




ARTICLE

<https://doi.org/10.1038/s41467-018-07585-0>

OPEN

Source-device-independent heterodyne-based quantum random number generator at 17 Gbps

Marco Avesani ¹, Davide G. Marangon¹, Giuseppe Vallone ^{1,2} & Paolo Villoresi ^{1,2}

Random numbers are commonly used in many different fields, ranging from simulations in fundamental science to security applications. In some critical cases, as Bell's tests and cryptography, the random numbers are required to be both private and to be provided at an ultra-fast rate. However, practical generators are usually considered trusted, but their security can be compromised in case of imperfections or malicious external actions. In this work we introduce an efficient protocol which guarantees security and speed in the generation. We propose a source-device-independent protocol based on generic Positive Operator Valued Measurements and then we specialize the result to heterodyne measurements. Furthermore, we experimentally implemented the protocol, reaching a secure generation rate of 17.42 Gbit/s, without the need of an initial source of randomness. The security of the protocol has been proven for general attacks in the finite key scenario.

¹Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padova, Italy. ²Istituto di Fotonica e Nanotecnologie —CNR, Via Trasea 7, 35131 Padova, Italy. Correspondence and requests for materials should be addressed to P.V. (email: paolo.villoresi@dei.unipd.it)

The possibility of generating random numbers by quantum processes is an invaluable resource in cryptography. Nowadays, common solutions based on pseudo or classical random number generators rely on deterministic processes, which are in principle predictable. On the contrary, quantum mechanics guarantees, from a theoretic point of view, that the outcome of the measurement is completely unpredictable. However, in a paranoid scenario (the usual framework of device-independent protocols), any imperfection in the physical realization of a quantum random number generator (QRNG) may leak information correlated with the generated numbers, the so-called side information¹. Such classical or quantum correlations could be exploited by an eavesdropper to correctly guess the measurement outcomes.

The maximal amount of randomness that can be extracted in presence of such side information is given by the so-called quantum conditional min-entropy². Several approaches have been proposed to lower bound it, depending on the number of assumptions required on the devices used in the generator. For “fully trusted” QRNGs^{3–5}, the min-entropy can be evaluated because pure input states and well characterized measurement devices are assumed (see ref. 6 for more details). In contrast, device-independent (DI) protocols, by exploiting entanglement, do not need any assumption: the violation of a Bell inequality directly bounds the min-entropy, without the need of trusting the generated state and the used measurement devices. Fully trusted QRNG, including all the commercial ones, are easy to realize, but they require strong assumptions for their use in cryptography. On the contrary, DI protocols offer the highest level of security, but their realization is still too demanding for any practical use^{7–11}.

Semi-device-independent (Semi-DI) protocols¹², are a promising approach to enhance the security with respect to standard “fully trusted” QRNG, achieving fast generation rate, dramatically larger than DI QRNG. These require some weaker assumptions to bound the side information. Such assumptions can be related to the dimension of the underlying Hilbert space^{13,14}, the measurement device^{6,11,15–17} or the source¹⁸, for example the mean photon number¹⁹ or the maximum overlap²⁰ of the emitted states.

In this work, we introduce a QRNG belonging to the family of the Semi-DI generators. In particular, we will describe a novel source-device-independent (Source-DI) protocol by exploiting continuous variable (CV) observables of the electromagnetic (EM) field. In previously realized CV-QRNGs^{15,21}, random numbers were generated by using a homodyne detector that measures a quadrature of the EM field. We propose and demonstrate a CV-QRNG based on heterodyne detection in the Source-DI framework: we will show how it is possible to obtain a lower bound on the eavesdropper quantum side information (i.e., the conditional min-entropy) and to achieve, to our knowledge, the fastest generation rate in the Semi-DI framework. The advantages of heterodyne measurement over homodyne are multiple: beside offering better tomography accuracy than homodyne^{22,23}, heterodyne measurement offers an increased generation rate since it allows a “simultaneous measurement” of both quadratures. In addition, the experimental setup is simplified with respect to the protocol based on homodyne introduced in¹⁵, as there is no need of an active switch to measure the two quadratures. Finally, it is possible to derive a constant lower bound on the conditional quantum min-entropy that does not change during the experiment. Our Source-DI protocol assumes a trusted detector but it does not make any assumption on the source: an eavesdropper may fully control it, manipulating it in order to maximize her ability to predict the outcomes of the generator. Such approach is very effective in taking into account any imperfect state preparation. Although these are the typical assumptions that hold for QRNGs in the Semi-DI framework,

