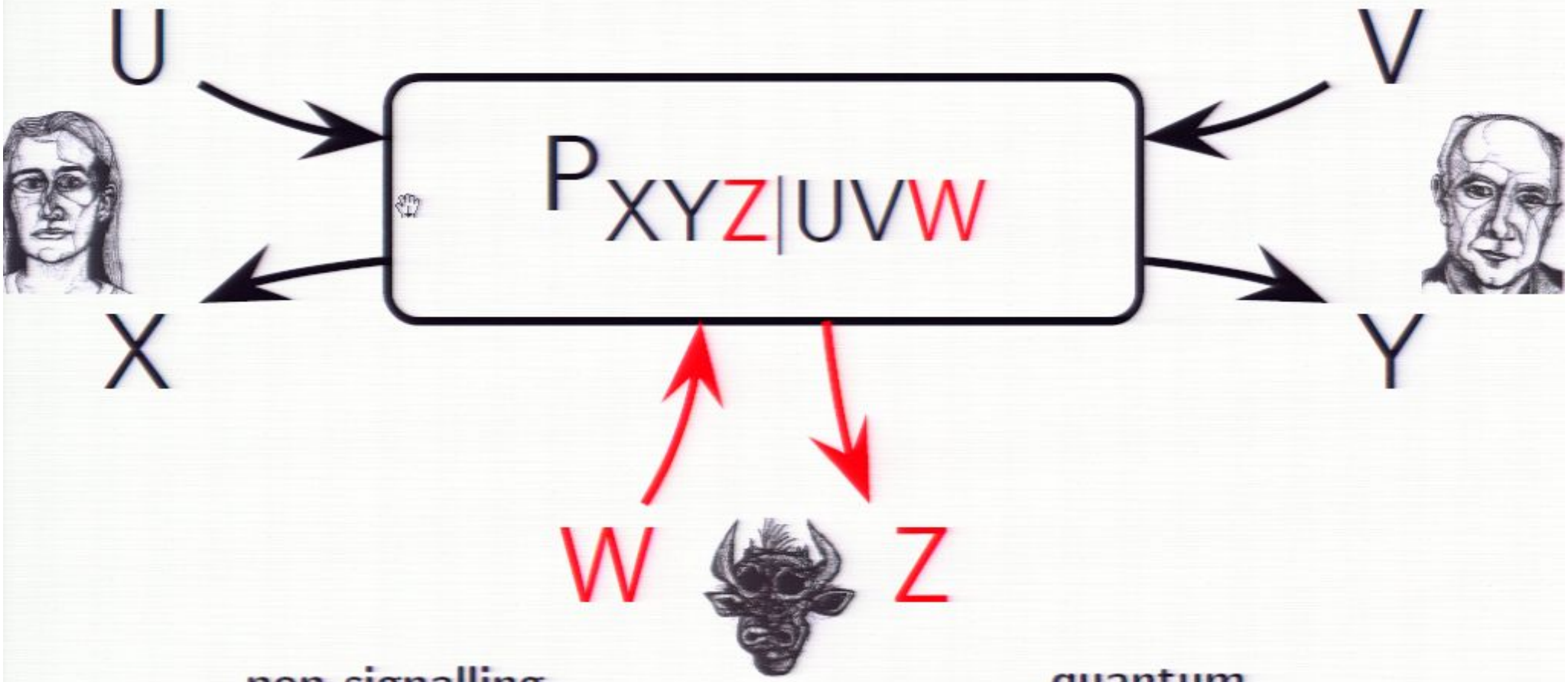
$P_{XYZ|UVW}$ corresponds to measuring a quantum state

[Mayers Yao 98]

