True Randomness from Realistic Quantum Devices

Daniela Frauchiger, Renato Renner and Matthias Troyer

Institute for Theoretical Physics
ETH Zurich

ETH zürich

IDQ
FROM VISION TO TECHNOLOGY

Why care about randomness?

Report: NSA paid RSA to make flawed crypto algorithm the default

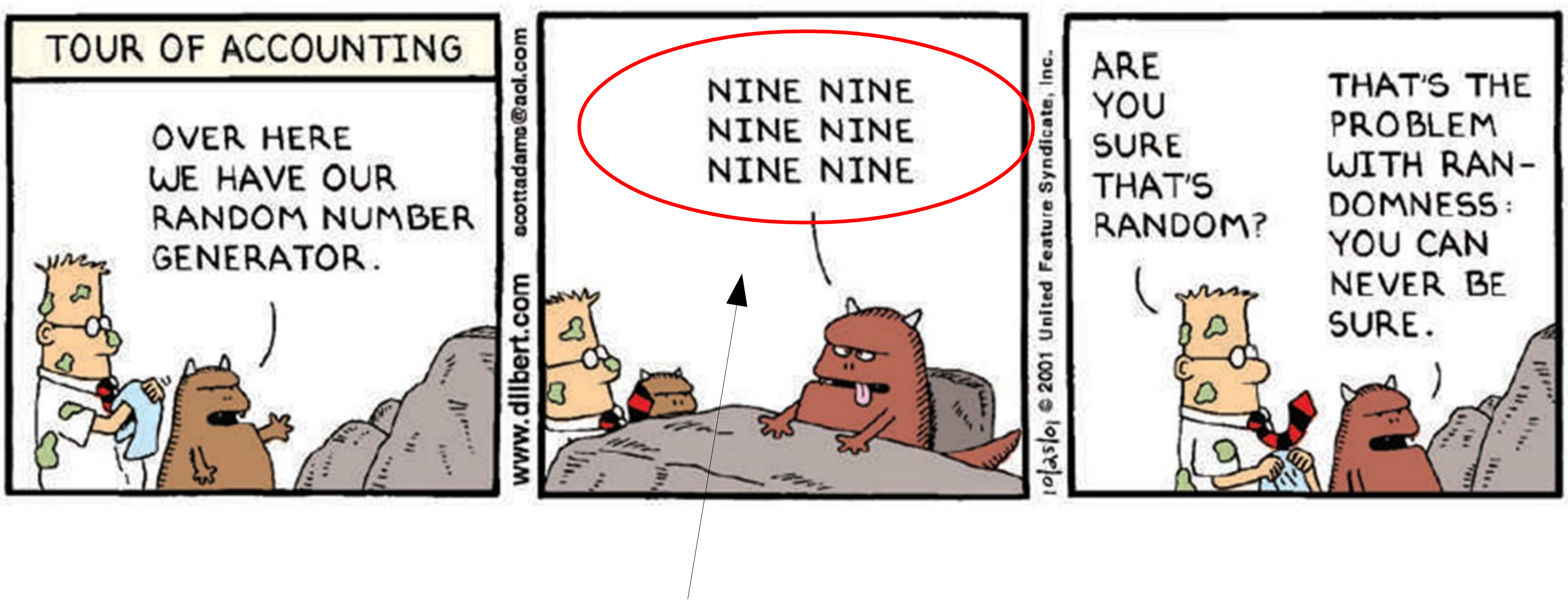
The NSA apparently paid RSA $10M to use Dual EC random number generator.

BAD RNG!

NIST Removes Dual_EC_DRBG Random Number Generator from Recommendations

What is a good RNG?

