Entropic Uncertainty Principle for certification of secure randomness [1]

Davide G. Marangon,[1] Giuseppe Vallone,[1] Marco Tomasin,[1] and Paolo Villoresi[1]

[1]*Department of Information Engineering, University of Padova, I-35131 Padova, Italy*

Among the most remarkable results in the Quantum Information Theory of the last five years, the protocols of Randomness Expansion [2] and Randomness Amplification [3] [4] should be considered. In fact, these protocols make it possible the generation of *true* random numbers, i.e. distributed in an uniform and independent way with respect to any possible side information, both classical and quantum. Randomness is indeed expanded or amplified by means of Bell's measurements on quantum correlated systems and the degree of unpredictability of the outcomes is put in relation with the violation of Bell's inequalities. According to the extent of the violation, one can estimate the amount extractable true random numbers, certified to be unpredictable also in the presence of some Local Hidden Variables theory.

A disadvantage of these protocols lies in the fact that, at present time, their experimental realization is extremely demanding because loophole-free violations of multiparties Bell inequalities are required. If the assumptions with respect LHV theories are relaxed, it turns out that for applications in both Classical and Quantum Information Technology, quantum random number generators (QRNG) based only on the Born's rule are far more practical to implement.

A typical QRNG implements the photon *welcher weg* paradigm, with a photon prepared in an eigenstate $|\psi\rangle$ of the observable Π_X, i.e. $\{|+\rangle, |-\rangle\}$, and measured with Π_Z. In the ideal case, $|\psi\rangle$ is *pure* and the least number of extractable true random bits associated to the binary outcomes $z \in Z$ is given by the min-classical entropy $H_\infty(Z) = -\log_2 \max_z \mathrm{Tr}\left[\Pi_Z |\psi\rangle\langle\psi|\right] = 1$. In practical realizations, although it results impossible to forge pure states or keep them pure (especially for commercial QRNG), $H_\infty(Z)$ continues to be used to quantify the randomness of the generator and, more importantly, to calibrate randomness extractors, as if the prepared state was a pure generic $|\psi\rangle = \cos(\theta)|0\rangle + e^{i\phi}\sin\theta|1\rangle$. A common practice is to assert the degree of randomness of a QRNG by means of tests of randomness which analyze a-posteriori the statistical quality of the numbers produced.

An approach consistent with the Quantum Information Theory must take into account the fact that a mixed state leaves room for side information. In particular, quantum side information might be exploited by an eavesdropper having access to a physical system E correlated with the measured one. In other words, the randomness extractable from a not pure state cannot be considered unpredictable in the sense of Born's rule: numbers obtained from a mixed system may appear random and present a high content of classical min-entropy (and consequently pass the tests) only because other degrees of freedom are ignored.

We propose a method which lets Alice, the user of the QRNG, to extract unpredictable and therefore secure bits from a quantum system A, also if it is not prepared in a pure state. In particular we accounts for the case of an eavedropper, Eve, who can use the quantum side information to predict the outcome of the generator holding a quantum system E correlated with A. This is possible by using the min-entropy conditioned on E, i.e. $H_{\min}(Z|E)$.

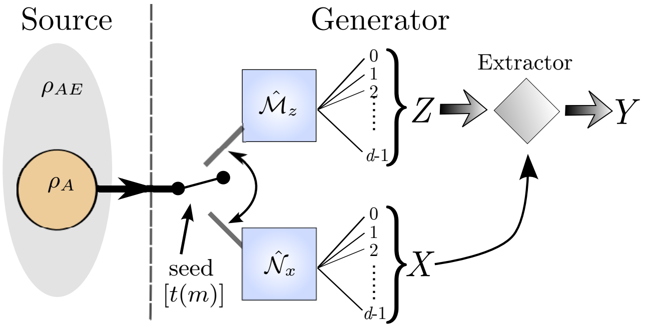

FIG. 1. Scheme of the QRNG. The source of randomness is the state ρ_A that can be correlated with a larger system E. An initial perfect random seed of length $t(m)$ is used to switch between the $\mathbb{Z}$ and $\mathbb{X}$ measurement basis, from which the random variables Z and X are extracted. The variable Z is used to generate the random sequence, while the variable X is used to evaluate how many true random bits can be extracted by Z. Y represents the final true random sequence.

