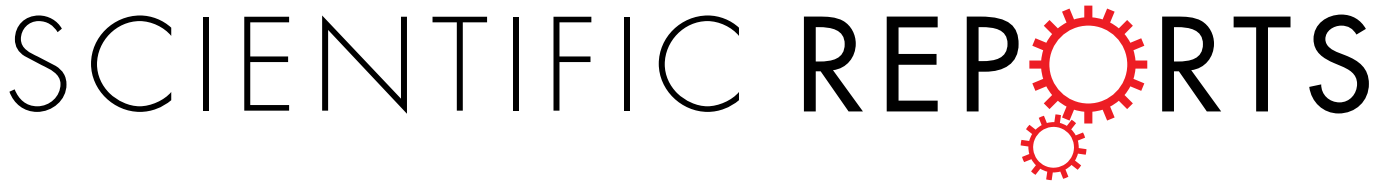

OPEN

Security of Semi-Device-Independent Random Number Expansion Protocols

Received: 01 May 2015
Accepted: 28 September 2015
Published: 27 October 2015

Dan-Dan Li[1,2], Qiao-Yan Wen[1], Yu-Kun Wang[1], Yu-Qian Zhou[1] & Fei Gao[1]

Semi-device-independent random number expansion (SDI-RNE) protocols require some truly random numbers to generate fresh ones, with making no assumptions on the internal working of quantum devices except for the dimension of the Hilbert space. The generated randomness is certified by non-classical correlation in the prepare-and-measure test. Until now, the analytical relations between the amount of the generated randomness and the degree of non-classical correlation, which are crucial for evaluating the security of SDI-RNE protocols, are not clear under both the ideal condition and the practical one. In the paper, first, we give the analytical relation between the above two factors under the ideal condition. As well, we derive the analytical relation under the practical conditions, where devices' behavior is not independent and identical in each round and there exists deviation in estimating the non-classical behavior of devices. Furthermore, we choose a different randomness extractor (i.e., two-universal random function) and give the security proof.

Truly random numbers have been wildly applied in many aspects such as numerical simulations of physical and biological systems, gambling and cryptography. As we know, the security of quantum key distribution (QKD) protocols depends on random selections of the prepared states and measurements so that adversary cannot utilize an attack to get secret information without being discovered.

There is no intrinsic randomness in the world of classical physics. In principle, any classical system admits a perfect description. And any observed randomness of a classical process is apparent (called as apparent randomness[1]), since it can be explained as the probabilistic mixture of deterministic classical events. Specially, the existing random number generators such as the linear feedback shift registers, which are characterized by using the deterministic algorithms, generate apparent randomness for us due to lacking of knowledge about their precise descriptions.

The advent of quantum physics makes it possible to produce intrinsic randomness. Colbeck *et al.*[2] gave a RNE protocol based on Greenberger-Horne-Zeilinger (GHZ) paradox. Pironio *et al.*[3] proposed a RNE protocol, where the generated randomness was certified by non-local correlation in the Clauser-Horn-Shimony-Holt (CHSH) test and quantified by min-entropy[4–6] of measurement outcomes. Fehr *et al.*[7] further characterized the amount of the generated randomness based on the ref. 3 and proposed a superpolynomial RNE protocol. Pironio *et al.*[8] analyzed that honest and dishonest device suppliers had influence on RNE and optimized conclusions of the ref. 3. The above protocols are categorized as DI-RNE ones, which make no assumption about the internal working of the devices.

As is well-known, DI-RNE protocols require entanglement, which results in negative effects on the complexity of devices and the rate of randomness generation. Thus the question whether we can generate randomness without any entanglement may arise. Fortunately, Li *et al.*[9] proposed SDI-RNE protocols without entanglement based on $2 \rightarrow 1$ quantum random access code (QRAC)[10,11] and the generated randomness was certified by non-classical correlation in the prepare-and-measure test. Furthermore, Li *et al.*[12] generalized the case of the ref. 9 to more general ones (i.e., $n \rightarrow 1$ QRAC) and pointed out $3 \rightarrow 1$ QRAC was the most efficient SDI-RNE protocols. These SDI-RNE protocols, where the users have

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [2]State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China. Correspondence and requests for materials should be addressed to F.G. (email: gaof@bupt.edu.cn)

no knowledge of internal working of the devices except for the dimension of the systems, are preferred since they are convenient for application.

The security of RNE protocols is of importance. As the security of QKD protocols[13–16] emphasizes key rate, the security of RNE ones focuses on the amount of the generated randomness. In the above mentioned DI-RNE protocols, the analytical relations between the amount of the generated randomness and Bell inequality violation was presented under the ideal and practical conditions[3,7,8]. And in the SDI scenario, the relation between the amount of the generated randomness and the degree of non-classical correlation was given by using Levenberg-Marquadrt (L-M) algorithm[9,12] and semi-definite programm (SDP) relaxation[17–19] under the ideal condition, respectively.

