Randomness can be amplified

Renato Renner, ETH Zurich

collaboration with Roger Colbeck, University of York

Outline

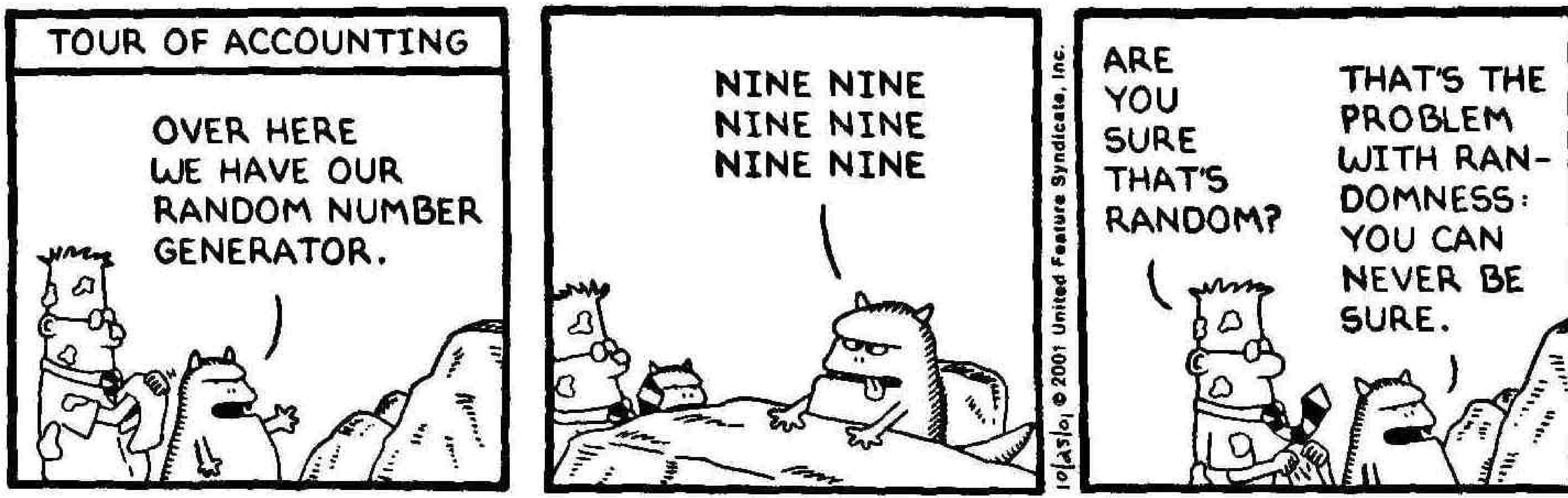
It may be difficult to assert that a process is random …

Outline

It may be difficult to assert that a process is random …

Outline

It may be difficult to assert that a process is random …



© Dilbert by Scott Adams

… but once you know it is just a little, you can amplify it and obtain perfectly random bits.

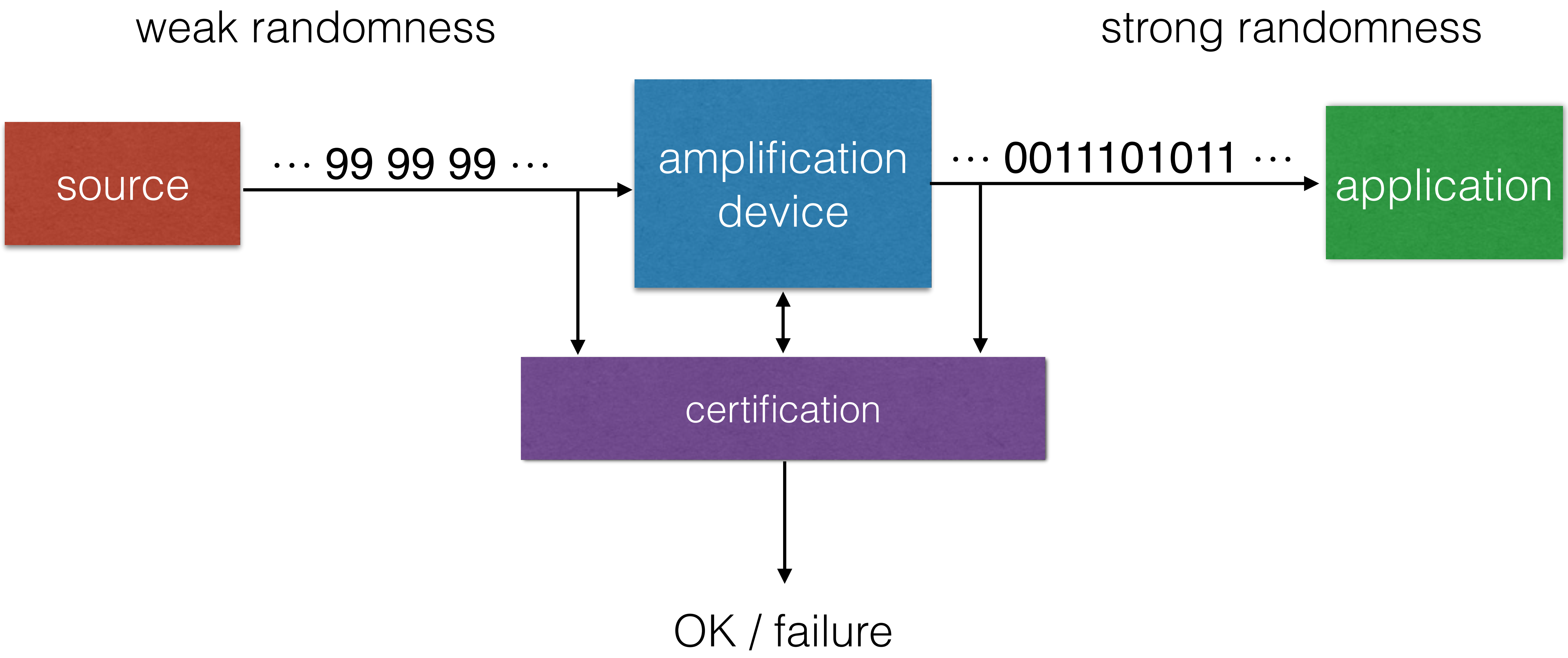
$\cdots$ 99 99 99 $\cdots$ → randomness amplification → $\cdots$ 0011101011 $\cdots$

Goal

Randomness amplification with certification

Goal

Randomness amplification with certification



Randomness

Random numbers are used in numerous applications:

Randomness

Random numbers are used in numerous applications:

- Gambling

Randomness

Random numbers are used in numerous applications:

- Gambling
- Simulation (e.g., Monte Carlo algorithms)

Randomness

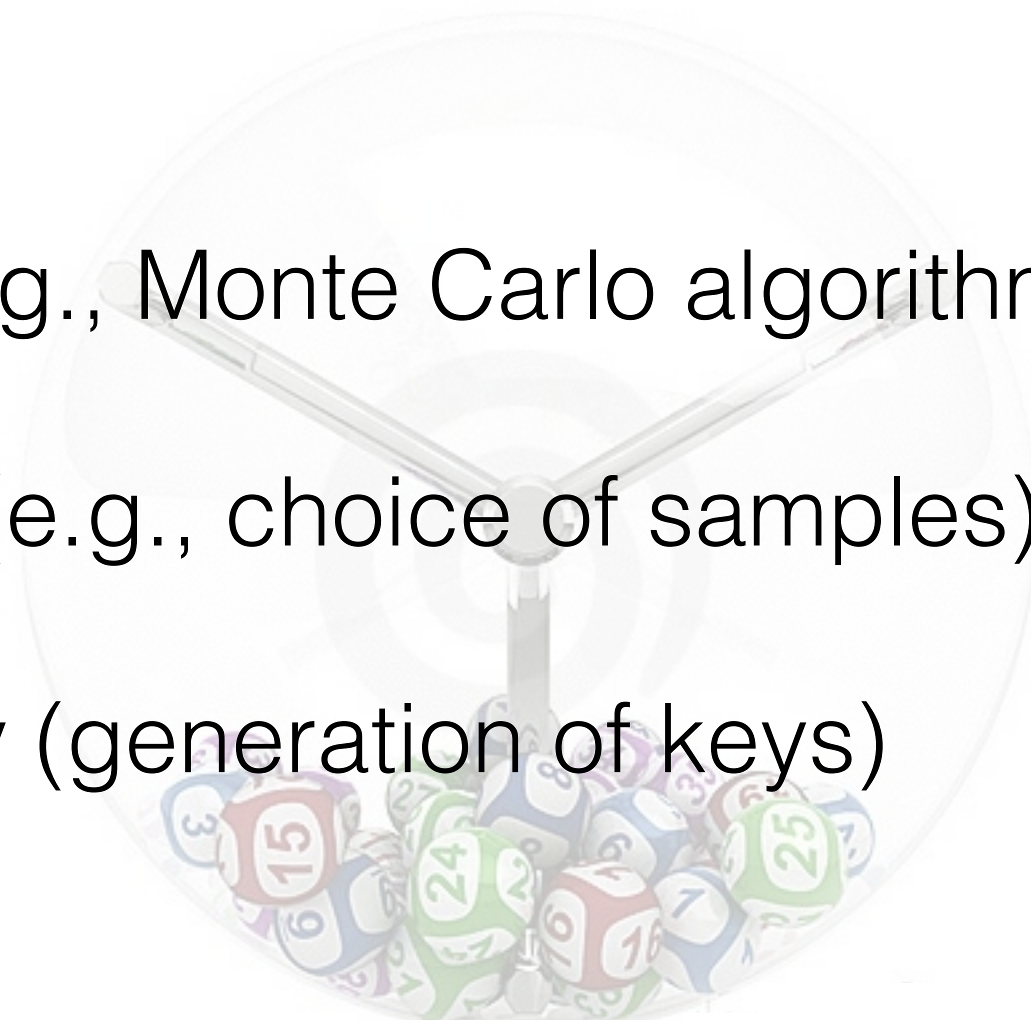
Random numbers are used in numerous applications:

- Gambling
- Simulation (e.g., Monte Carlo algorithms)
- Experiments (e.g., choice of samples)

Randomness

Random numbers are used in numerous applications:

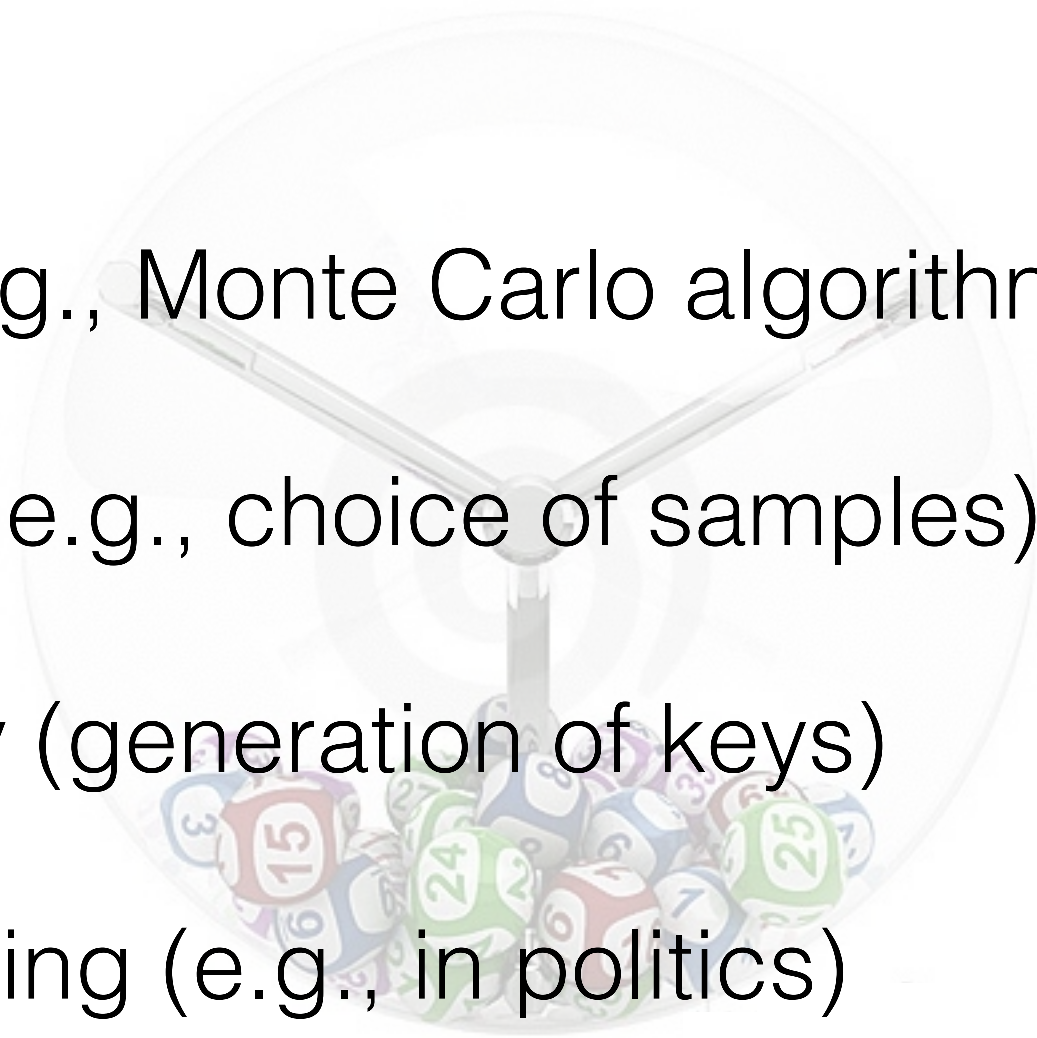
- Gambling
- Simulation (e.g., Monte Carlo algorithms)
- Experiments (e.g., choice of samples)
- Cryptography (generation of keys)



Randomness

Random numbers are used in numerous applications:

- Gambling
- Simulation (e.g., Monte Carlo algorithms)
- Experiments (e.g., choice of samples)
- Cryptography (generation of keys)
- Decision-making (e.g., in politics)



Quality of randomness is crucial

RELATED VIDEO

Obama on surveillance: "There may be another way of skinning the cat"

RELATED TOPICS

Politics »

(Reuters) - As a key part of a campaign to embed encryption software that it could crack into widely used computer products, the U.S. National Security Agency arranged a secret $10 million contract with RSA, one of the most influential firms in the computer security industry, Reuters has learned.

