Certified randomness in Quantum Physics

Yi-Shan Wu

June 25, 2017

1 Introduction

Randomness is frequently required in several places, such as math, physics, cryptography, even in our daily life. For example, when drawing lots, we usually expect that the output is highly random. That is, everyone is selected with almost equal probability. Thus, we need a random number generator(RNG). In statistical viewpoint, we can already gain random bit close to uniform today. However, classically, this classical random number are generated in deterministic, which means we know every step of the algorithm starting from a seed. This kind of randomness is called "pseudo-randomness".

Is pseudo-randomness enough for us? The answer is no. Take cryptography for example, if a bad guy knew the seed for RNG, or he observe the random number sequence for a long time, he might be able to know what's the random bit we are going to produce next. It is really dangerous since that guy may know the key we use.

Therefore, we need something to help produce "true-random" bits. Who is our savior? It may be quantum random number generator(QRNG). The reason for putting hope on QRNG is that there is intrinsic probability in quantum mechanics.

In the remaining report, we are going to introduce in section 2 that how to check whether there is quantumness in a machine if you are told that there is a QRNG. In section 3, we are going to introduce the relationship between "quantumness" and "randomness". In the last part, we are going to show the experiment results published in Nuture.

2 Test Quantumness by CHSH game

In class, we have already known that Bell's inequality draws an important distinction between classical mechanics and the world described by quantum mechanics. Thus, we are going to make use of the Bell's inequality to help us test whether there is

quantumness in a claimed "Quantum" Random Number Generator.
In the following of the section, we are going to review the CHSH game taught in class, and it is usually used by physicists. Next, we are going to introduce another version of CHSH game, which is often used in computer science. Although they are described in different ways, they are actually equal.

2.1 CHSH game in physics

We use the version introduced in [1]. The experiment setup is illustrated in Figure 1. Two particles are prepared and delivered by Charlie. Alice has two kinds of measurements: M_Q and M_R, while Bog has also two kinds of measurements: M_S and M_T. The outcomes of the measurements are $1, -1$. For Alice and Bob, when receiving a particle from Charlie, they perform a measurement respectively. Alice and Bob don't know which measurement they will choose to perform. Rather, they use some random bits to decide which measurement to perform right after receiving the particle.

Figure 1: Cited from [1]. Schematic experimental setup for the Bell inequalities. Alice can choose to measure either Q or R, and Bob chooses to measure either S or T . They can discuss before the game start. However, they can not contact any longer right after the game starts.

Theorem 1. *Classically,* $\mathsf{E}[QS] + \mathsf{E}[RS] + \mathsf{E}[RT] - \mathsf{E}[QT] \leq 2$*.[1]*

Proof. $QS + RS + RT - QT = (Q + R)S + (R - Q)T$. Since that $Q, R = \pm 1$, it follows that either $Q + R = 0$ or $R - Q = 0$. Both of these two cases give that $QS + RS + RT - QT = \pm 2$.
Suppose $p(q, r, s, t)$ is the probability that, before the measurements are performed,

the system is in a state where $Q = q$, $R = r$, $S = s$, and $T = t$. Thus, we have

$$\begin{aligned}\mathsf{E}[QS + RS + RT - QT] &= \sum_{q,r,s,t} p(q,r,s,t)(qs + rs + rt - qt) \\ &\leq \sum_{q,r,s,t} p(q,r,s,t) \times 2 \\ &\leq 2\end{aligned}$$

Also,

$$\begin{aligned}\mathsf{E}[QS + RS + RT - QT] = &\sum_{q,r,s,t} p(q,r,s,t)qs + \sum_{q,r,s,t} p(q,r,s,t)(rs) \\ &+ \sum_{q,r,s,t} p(q,r,s,t)(rt) - \sum_{q,r,s,t} p(q,r,s,t)(qt) \\ =&\mathsf{E}[QS] + \mathsf{E}[RS] + \mathsf{E}[RT] - \mathsf{E}[QT]\end{aligned}$$

Thus,

$$\mathsf{E}[QS] + \mathsf{E}[RS] + \mathsf{E}[RT] - \mathsf{E}[QT] \leq 2$$

□

2.2 CHSH game in computer science

We adopted the version introduced in [3]. The experiment setup is illustrated in Figure 2.