Modelling Attacks



Device-Independent Quantum Key Distribution



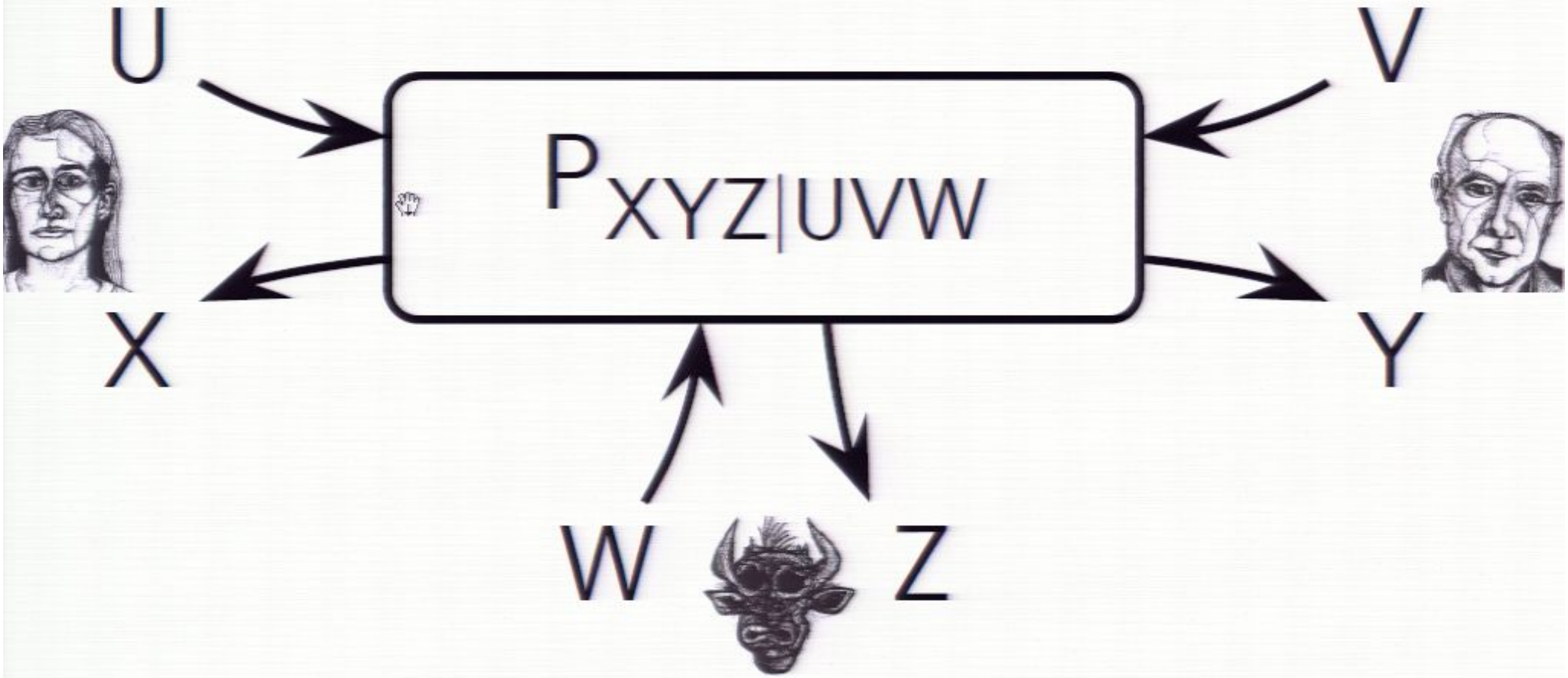
non-signalling

no message transmission via physical device [Barrett Hardy Kent 05]