this protocol features an important difference. Previous protocols counteract the eavesdropper via an active measurement strategy on the state, which implies the need for additional randomness to certify the numbers. Instead here the removal of the active basis switch has a deep impact on the type of protocol implemented: in this scheme no external initial randomness is required, making it a randomness generation protocol and not a randomness expansion protocol, unlike previous Semi-DI and DI realizations. Moreover, we will show the results of a practical realization of the protocol with a compact fiber optical setup that employs only standard telecom components. The electric signals coming from the detectors are digitalized in burst mode by an oscilloscope and further post-processed, achieving an equivalent generation rate of secure random numbers > 17 Gbit/s.

Results

A heterodyne QRNG. In standard CV-QRNGs, random numbers are obtained by measuring with an homodyne detector a quadrature observable of the EM fields, typically prepared in a vacuum state. CV-QRNGs are characterized by high generation rates owing to the use of fast photodiodes instead of (slow) single-photon detectors: continuous spectrum of the observables typically assures more than one bit of entropy per measurement and the use of photodiodes with high-bandwidth allow to sample the quadratures at GSample/s. In our QRNG, we implement a heterodyne detection scheme where two “noisy quadrature observables” are measured simultaneously^{24,25}. More precisely, an heterodyne measurement corresponds to the following positive operator value measurement (POVM) $\{\hat{\Pi}_\alpha\}_{\alpha \in \mathbb{C}}$ where

$$\hat{\Pi}_\alpha = \frac{1}{\pi} |\alpha\rangle\langle\alpha|, \quad (1)$$

and $|\alpha\rangle$ is the coherent state with complex amplitude α . If we define ρ_A as the density matrix of the EM field, the output of the heterodyne measurement is represented by the random variable X

$$X = \{q, p\}, \quad q = \Re(\alpha), p = \Im(\alpha), \quad (2)$$

distributed according to the following probability density function known as Husimi function:

$$Q_{\rho_A}(\alpha) = \text{Tr}[\hat{\Pi}_\alpha \rho_A] = \frac{1}{\pi} \langle\alpha|\rho_A|\alpha\rangle. \quad (3)$$

In an ideal scenario where the QRNG user (Alice) can trust the source of random states, such scheme has the immediate advantage of doubling the generation rate with respect to an homodyne receiver. As the “raw” random numbers X are typically not uniformly distributed, it is essential to process them with a randomness extractor²⁶. A randomness extractor compresses the input string of raw numbers, such that the shorter output string is composed by i.i.d. random bits.

In a real implementation, any heterodyne measurement is discretized. This means that the possible outcomes X_δ of the measure are discrete with a resolution given by δ_q and δ_p for the two “quadratures”. The discretized version of the POVM element $\hat{\Pi}_\alpha$ is then given by $\hat{\Pi}_{m,n}^\delta = \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp \hat{\Pi}_{q+ip}$ and the possible outputs are distributed according to a discretized version of the Husimi function:

$$Q_{\rho_A}^\delta(m, n) = \text{Tr}[\hat{\Pi}_{m,n}^\delta \rho_A] = \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp Q_{\rho_A}(q + ip). \quad (4)$$

In a fully trusted QRNG, when the source is trusted and the input state is pure (such as for the vacuum) or the privacy of the

generated numbers is not a concern, the number of random bits that can be extracted per sample is given by the so-called classical min-entropy of X_δ

$$H_{\min}(X_\delta) = -\log_2 \left[\max_{m,n} Q_{\rho_A}^\delta(m,n) \right]. \quad (5)$$

However, ultrafast generation is worthless for cryptographic applications if the numbers are not secure and private. If security is important, quantum side information must be also taken into account and the conditional quantum min-entropy $H_{\min}(X|\mathcal{E})$ ^{2,27-29} must be evaluated. We recall that in the Source-DI framework, an eavesdropper may have full control of the source and then may have some prior information on the generated numbers. We will show that with a heterodyne scheme it is possible to generate unpredictable and secure numbers also when the source of quantum states is controlled by the eavesdropper.