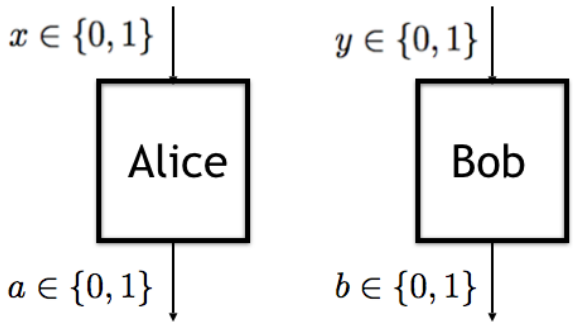

Figure 2: Schematic experimental setup for another CHSH game. Alice receives x and then output a. Bob has receives y and then output b. Alice and Bob win $\Leftrightarrow a \oplus b = x \wedge y$.

Two random bits $x \in \{0,1\}$ and $y \in \{0,1\}$ are prepared and delivered by Charlie.

Alice has a function $f_A : \{0,1\} \to \{0,1\}$,receiving x and then output a. Bob has a function $f_B : \{0,1\} \to \{0,1\}$, receiving y and then output b. Alice and Bob have to come up with some methods to win the game. However, they can not contact any longer right after the game starts. Alice and Bob win $\Leftrightarrow a \oplus b = x \wedge y$, where $\oplus$ denotes the XOR operation.

2.2.1 Classical method

Classically, it is easy to ensure that they win the game with probability $\frac{3}{4}$. As illustrated in table 1, it is obvious that only when both x and y are 1 will $x \wedge y$ be 1. Thus, the probability $\frac{3}{4}$ can be trivially achieved by always sending $a = b = 0$. However, we will show in the following theorem that $\frac{3}{4}$ is the best we can obtain by classical strategies.

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

a	b	$a \oplus b$
0	0	0
1	0	1
0	1	1
1	1	0

Table 1: Playing CHSH game using classical method. Alice and Bob win $\Leftrightarrow a \oplus b = x \wedge y$

Theorem 2. *In the previous scenario, no classical strategies can cause Alice and Bob to win with probability more than* $\frac{3}{4}$.

Proof. Assume for the sake of contradiction that there is a strategy causes them to win with probability more than $\frac{3}{4}$. The function $f_A : \{0,1\} \to \{0,1\}$ Alice uses can be either a constant function zero or one, the function $f_(x) = x$, or the function $f_(x) = 1 - x$.
We now first analyze a constant function $f_A(x) = 0$, and it is similar to the case $f_A(x) = 1$.

$$\because a \oplus b = x \wedge y, \text{ and } a = 0$$

$$\therefore b = x \wedge y$$

$$\text{If } \begin{cases} y = 0 \\ y = 1 \end{cases} \text{ then, output } \begin{cases} b = 0 \\ b = x \end{cases} \Rightarrow \begin{cases} \Pr[\text{win}] = 1 \\ \text{since Bob doesn't know } x, \Pr[\text{win}] = \frac{1}{2} \end{cases}$$

It is obvious that the probability of winning the game is no more than $\frac{3}{4}$.
Second, for the function $f_A(x) = x$,

$$\because x \oplus b = x \wedge y, \text{ and } a = 0$$

$$\therefore b = (x \wedge y) \oplus x$$

If $\begin{cases} y = 1 \\ y = 0 \end{cases}$ then, output $\begin{cases} b = 0 \\ b = x \end{cases} \Rightarrow \begin{cases} \Pr[\text{win}] = 1 \\ \text{since Bob doesn't know } x, \Pr[\text{win}] = \frac{1}{2} \end{cases}$

Analysis for the function $f_A(x) = 1 - x$ is similar to $f_A(x) = x$. Thus, it is obvious thatthe probability of winning the game is no more than $\frac{3}{4}$. □

2.2.2 Quantum method

Strategy for Alice and Bob if they are able to share quantum information.

1. Alice and Bob share an EPR pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Alice take the first bit while Bob take the second bit.