There are some problems worth thinking about in the SDI-RNE protocols. The analytical relation between the amount of the generated randomness and the degree of non-classical correlation under the ideal condition is missing. In practice, the behavior of the device is not identical and independent in each round and there exists deviation in estimating the non-classical behavior of the devices. It is natural to ask that the amount of the generated randomness and the degree of non-classical correlation satisfy what kind of analytical relation considering the above practical conditions.

In the paper, we give the analytical relation between the amount of the generated randomness and the degree of non-classical correlation under the ideal condition. Furthermore, we consider the practical conditions and establish the analytical relation which is described by a lower bound on the amount of the generated randomness based on the non-classical behavior of the devices. Finally, we choose two-universal random function[20] as randomness extractor and give the security proof.

Results

The model of SDI-RNE protocols[12]. Suppose that the relevant dimension d of the quantum systems are- known, in this work we take $d=2$. But the prepared states and measurement are not described. Generally, Alice's and Bob's black boxes are systems for state preparation ($\mathcal{P}$) and measurement ($\mathcal{M}$). Alice chooses n bits $x=x_0x_1 \ldots x_{n-1}\in\{0, 1\}^n$ at random, and sends the encoded state $\rho_x \in \mathbb{C}^2$ to Bob. Then Bob chooses a measurement operator M_y^b acting on the state ρ_x with input parameter $y\in\{0, 1, ..., n-1\}$ and output parameter $b\in\{0, 1\}$, where $M_y^b \geq 0$, $\sum_b M_y^b = I_2$. After repeating the procedure infinite times, Alice and Bob can get the probability distribution $P(b|x, y) = tr\left(\rho_x M_y^b\right)$. The generated randomness can be certified by the non-classical correlation.

Denote

$$\mathcal{W} = \sum_{b,x,y} (-1)^{x_y} P(b = 0|x, y), \tag{1}$$

called as $\mathcal{W}$ *expression*. If the systems admit a classical description, then $\mathcal{W}$ expression based on $2\rightarrow 1$ QRAC satisfies $\mathcal{W} \leq 2$, denoted as $\mathcal{W}_{2\rightarrow 1}^{\text{classical}} \leq 2$ simply. Obviously, if the systems contain the non-classical correlation (i.e., certain measurements act on quantum states), the data can violate the above inequality and makes $\mathcal{W}$ expression value up to $2\sqrt{2}$ ($\mathcal{W}_{2\rightarrow 1}^{\text{quantum}} \leq 2\sqrt{2}$). Similarly, $\mathcal{W}$ expression based on $3\rightarrow 1$ QRAC satisfy $\mathcal{W}_{3\rightarrow 1}^{\text{classical}} \leq 6$, $\mathcal{W}_{3\rightarrow 1}^{\text{quantum}} \leq 4\sqrt{3}$.

The amount of randomness of output b conditioned on the inputs x, y can be characterized by the *min-entropy*[4]

$$H_{\min}(B|X, Y)_P = -\log_2 \mathbf{p}(B|X, Y), \tag{2}$$

where the *maximal guessing probability*[4] of B given X, Y is

$$\mathbf{p}(B|X, Y) = \max_{b,x,y} P(b|x, y). \tag{3}$$

Based on equation (2), exploring a lower bound on min-entropy is equivalent to the upper bound on maximal guessing probability. So, to calculate the amount of the generated randomness can be converted into exploring maximal guessing probability for given value of $\mathcal{W}$ expression in the following optimization problem.

$$\text{maximize} \quad \mathbf{p}(B|X, Y) \tag{4}$$

subject to:

$$P(b|x, y) = tr\left(\rho_x M_y^b\right), \tag{5}$$

$$\sum_{b,x,y} (-1)^{x_y} P(b = 0|x, y) = \mathcal{W}, \tag{6}$$

where the optimization is carried out by arbitrary quantum state ρ_x and positive operator valued measure (POVM) $\{M_y^0, M_y^1\}$ defined over two dimensional Hilbert space.

Analytical relation under the ideal condition. We give the analytical relation between the maximal guessing probability and the corresponding maximal value of $\mathcal{W}$ expression. Moreover, we get the explicit bounds of $\mathcal{W}$ expression when there is the generated randomness. In other words, we gain the reason why there is not the generated randomness when the data just violates the classical bound of $\mathcal{W}$ expression. Here, we mainly give the results of the primitive ones (proved in the Supplementary Information).