Documents leaked by former NSA contractor Edward Snowden show that the NSA created and promulgated a flawed formula for generating random numbers to create a "back door" in encryption products, the New York Times reported in September. Reuters later reported that RSA became the most important distributor of that formula by rolling it into a software tool called Bsafe that is used to enhance security in personal computers and many other products.

Undisclosed until now was that RSA received $10 million in a deal that set the NSA formula as the preferred, or default, method for number generation in the BSafe software, according

Quality of randomness is crucial

RELATED VIDEO

Obama on surveillance: "There may be another way of skinning the cat"

RELATED TOPICS

Politics »

(Reuters) - As a key part of a campaign to embed encryption software that it could crack into widely used computer products, the U.S. National Security Agency arranged a secret $10 million contract with RSA, one of the most influential firms in the computer security industry, Reuters has learned.

Documents leaked by former NSA contractor Edward Snowden show that the NSA created and promulgated a flawed formula for generating random numbers to create a "back door" in encryption products, the New York Times reported in September. Reuters later reported that RSA became the most important distributor of that formula by rolling it into a software tool called Bsafe that is used to enhance security in personal computers and many other products.

Undisclosed until now was that RSA received $10 million in a deal that set the NSA formula as the preferred, or default, method for number generation in the BSafe software, according

We need to “test” randomness. But how?

How is randomness generated in practice?

- Pseudo-random number generation

seed

```
seed = seed*1103515245+12345
return (seed / 65536) % 32768
```

··· 0011101011 ···

How is randomness generated in practice?

- Pseudo-random number generation

seed →

```
seed = seed*1103515245+12345
return (seed / 65536) % 32768
```

→ ··· 0011101011 ···

- “Classical” hardware

→ ··· 0011101011 ···

How is randomness generated in practice?

- Pseudo-random number generation

seed →

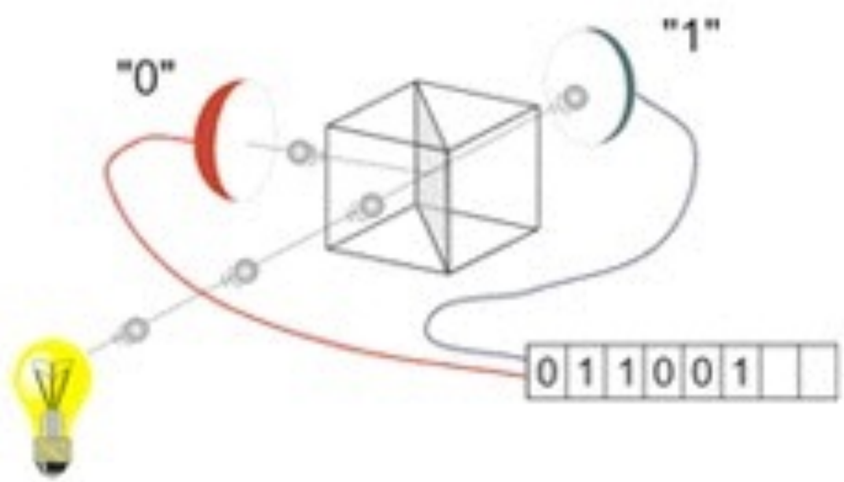
```
seed = seed*1103515245+12345
return (seed / 65536) % 32768
```

→ ··· 0011101011 ···

- “Classical” hardware

→ ··· 0011101011 ···

- Quantum hardware



→ ··· 0011101011 ···

Statistical tests

→ 00101111010111010 → statistical test → OK

Statistical tests

Note: Statistical tests are not sufficient.

→ 00101111010111010 → statistical test → OK

Statistical tests

Note: Statistical tests are not sufficient.

→ 0010111101011010 → statistical test → OK

→ 0010111101011010 → statistical test → OK

The importance of being unpredictable

→ 00101111010111010

The importance of being unpredictable

→ 0010111101011101

Safe to use as a lottery machine.

The importance of being unpredictable

→ 00101111010111010

→ 00101111010111010

Safe to use as a lottery machine.

The importance of being unpredictable

→ 0010111101010111010

Safe to use as a lottery machine.

→ 0010111101010111010

Better not use as a lottery machine.

The importance of being unpredictable

→ 0010111101011010

Safe to use as a lottery machine.

→ 0010111101011010

Better not use as a lottery machine.

➡ unpredictability is crucial

How to check unpredictability?

Given a sequence of bits, it is impossible to prove that they were unpredictable.

→ 0010111101011010

↓

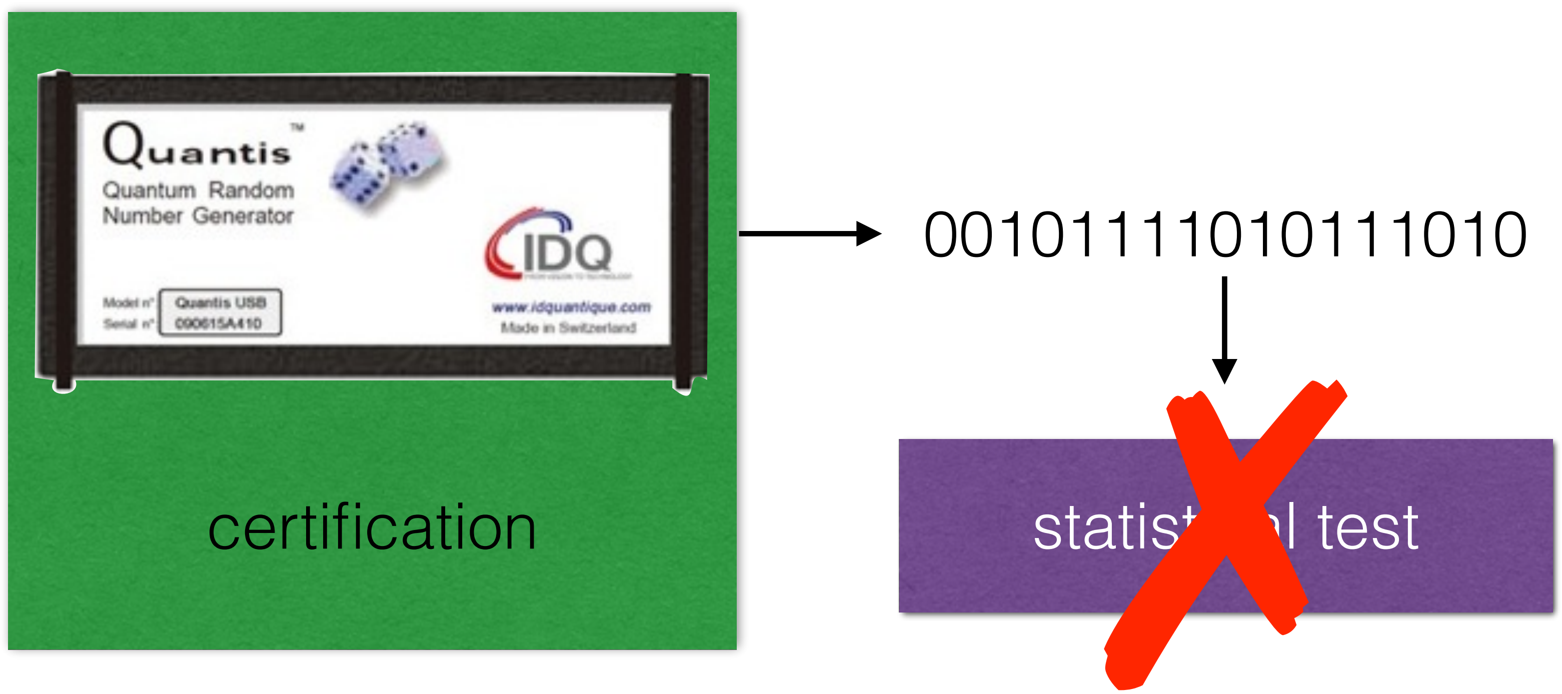
statistical test

How to check unpredictability?

Given a sequence of bits, it is impossible to prove that they were unpredictable.

How to check unpredictability?

Given a sequence of bits, it is impossible to prove that they were unpredictable.



Idea: “certification” of process

Rather than the actual output, consider the process that generates it.

Certification of randomness

Certification of randomness

COMPLIANCE TESTING LABORATORY

Certificate of Compliance

This is to certify that the Random Number Generator

Quantis-v10.10.08

by

ID Quantique SA

REF : CTL-037/37001

has been tested by

CTL, Compliance Testing Laboratory

and has been found to be *suitably unpredictable and fit for purpose*

Issue Date: 30.03.2011

Technical Compliance Manager, CAST Limited

CAST LTD Compliance Testing Laboratory,
A company approved and certified under the Online Gambling Regulation Act 2001 and accredited by UKAS for UK Testing

Compliance Testing Laboratory, Tŷ Menai, Ffordd Penlan, Parc Menai Business Park, Bangor, Gwynedd LL57 4HJ

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Metrology METAS

Certificate of Conformity No 151-04687

Object	**Quantum Random Number Generator** Quantis-USB S/N 070222A410 Quantis-PCI-1 S/N 08338A310 Quantis-PCI Express S/N 1002251A210
Applicant	**id Quantique SA** Ch. De la Marbrerie 3 1227 Carouge/Geneva Switzerland
Requirements	The output of the Quantis random number generator has to pass all DIEHARD Battery of Tests, confirming that the random number generator distributes numbers with sufficient non-predictability, fair distribution and lack of bias to particular outcomes. Specifically: 10 data sets consisting of 1E8 bits per data set is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6.
Confirmation	The tested Quantis-USB, Quantis-PCI-1 and Quantis-PCI Express have passed all DIEHARD Battery of Tests. The sequence of random bits generated cannot be predicted. The sequence of random bits generated cannot be reproduced.
Remarks	The testing procedure used is described in the annex document "Annex_METAS_151-04687"

CH-3003 Bern-Wabern, 10 May 2010

For the Test — Dr.Damian Twerenbold

Division Mechanics, Radiation and Time — Dr.Philippe Richard, Vice-Director

This document may not be published or forwarded other than in full. 1/1

METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

Generating certified randomness

Device-dependent


Certificate of Compliance

This is to certify that the Random Number Generator

Quantis-v10.10.08

by

ID Quantique SA

REF : CTL-037/37001

has been tested by

CTL, Compliance Testing Laboratory

and has been found to be *suitably unpredictable and fit for purpose*

Issue Date: 30.03.2011

Technical Compliance Manager, CAST Limited

CAST LTD Compliance Testing Laboratory,
A company approved and certified under the Online Gambling Regulation Act 2001 and accredited by UKAS for UK Testing

Compliance Testing Laboratory, Tŷ Menai, Ffordd Penlan, Parc Menai Business Park, Bangor, Gwynedd LL57 4HJ

- requires accurate and trusted model of device
- practical (commercially available)

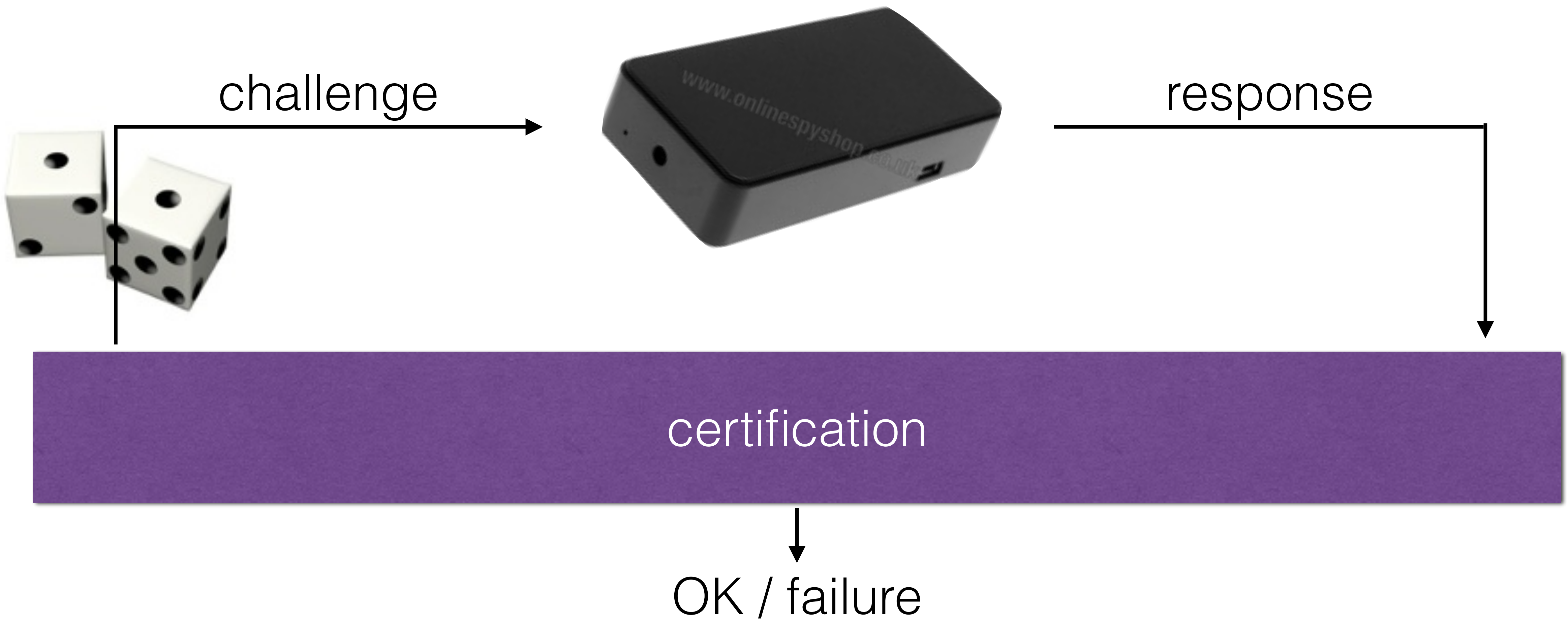
➡ poster by Daniela Frauchiger

Device-independent

- independent of details of device (no trust required)
- experimentally challenging (high-quality entanglement)