A secure POVM-based QRNG. In our Source-DI framework, Alice does not make any assumption on ρ_A , such as its dimension or purity: the source may be even controlled by a malicious QRNG manufacturer, Eve. This framework is well suited to deal with imperfect sources of quantum states⁶. On the contrary, Alice carefully characterizes her local measurement apparatus and trusts it.

In this scenario, Eve is assumed to prepare the state ρ_A to be measured. In particular, Eve will prepare ρ_A in order to maximize her guessing probability P_{guess} of the outcomes of Alice heterodyne measurement. If the state ρ_A is not pure, it can be prepared by Eve as a incoherent superposition of states τ_β^A with probabilities $p(\beta)$, such as $\rho_A = \int p(\beta) \tau_\beta^A d\beta$. As shown below, for quantum state ρ_A with positive Glauber–Sudarshan representation, Eve optimizes her strategy by using τ_β^A that are coherent states.

When Eve generates the state τ_β^A , the best option for her is to bet on the heterodyne outcome with higher probability, namely $\max_{m,n} \text{Tr} [\hat{\Pi}_{m,n}^\delta \tau_\beta^A]$. On average, Eve’s probability of guessing correctly the output of the heterodyne measurement can be written as $P_{\text{guess}}(X_\delta|\mathcal{E}) = \int p(\beta) \max_{m,n} \text{Tr} [\hat{\Pi}_{m,n}^\delta \tau_\beta^A] d\beta$. Having full control of the source, given the state ρ_A , Eve chooses the decomposition $\{p(\beta), \tau_\beta^A\}$ that maximizes P_{guess} . We note that the states $\hat{\tau}_k$ are, in general, not orthogonal. In such scenario, quantum correlations between Alice and Eve are modeled by a shared a pure bipartite state ρ_{AE} . The states τ_k are related to the optimal measurement that Eve should perform on ρ_{AE} in order to maximize her guessing probability.

According to the Leftover Hash Lemma^{27,30}, the extractable randomness in the presence of side information is quantified by the quantum conditional min-entropy

$$H_{\min}(X_\delta|\mathcal{E}) = -\log_2 P_{\text{guess}}(X_\delta|\mathcal{E}), \quad (6)$$

where $P_{\text{guess}}(X_\delta|\mathcal{E})$ is maximum probability of guessing X_δ conditioned on the quantum side information \mathcal{E}

$$P_{\text{guess}}(X_\delta|\mathcal{E}) = \max_{\{p(\beta), \tau_\beta^A\}} \int p(\beta) \max_{m,n} \text{Tr} [\hat{\Pi}_{m,n}^\delta \tau_\beta^A] d\beta. \quad (7)$$

The maximization in (7) is performed over all possible decomposition $\{p(\beta), \tau_\beta^A\}$ that satisfy $\rho_A = \int p(\beta) \tau_\beta^A d\beta$. The above considerations are valid not only for the heterodyne measurement, but are correct for any POVM measurement (also with Hilbert spaces of finite dimensions).

Figure 1 represents a general protocol within this framework. In the case of infinite precision $\delta_p, \delta_q \rightarrow 0$ (i.e., the continuum limit) it is possible to define the differential quantum min-entropy as $h_{\min}(X|\mathcal{E}) = \lim_{\delta_p, \delta_q \rightarrow 0} [H_{\min}(X_\delta|\mathcal{E}) + \log_2 \delta_p \delta_q]$ ²⁹ and a corresponding $p_{\text{guess}}(X|\mathcal{E}) = 2^{-h_{\min}(X|\mathcal{E})}$. In this case p_{guess} is a probability density and not a proper probability such as P_{guess} .