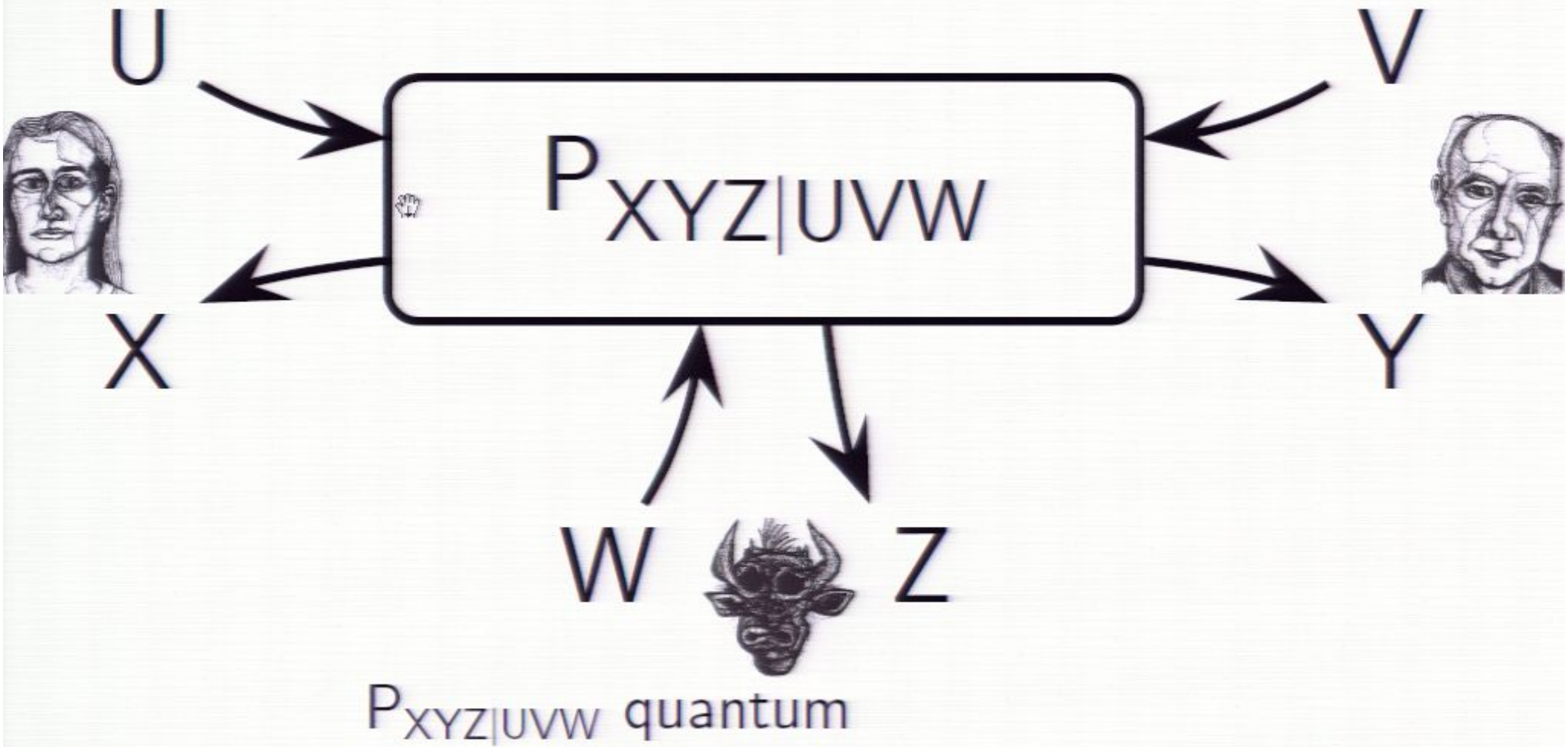
quantum

$P_{XYZ|UVW}$ corresponds to measuring a quantum state [Mayers Yao 98]