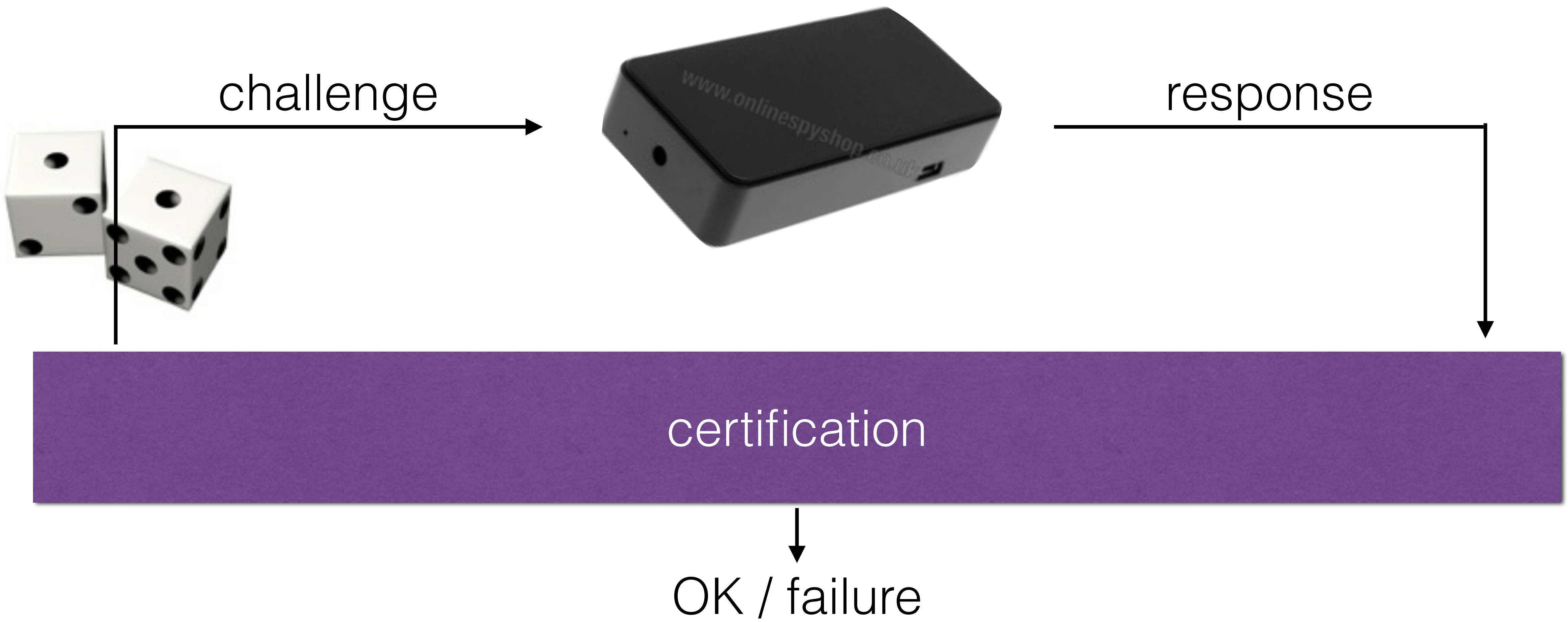
➡ this talk

Certification of randomness



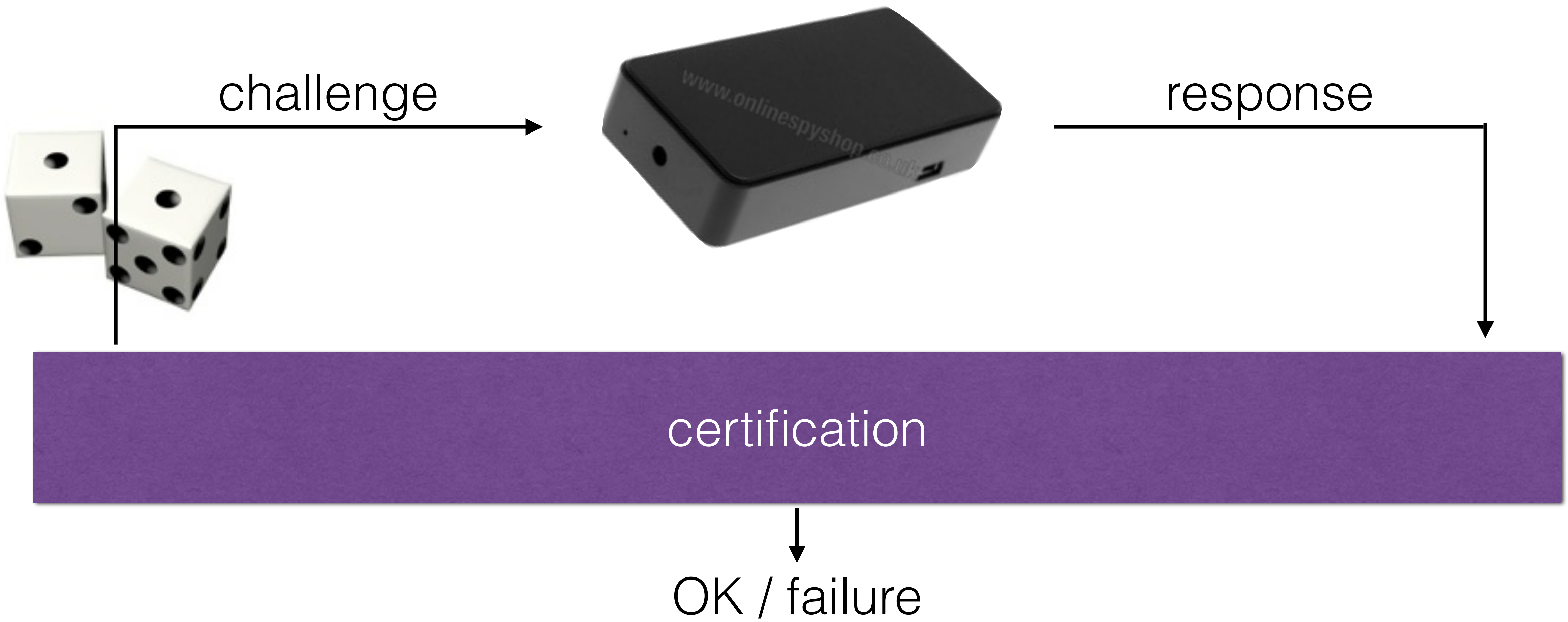
- Challenge/response protocol

Certification of randomness



- Challenge/response protocol
- Challenges need to be generated at random

Certification of randomness

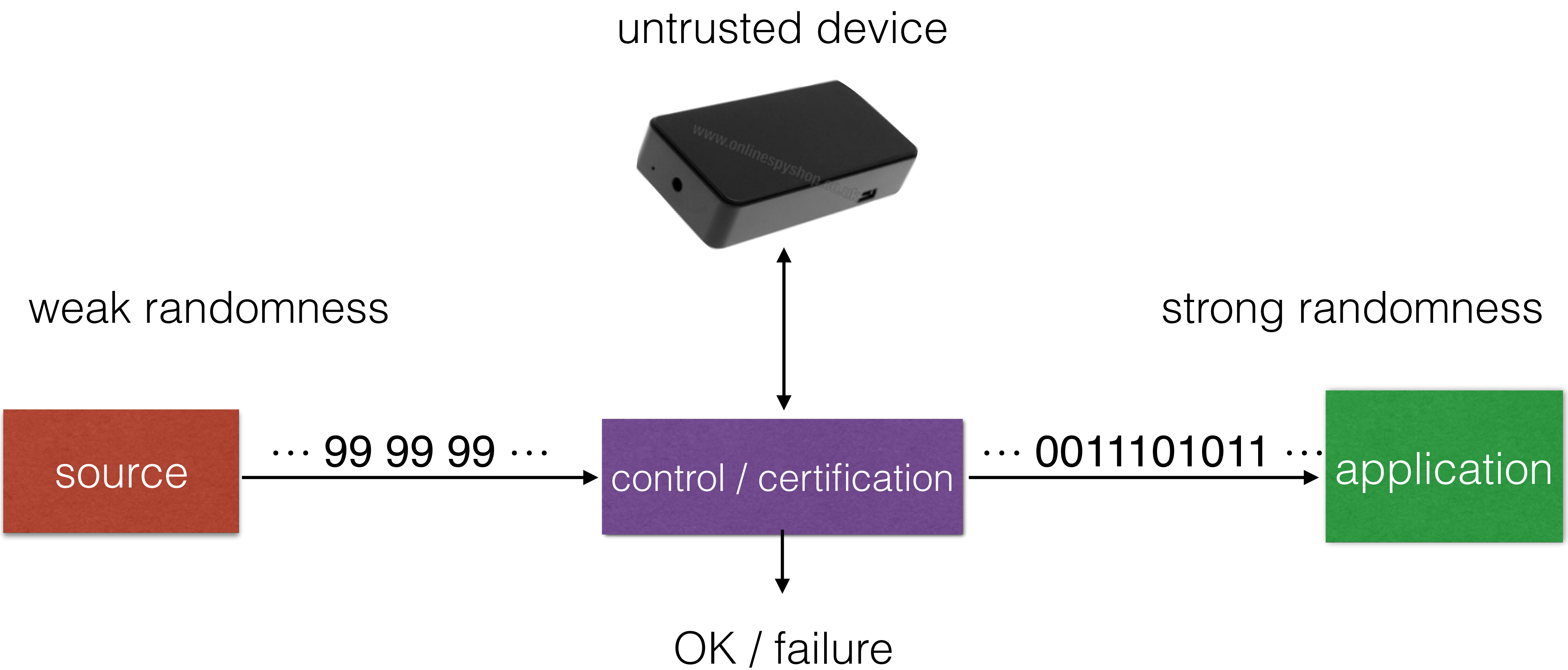


- Challenge/response protocol
- Challenges need to be generated at random

➡ Requires randomness in the first place :-(

Certified randomness amplification

Basic setup



But what is randomness really?

How to define randomness?

Guiding principle:

Capture operational needs.

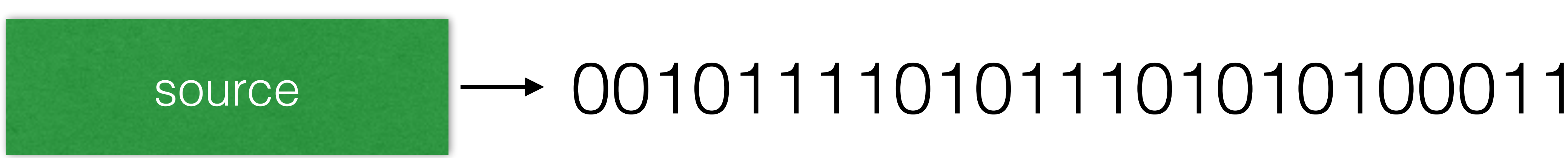
How to define randomness?

Guiding principle:

Capture operational needs.

Intuitive requirement: unpredictability

Each new bit uniformly distributed and independent of anything else.



How to define randomness?

Intuitive requirement:

Each new bit uniformly distributed and independent of anything else.

Formal definition uses random variables

$$X_1 X_2 \cdots X_n$$

How to define randomness?

Intuitive requirement:

Each new bit uniformly distributed and independent of anything else.

Formal definition uses random variables

source $\longrightarrow$ $X_1 X_2 \cdots X_n$

Necessary condition:

$$P_{X_i | X_1 \cdots X_{i-1}} = P_U \quad (\forall i)$$

where P_U is the uniform distribution

How to define randomness

Necessary criterion: $P_{X_i|X_1 \cdots X_{i-1}} = P_U \quad (\forall i)$

This is however not sufficient!

→ 00101111010111010

good randomness

$P_{X_i|X_1 \cdots X_{i-1}} = P_U$

How to define randomness

Necessary criterion: $P_{X_i|X_1\cdots X_{i-1}} = P_U \quad (\forall i)$

This is however not sufficient!