2. Alice receives x from Charlie, and if $x = 1$, then Alice applies a rotation by $\frac{\pi}{8}$ to her qubit. Bob receives y from Charlie, and if $y = 1$, then Bob applies a rotation by $-\frac{\pi}{8}$ to his qubit.

3. Alice and Bob then measure their qubits and get the output a and b respectively. The order in which Alice and Bob perform does not matter.

Theorem 3. *The strategy above provides a method to win the game with probability at least 0.8.*

Proof. The intuition behind the proof is that recall the classical case, Alice and Bob can win the game by always sending $a = b = 0$ unless $x = y = 1$. Thus, it seems that the states are "close" to one another unless $x = y = 1$.
Note that $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ can be written as $\frac{1}{\sqrt{2}}[1001]^T$.

1. If $x = y = 0$, then Alice and Bob apply $I \otimes I$ to EPR pair

$$\Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \Rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

   In the case that $x = y = 0$, Alice and Bob win if and only if $a = b$. After applying measurement, Alice and Bob get $a = b$ with probability 1.

2. If $x = 1$, $y = 0$, then Alice apply rotation by $\frac{\pi}{8}$ to her qubit. That is, to apply $\begin{bmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix} \otimes I$ to EPR pair.

$$\Rightarrow \begin{bmatrix} \cos\frac{\pi}{8} & 0 & -\sin\frac{\pi}{8} & 0 \\ 0 & \cos\frac{\pi}{8} & 0 & \sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} & 0 \\ 0 & -\sin\frac{\pi}{8} & 0 & \cos\frac{\pi}{8} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\frac{\pi}{8} \\ -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} \\ \cos\frac{\pi}{8} \end{bmatrix}$$

We can rewritten the final state as

$$\frac{1}{\sqrt{2}}(\cos\frac{\pi}{8}|00\rangle - \sin\frac{\pi}{8}|01\rangle + \sin\frac{\pi}{8}|10\rangle + \cos\frac{\pi}{8}|11\rangle)$$

$$\Rightarrow a = b \text{ with probability } \cos^2\frac{\pi}{8}$$

In the case that $x = 1$ and $y = 0$, Alice and Bob win if and only if $a = b$. After applying measurement, Alice and Bob get $a = b$ with probability $\cos^2\frac{\pi}{8}$.

3. If $x = 0$, $y = 1$, then Bob apply rotation by $-\frac{\pi}{8}$ to his qubit. That is, to apply $I \otimes \begin{bmatrix} \cos -\frac{\pi}{8} & \sin\frac{\pi}{8} \\ \sin -\frac{\pi}{8} & \cos -\frac{\pi}{8} \end{bmatrix}$ to EPR pair. By similar calculation, Alice and Bob get $a = b$ with probability $\cos^2\frac{\pi}{8}$.

4. If $x = 1$, $y = 1$, Alice and Bob win the game if and only if $a \neq b$. By some calculation, Alice and Bob win with probability $\frac{1}{2}$

Thus, the overall probability to win is $\frac{1}{4} \cdot 1 + \frac{1}{4} \cdot \cos^2\frac{\pi}{8} + \frac{1}{4} \cdot \cos^2\frac{\pi}{8} + \frac{1}{4} \cdot \frac{1}{2} \geq 0.8$. □

Thus, we can check whether there is quantumness in a machine by playing CHSH game. If the probability to win the game is higher then 0.8, we know that the machine might contain quantumness.

3 Quantumness and Randomness

We establish a link between quantumness and randomness in the section by the following two steps. First, give scores to every output pair (a, b) given an input pair (x, y), and estimate the expected total score Alice and Bob can get rather than just estimate the probability of winning the game. The expected total score of the game is called Bell expectation. Second, we introduce "min-entropy" to help us find out the relation between Bell expectation and randomness. Thus, we conclude that the violation of Bell's inequality guarantees the system to possess intrinsic randomness.