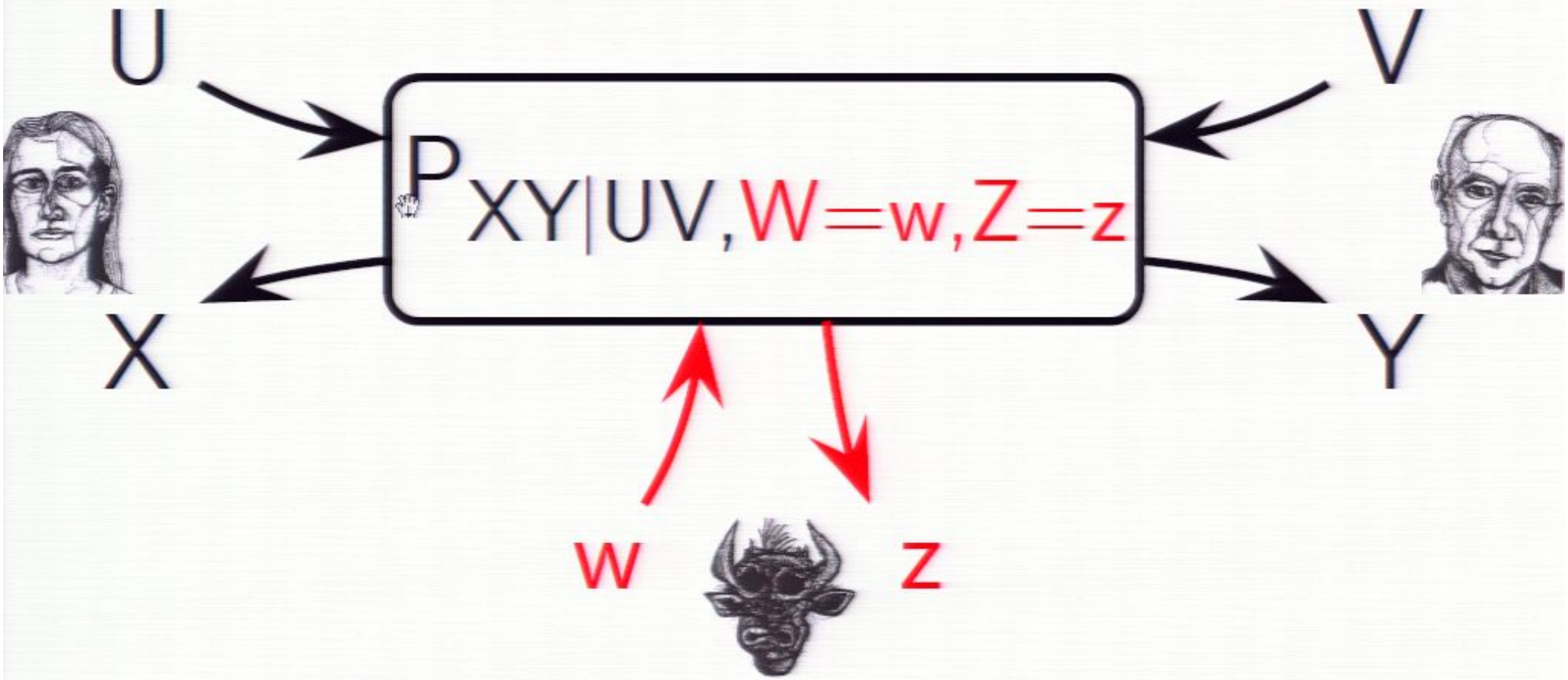
Modelling Attacks



Modelling Attacks



Modelling Attacks



$P_{XYZ|UVW}$ quantum

$\Longrightarrow$ $P_{XY|UV,W=w,Z=z}$ quantum

Modelling Attacks

$$P_{XY|UV} = p(z_0|w)\cdot P_{XY|UV,W=w,Z=z_0} + p(z_1|w)\cdot P_{XY|UV,W=w,Z=z_1}$$

quantum quantum

Modelling Attacks

$$P_{XY|UV} = p(z_0|w)\cdot P_{XY|UV,W=w,Z=z_0} + p(z_1|w)\cdot P_{XY|UV,W=w,Z=z_1}$$

quantum quantum

max: $P(X=z)$

s.t.: $\sum_z P_{XY|UV,W=w,Z=z} = P_{XY|UV}$

$P_{XY|UV,W=w,Z=z}$ quantum

Modelling Attacks

$$P_{XY|UV} = p(z_0|w)\cdot P_{XY|UV,W=w,Z=z_0} + p(z_1|w)\cdot P_{XY|UV,W=w,Z=z_1}$$

quantum quantum

SDP

[Navascués,Pironio,Acín 07]

max: $P(X=z)$

s.t.: $\sum_z P_{XY|UV,W=w,Z=z} = P_{XY|UV}$

$P_{XY|UV,W=w,Z=z}$ quantum

Modelling Attacks

$$P_{XY|UV} = p(z_0|w)\cdot P_{XY|UV,W=w,Z=z_0} + p(z_1|w)\cdot P_{XY|UV,W=w,Z=z_1}$$

quantum ~~quantum~~ quantum

SDP

[Navascués,Pironio,Acín 07]

$$\begin{aligned} \max:\quad & b^T \cdot \Gamma \\ \text{s.t.:}\quad & A\cdot\Gamma = c \\ & \Gamma \succeq 0 \end{aligned}$$