→ good randomness 00101111010111010

$P_{X_i|X_1\cdots X_{i-1}} = P_U$

→ bad randomness 00101111010111010

$P_{X_i|X_1\cdots X_{i-1}} = P_U$

How to define randomness

Necessary criterion: $P_{X_i|X_1\cdots X_{i-1}} = P_U \quad (\forall i)$

This is however not sufficient!

good randomness

→ 0010111101011101 0

$P_{X_i|X_1\cdots X_{i-1}} = P_U$

bad randomness

→ 0010111101011101 0

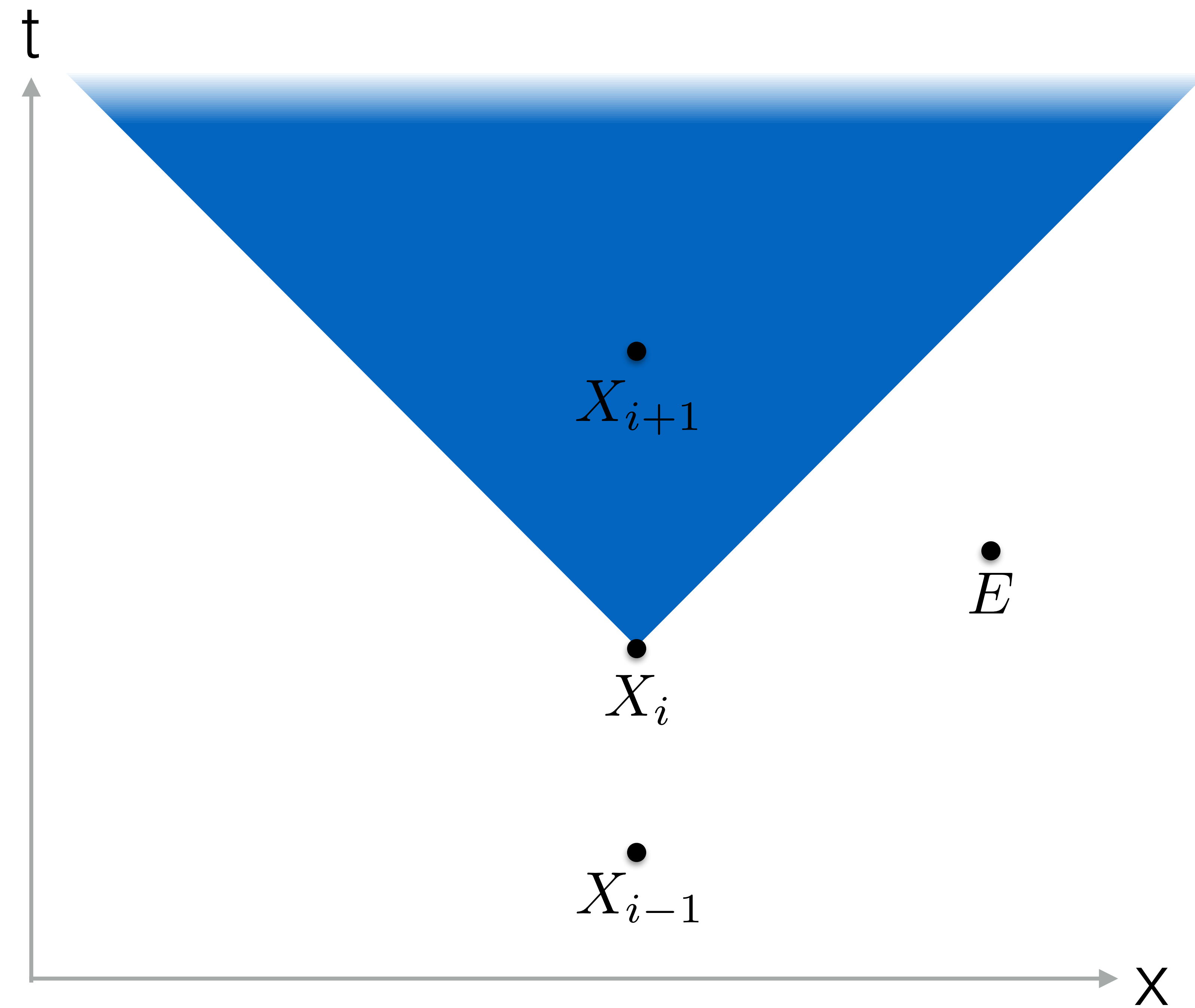
$P_{X_i|X_1\cdots X_{i-1}} = P_U$

➡ definition must be time-dependent

Refined definition

Necessary and sufficient criterion:

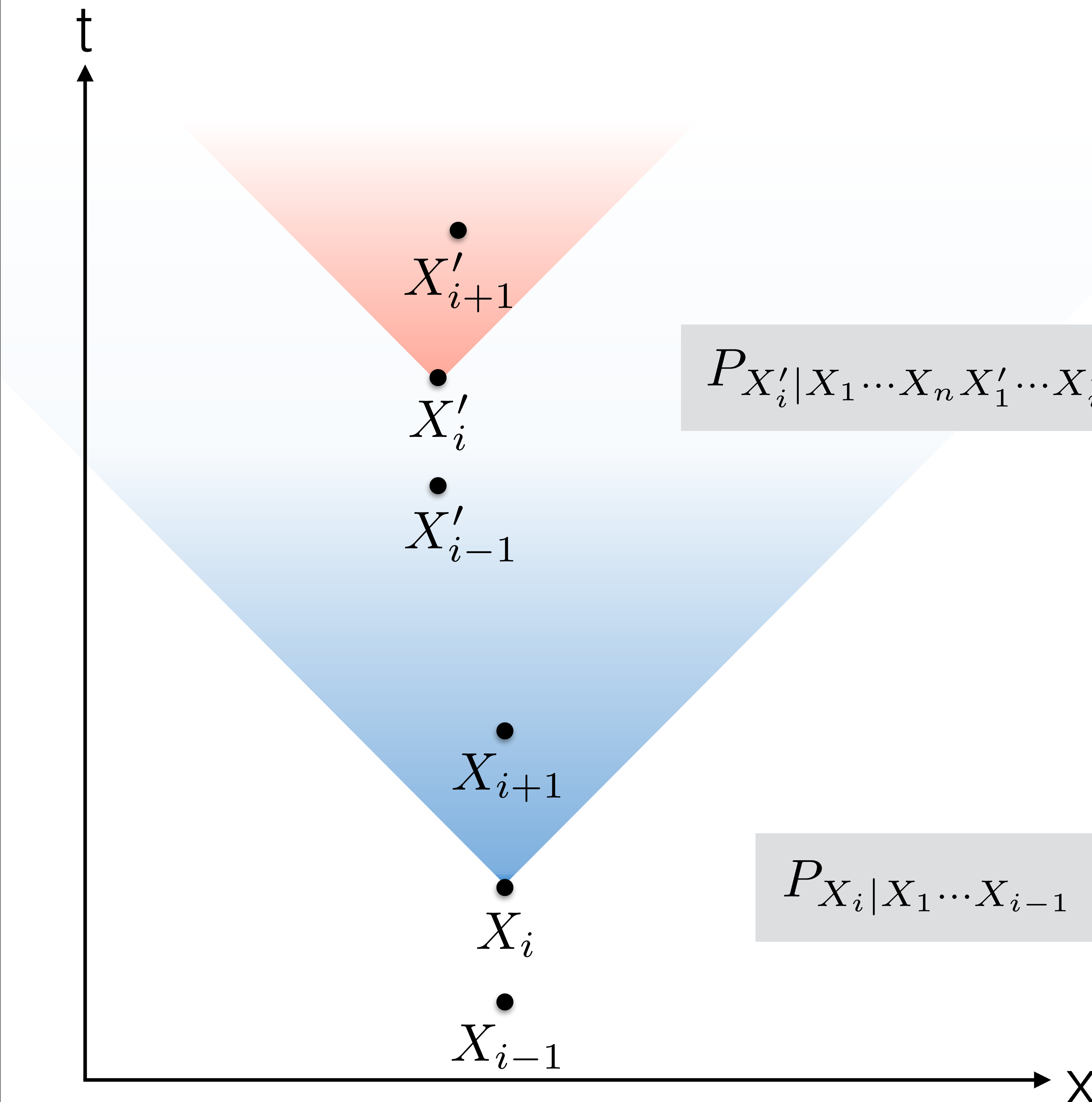
X_i is *random* if it is uniform and independent of anything outside its future light cone.



Specifically:

$$P_{X_i|X_1 \cdots X_{i-1}E} = P_U$$

Refined definition: example

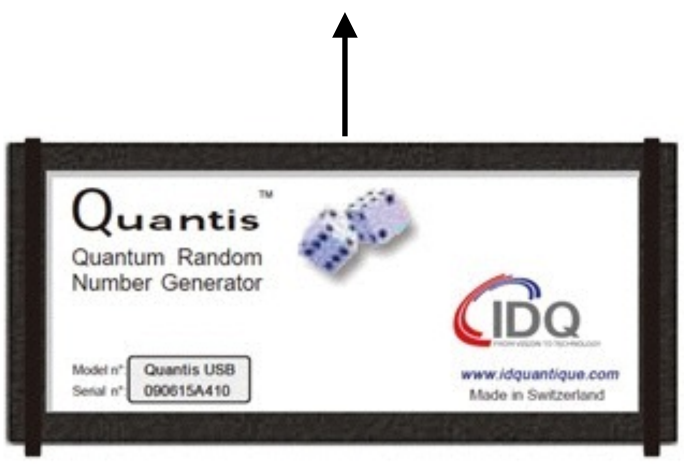


$$P_{X'_i|X_1\cdots X_n X'_1\cdots X'_{i-1}} = P_U$$

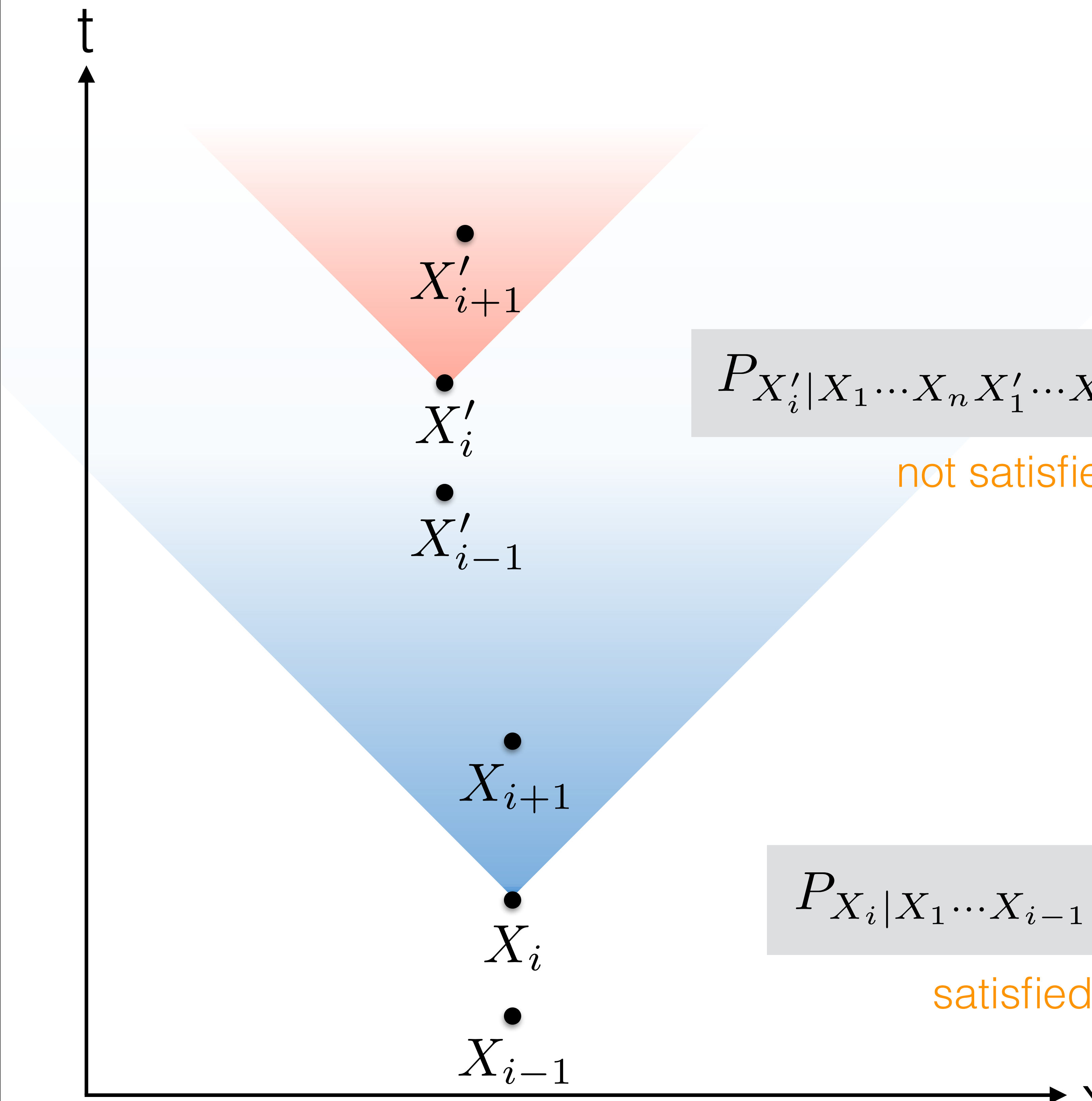
$X'_1 X'_2 \cdots X'_n$

$$P_{X_i|X_1\cdots X_{i-1}} = P_U$$

$X_1 X_2 \cdots X_n$



Refined definition: example



$$P_{X'_i|X_1\cdots X_n X'_1\cdots X'_{i-1}} = P_U$$

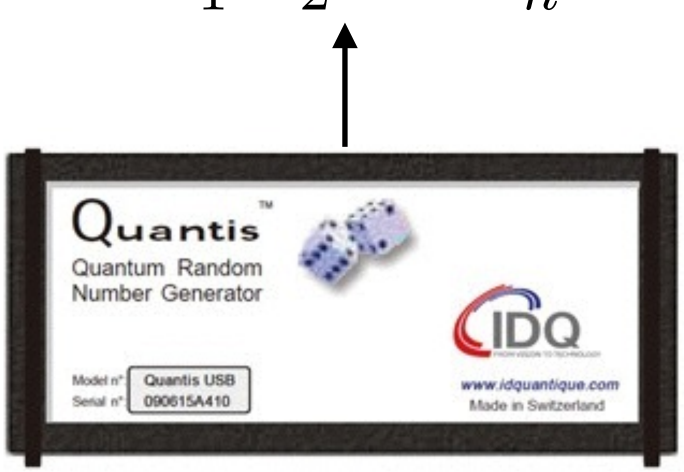
not satisfied

$$P_{X_i|X_1\cdots X_{i-1}} = P_U$$

satisfied

$X'_1 X'_2 \cdots X'_n$

$X_1 X_2 \cdots X_n$



Is quantum randomness "truly" random?