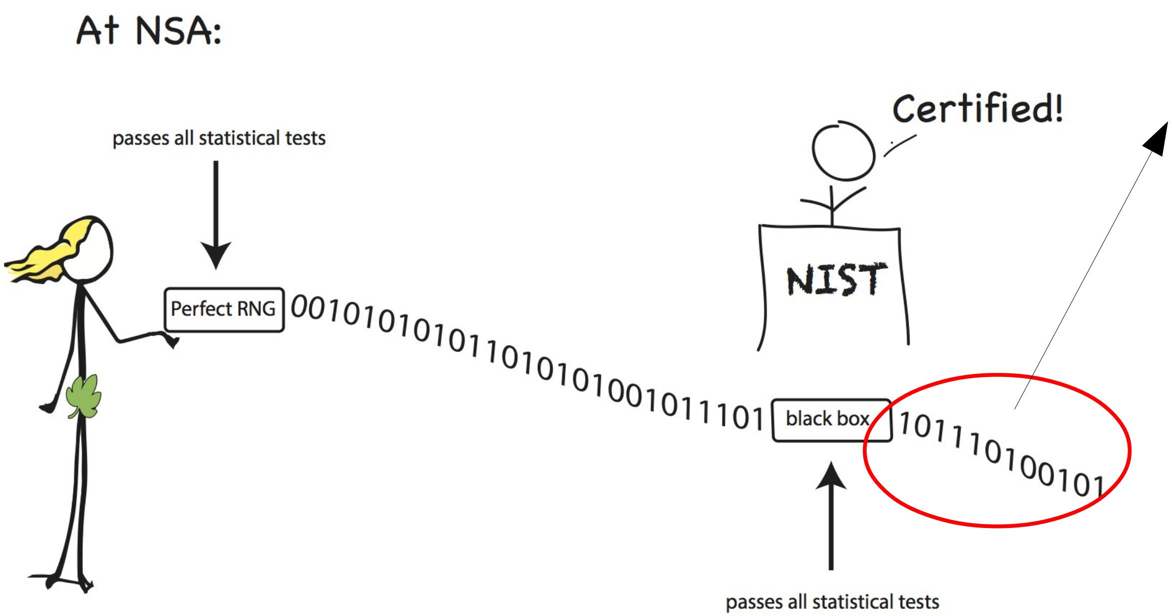
How to (not) verify good randomness



In general statistical tests are used to “verify” the randomness of such a sequence: the look for recognizable patterns.

Does it suffice?

No, statistical tests do not suffice...



These bits are perfectly **predictable** by Eve.

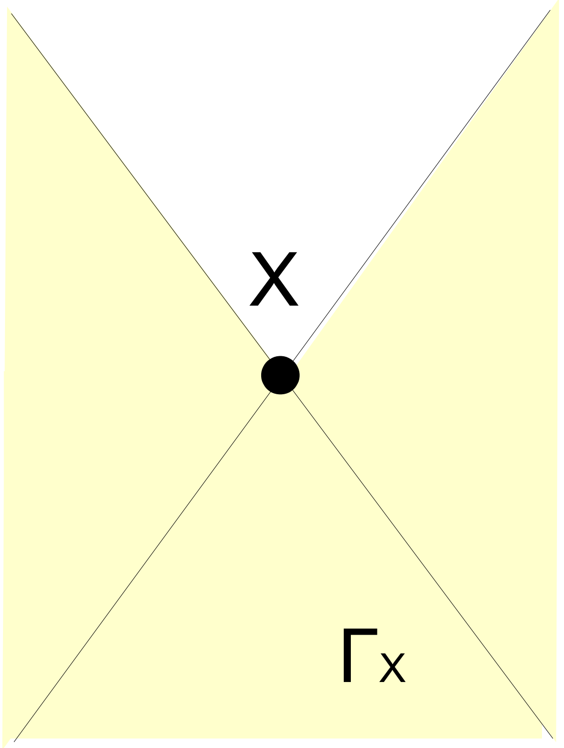
They cannot be used for any application where **unpredictability** is relevant e.g. in cryptographic scenarios!

Unpredictability is not a feature of individual values and therefore cannot be verified by any statistical test...

How to define randomness

Definition: X is called **ε-truly random** if it is ε-close to uniform and uncorrelated to the set Γ_X of all other space time variables which are not in the future light cone of X.

$$\frac{1}{2}\|P_{X\Gamma_X} - P_{\bar{X}} \times P_{\Gamma_X}\|_1 \leq \epsilon$$



How to generate true randomness

Pseudo Random Number Generators?