3.1 Bell expectation

We use the concept introduced in [4]. We introduce here another form of winning condition. It is equivalent to the original one, but is easier for us to estimate Bell expectation.

$$a \oplus b = x \wedge y, \text{ where } a, b \in \{0, 1\}, x, y \in \{0, 1\}$$
$$\Leftrightarrow a \cdot b = (-1)^{xy}, \text{ where } a, b \in \{1, -1\}, x, y \in \{0, 1\}$$

It is easy to check that if $x = y = 1$, Alice and Bob win if $a \neq b$. Otherwise, Alice and Bob win if $a = b$. We then give scores c_{abxy} to every (a, b) given (x, y)

$$c_{abxy} = \begin{cases} 1, & \text{if } a \cdot b = (-1)^{xy} \\ -1, & \text{if } a \cdot b \neq (-1)^{xy} \end{cases}$$

We can show all possible results by a table:

(a,b)\(x,y)	(0,0)	(0,1)	(1,0)	(1,1)
(1,1)	1	1	1	-1
(1,-1)	-1	-1	-1	1
(-1,1)	-1	-1	-1	1
(-1,-1)	1	1	1	-1

Table 2: table for c_{abxy}

The Bell expectation I is to calculate the expected score Alice and Bob can get in the CHSH game described in section (2.2).

$$I = \sum_{abxy} c_{abxy} P(ab|xy) \tag{1}$$

To be clear, this equation can be rewritten as

$$I = \sum_{xy} (-1)^{xy} [P(a = b|xy) - P(a \neq b|xy)] \tag{2}$$

It is not hard to obtain that every classical (deterministic) method satisfies $I \leq 2$. For example, for the constant function $f_A(x) = 0$ is classical case, we can get $I = 2$, while in some other cases, we can get $I = -2$. However, measurements performed on entangled states can violate the inequality. Take the measurement in section (2.2.2) for example. Consider (x,y)=(0,0), (0,1), (1,0) and (1,1) respectively and in order, we get $I = 1 \cdot 1 + 1 \cdot (\cos^2 \frac{\pi}{8} - (1 - \cos^2 \frac{\pi}{8})) + 1 \cdot (\cos^2 \frac{\pi}{8} - (1 - \cos^2 \frac{\pi}{8})) + (-1) \cdot (\frac{1}{2} - \frac{1}{2}) = 4 \cos^2 \frac{\pi}{8} - 1 \approx 2.414$

3.2 Min-entropy

When we are talking about communication, we are often interested in how much information we can get per message. Consider the measurement of a string X. Suppose a set of $|x\rangle$ are the possible results (states) of measurement with probability p_x, which is supposed to be no uniform.
It is known in physics that the higher the entropy, the higher the randomness, and the lesser the information we can get. One very important measure of the randomness is the Shannon entropy, estimating the expected value of the information contained in a message.

Definition 4. *Shannon Entropy:*

$$H(X) = -\sum_x p_x \log p_x$$

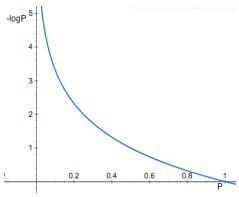

Figure 3: probability P v.s. $-\log_2 P$

For example, if we can get some result with probability of 1, then $H(X) = 0$, it is actually deterministic. However, the Shannon entropy is not meaningful in cryptography. Suppose Eve is going to guess the key Alice and Bob are using with only 1 chance. There are two situations:

	A	B	C	D
situation 1	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
situation 2	$\frac{4}{10}$	$\frac{3}{10}$	$\frac{2}{10}$	$\frac{1}{10}$

Table 3: The key Alice and Bob use can be one of the four strings A, B, C and D. In situation 1, they appear with equal probability while in situation 2, they are distributed non-uniform.

In situation 1, Eve has no idea which to choose since no single choice is apparently better others. However, in situation 2, it is reasonable for Eve to choose A, since A appears with the highest probability. Thus, we have the definition of min-entropy, caring about the choice with the "maximum" probability.

Definition 5. *Min-Entropy:*

$$H_{min}(X) = -\log max_x p_x$$

If the base of logarithm is 2, then the unit of min-entropy would be "bit". For example, the min-entropy of situation 1 described above is 2. That is, if we draw an event according to situation 1, it is equivalent to draw 2 truly random bit.