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

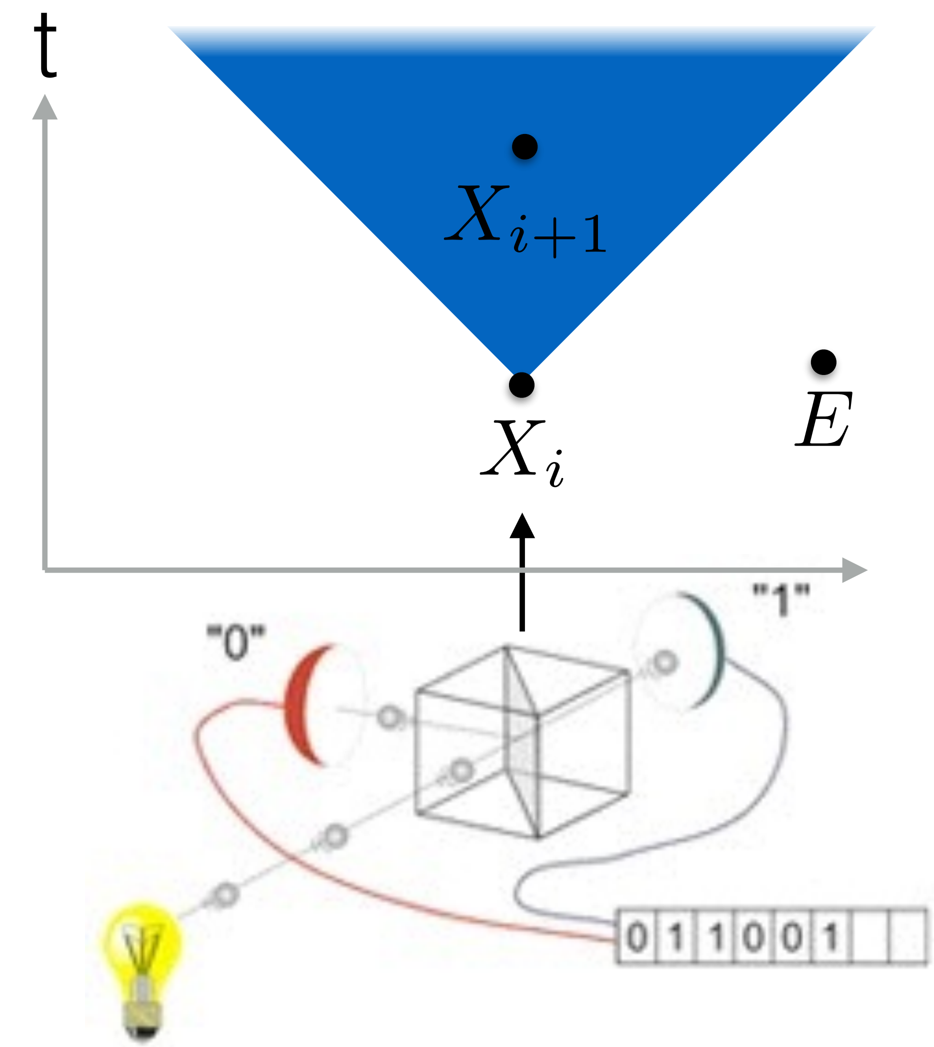
ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question

Can the criterion be met?

Criterion for "true" randomness:

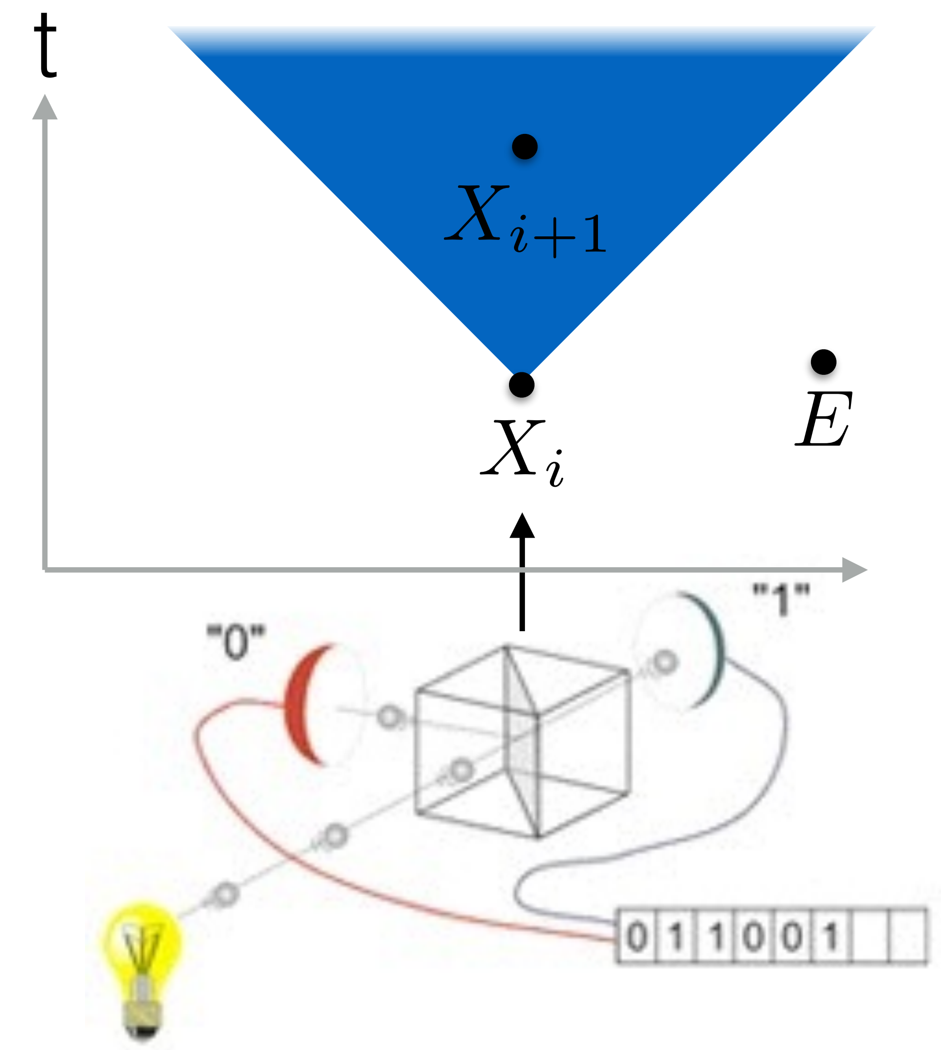
X_i is *random* if it is uniform and independent of anything outside its future light cone.



Can the criterion be met?

Criterion for "true" randomness:

X_i is *random* if it is uniform and independent of anything outside its future light cone.

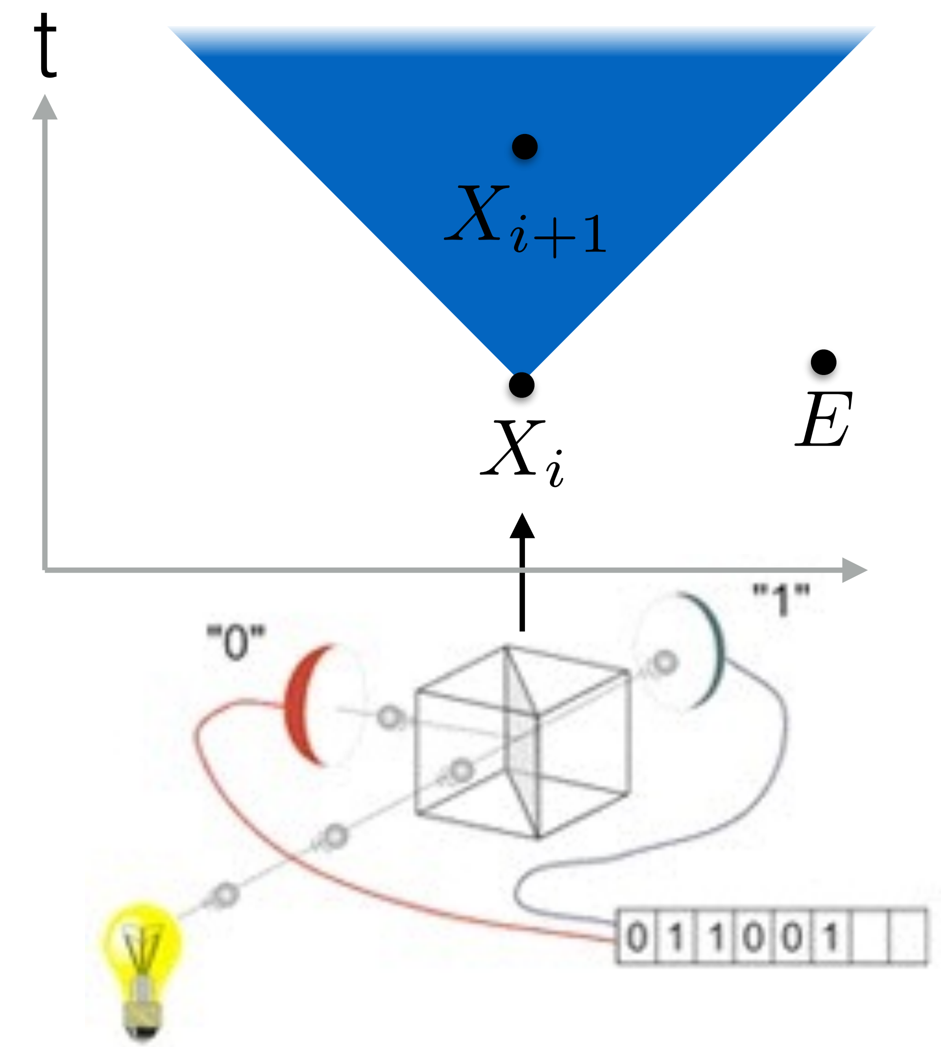


Within quantum theory, randomness of X_i follows from the Born rule.

Can the criterion be met?

Criterion for “true” randomness:

X_i is *random* if it is uniform and independent of anything outside its future light cone.



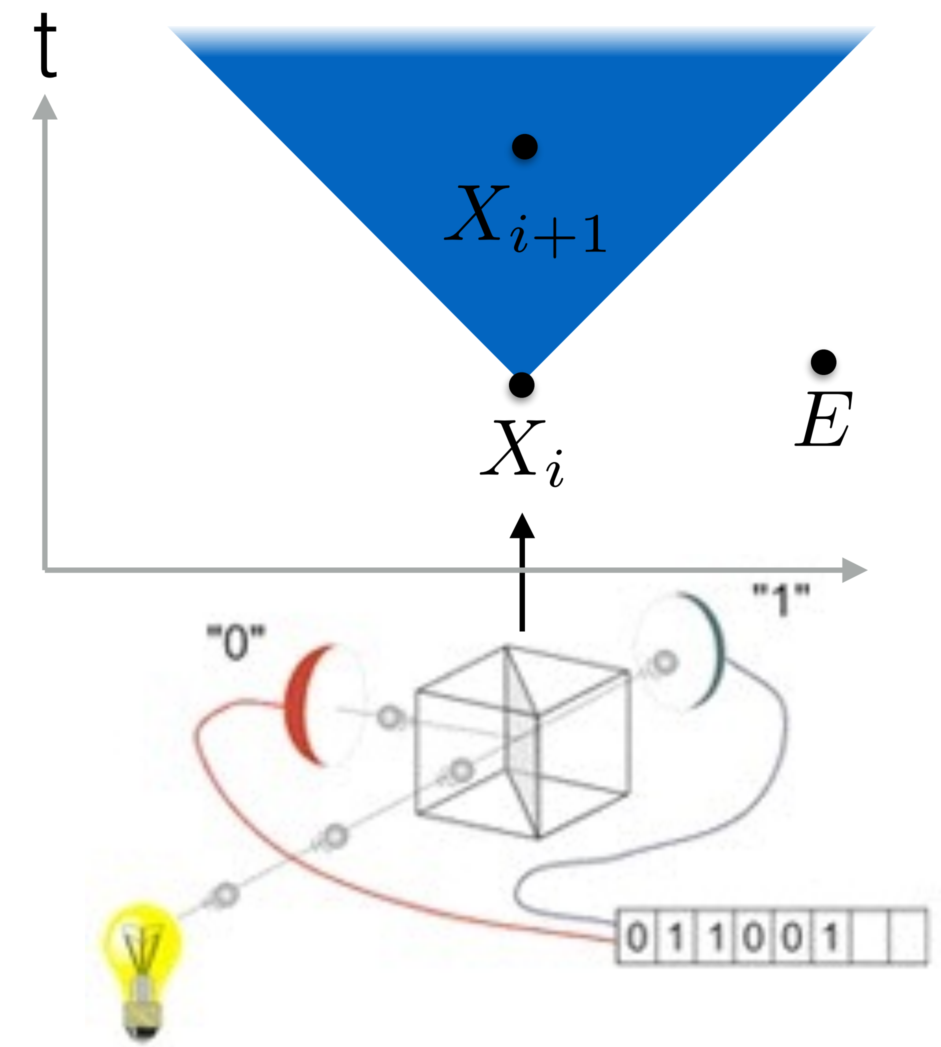
Within quantum theory, randomness of X_i follows from the Born rule.

However, whether it is really random depends on the completeness of quantum theory.

Can the criterion be met?

Criterion for "true" randomness:

X_i is *random* if it is uniform and independent of anything outside its future light cone.



Within quantum theory, randomness of X_i follows from the Born rule.