Theorem 1. *Suppose that SDI-RNE protocol based on $2\rightarrow 1$ QRAC is associated with two dimensional Hilbert space. The analytical relation between the maximal guessing probability* $\mathbf{p}$ *and the corresponding maximal value of* $\mathcal{W}$ *expression is given as*

$$\mathcal{W}_{\mathbf{p}}^{\max} = \max_r \left\{ r + (2\mathbf{p}-1)r^2 + 2\sqrt{1-r^2} + 2\sqrt{\mathbf{p}(1-\mathbf{p})}\, r\sqrt{1-r^2} \right\}, \tag{7}$$

where $\mathbf{p} \in \left[\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right), 1\right]$ *and r is one of the real roots of equation* (8) *with a variable x*

$$\begin{aligned} &4x^4 + 4[(2\mathbf{p}-1) + 4\sqrt{\mathbf{p}(1-\mathbf{p})}\,]x^3 + x^2 \\ &\quad - 4[(2\mathbf{p}-1) + 2\sqrt{\mathbf{p}(1-\mathbf{p})}\,]x - (2\mathbf{p}-1)^2 = 0. \end{aligned} \tag{8}$$

According to the analytical relation (7), denoted as $\mathcal{W}_{\mathbf{p}}^{\max} = g_1(\mathbf{p})$, we explore the critical value of $\mathcal{W}$ expression conditioned on there exists the generated randomness. Let $\mathbf{p}=1$ (i.e., there is not the generated randomness of the outputs), we get $\mathcal{W}_{\mathbf{p}=1}^{\max} = 2.6403$ ($r=0.7904$) by taking over all the real roots of the equation expressed as $4x^4+4x^3+x^2-4x-1=0$. Further, we learn that g_1 is the monotonically decreasing and continuous function. As long as $\mathcal{W} > 2.6403$, the outputs exhibit randomness ($\mathbf{p}<1$).

Theorem 2. *Suppose that SDI-RNE protocol based on $3\rightarrow 1$ QRAC is associated with two dimensional Hilbert space. The analytical relation between the maximal guessing probability* $\mathbf{p}$ *and the corresponding maximal value of* $\mathcal{W}$ *expression is given as*

$$\begin{aligned} \mathcal{W}_{\mathbf{p}}^{\max} = \max_{\{(r,s,u,v)\}} \Bigg\{ & (2\mathbf{p}-1)r^2 + (2\mathbf{p}-1)\frac{\sqrt{1-m^2}}{m} r\sqrt{1-r^2} \\ & + \frac{(2\mathbf{p}-1)s + \sqrt{1-s^2}\sqrt{m^2-(2\mathbf{p}-1)^2}}{2m} \Big[\left(rv + \sqrt{1-r^2}\sqrt{1-v^2}\right) m \\ & + \left(\sqrt{1-r^2}v - r\sqrt{1-v^2}\right)\sqrt{1-m^2} \Big] + \frac{1}{2}\sqrt{4r^2+1+4rsv} \\ & + \sqrt{4r^2+1-4rsv} + \sqrt{4(1-r^2)+1+4\sqrt{1-r^2}s\sqrt{1-v^2}} \\ & + \sqrt{4(1-r^2)+1-4\sqrt{1-r^2}s\sqrt{1-v^2}} \Bigg\}, \end{aligned} \tag{9}$$

where $\mathbf{p} \in \left[\frac{1}{2}\left(1+\frac{1}{\sqrt{3}}\right), 1\right]$ *and the values of* (r, s, v, m) *is one of the real roots of the equation set in variables* (x, y, z, u) *in the* Supplementary Information.

Similar to the above analysis, we calculate the critical value of $\mathcal{W}$ expression conditioned on there exists the generated randomness. Let $\mathbf{p}=1$, we get $\mathcal{W}_{\mathbf{p}=1}^{\max} = 6.6543$ $((r, s, v, m) = (0.7730, 0.3837, -0.1529, 1))$ by taking over all the real roots of the equation set in the Supplementary Information. So, we conclude that as long as $\mathcal{W} > 6.6543$, the generated randomness can be certified.

Analytical relation under the practical condition. In practice, there exist some unideal factors during the experiment, for example, the behavior of the devices is not identical and independent in each round, and estimating the non-classical behavior of the devices causes deviation. We establish the analytical relation between the amount of the generated randomness and the degree of non-classical correlation under the practical condition. As well, our result can be applied to any RNE protocols with quantum system of arbitrary dimension and a general form of $\mathcal{W}$ expression in the SDI scenario.

Description of the devices used *t* times in succession. We consider a pair of devices $(\mathcal{P}\&\mathcal{M})$, where the state preparation $(\mathcal{P})$ and measurement $(\mathcal{M})$ can be regarded as two black boxes. The preparation box contains a set of arbitrary states $\rho \in \mathbb{C}^2$ and the measurement box contains a sequence of

arbitrary measurements $\left\{M_{y_i}^{b_i}\right\}$ defined over two-dimensional Hilbert space, where measurement operator $M_{y_i}^{b_i}$ represents input parameter y_i and output parameter b_i.

We make the most basic assumptions as follows:

(1) the preparation system and the measurement system conform to the quantum theory;
(2) there is no additional communication between the state preparation system and the measurement system in each round. That is, the state preparation system and the measurement system have a single qubit for communication and are not allowed to divulge information to eavesdropper in each round;
(3) the inputs X, Y are random variables that are independent and uncorrelated with the devices.