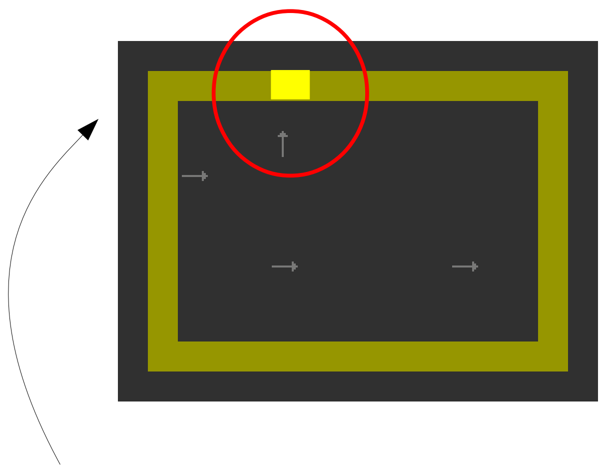
```
In[1]:=
        SeedRandom[1];
        RandomInteger[{0, 1}, 10]
Out[2]=
        {1, 1, 0, 1, 0, 0, 0, 1, 0, 1}

In[3]:=
        SeedRandom[1];
        RandomInteger[{0, 1}, 10]
Out[4]=
        {1, 1, 0, 1, 0, 0, 0, 1, 0, 1}
```

Must be initialized with a truly random seed in order to be computationally indistinguishable from a truly random sequence...

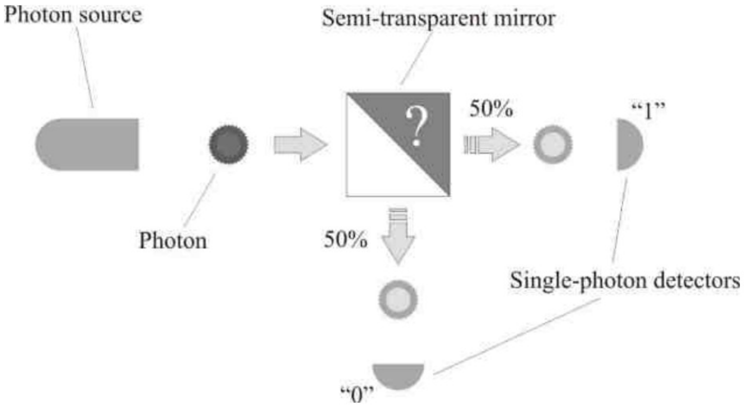
Hardware based RNGs?

Based on chaotic systems



only random under certain assumptions about the accessible information

Based on quantum systems



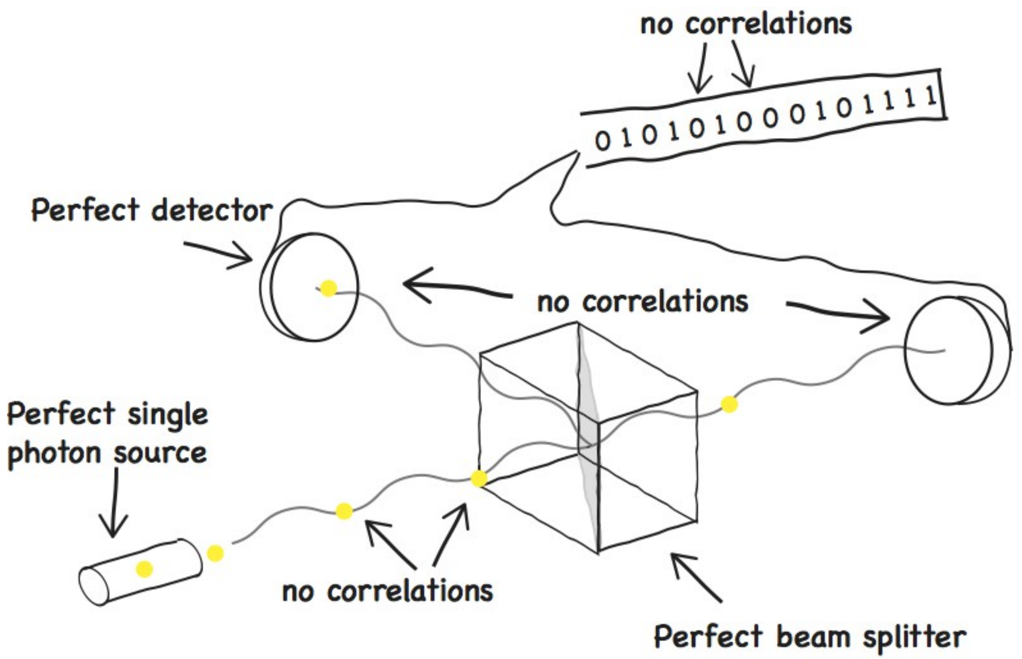
if the input state is pure and the measurement projective:

Intrinsically random!

