Keeping secrets from an almost all-powerful adversary

Sammy Ragy

University of BRISTOL

QUANTUM COMMUNICATIONS HUB

Random numbers and secrets

1

Your bank PIN is a 4-digit ‘random’ number.

Encryption algorithms need random numbers

An agreed random labelling enables secret message transmission

Message	Possible labelling					
We attack at dawn	1	1	2	2	3	3
We attack at dusk	2	3	1	3	1	2
Let’s try chatting instead	3	2	3	1	2	1

Guessing games

Randomness is relative

2

$$p(\text{heads}) = \frac{2}{3} \qquad p(\text{tails}) = \frac{2}{3}$$

A guessing game

1. Both coins are in a bag.
2. You draw a coin, but you do not know which.
3. I have hidden a mark on one of the coins, so I can tell the difference.

Result

I guess right 2/3 of the time, you do 1/2 the time.

Takeaway

Increased knowledge of the physics underlying a random process enables us to better predict its outcomes.

A quantum coin

Perfect knowledge = perfect predictability?

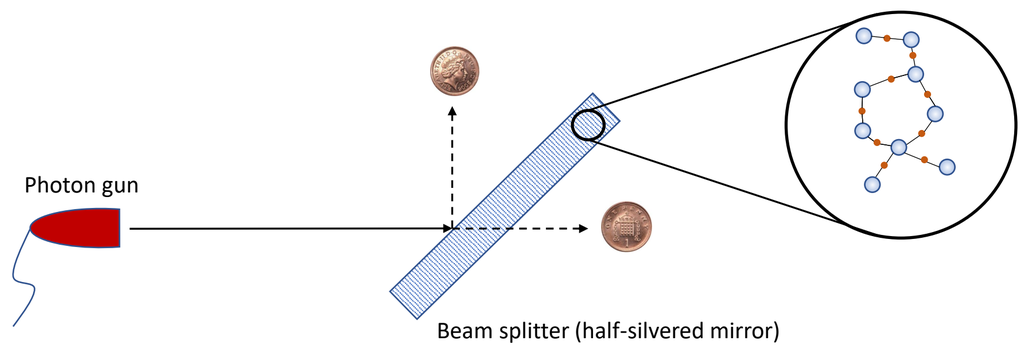
3

Quantum physics

Quantum physics is taken to be indeterministic: even with perfect knowledge of a system, the outcome may be unpredictable.

The catch

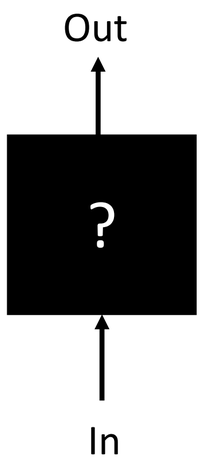
Real experiments do not match idealised models. A half-silvered mirror consists of many molecules and can exhibit imperfect behaviour, and a tampering eavesdropper can throw things further off course.



Black boxes

Removing the assumptions of our models.

4



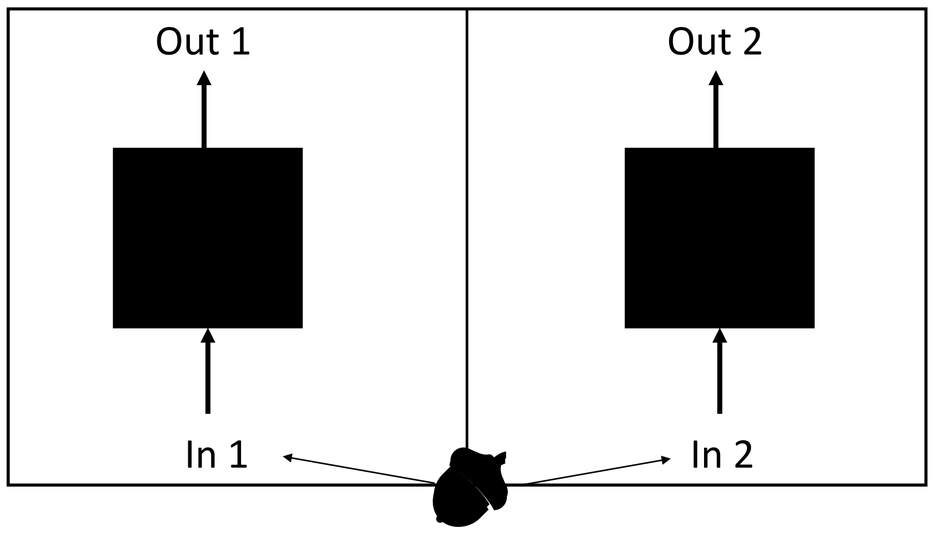
We regard a physical system as a ‘black box’ which transforms inputs to outputs.

In a real experiment, the input corresponds to a choice of measurement, e.g. we can choose to measure the position of a particle, or we can choose to measure its momentum, and the output will be the result of the measurement. However, we leave these details out of the model.

Self-testing

The key ingredient

5



The adversary provides the black boxes, and she controls the world outside our lab. How can we prove security if she knows (almost) everything, and we know (almost) nothing? We need:

1. Some initial secret randomness – a *seed* to select our inputs.
2. The ability to block the devices from communicating.
3. The ability to (deterministically) process information in a trusted way.

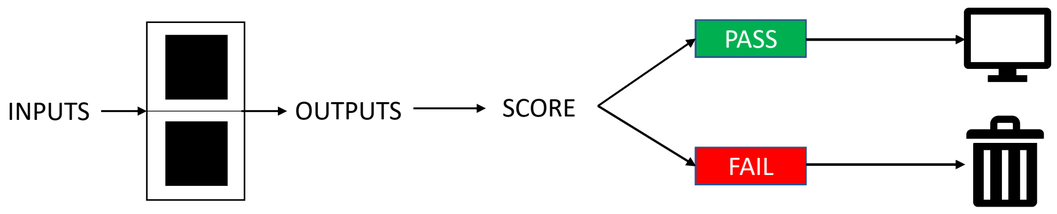
This allows the devices to ‘self test’. We can deduce constraints on the underlying systems based purely on statistical tests performed on the inputs and outputs – the data verifies its own quality.

The protocol

A first demonstration of randomness expansion

6

1. We repeatedly feed the devices inputs and record their outputs.
2. We ‘score’ the resulting data (outputs and inputs together).
3. If we pass a certain threshold score, we keep the data, otherwise we dispose of the data (and devices!).



We achieved the first demonstration of randomness expansion in the black-box setting. This required cutting-edge developments on both the theoretical and experimental fronts. In 19 hours we achieved what would have taken over 100,000 hours three years previously.

Randomness in	Randomness out	Net gain
678 Mb	935 Mb	257 Mb

The paper

REF

Device-independent randomness expansion against quantum side information, Wen-Zhao Liu, Ming-Han Li, Sammy Ragy et al., *Nature Physics* volume 17, pages 448–451 (2021).

Work done while S Ragy was employed by the University of York.