No constrains are imposed on the states and measurements except for their dimension and the above assumptions. But the behavior of devices is not identical and independent in each round i, which implies that the previous $i-1$ states, measurement operators and measurement outcomes affect the ith measurement outcomes. Note that we assume that the state preparation system are not entangled with the measurement system or any other party in the following calculation of the amount of generated randomness, which is similar to that in previous work[7,8].

We denote the inputs by $x_i \in \mathbf{X}$, $y_i \in \mathbf{Y}$ and the measurement output by $b_i \in \mathbf{B}$ in the ith round. We denote the first i inputs by $x^i = (x_1, x_2, ..., x_i)$ and define y^i, b^i similarly. The devices' behavior cannot be identical and independent in each round. That is, the behavior of devices varies from one round to another making use of internal memory, which is depicted by a sequence of unitrary transformations $U_0, ..., U_{t-1}$ acting on $\mathbb{H}_P \otimes \mathbb{H}_M$. U_{i-1} is used for the state and the measurement operator before the ith round ($U_0 = I$ in the first round). In details, suppose that Alice chooses the state ρ_{x_1} at will and Bob chooses the measurement setting $M_{y_1}^{b_1}$ in the first round, we get $P(b_1|x_1, y_1) = tr\left(\rho_{x_1} M_{y_1}^{b_1}\right)$. Alice and Bob choose ρ_{x_2}, $M_{y_2}^{b_2}$ at random, due to un-identical and dependent between rounds, we get $P(b_2|x_2, y_2, b_1, x_1, y_1) = tr\left(U_1 \rho_{x_2} M_{y_2}^{b_2} U_1^{\dagger}\right)$, where the operation U_1 encodes the information of the inputs x_1, y_1 and output b_1 in the first round. The given conditional probability distribution $P_{B^t|X^tY^t}(b^t|x^t, y^t)$, which describes the input-output behavior of t sequential interactions with the devices ($\mathcal{P}$ & $\mathcal{M}$), is defined as

$$P_{B^t|X^tY^t}(b^t|x^t y^t) = \prod_{i=1}^{t} P(b_i|x_i y_i b^{i-1} x^{i-1} y^{i-1}) = \prod_{i=1}^{t} P(b_i|x_i y_i e^{i-1}), \tag{10}$$

where $P(b_i|x_i y_i e^{i-1}) = tr\left(U_{i-1} \rho_{x_i} M_{y_i}^{b_i} U_{i-1}^{\dagger}\right)$, $e^{i-1} = b^{i-1} x^{i-1} y^{i-1}$. The first equality holds because of successive Bayes' principle and the second one shows that the output in the ith round is determined by the inputs of the ith round and the pervious inputs and outputs.

We learn that there is one-to-one correspondence between the maximal guessing probability and the corresponding maximal value of $\mathcal{W}$ expression based on the analytical relations (i.e., collectively called g_1) in the above part. The analytical relations show

$$\mathbf{p} = 2^{\log_2 g_1^{-1}\left(\mathcal{W}_{\mathbf{p}}^{\max}\right)} \leq 2^{\log_2 g_1^{-1}(\mathcal{W})} = 2^{-g(\mathcal{W})}, \tag{11}$$

where g_1 is the monotonically decreasing and continuous function of the corresponding maximal value of $\mathcal{W}$ and $g = -\log_2 g_1^{-1}(\mathcal{W})$ is the convex function of the value of $\mathcal{W}$ expression.

Estimating the degree of non-classical correlation. Here, we estimate $\mathcal{W}$ expression value to characterize the degree of non-classical correlation.

For the first round, $\mathcal{W}$ expression value is established by $\mathcal{W}_1[b_1, x_1, y_1] = \mathcal{W}[P(b_1|x_1 y_1)]$. For other rounds, there are slightly different because of the present round depending on the inputs and outputs of the previous rounds. So, $\mathcal{W}$ expression value in the ith round is $\mathcal{W}_i[b^i, x^i, y^i] = \mathcal{W}[P(b_i|x_i y_i e^{i-1})]$.

Let

$$\overline{\mathcal{W}}[b^t, x^t, y^t] = \frac{1}{t}\sum_{i=1}^{t} \mathcal{W}_i[b^i, x^i, y^i] \tag{12}$$

be the average value of $\mathcal{W}$ expression, averaged over t rounds. In order to estimate the average value $\overline{\mathcal{W}}$, we introduce the following estimator $\hat{\mathcal{W}}$, determined from the observed statistics:

$$\hat{\mathcal{W}}[b^t, x^t, y^t] = \frac{1}{t}\sum_{i=1}^{t} \hat{\mathcal{W}}_i, \tag{13}$$

where $\hat{\mathcal{W}}_i = \sum_{b,x,y} \alpha_{b,x,y} \frac{\chi(x_i = x, y_i = y, b_i = b)}{P_X(x) P_Y(y)}$ is the observed value of $\mathcal{W}$ expression in the ith round and $\chi(x)$ is the indictor function:

$$\chi(x) = \begin{cases} 1, & \text{if } x \text{ is observed,} \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

We derive the result of estimating the average value $\overline{\mathcal{W}}$ in the following (proved in the Supplementary Information).