Theorem [informal version]

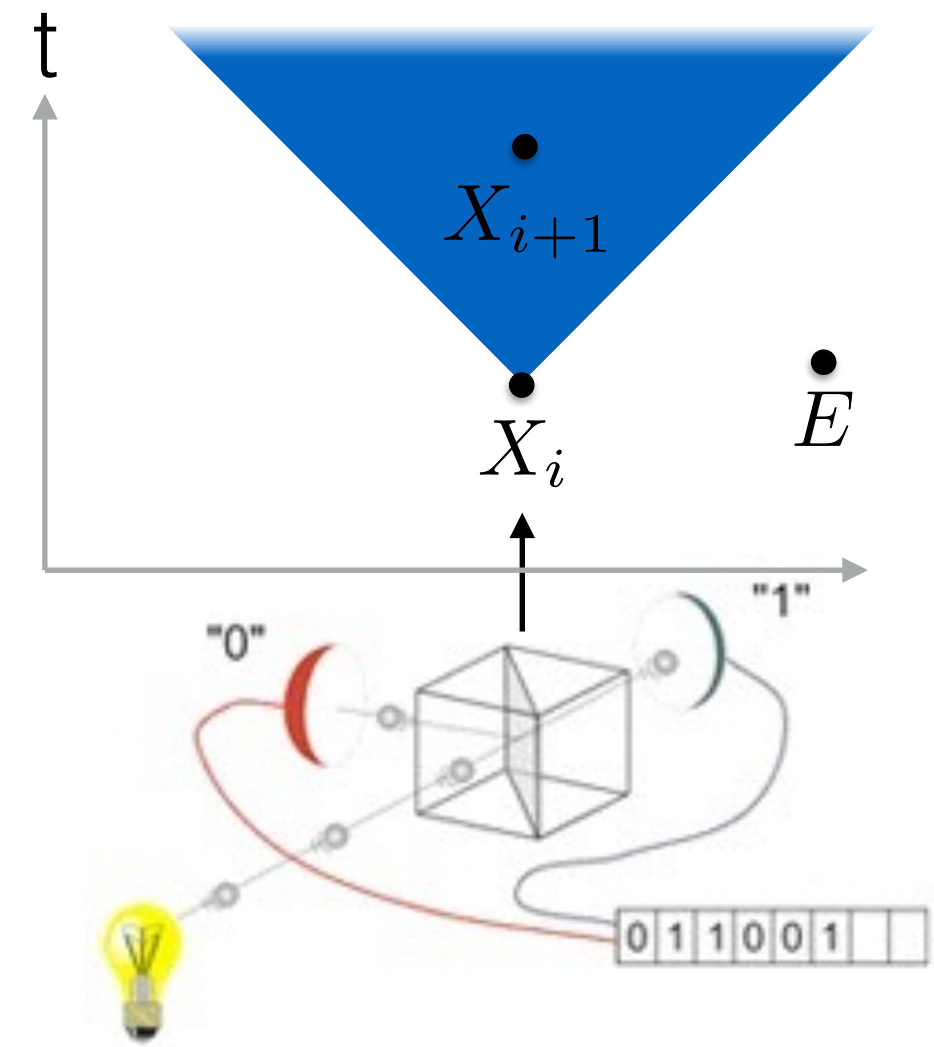
No extension of quantum theory that is compatible with "free choice" can improve on the predictions of quantum theory.

Colbeck and RR, *Nat. Comm.* **2**, 411 (2011)

Can the criterion be met?

Criterion for “true” randomness:

X_i is *random* if it is uniform and independent of anything outside its future light cone.



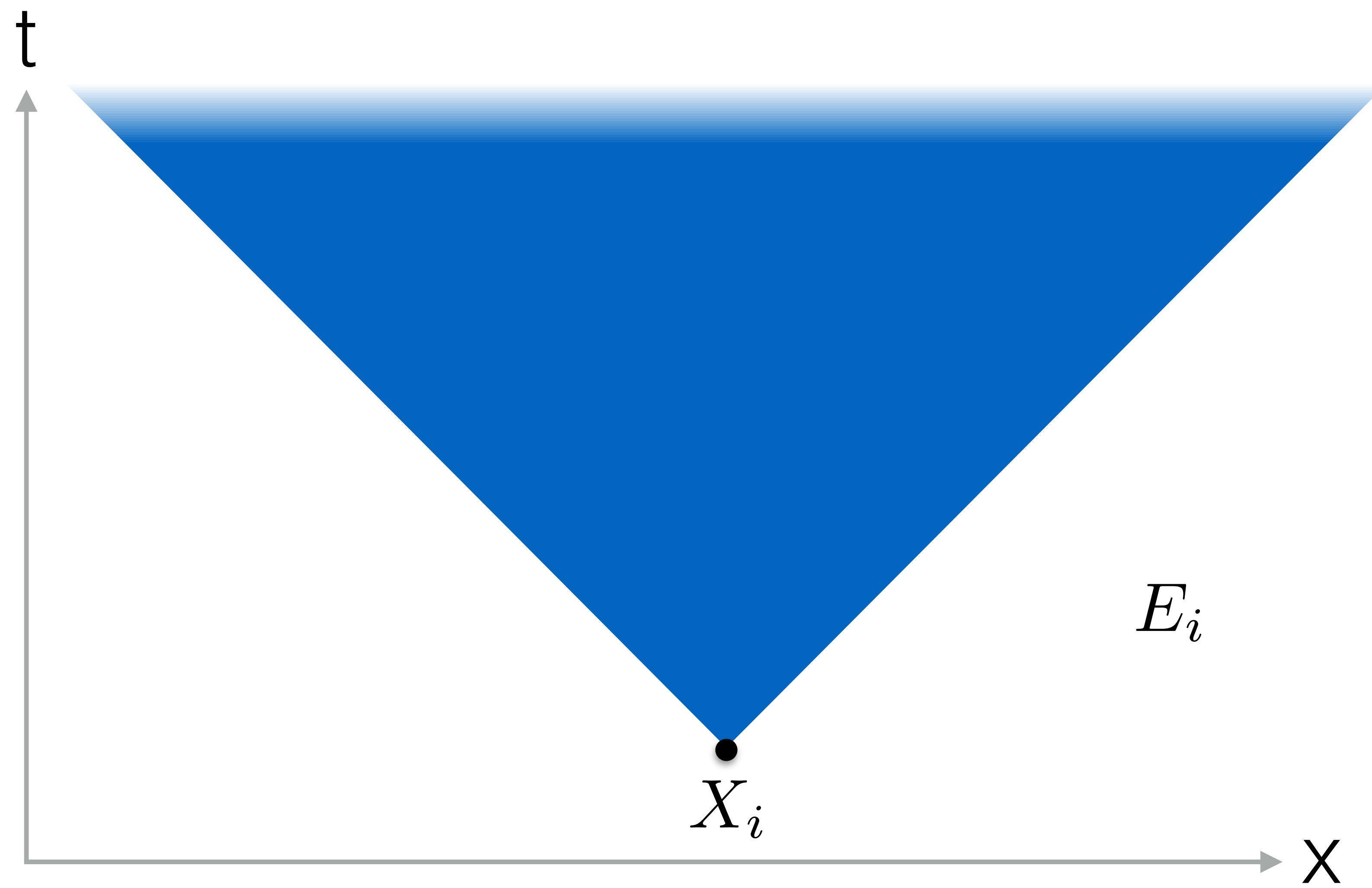
Within quantum theory, randomness of X_i follows from the Born rule.

Theorem [informal version]

No extension of quantum theory that is compatible with “free choice” can improve on the predictions of quantum theory. Colbeck and RR, *Nat. Comm.* **2**, 411 (2011)

True randomness generation possible with trusted devices!

Imperfect randomness



Necessary and sufficient criterion:

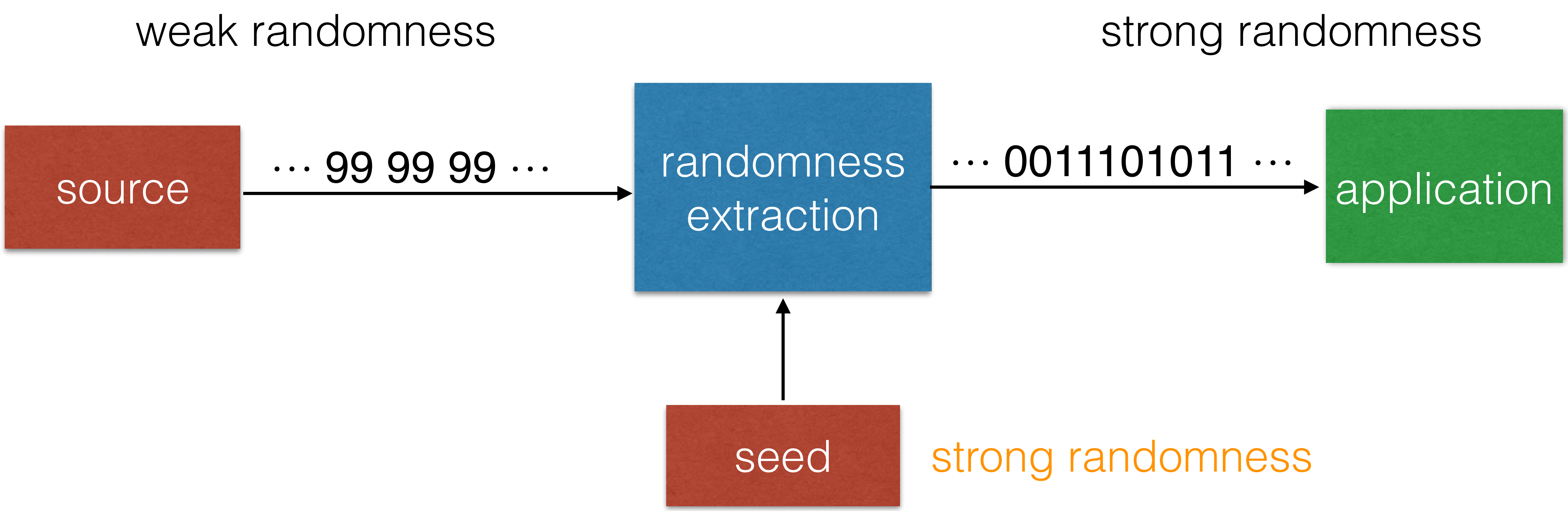
X_i is ε-*random* if

$$\|P_{X_i|E_i} - P_U\|_1 \leq 2\varepsilon$$

where E_i denotes everything outside the future of X_i.

Comparison: randomness extractors

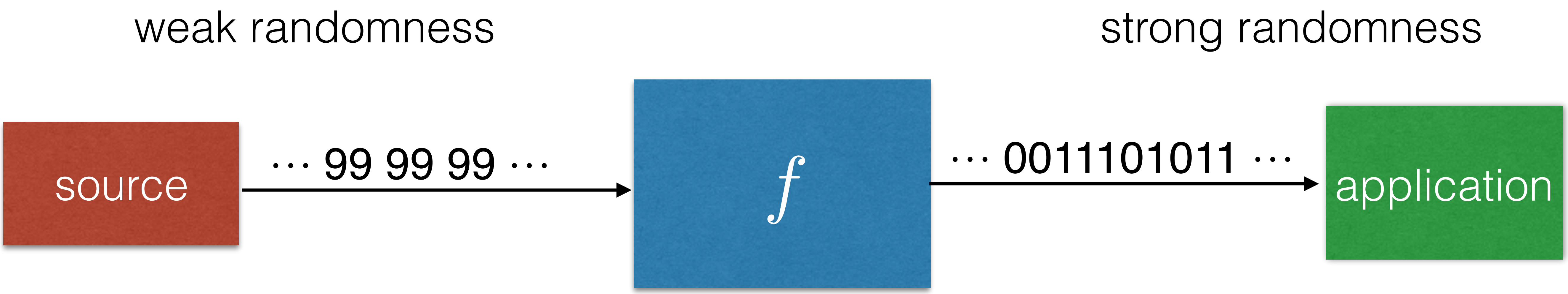
Comparison: randomness extractors



Randomness extractors take a random seed as an additional input.

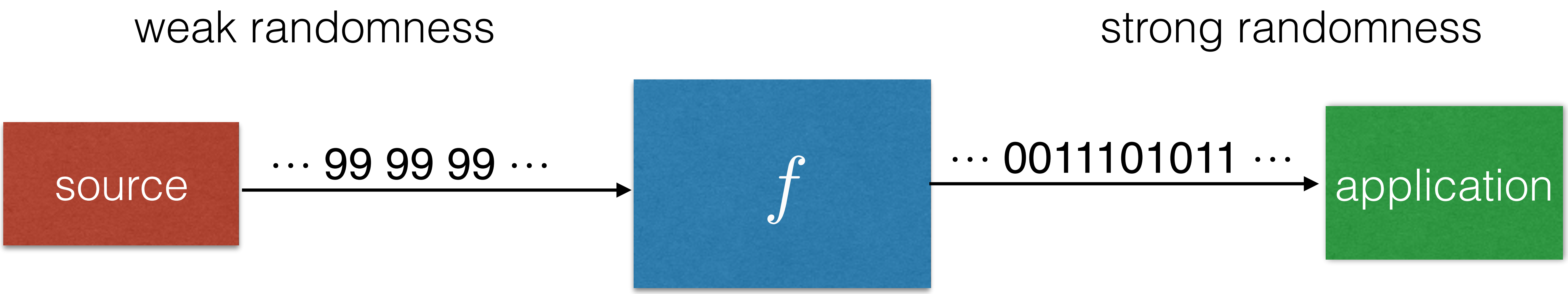
Comparison: randomness extractors

Is the seed really necessary?



Comparison: randomness extractors

Is the seed really necessary?



Lemma (Santha and Vazirani)

There exists no function f such that the output $f(X)$ is uniform for any ε-random input X.

Proc. of FOCS-84, 434–440 (1984)

Doesn't this rule out randomness amplification?

Doesn't this rule out randomness amplification?

Lemma (Colbeck and RR) [informal version]

For any $\epsilon < \epsilon_0$ there exists a device-independent protocol whose output $f(X)$ is uniform for any ε-random input X.

Nature Physics **8**, 450–453 (2012)

Doesn't this rule out randomness amplification?