An exact estimation of the min-conditional entropy would require the knowledge of the information possesed by Eve but typically Alice does not even know whether there is an eavesdropper. However a bound to $H_{\min}(Z|E)$ can be derived by adapting to the case of QRNG the *uncertainty principle* for min- and max- conditional entropies introduced in [5]. In the protocol we devised then, two kinds of measurements are performed: given e.g. a qubit supposedly prepared in the $|\psi\rangle = |+\rangle$ state, random numbers $z \in Z$ are obtained by projecting it onto the $\{|0\rangle, |1\rangle\}$ basis but, in addition, the measurement basis is randomly swapped to $\{|+\rangle, |-\rangle\}$ with outcomes $x \in X$. By means of these *check* measurements it is then possible to estimate the bound to $H_{\min}(Z|E)$ by applying the entropic uncertainty principle adapted to the QRNG case, i.e.

$$H_{\min}(Z|E) \geq \log_2 d - H_{\max}(X)$$

where d is the dimension of the Hilbert space and $H_{\max}(X)$ corresponds to the Rényi entropy of order 1/2. E.g. for the qubit case $\log_2 d = 1$: if the state is pure $H_{\max}(X)$ is null and therefore the bound corresponds to ideal value of $H_{\min}(Z)$, cfr. Figure 1. On the contrary if the state is mixed $H_{\min}(Z|E)$ is always less than the value one would be obtained using the classical min-entropy.

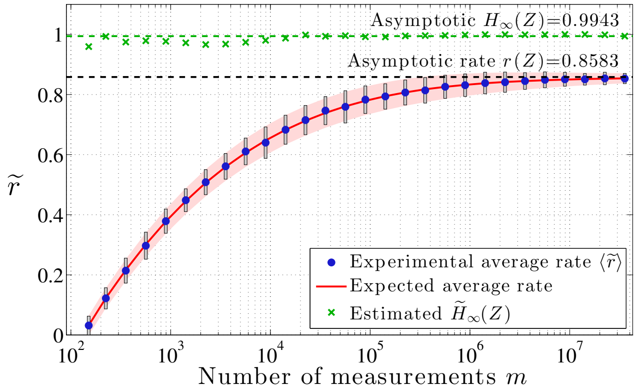

FIG. 2. Average experimental rate for a qubit QRNG. With blue circles we show the experimental average rate $\tilde{r}$ of true random bits per measurement, while the continuous red line represent the theoretical prediction. Shaded red area represents the theoretical standard deviation of the rate, while gray rectangles show the experimental standard deviation of the rate. Green crosses show the classical min-entropy estimated on the Z random variable.

To test the protocol, we experimentally implemented QRNGs employing both qubits and ququarts. In particular the results of the experiment for the qubit case are presented in Figure 2: the average neat amount of true random bits $\tilde{r}$ is plotted as a function of the number m of measurements being $\lceil\sqrt{m}\rceil$ the number of measurements used for the check basis. It is interesting to note, therefore, that since the experimental state is not pure, $H_{\min}(Z)$ would always overestimate the true content of random bits extractable from the QRNG.

By calibrating randomness extractors on the value of $H_{\min}(Z|E)$ Alice can extract only the randomness of quantum origin, getting rid of the so-called accidental randomness due to the mixedness of the state and possibly known by Eve. In particular, part of the extracted bits can be fed back into the generator for the further selection of the check measurements, achieving then a quadratic expansion of the initial random seed used for the first estimation of the entropy.

On this regard, conversely to the extraction based on a-posteriori erroneous entropy estimation, this protocol can be regarded as a dynamical extractor which provides resiliency to the generator against those factors which could make the state less pure and then the outcome less unpredictable.

[1] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 52327 (2014).
[2] S. Pironio, A. Acín, S. Massar, a. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. a. Manning, and C. Monroe, Nature **464**, 1021 (2010).
[3] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[4] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).
[5] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 5 (2009), arXiv:0909.0950.