Lemma 3. *Let the symbols be the same as before. For any $\delta > 0$, the average value $\overline{\mathcal{W}}$ and the observed average value $\hat{\mathcal{W}}$ satisfy*

$$P(\overline{\mathcal{W}} \geq \hat{\mathcal{W}} - \delta) \geq 1 - 2^{\frac{-t\delta^2}{2ln2\mu^2}}, \tag{15}$$

where $\mu = \frac{\alpha_{\max}}{P_{\min}} + W_Q$, $\alpha_{\max} = \max|\{\alpha_{b,x,y}\}|$, $P_{\min} = \min\{P(x)P(y)\}$ and W_Q is the maximal value of $\mathcal{W}$ expression allowed by quantum theory.

From inequality (15), we learn that the average value $\overline{\mathcal{W}}$ can be larger than the observed average value $\hat{\mathcal{W}}$ up to some δ with probability 1 when experiment's rounds tend toward infinity.

Bounding the min-entropy. Here, we proceed with the last step to get the analytical relation between the amount of the generated randomness and the observed average value $\hat{\mathcal{W}}$ under the practical conditions. Just as the refs 7, 8 consider the average Bell value in some interval as a prior condition to make the min-entropy meaningful in the DI case, we use the technique[7] to quantify the generated randomness, which is depicted by a lower bound on min-entropy of outputs conditioned on the event that the observed average value $\hat{\mathcal{W}}$ lies in some interval.

Denote W_0 by the maximal value of $\mathcal{W}$ expression conditioned on $H_{\min}(B^t|X^tY^t) = 0$. $W_0 > W_{cl}$ (the classical bound of $\mathcal{W}$ expression), which is different from that of Bell experiments. We partition the interval $[W_0, W_Q] \subset R$ into $\mathfrak{L}$ disjoint blocks: $[W_0, W_Q] = \Phi_1 \cup \Phi_2 \cup \ldots \cup \Phi_{\mathfrak{L}}$ with $\Phi_l = [W_{l-1}, W_l)$.

Here, a basic event space $\mathfrak{G}$ is the set that includes all possible (b^t, x^t, y^t, l) for the above experiment. Define an event $\mathcal{G}_1 = \{(b^t, x^t, y^t, l) | \overline{\mathcal{W}} \geq \hat{\mathcal{W}} - \delta\}$. According to Lemma 3, the event $\mathcal{G}_1$ occurs with high probability. In fact, the values of (b^t, x^t, y^t) can determine the value of $\hat{\mathcal{W}}$ and random variable l. Next, we define an event $\mathcal{G}_2 = \left\{(b^t, x^t, y^t, l) \middle| P(\mathcal{G}_1|x^t, y^t) \geq \frac{1}{2}\right\}$ and an event $\mathcal{G}_3 = \left\{(b^t, x^t, y^t, l) \middle| P_{L|X^tY^t\mathcal{G}_1}(l|x^t, y^t) \geq \frac{1}{\mathfrak{L}^2}\right\}$. Let $\mathcal{G}_1 \cap \mathcal{G}_2 \cap \mathcal{G}_3$ be the good event, denoted as $\mathcal{G}$. We call $\mathcal{G}_1 \cap \mathcal{G}_2 \cap \mathcal{G}_3$ as the good event (i.e., $\mathcal{G}$) since we can get the amount of the generated randomness as long as all of the events ($\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$) occur. Note that an event is a set that contains one or more results of a basic event space, which is a subset of the basic event space. As well, each result of an event is a element (basic event).

The following lemma is proven in the Supplementary Information.

Lemma 4. *There exist the above good event $\mathcal{G}$ with probability*

$$P(\mathcal{G}) \geq 1 - 3 \cdot 2^{\frac{-t\delta^2}{2ln2\mu^2}} - \frac{1}{\mathfrak{L}}. \tag{16}$$

We try to put a bound on the min-entropy of the outputs B^t conditioned on the inputs (X^t, Y^t) and the observed average value $\hat{\mathcal{W}}$ in some interval.

Theorem 5. *Let (X, Y) be identical, independent and random sources and $\delta > 0$ be an arbitrary parameter. For any devices' behavior, the observed distribution $P = \{P(b^t, x^t, y^t)\}$ characterizing successive t rounds satisfies*

$$H_{\min}(B^t|X^t, Y^t, l, \mathcal{G}) \geq tg(W_l) - 2 \log \mathfrak{L} - 1 \tag{17}$$

for all $x^t \in X^t$, $y^t \in Y^t$, $l \in \{0, \ldots, \mathfrak{L} - 1\}$ with $P(\mathcal{G}) \geq 1 - 3 \cdot 2^{\frac{-t\delta^2}{2ln2\mu^2}} - \frac{1}{\mathfrak{L}}$, $P_{B^tX^tY^tL|\mathcal{G}}(b^t, x^t, y^t, l) > 0$.

