A Practical Approach to True Quantum Randomness Generation

ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Daniela Frauchiger and Renato Renner

In collaboration with IDQ

True Randomness?

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

→ **First, we have to agree on a definition.**

Considering the randomness of the *generating process* instead of the sequence allows a definition which is computable:

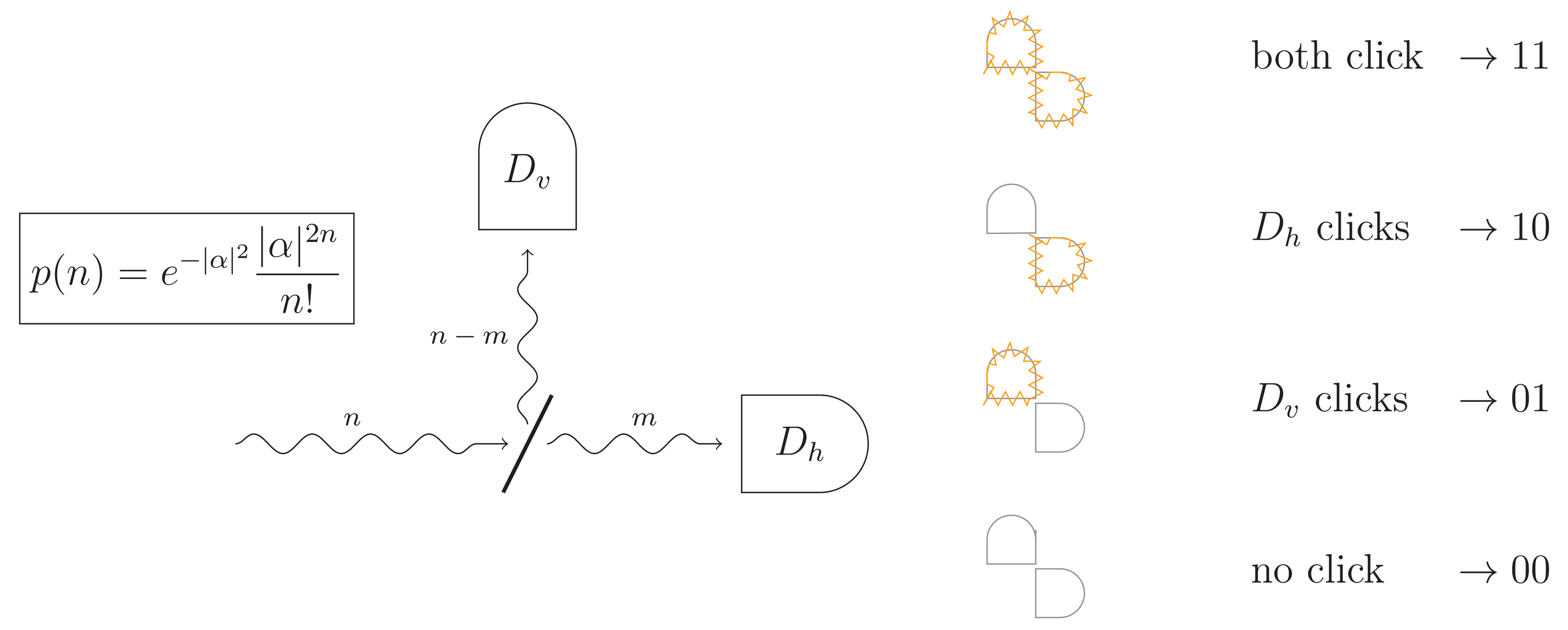
> ***A process is random, if its outcome is not predictable given all the information available before the number is generated.***

Quantum Random Number Generation

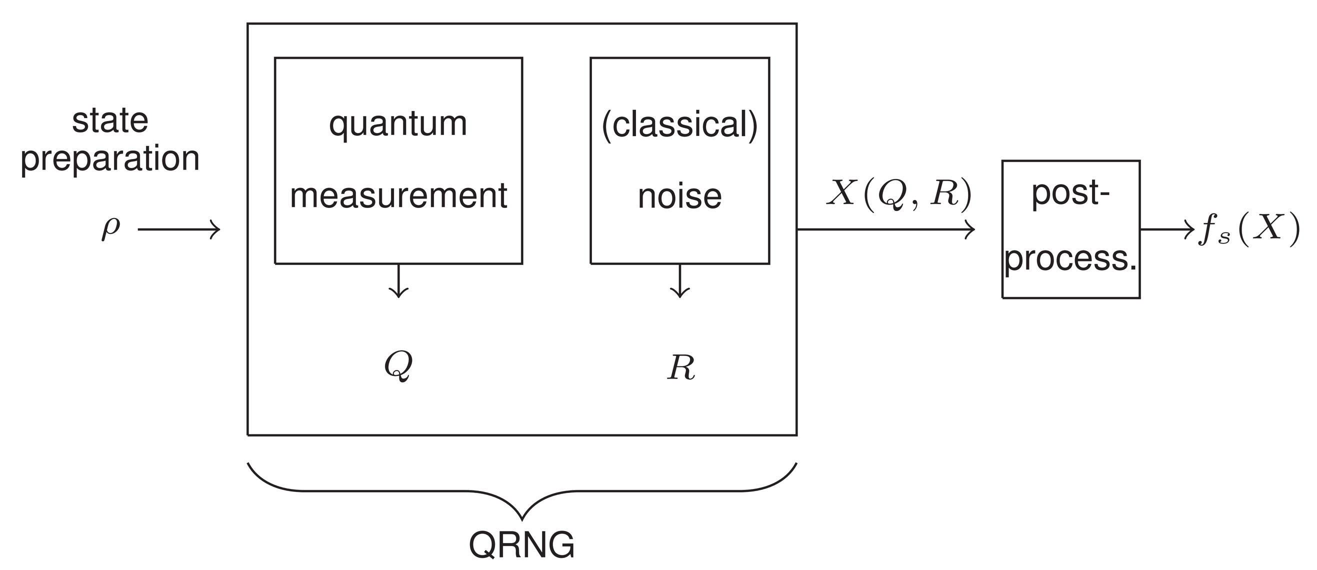
Advantage of using quantum systems: ***unpredictability of the randomness can be proven*** based on physical principles.