By exploiting the properties of POVMs, we derive a lower bound on $H_{\min}(X_\delta|\mathcal{E})$ (and thus an upper bound on $P_{\text{guess}}(X_\delta|\mathcal{E})$).

Proposition 1. For any POVM, $\{\hat{\Pi}_x\}_{x \in X}$ the quantum conditional min-entropy $H_{\min}(X|\mathcal{E})$ is lower-bounded by $H_{\text{low}} = -\max_{\{x \in X, \tau_A \in \mathcal{H}_A\}} \log_2 (\text{Tr} [\hat{\Pi}_x \tau_A])$.

If the POVM reduce to projective measurements, the above bound is trivial, as it is always possible to find a state τ_A such that $\text{Tr} [\hat{\Pi}_x \tau_A] = 1$: in this case, no randomness can be extracted. However, for an overcomplete set of POVM we may have $\max_{\{x, \tau_A\}} \text{Tr} [\hat{\Pi}_x \tau_A] < 1$ and therefore randomness can always be extracted. We now exploit the above proposition for the specific case of heterodyne measurement.

Corollary 1. For the heterodyne measurement, the quantum conditional min-entropy is lower-bounded by

$$H_{\min}(X_\delta|\mathcal{E}) \geq -\max_{\{m,n,\tau_A\}} \log_2 (\text{Tr} [\hat{\Pi}_{m,n}^\delta \tau_A]) = \log_2 \frac{\pi}{\delta_q \delta_p}. \quad (8)$$

The corresponding differential min-entropy $h_{\min}(X|\mathcal{E})$ is lower-bounded by $\log_2 \pi$. The bounds are tight, i.e., $h_{\min}(X|\mathcal{E}) = \log_2 \pi$ and $H_{\min}(X_\delta|\mathcal{E}) = \log_2 \frac{\pi}{\delta_q \delta_p} + O(\delta)$, for quantum state with positive Glauber–Sudarshan $\mathcal{P}(\alpha)$ representation.

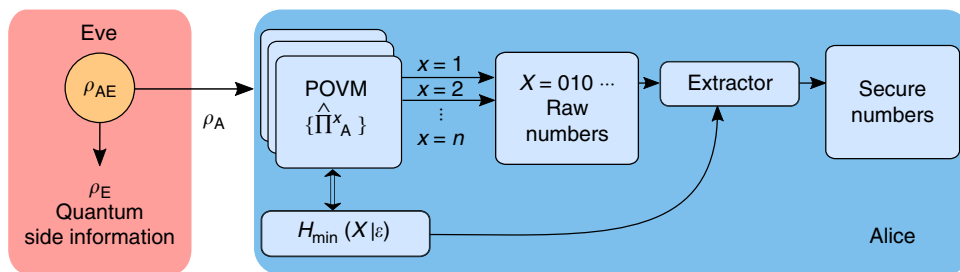


Fig. 1 Structure of the Source-DI protocol. In the general Source-DI scenario, Eve prepares the state ρ_A that she sends to Alice such that her purification gives her the maximal guessing probability on Alice’s outcome. The structure of the POVM chosen by Alice to measure ρ_A already impose a lower bound on $H_{\min}(X|\mathcal{E})$, independently from the input state or the output of her measurement (see Proposition 1). This bound is used to calibrate an extractor that returns, at each round of the protocol, secure random bits when applied to Alice’s outcome