Proof. Without loss of generality, suppose that l is the unique value with $W_{l-1} \leq \hat{\mathcal{W}} - \delta < W_l$.

Let $(b^t, x^t, y^t, l) \in \mathcal{G}_2 \cap \mathcal{G}_3$, we consider nontrivial cases, i.e., $(b^t, x^t, y^t, l) \in \mathcal{G}_1$. Otherwise, $P(b^t|x^t, y^t, l, \mathcal{G}_1) = 0$.

According to the description of $\mathcal{G}$, we get

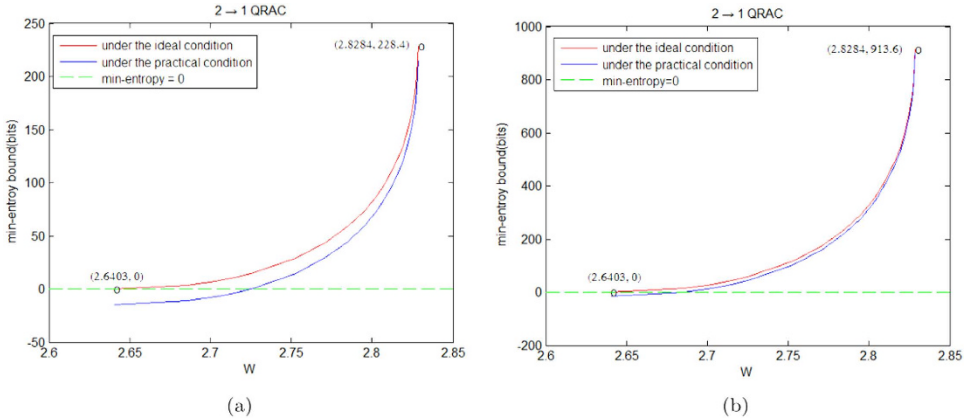

Figure 1. Compare the lower bound on the amount of the generated randomness in the SDI-RNE protocol based on $2 \rightarrow 1$ QRAC under the different conditions. (**a**) Under the condition of the experiment's rounds $t = 1000$. (**b**) Under the condition of the experiment's rounds $t = 4000$.

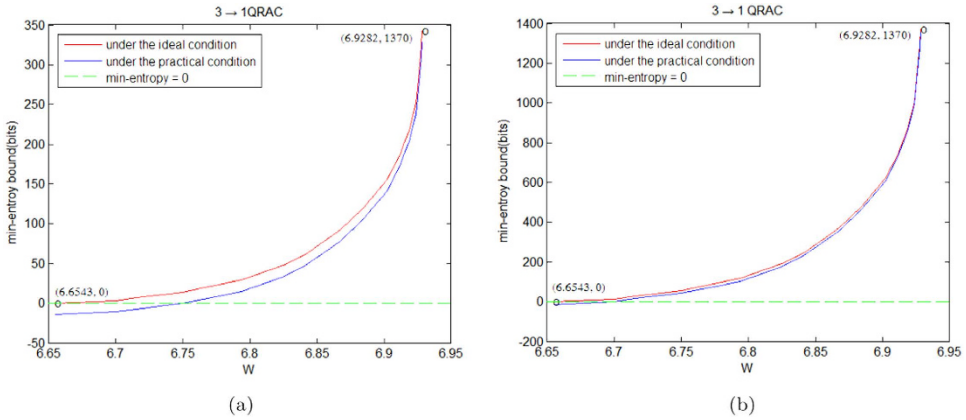

Figure 2. Compare the lower bound on the amount of the generated randomness in the SDI-RNE protocol based on $3 \rightarrow 1$ QRAC under the different conditions. (**a**) Under the condition of the experiment's rounds $t = 1000$. (**b**) Under the condition of the experiment's rounds $t = 4000$.

$$\begin{aligned}
\mathbf{p}(B^t|X^t, Y^t, l, \mathcal{G}_1) &= \max_{b^t,x^t,y^t} P_{B^t|X^tY^tL\mathcal{G}_1}(b^t|x^t, y^t, l) \\
&= \max_{b^t,x^t,y^t} \frac{P_{B^tL\mathcal{G}_1|X^tY^t}(b^t, l|x^t, y^t)}{P_{L\mathcal{G}_1|X^tY^t}(l|x^t, y^t)} \\
&\leq \max_{b^t,x^t,y^t} \frac{P_{B^t|X^tY^t}(b^t|x^t, y^t)}{P_{\mathcal{G}_1|X^tY^t} \cdot P_{L|X^tY^t\mathcal{G}_1}(l|x^t, y^t)} \\
&\leq 2L^2 2^{-tg(W_l)}, \qquad (18)
\end{aligned}$$

where the penultimate inequality holds because of $P_{B^tL\mathcal{G}_1|X^tY^t}(b^t, l|x^t, y^t) \leq P_{B^t|X^tY^t}(b^t|x^t, y^t)$ and the last one holds by using equations (10), (11) and (12).