Modelling Attacks

$$P_{XY|UV} = p(z_0|w)\cdot P_{XY|UV,W=w,Z=z_0} + p(z_1|w)\cdot P_{XY|UV,W=w,Z=z_1}$$

quantum quantum

SDP

[Navascués,Pironio,Acín 07]

$$P_{guess} \leqslant$$

max:	$b^T \cdot \Gamma$
s.t.:	$A\cdot\Gamma=c$
	$\Gamma \succeq 0$

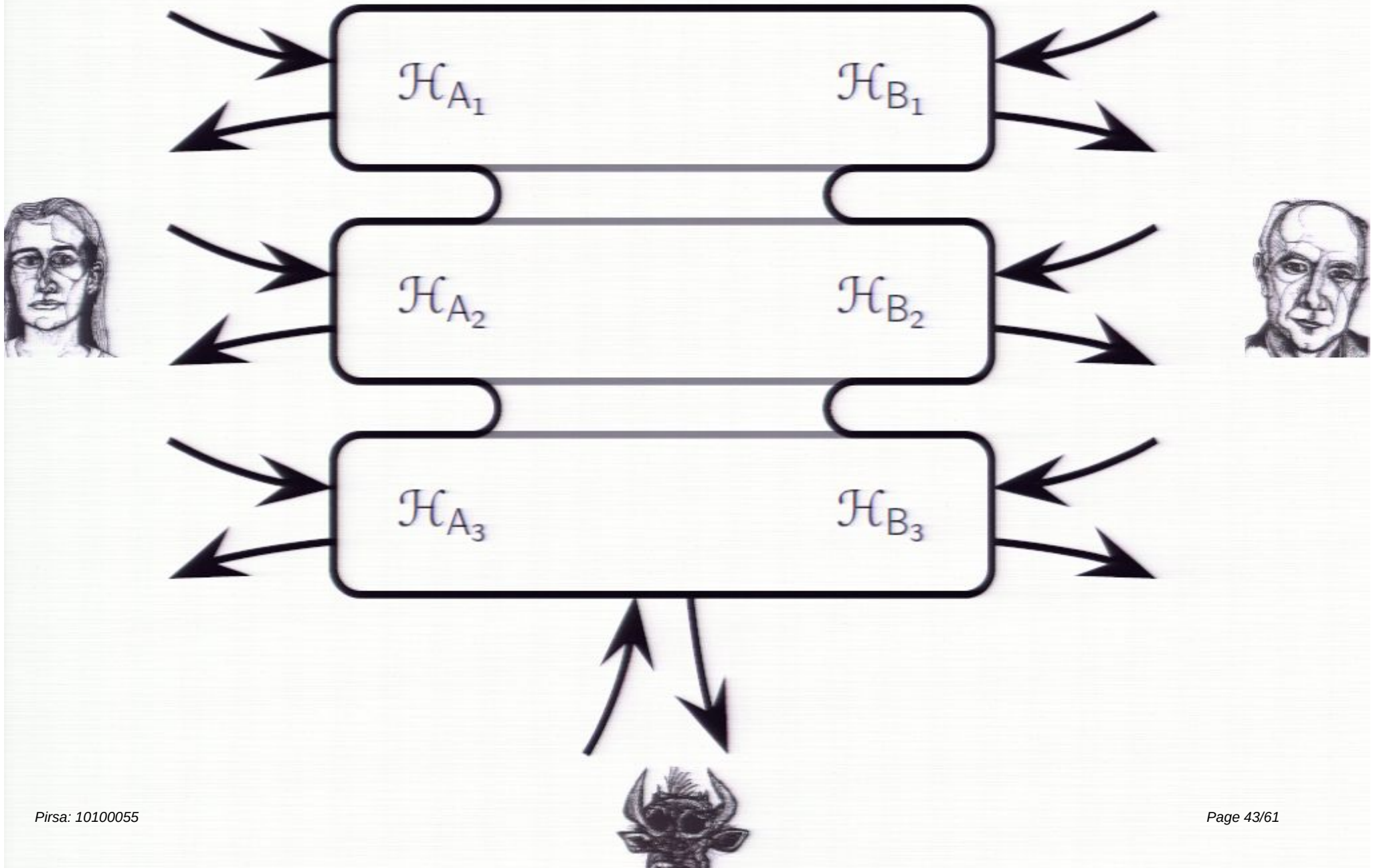
DUAL

min:	$c^T \cdot \lambda$
s.t.:	$A^T \cdot \lambda \preceq b$