3.3 simulation

In this section, we have introduced Bell expectation and Min-entropy. Here we are going to combine these two concept to show that violation of Bell inequality guarantees the exist of randomness.
Assume ρ to be quantum system shared by Alice and Bob. $M_{a|x}$ is an measurement operator using x measurement and then output a, and $M_{b|y}$ is similar. Then, solve the following maximization problem to get the relation between Bell expectation and min-entropy.[4]

$$P^*(a,b|x,y) = \max\ P(a,b|x,y) \tag{3}$$

$$\text{subject to } \Sigma_{abxy} c_{abxy} P(a,b|x,y) = I \tag{4}$$

$$P(a,b|x,y) = tr(\rho M_{a|x} \otimes M_{b|y}) \tag{5}$$

Equation (4) is the Bell expectation of the CHSH game. Equation (5) is the measurement probability. Solve the optimization problem (semi-definite programming problem), we obtain the following figure.

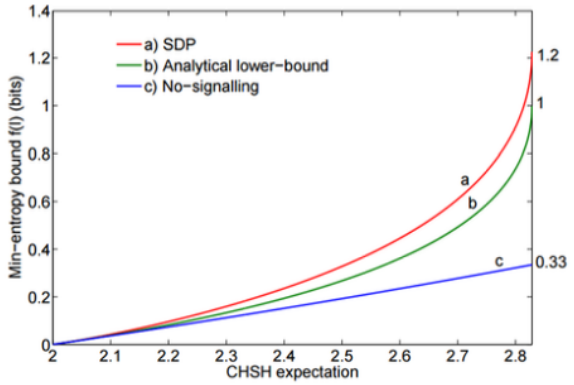

Figure 4: The red line is the result of semi-definite programming (SDP)

The red line shows that if the Bell expectation (CHSH expectation) is greater than 2, then the result of SDP guarantee that there is lower bound for the randomness. Furthermore, the more violation the Bell inequality, the more the randomness. The exists of randomness also guarantee that even Eve tries to cheat, she can get little information from a message.

4 Experiment

4.1 Setup

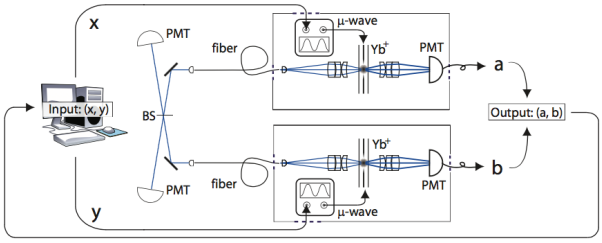

Figure 5: Cited from [4]. Experimental realization of QRNG using two Yb+ qubits trapped in independent vacuum chambers.

4.2 Result

The QRNG is made to play CHSH game for several times. The following table is the result of the game, where $N(a, b, x, y)$ is the number of events.

Inputs (x, y)	Rotations (φ_x, φ_y)	$N(0,0;x,y)$	$N(0,1;x,y)$	$N(1,0;x,y)$	$N(1,1;x,y)$	Total events	$P(a=b\|xy)$
0,0	0°, 45°	293	94	70	295	752	0.782
0,1	0°, 135°	298	70	74	309	751	0.808
1,0	90°, 45°	283	69	64	291	707	0.812
1,1	90°, 135°	68	340	309	89	806	0.195

Figure 6: Cited from [4]. Result of CHSH game done by QRNG. The data then indicate that $I = \sum_{xy}(-1)^{xy}[P(a=b|xy) - P(a\neq b|xy)] = 2.414 \pm 0.058$

We can see from figure 6 that the Bell expectation of QRNG is really greater than 2. Thus, the simulation result in figure 4 ensure that there is randomness in this QRNG.

5 Conclusion

True random number is especially important to cryptographic research. Thus, the essential of quantum random number generator is that it can generate true (unpredictable) random number rather than pseudo random number generated by traditional random number generator. Applying CHSH game, the randomness can be guaranteed by Bell inequality. And the more violation to Bell inequality, the more the randomness.

References

[1] Quantum computation and Quantum information, chapter 2, Nielson and Chuang, 2010

[2] Quantum cryptography lecture note, edX

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett,. 23(15):880-884, 1969.

[4] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bells theorem. 2009.