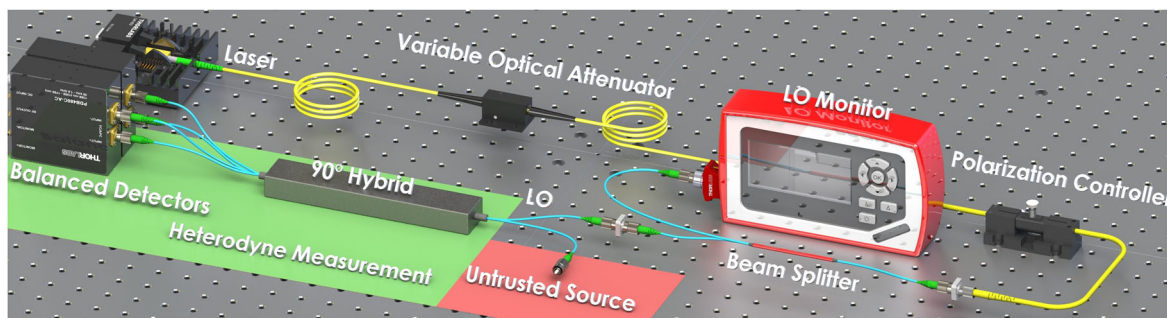


Fig. 2 Schematic representation of the experimental setup. The setup consists of a 1550 nm laser used as a LO, measured in real time. The heterodyne detection is performed by a 90° optical hybrid and a pair of balanced InGaS detectors. The VOA is used during the calibration phase. Only commercial off-the-shelf devices were used

The proofs of Proposition 1 and Corollary 1 are given in the Methods section. By using an heterodyne measurement scheme, a quantum tomography of the input state is also obtained³¹: although Alice generates the raw random numbers, she also reconstructs the state ρ_A . Then it is possible to evaluate numerically the quantum conditional min-entropy by using (6) and (7). Although for a qubit system, this problem was elegantly addressed by³², it is not of easy solution in the CV case. On the other hand, Corollary 1 gives an easy lower bound on $H_{\min}(X_\delta|\mathcal{E})$. Alice knows that even if Eve forges a state with an optimal \mathcal{E} , such side information will not let Eve guess the heterodyne outcome with a probability larger than $\frac{\delta_q \delta_p}{\pi}$. In the presence of an imperfect source of quantum states, this is the most conservative strategy to adopt, but ensures the generation of completely secure random numbers while avoiding a complex numerical maximization (a discussion about the robustness of the protocol against general attacks can be found in the Methods section). It is worth to note that the min-entropy of the random numbers is bounded by a function that depends on the measurement resolution only. The measurement, in this scenario, is under control of the user: Alice can readily obtain the min-entropy (8) by measuring δ_p and δ_q of her well characterized apparatus. The min-entropy is constant and Alice does not need to worry updating its value, as long as she trusts the apparatus. In the case of imperfect heterodyne measurement Proposition 1 can be still used: the characterization of the measurement apparatus allows to define what are the actual POVM $\tilde{\Pi}_{m,n}^\delta$ corresponding to such measurement. In Eq. (8) the ideal POVM $\hat{\Pi}_{m,n}^\delta$ should be replaced by the operators $\tilde{\Pi}_{m,n}^\delta$. The bound $\log_2 \frac{\pi}{\delta_q \delta_p}$ should be modified accordingly and its explicit value depends on the actual form of the operators $\tilde{\Pi}_{m,n}^\delta$.

It is worth noticing that in many cases such lower bound is (almost) tight: indeed, coherent and thermal states have positive Glauber–Sudarshan $\mathcal{P}(\alpha)$ function and for those states the bound $\log_2 \pi$ on the differential min-entropy is tight (the bound of the min-entropy is almost tight due to discretization). Moreover, in contrast to other Semi-DI QRNG where the min-entropy needs to be estimated in real time to provide security^{13,15,20}, in our protocol it depends on the structure of the heterodyne POVM and it is always constant. Hence, Alice can apply on X_δ a randomness extractor calibrated on $\log_2 \frac{\pi}{\delta_q \delta_p}$ and erase any guessing advantage of Eve.