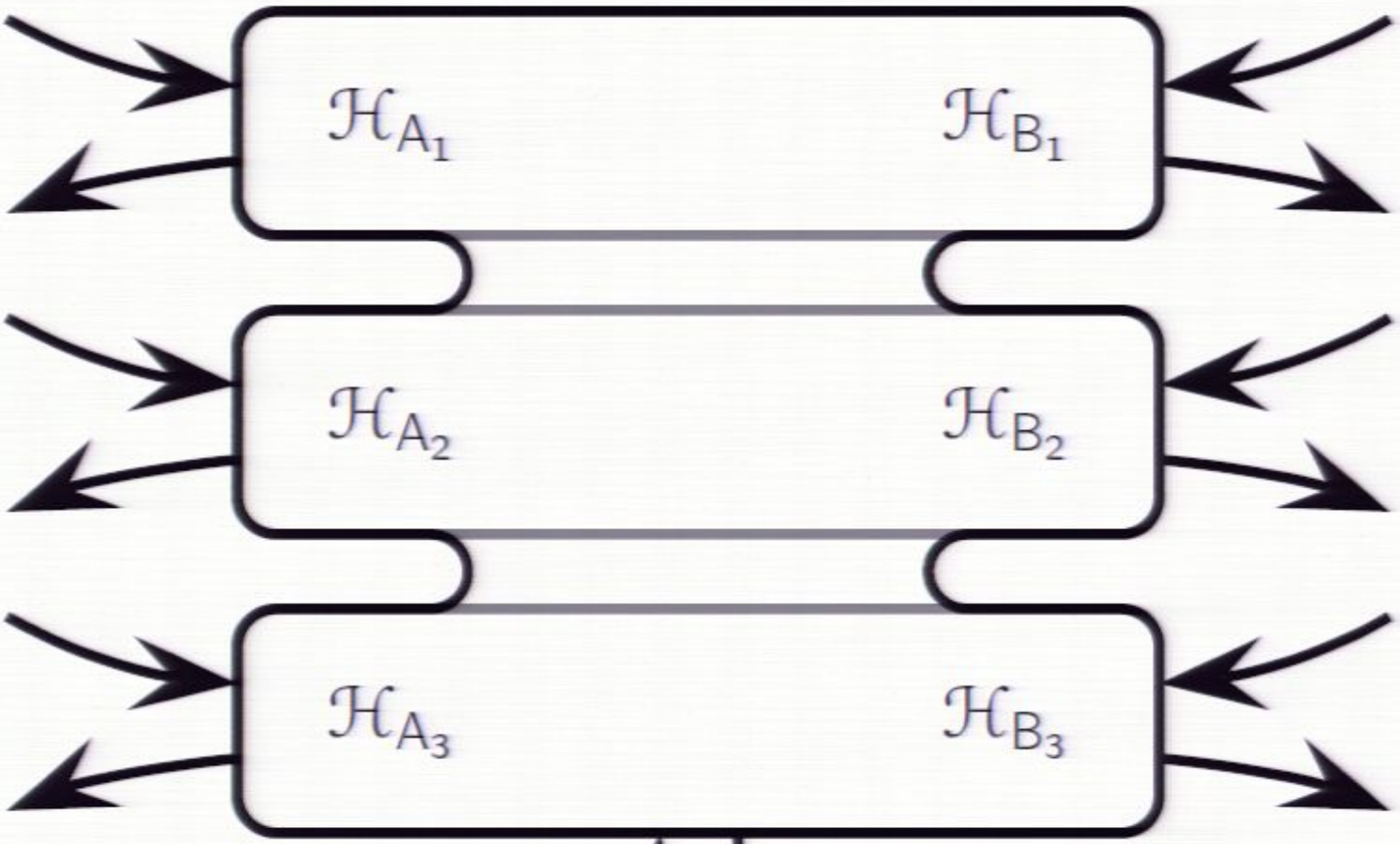
Coherent Attacks

Coherent Attacks

Coherent Attacks



Coherent Attacks



Condition: measurements on different subsystems commute

Attacks on Several Systems

max: $b^T \cdot \Gamma$

s.t.: $A \cdot \Gamma = c$

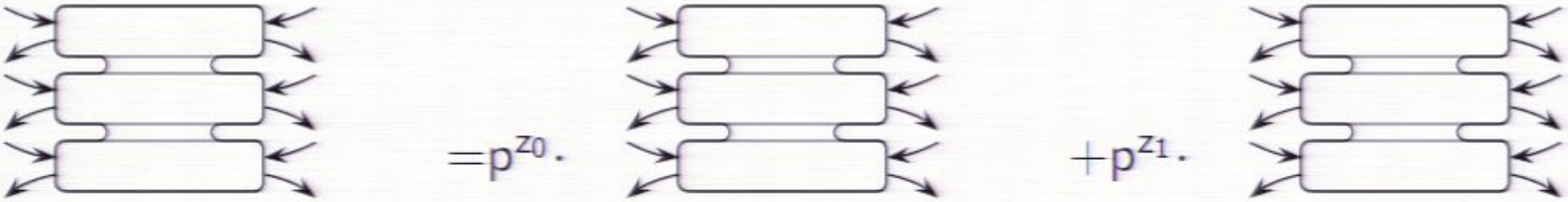
$\Gamma \succeq 0$

$P_{guess} \leqslant$