In practice the resulting raw randomness also depends on ***classical noise*** i.e., processes whose outcomes depend on possibly preexisting data.

Example: Classical noise due to limited detector efficiency and the source in a beam splitter.



Leftover Hash Lemma with Side Information



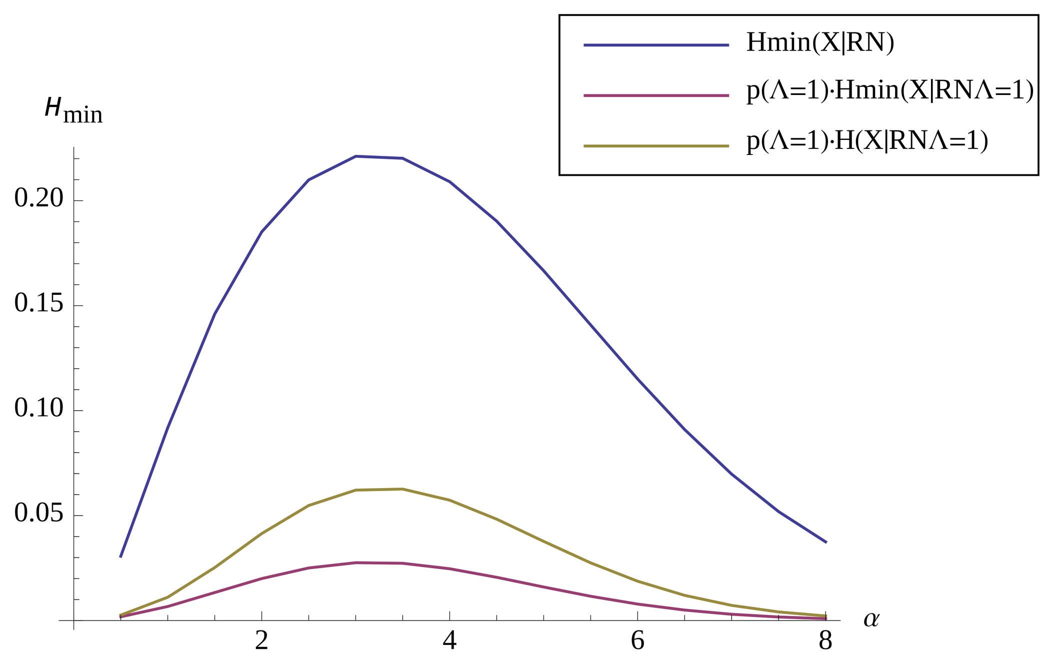
Let R be a an arbitrary random variable and let X be a random variable with range $\{0,1\}^l$. Let $\{f_s\}_{s\in\mathcal{S}}$ be a two-universal family from $\{0,1\}^l$ to $\{0,1\}^m$ with S distributed uniformly and independent of X and R. Then the distance from uniform of $P_{f_s(X)}$ given SR is bounded by

$$||P_{f_s(X)SR} - U_m \times P_{SR}||_1 \leq 2^{-\frac{1}{2}(H_{\min}(X|R)-m)} := \epsilon_{\text{hash}},$$

where and U_m is the uniform distribution on $\{0,1\}^m$. [1],[2]

Results

Extractable entropy rate before and after a pre-processing discarding the events 00 and 11 for $\mu = 0.1$ depending on the mean photon number. The min-entropy corresponds to a lower and the Shannon entropy to an upper bound on the number of true random bits that can be generated by post-processing by hashing.



Conclusion: The extractable entropy rate is maximal if the post-processing is applied to the raw randomness.
For another example of a QRNG to which the framework is applied see the poster of Mathilde Soucarros et al.

Comparison to other Approaches

- Classical noise is taken into account as side information, which is necessary to meet the above definition of true randomness.
- Compared to device-independent randomness generation [3] our approach does not rely on the existence of initial randomness. The price we pay is the assumption that the process generating the raw randomness is correctly described by a model.
- The framework can be applied for any implementation of a QRNG.
- Proof of randomness does not rely on any completeness assumption regarding the model or quantum theory [4].

References

[1] G. Brassard, et al. IEEE Transactions on, vol.41, no.6, (1995).

[2] R. Renner and R. König, Proc. of TCC 2005, LNCS, Springer, vol. 3378 (2005).

[3] S.Pironio, et al. Nature 464, 1021 (2010).

[4] R. Colbeck and R. Renner Nat Commun 2 (2011).