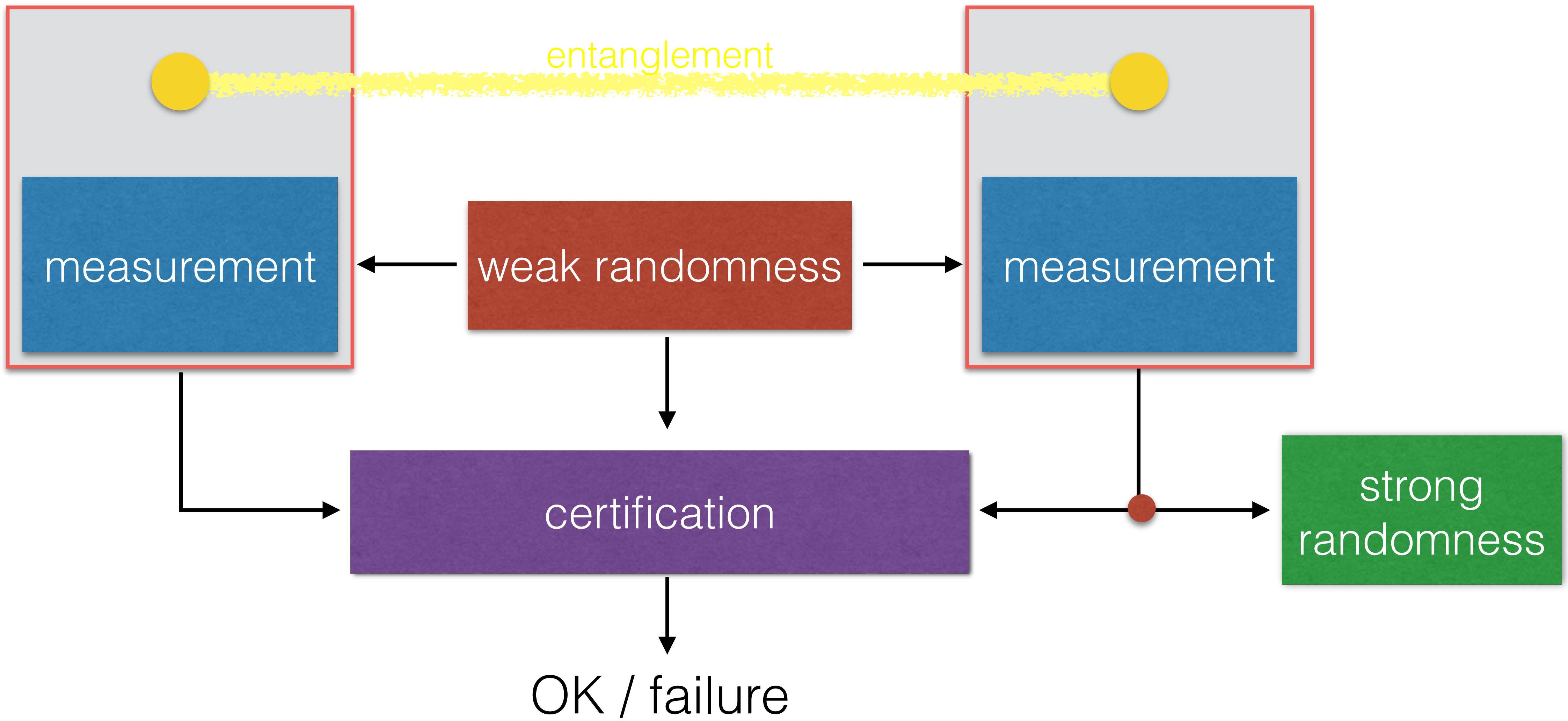
Lemma (Colbeck and RR) [informal version]

For any $\epsilon < \epsilon_0$ there exists a device-independent protocol whose output $f(X)$ is uniform for any ε-random input X.

Nature Physics **8**, 450–453 (2012)

No contradiction: protocol may access quantum device.

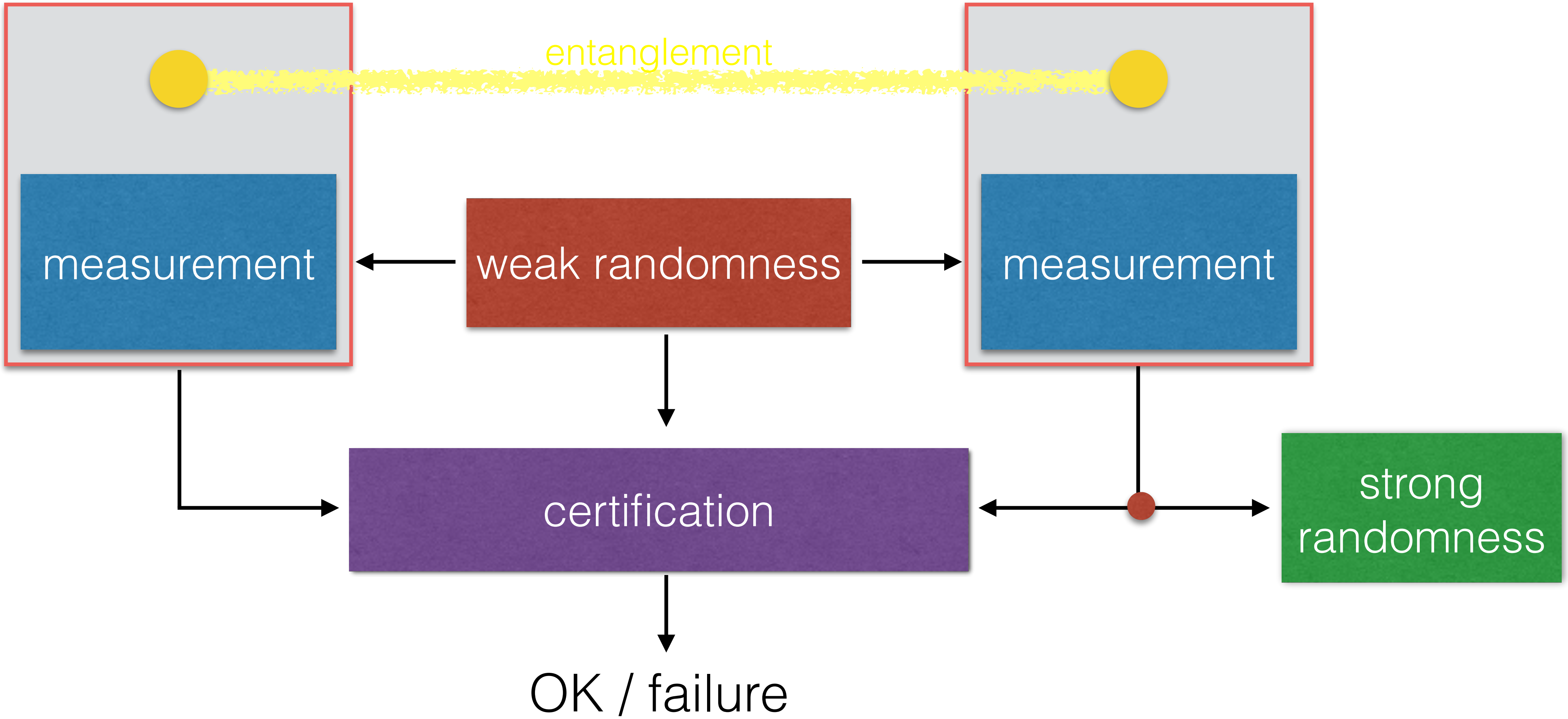
Idea: Bell-type setup



Protocol idea

- choose measurement settings using weak randomness

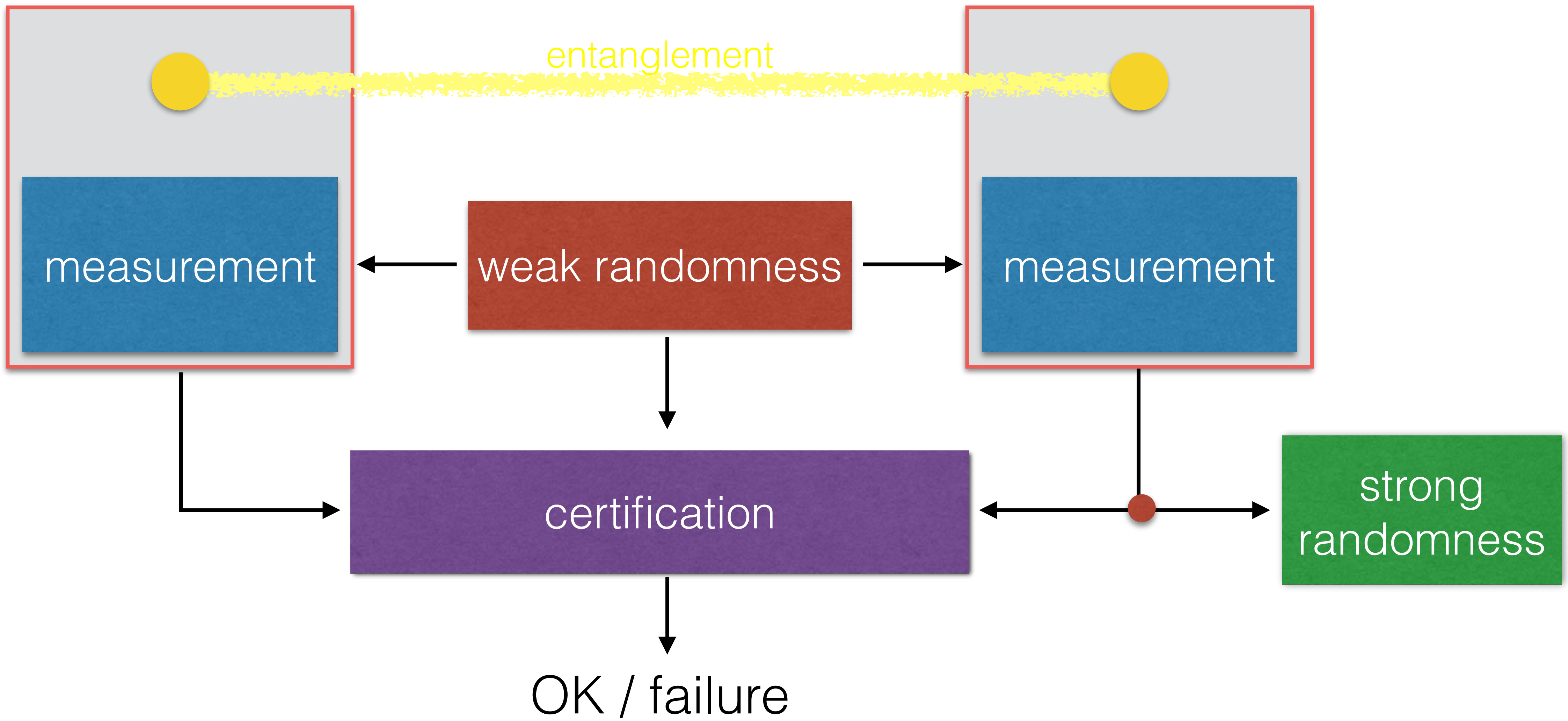
Idea: Bell-type setup



Protocol idea

- choose measurement settings using weak randomness
- test correlations (chained Bell inequality)
  [Pearle, Phys. Rev. D, 1970] and [Braunstein, Caves, Ann. Phys. 1990]

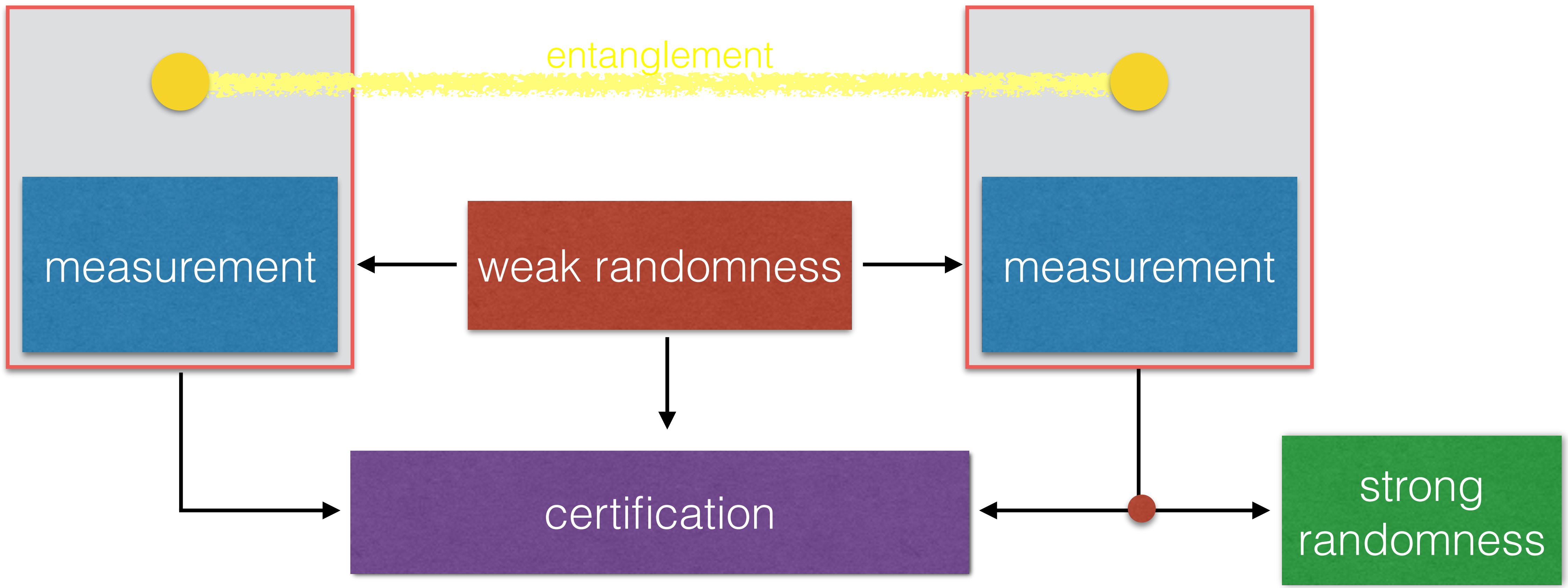
Idea: Bell-type setup



Protocol idea

- choose measurement settings using weak randomness
- test correlations (chained Bell inequality)
  [Pearle, Phys. Rev. D, 1970] and [Braunstein, Caves, Ann. Phys. 1990]
- output one of the measurement outcomes, chosen using weak randomness