min: $c^T \cdot \lambda$

s.t.: $A^T \cdot \lambda \preceq b$

Attacks on Several Systems



max: $b^T \cdot \Gamma$

s.t.: $A \cdot \Gamma = c$

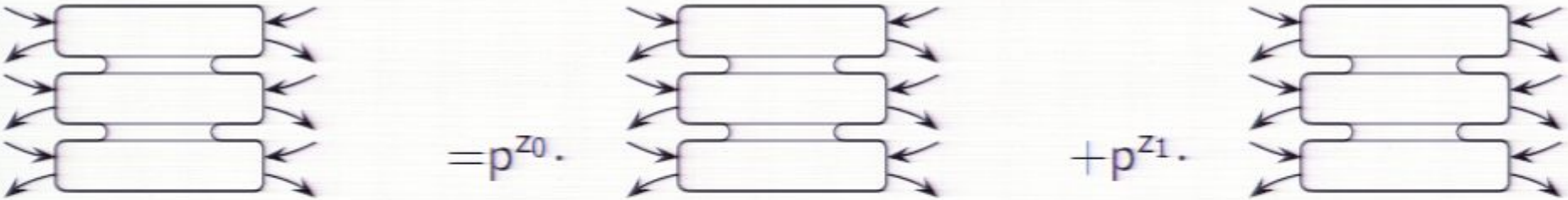
$\Gamma \succeq 0$

$P_{guess} \leqslant$

min: $c^T \cdot \lambda$

s.t.: $A^T \cdot \lambda \preceq b$

Attacks on Several Systems



Condition [HR 10]