Experimental implementation. The proposed new protocol has been implemented with an all-fiber setup at telecom wavelength with the scheme in Fig. 2; in this way is possible to exploit the availability of fast off-the-shelf components for classical telecommunication while keeping the setup compact. The heart of the

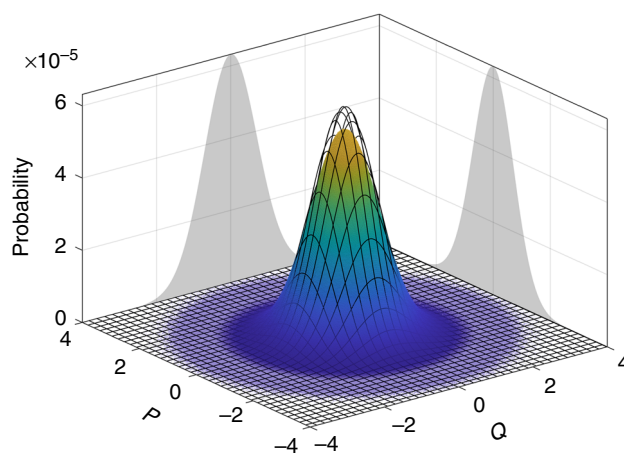


Fig. 3 Experimental state tomography. The plot shows the Husimi function for the vacuum (meshed curve) and the measured state (colored histogram). The projections refer to the experimental data. The measured variance is slightly larger than the one expected for the vacuum due to the electronic noise that widens the distribution

experiment lies in the heterodyne detection of the vacuum state, that samples the Q-function with the help of a coherent field $|\alpha\rangle$ of a Local Oscillator (LO). As we work in the Source-DI scenario, from the point of view of security, the quantum state measured can be fully controlled by Eve, because we do not assume anything about the source. After the heterodyne detection, a 10-bit analog-to-digital converter (ADC) digitizes two analog signals, each one proportional to one of the quadrature (q, p).

These signals directly sample the Q-function in the phase space, as shown in Fig. 3. The resolution of the ADC can be directly converted to the equivalent resolution in the phase space, thanks to the calibration function (for more info see Supplementary Note 1); in our case we obtained $\delta q = (14.05 \pm 0.02) \cdot 10^{-3}$ and $\delta p = (14.14 \pm 0.02) \cdot 10^{-3}$, respectively.

The raw data are then digitally filtered, taking only a 1.25 GHz window in the central part of the spectrum obtained by the detectors. In such way the classical noise that is coupled with the detector is filtered. Finally, the data are downsampled at 1.25 GSamples/s, matching the bandwidth of the signal and removing any correlation introduced by the oversampling.

We acquired $6 \cdot 10^{10}$ measurements obtaining $\sigma_q^2 = 0.55135 \pm 0.00001$ and $\sigma_p^2 = 0.56732 \pm 0.00001$. As it can be seen from Fig. 3, the measured Q-function is slightly larger than the one expected for a pure vacuum state, where both variances are expected to be equal to 1/2. The increase of the variances is due to classical noise of the detectors: in our approach such noise is regarded as a

“spreading” of the Q-function. Then, the effect of the electronic noise in reducing the generation rate is already included in our analysis for the quantum min-entropy. For more details see the Supplementary Notes 1 and 2.

The classical min-entropy $H_{\min}(X_\delta)$ corresponds to the larger probability of output and it is given by

$$H_{\min}(X_\delta) = 14.100. \tag{9}$$

However, the quantum min-entropy can be lower-bounded by Eq. (8). With the quadrature resolutions used for the experiment, we obtain

$$H_{\min}(X_\delta|\mathcal{E}) \geq 13.949, \tag{10}$$

for an equivalent secure generation rate of 17.42 Gbit/s. It is worth noticing that the high gain in security guaranteed by the conditional quantum min-entropy of Eq. (10) with respect to the classical min-entropy Eq. (9) implies a very small reduction of the generation rate (from 14.10 to 13.949 bits per sample). As said, such small reduction is experimentally owing to the electronic noise that slightly increases the quadrature variances with respect to the ideal value of 1/2. We also note that the generation rate can be improved by using an ADC with resolution larger than 10 bits.