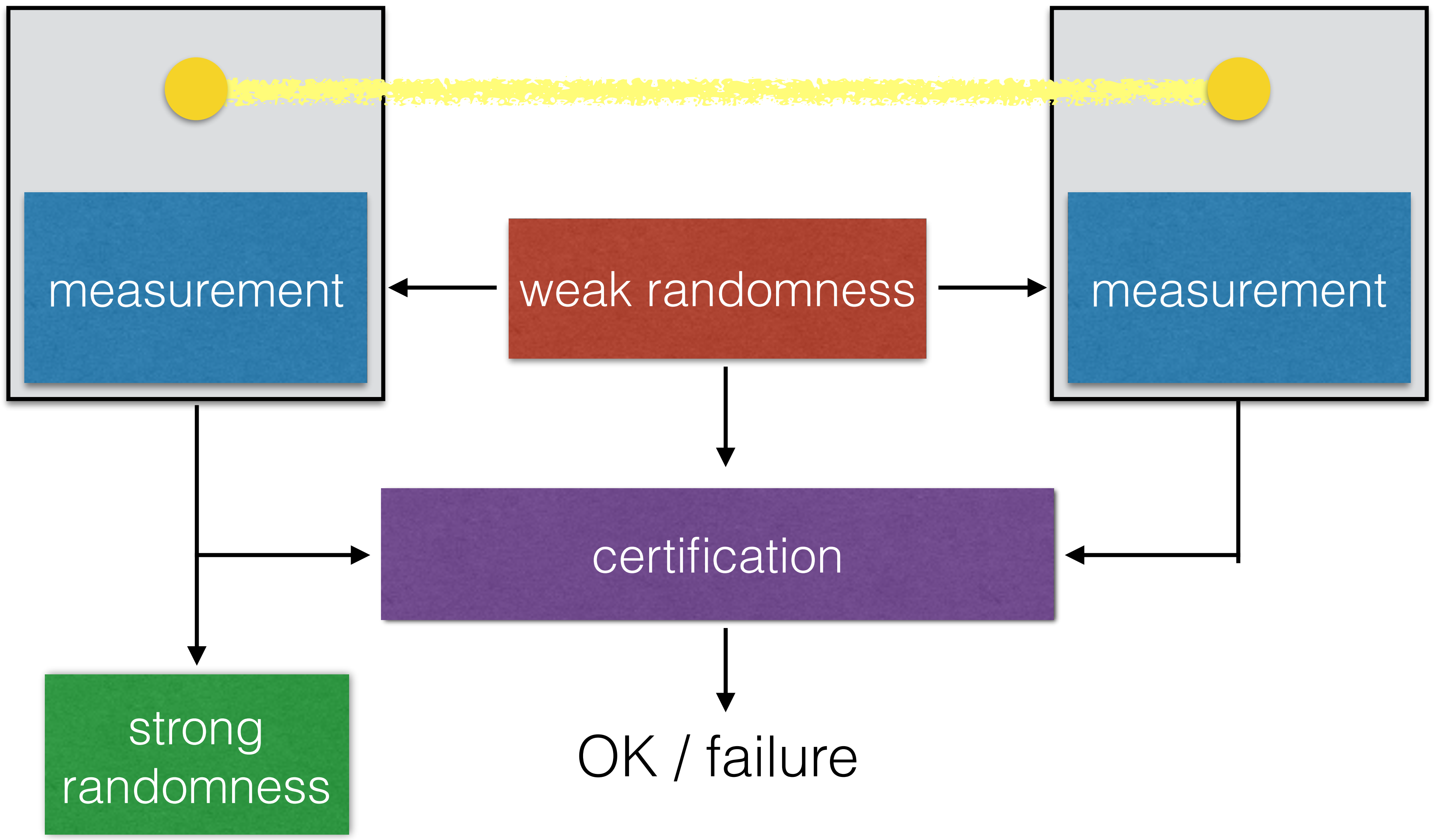
Assumptions



Certification is valid if

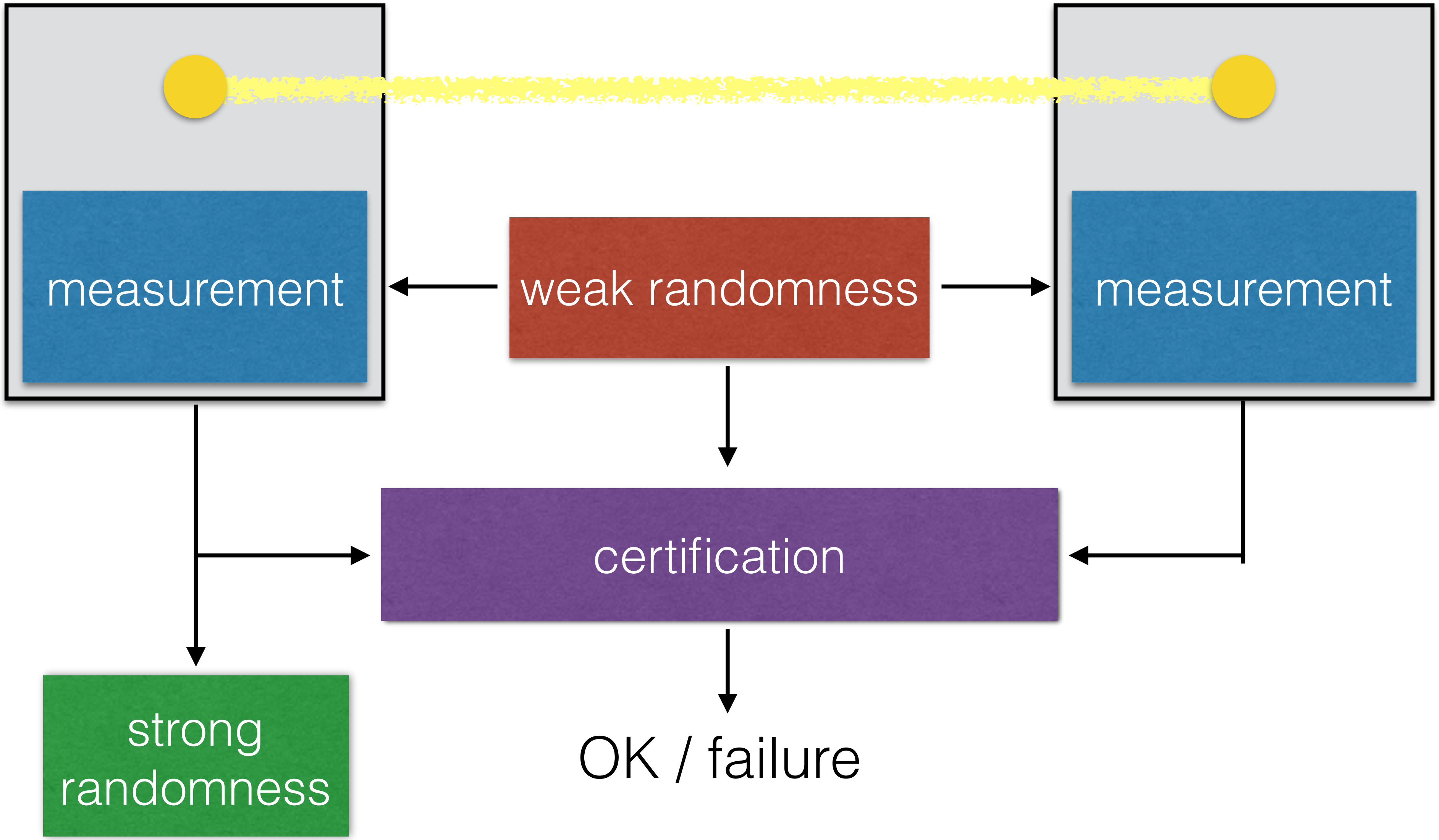
- weak randomness at least ε-random
- two devices isolated from each other

Role of quantum theory



- certification produces positive output if correlations are the ones predicted by quantum theory

Role of quantum theory



- certification produces positive output if correlations are the ones predicted by quantum theory
- however, certificate is valid independently of whether quantum theory is correct or complete

Results

Results

- Colbeck and RR in 2011: $\varepsilon < 0.08$

Results

Results

- Colbeck and RR in 2011: $\varepsilon < 0.08$
- Gallego *et al.* in 2012: $\varepsilon < 0.5$

Results

Results

- Colbeck and RR in 2011: $\varepsilon < 0.08$
- Gallego *et al.* in 2012: $\varepsilon < 0.5$
- 2013: noise tolerance

Results

Results

- Colbeck and RR in 2011: $\varepsilon < 0.08$
- Gallego *et al.* in 2012: $\varepsilon < 0.5$
- 2013: noise tolerance
- 2014: improved efficiency

Implications for quantum theory

Corollary [informal version]

Arbitrarily weak randomness is sufficient to carry out Bell-type experiments and conclude that quantum theory is complete.

see also Colbeck and RR, *Nat. Comm.* **2**, 411 (2011)

Summary

Results

Summary

Results

- Randomness can be generated under weak assumptions:
  - ✳ seed randomness may be arbitrarily weak
  - ✳ devices may be untrusted.

Summary

Results

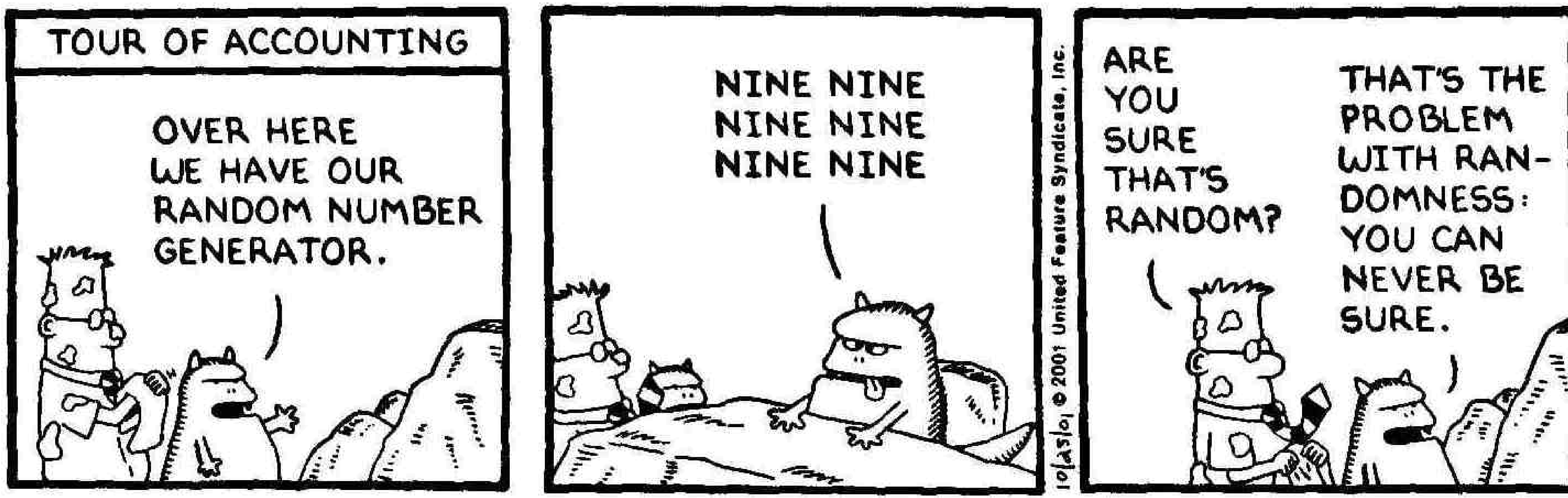
- Randomness can be generated under weak assumptions:
  - ✳ seed randomness may be arbitrarily weak
  - ✳ devices may be untrusted.
- Completeness of quantum theory can be experimentally verified using weak randomness only.

Summary of summary

We do not know whether there is randomness …

Summary of summary

We do not know whether there is randomness …



… but if there is just a little bit, we can amplify it and make it perfect.

$\cdots$ 99 99 99 $\cdots$ → randomness amplification → $\cdots$ 0011101011 $\cdots$

Literature

- Colbeck, RR, Randomness can be amplified, *Nature Physics* **8**, 450–453 (2012)
- Gallego, Masanes, de la Torre, Dhara, Aolita, Acin, Full randomness from arbitrarily deterministic events, *Nature Communications* **4**, 2654 (2013)
- Mironowicz and Pawlowski, Amplification of arbitrarily weak randomness, arXiv:1301.7722 (2013)
- Grudka, Horodecki^3, Pawłowski, Ramanathan, Free randomness amplification using bipartite chain correlations, arXiv:1303.5591
- Plesch, Pivoluska, Single min-entropy random sources can be amplified, arXiv:1305.0990
- Ramanathan, Brandao, Grudka, Horodecki^3, Robust device independent randomness amplification, arXiv:1310.4544
- Coudron and Yuen, Infinite randomness expansion and amplification with a constant number of devices, arXiv:1310.6755
- Bouda, Pawlowski, Pivoluska, Plesch, Device-independent randomness extraction for arbitrarily weak min-entropy source, arXiv:1402.0974
- Chung, Shi, Wu, Robust device-independent randomness amplification from any min-entropy source, arXiv:1402.4797
- Dhara, de la Torre, Acín, Can observed randomness be certified to be fully intrinsic?, *Physical Review Letters* **112**, 100402 (2014)

Thank you for your attention