$$P_{\text{guess}} \leqslant$$

$$P^n_{\text{guess single}} =$$

max: $b^{T\otimes n}\cdot\Gamma$

s.t.: $A^{\otimes n}\cdot\Gamma = c^{\otimes n}$

$\Gamma \succeq 0$

min: $c^{T\otimes n}\cdot\lambda^{\otimes n}$

s.t.: $A^{T\otimes n}\cdot\lambda^{\otimes n} \preceq b^{\otimes n}$

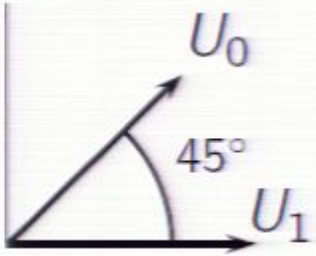
Protocol

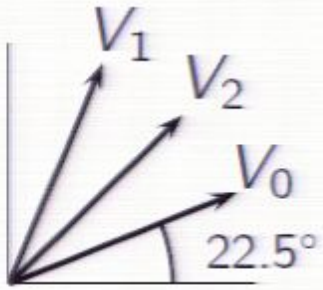
Protocol

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ 

Protocol

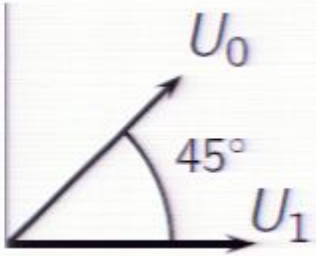
$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

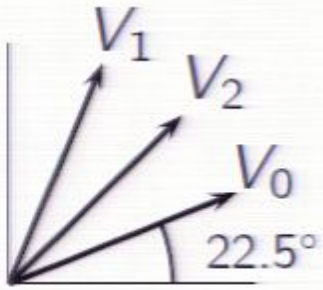




Protocol

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ ⟶

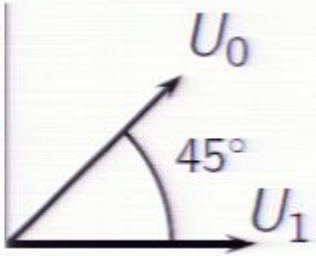


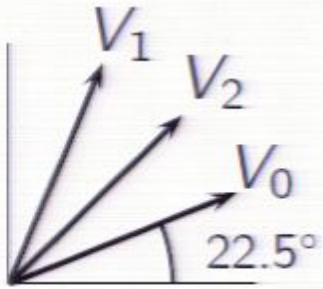


E: estimate $P_{\text{guess single}}$ and error δ

Protocol

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ ⟶



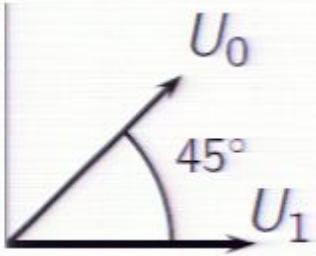


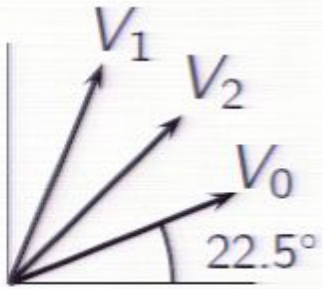
'E: estimate $P_{\text{guess single}}$ and error δ

R [BS93,ILL89]: $m=f(X) \xrightarrow{m,f,|m|=n\cdot h(\delta)} Y'=f(X)$

Protocol

$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ ⟶





E: estimate $P_{\text{guess single}}$ and error δ

R [BS93,ILL89]: $m=f(X) \xrightarrow{m,f,|m|=n\cdot h(\delta)} Y'=f(X)$

A [RK05]: $s=f'(X) \xrightarrow{f'} s'=f'(Y')$

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Thank you

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Thank you

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Thank you

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Thank you

Conclusion and Open questions

Device-independent QKD possible under additional condition on subsystems

- coherent attack $\approx$ individual attack
- secure against the most general adversary
- composable security

Additional condition necessary?

Other applications?

Thank you