QRNG: produce true randomness....

... in theory. And in practice?

The problem of the noise



A realistic device is not perfect...

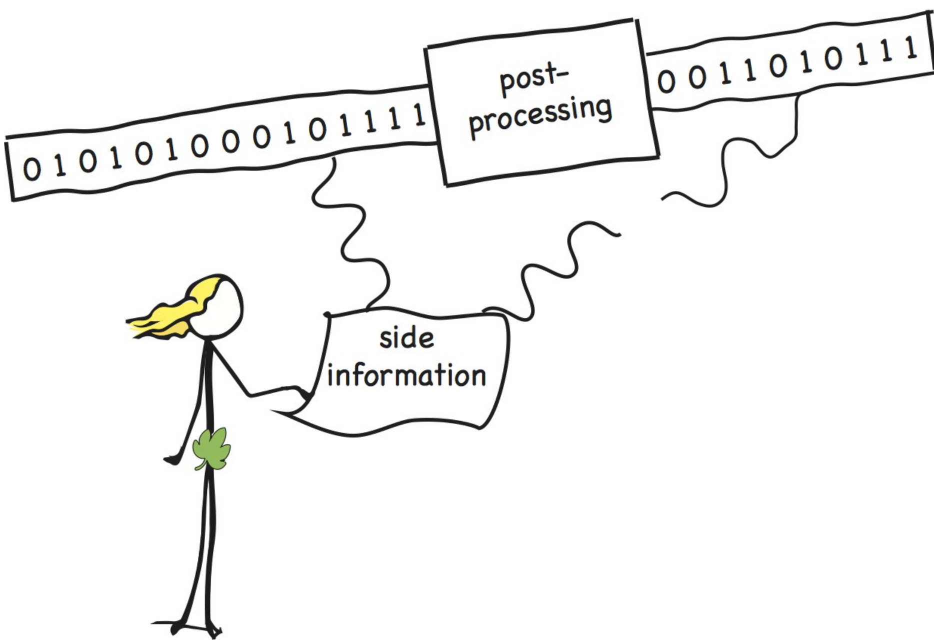
Output may be correlated to noise and hence, not truly random anymore....

Luckily this can be fixed :-)

Leftover Hash Lemma with Side Information

Let F be a family of two-universal hash functions from X to $\{0,1\}^l$. Then

$$\frac{1}{2}\left\|\rho_{F(X)EF} - \rho_{\bar{Z}} \otimes \rho_{EF}\right\|_1 \leq 2^{-\frac{1}{2}(H_{\min}(X|E)-\ell)} := \epsilon$$



$\bar{Z}$: uniform distribution on $\{0,1\}^l$

E: (quantum) side information

Modeling a QRNG

Not any RNG that can be modeled within QM is a QRNG...

Randomness relies on assumptions...

Randomness is fundamentally unpredictable....

... if it comes from a projective measurement on a pure state!

In practice:

- state is not pure but a mixture
- measurement is a POVM

...Noise...