Furthermore, with the above inequality, it is easy to show that

$$\begin{aligned}
H_{\min}(B^t|x^t, y^t, l, \mathcal{G})_p &= -\log_2 \max_{b^t} P_{B^t|x^ty^tL\mathcal{G}}(b^t|x^t, y^t, l, \mathcal{G}) \\
&\geq tg(W_l) - 2 \log \mathfrak{L} - 1. \qquad (19)
\end{aligned}$$

Here, suppose that disjoint blocks $\mathfrak{L} = 100$, $\delta = 0.0001$ and the experiment's rounds $t = 1000$, 4000, respectively. Under the ideal and practical conditions, we compare the lower bound on min-entropy of the generated randomness of SDI-RNE protocols based on $2 \rightarrow 1$ and $3 \rightarrow 1$ QRACs in Figs 1 and 2, respectively. Obviously, when rounds of experiments is increasing and the number of the disjoint blocks

is fixed, the Figures reveal that the gap of the amount of the generated randomness between the ideal and practical conditions is rapidly closing. Note that W in the Figures represents the observed average value.

Randomness extraction. As we know, by using a randomness extractor[20,21], the outputs b^t can be converted to a string that is nearly uniform and uncorrelated to the information of an adversary.

We propose a SDI-RNE protocol with another randomness extractor which is different from ones of the refs 7, 8. The users ask providers for two devices, where state preparation $(\mathcal{P})$ has 2^n settings and measurement $(\mathcal{M})$ has n settings and can make two possible output 0, 1. Furthermore, the users ask that these devices satisfy the most basic assumptions. But, they have no knowledge of the internal working of devices except for their dimension. The protocol is presented in the following.

The users allow a single qubit to communicate in each round and do not send any information outside the laboratory.

(1) Divide their initial truly random string $\mathfrak{S}$ into S_1 and S.
(2) Introduce $(x_i, y_i) \in S_1$ into the devices and obtain output b_i.
(3) Repeat step (2) until exhausting S_1 and build a output string.
(4) Calculate the observed average value and determine the value l that $\hat{\mathcal{W}} - \delta \in \Phi_l$. If $\hat{\mathcal{W}} - \delta < W_0$, the protocol aborts.
(5) Make use of S to choose the two-universal random function f and obtain a finial string. Based on Theorem 5, the length of the finial string is

$$n_s = 2\ \log\left(\epsilon_{sec} - 3 \cdot 2^{\frac{-t\delta^2}{2\ \ln\ 2\mu^2}} - \frac{1}{\mathfrak{L}}\right) + tg\,(W_l) - 2\ \log\ \mathfrak{L} + 1. \tag{20}$$

In order to prove security of the proposed protocols, we make the lemma for preparation (proved in the Supplementary Information).

Lemma 6. *Suppose that* $f\colon \{0,1\}^t \to \{0,1\}^{n_s}$ *is the two-universal random function*[22] *and* $r^{n_s} = f\,(b^t)$, *where* $b^t \in \{0,1\}^t$. *We get*

$$\sum_{r^{n_s},f} |P\,(r^{n_s}, f|x^t, y^t, l, \mathcal{G}) - 2^{-n_s} P\,(f|x^t, y^t, l, \mathcal{G})| \le \sqrt{2^{n_s}\mathbf{p}\,(b^t|x^t, y^t, l, \mathcal{G})}\,. \tag{21}$$

Theorem 7. *The proposed SDI-RNE protocol is* ϵ_{sec} *secure. That is, it is* ϵ_{sec} *indistinguishable from a ideal protocol.*

Proof. Based on the definition of security of protocol, we get

$$\begin{aligned}
&d\,(P_{R^{n_s}, X^t, Y^t, L, \mathfrak{F}}, 2^{-n_s} P_{X^t, Y^t, L, \mathfrak{F}}) \\
&= \frac{1}{2} \sum_{r^{n_s}, x^t, y^t, l, f} |P\,(r^{n_s}, x^t, y^t, l, f) - 2^{-n_s} P\,(x^t, y^t, l, f)| \\
&\le \frac{1}{2}\left[\sum_{r^{n_s}, x^t, y^t, l, f} |P\,(r^{n_s}, x^t, y^t, l, f|\mathcal{G}) - 2^{-n_s} P\,(x^t, y^t, l, f|\mathcal{G})| + 2P\,(\overline{\mathcal{G}})\right] \\
&\le \frac{1}{2} \sum_{x^t, y^t, l} P\,(x^t, y^t, l|\mathcal{G}) \sum_{r^{n_s}, f} |P\,(r^{n_s}, f|x^t, y^t, l, \mathcal{G}) - 2^{-n_s} P\,(f|x^t, y^t, l, \mathcal{G})| + P\,(\overline{\mathcal{G}}) \\
&\le \frac{1}{2} \sum_{x^t, y^t, l} P\,(x^t, y^t, l|\mathcal{G}) \sqrt{2^{n_s}\mathbf{p}\,(b^t|x^t, y^t, l, \mathcal{G})} + P\,(\overline{\mathcal{G}}) \\
&\le \epsilon_{sec}.
\end{aligned} \tag{22}$$

The penultimate inequality holds by using by the above Lemma 6.