In addition, these rates are not calculated in the asymptotic regime, i.e., in the limit of infinite repetitions of the protocol, but are valid for single-shot measurements. In fact, the conditional min-entropy $H_{\min}(X_\delta|\mathcal{E})$ is not estimated from the data, but it is bounded considering the structure of the POVM and the optimal strategy for the attacker, making it independent from the number of rounds of the protocol. Finally, a Toeplitz randomness extractor³³ is calibrated using $H_{\min}(X_\delta|\mathcal{E})$, and extracts the certified numbers from the raw data. As a final check, we applied a series of statistical tests from the DieHarder and NIST suite: all of them are successfully passed (see Supplementary Note 4).

Discussion

In this work, we demonstrated the versatility of heterodyne detection scheme for the generation of secure random numbers in a CV Source-DI framework, where no assumption on the source of quantum state is required. In fact, exploiting the properties of the POVM implemented by the heterodyne measurement, in Corollary 1 we obtained a direct lower bound to the conditional min-entropy, and hence on its security. This bound, also valid in the non-asymptotic regime, enables the user to erase all the side information related with an imperfect or malicious source of quantum states. Compared with previous Source-DI QRNGs^{6,12,15} this security is obtained without affecting the generation rate: in the previous protocols, part of the generated numbers were consumed to estimate and update the bound to the conditional min-entropy. In the protocol introduced here, the bound is constant, as it is determined by the resolution of the trusted measurement apparatus only. Hence, all the secure numbers are available to the user. Such simplification has many advantages for any practical implementation of the protocol. In particular, our protocol does not rely on external randomness to work, making it a standalone random number generator, whereas previous Semi-DI QRNG are based on randomness expansion protocols, that require either an initial seed or an external source of randomness to work.

Our approach allows to merge the speed of heterodyne measurements and the security of semi-DI protocols. Indeed, we realized the protocol with off-the-shelf components achieving, with an off-line post-processing, an equivalent rate of 17.42 Gbit/s,

Methods

Lower bound on the quantum conditional min-entropy. In this section, we give a proof of the proposition and the corollary that enable us to lower bound the quantum conditional min-entropy $H_{\min}(X|\mathcal{E})$.

Proposition 1. For any POVM, $\{\hat{\Pi}_x\}$ the quantum conditional min-entropy $H_{\min}(X|\mathcal{E})$ is lower-bounded by $H_{\text{low}} = -\max_{\{x, \tau_A \in \mathcal{H}_A\}} \log_2(\text{Tr}[\hat{\Pi}_x \tau_A])$.

Proof. Given a set of POVM $\{\hat{\Pi}_x\}$, the maximum over x in (7) is bounded by $\max_x \text{Tr}[\hat{\Pi}_x \tau_A^\alpha] \leq \max_{x, \tau_A} \text{Tr}[\hat{\Pi}_x \tau_A]$. Then Eq. (7) is upper bounded by:

$$\begin{aligned} P_{\text{guess}}(X|\mathcal{E})_{\min} &\leq \max_{\{x, \tau_A\}} \text{Tr}[\hat{\Pi}_x \tau_A] \max_{\{p(\beta), \tau_A\}} \int p(\beta) d\beta \\ &= \max_{\{x, \tau_A \in \mathcal{H}_A\}} \text{Tr}[\hat{\Pi}_x \tau_A] \end{aligned} \tag{11}$$

from which the bound on the min-entropy follows by using (6).

It is possible to specialize this result in the case of heterodyne detection, showing that the bound is always non-trivial:

Corollary 1. For the heterodyne measurement, the quantum conditional min-entropy $H_{\min}(X_\delta|\mathcal{E})$ is lower-bounded by $\log_2 \frac{\pi}{\delta_q \delta_p}$. The corresponding differential min-entropy $h_{\min}(X|\mathcal{E})$ is lower-bounded by $\log_2 \pi$. The bounds are tight, i.e., $h_{\min}(X|\mathcal{E}) = \log_2 \pi$ and $H_{\min}(X_\delta|\mathcal{E}) = \log_2 \frac{\pi}{\delta_q \delta_p} + O(\delta)$, for quantum state with positive Glauber–Sudarshan $\mathcal{P}(\alpha)$ representation.