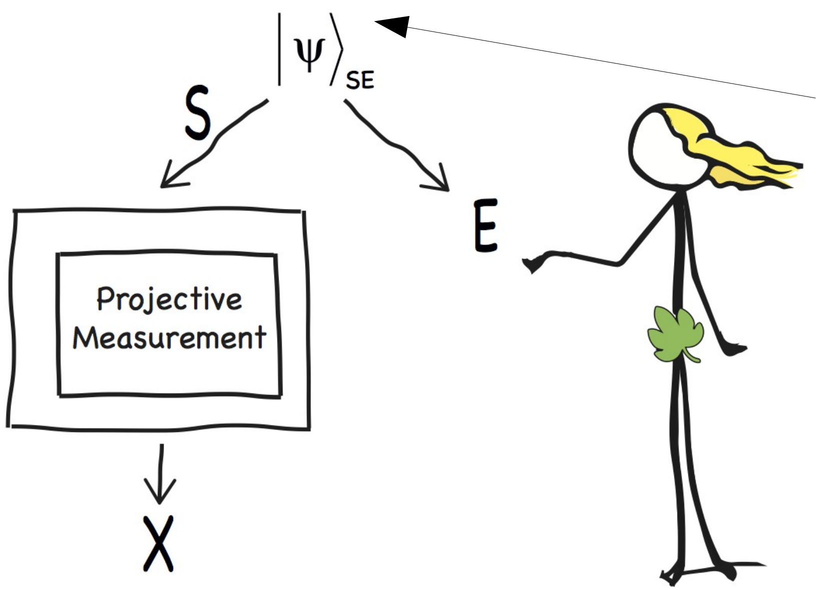
adversary can be entangled i.e. she knows component of mixture...

... side information!

can be seen as projective measurement on larger space with mixed input state (Naimark extension)

Model of a QRNG

Define a QRNG by a input state ρ_S and a projective measurement $\{\Pi_S^x\}_{x\in\mathcal{X}}$. Raw randomness X is distributed according to Born rule $P_X(x) = \mathrm{tr}(\Pi_S^x \rho_S)$.



All side information can be obtained from a purifying system E.

→ By the leftover hash lemma with side information $H_{min}(X|E)$ corresponds to the amount of extractable true randomness...

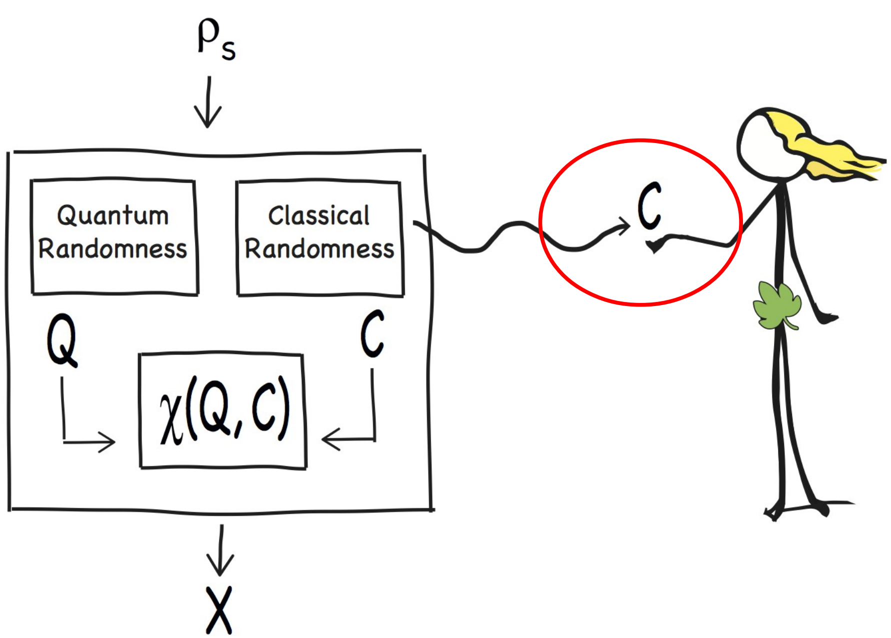
... not $H_{min}(X)$

... and not the Shannon entropy H(X) or H(X|E)

How to calculate $H_{min}(X|E)$ in practice

quantum min-entropy... may be hard to calculate...

idea: find a classical RV C with is just as good as quantum side information E such that $H_{\min}(X|C) \leq H_{\min}(X|E)$



C may be obtained from a measurement on S such that...

1. it does not interfere with the measurement carried out by the QRNG
2. it is maximally informative: post-measurement state conditioned on C is pure

...such a measurement is called a **Maximum Classical Noise Model**

For technical details see:

ARXIV:1311.4547

Summary

- Statistical test do not suffice to verify randomness
- true randomness: is unpredictable
- noise: should be treated as side information E
- $H_{min}(X|E)$: amount of extractable randomness that is independent of E
- presented framework allows to model any QRNG and calculate $H_{min}(X|E)$ in practice

Thank you :)