Discussion

In the paper, we have showed the analytical relations between the amount of the generated randomness and the degree of non-classical correlation under the ideal and practical conditions. As a byproduct, the critical values of $\mathcal{W}$ expression have been presented when there exists the generated randomness. Moreover, the case, where the adversary holds the classical side information[8] of the devices, can be regarded as our case conditioned on the particular value of the side information. Finally, we choose the two-universal function as randomness extraction and give the security proof. Whereas, there are still

interesting questions that remain open. How can we quantify the generated randomness by directly using the observed probability distribution. Furthermore, for a given observed probability distribution, whether and how to find an optimal witness of given dimension with the method in the refs 19.

References

1. Dhara, C., De La Torre, G. & Acn, A. Can observed randomness be certified to be fully intrinsic. *Phys. Rev. Lett.* **112,** 100402 (2014).
2. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A: Math. Theor.* **44,** 095305 (2011).
3. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* (London) **464,** 1021 (2010).
4. Köenig, R., Renner, R. & Schaffner, C. The operational meaning of min and max-entropy. *IEEE Trans. Inf. Theory* **55,** 4337–4347, (2009).
5. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min and max-entropies. *IEEE Trans. Inf. Theory* **56,** 4674–4681 (2010).
6. Köning, R. & Renner, R. Sampling of min-entropy relative to quantum konwledge. *IEEE Trans. Inf. Theory* **57,** 4760–4787 (2011).
7. Fehr, S., Gelles, R. & Schaffner, C. Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A* **87,** 012335 (2013).
8. Pironio, S. & Massar, S. Security of practical private randomness generation. *Phys. Rev. A* **87,** 012336 (2013).
9. Li, H. W. *et al.* Semi-device-independent random-number expansion without entanglement. *Phys. Rev. A* **84,** 034301 (2011).
10. Ambainis, A., Leung, D., Manciska, L. & Ozols, M. Quantum random access codes with shared randomness. e-print arXiv:quant-ph/0810.2937v3.
11. Pawłowski, M. & Éukowski, M. Entanglement-assisted random access codes. *Phys. Rev. A* **81,** 042326 (2010).
12. Li, H. W., Pawłowski, M., Yin, Z. Q., Guo, G. C. & Han, Z. F. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random acess codes. *Phys. Rev. A* **85,** 052308 (2012).
13. Acn, A. *et al.* Device-independent security of quantum cryprography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
14. Christandle, M., Renner, R. & Ekert, A. A generic security proof for quantum key distribution. e-print arXiv: quant-ph/0402131.
15. Masanes, S., Pironio, S. & Acn, A. Security device-independent quantum key distribution with causally independent measurement devices. *Nature Commun.* **2,** 238–251 (2011).
16. Masanes, L., Renner, R., Christandl, M., Winter, A. & Barrett, J. Full security of quantum key distribution from no-signalling contraints. *IEEE Trans. Inf. Theory* **60,** 4973–4986 (2014).
17. Li, H. W. *et al.* Relation between semi- and fully-device-independent protocols. *Phys. Rev. A* **87,** 020302(R) (2013).
18. Mironowicz, P., Li, H. W. & Pawłowski, M. Properties of dimension witnesses and their semidefinite programming relaxations. *Phys. Rev. A.* **90,** 022322 (2014).
19. Navascués, M. & Vértesi, T. Bounding the set of finite dimensional quantum correlations. *Phys. Rev. Lett.* **115,** 020501 (2015).
20. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's ertractor in the presence of quantum side information. e-print arXiv: quant-ph/0912.5514v3.
21. Aroya, A. B. & Shma, A. T. Better short-seed quantum-proof extractors. *Theoretical Computer Science* **419,** 17–25 (2012).
22. Bennett, C. H., Brassard, G., Crepeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41,** 1915–1923 (1995).

Acknowledgements

This work is supported by NSFC (Grant Nos. 61272057, 61170270), Beijing Higher Education Young Elite Teacher Project (Grant Nos. YETP0475, YETP0477).

Author Contributions

D.L., Q.W., Y.W. and Y.Z. analyzed the previous DI-RNE and SDI-RNE protocols. Y.Z. and D.L. derived the analytical relation, F.G., D.L. and Y.W. analyzed other aspects, wrote the main manuscript text and prepared all figures. All authors reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Li, D.-D. *et al.* Security of Semi-Device-Independent Random Number Expansion Protocols. *Sci. Rep.* **5**, 15543; doi: 10.1038/srep15543 (2015).