Proof. It is well known that the Husimi function $Q_{\rho_A}(q + ip)$ is upper bounded by $\frac{1}{\pi}$. Then, $\forall \tau_A$, the following inequality holds:

$$\begin{aligned} \text{Tr}[\hat{\Pi}_{m,n}^\delta \tau_A] &= \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp Q_{\rho_A}(q + ip) \\ &\leq \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp \frac{1}{\pi} \\ &\leq \frac{\delta_q \delta_p}{\pi} \end{aligned} \tag{12}$$

By Proposition 1, it follows that $H_{\min}(X_\delta|\mathcal{E}) \geq \log_2 \frac{\pi}{\delta_q \delta_p}$. By the definition of differential quantum min-entropy as $h_{\min}(X|\mathcal{E}) = \lim_{\delta_p, \delta_q \rightarrow 0} [H_{\min}(X_\delta|\mathcal{E}) + \log_2 \delta_p \delta_q]$ it follows that $h_{\min}(X|\mathcal{E}) \geq \log_2 \pi$. To show the tightness, we note that any matrix ρ_A can be written as $\rho_A = \int \mathcal{P}(\alpha) |\alpha\rangle \langle \alpha| d^2 \alpha$ where $\mathcal{P}(\alpha)$ is the Glauber–Sudarshan P-function. If $\mathcal{P}(\alpha)$ is positive it can be interpreted as a probability density and the state ρ_A can be seen as an incoherent superposition of coherent states. For small δ_p and δ_q the guessing probability of Eq. (7) becomes

$$P_{\text{guess}}(X_\delta|\mathcal{E}) = \delta_q \delta_p \max_{\{p(\beta), \tau_A^\alpha\}} \int p(\beta) \max_{\alpha} Q_{\tau_A^\alpha}(\alpha) + O(\delta^3). \tag{13}$$

As coherent states maximize the value of the Husimi function $Q_{\tau_A^\alpha}(\alpha)$, then the optimal decomposition in (13) is precisely $\{\mathcal{P}(\alpha), |\alpha\rangle \langle \alpha|\}$ such that $P_{\text{guess}}(X_\delta|\mathcal{E}) = \frac{\delta_q \delta_p}{\pi} + O(\delta^3)$ and $H_{\min}(X_\delta|\mathcal{E}) = \log_2 \frac{\pi}{\delta_q \delta_p} + O(\delta)$. The differential quantum conditional min-entropy is then exactly $h_{\min}(X|\mathcal{E}) = \log_2 \pi$.

Security against coherent attacks. In the previous subsection we evaluated the quantum conditional min-entropy $H_{\min}^{(1)}(X|\mathcal{E})$ for a single run of the protocol. Usually this corresponds to consider security against only individual attacks. However, as we calculate the min-entropy on the worst state $\tau^{(1)}$ that is allowed by physics, this result holds also for coherent attacks. In this section, we will show it explicitly, by bounding the min-entropy for n runs of the protocol $H_{\min}^{(n)}(X|\mathcal{E})$ in terms of the min-entropy for a single run of the protocol $H_{\min}^{(1)}(X|\mathcal{E})$. When Eve performs a coherent attack, she can prepare a general n -partite state $\hat{\tau}^{(n)}$ to maximize her probability of guessing the n outcomes of Alice measurements, that can be written as

$$\hat{\Pi}_x \equiv \hat{\Pi}_{x_1} \otimes \hat{\Pi}_{x_2} \otimes \dots \otimes \hat{\Pi}_{x_n}. \tag{14}$$

The guessing probability of Eve for n runs of the protocol $P_{\text{guess}}^{(n)}(X|\mathcal{E})$ can be

written as

$$P_{\text{guess}}^{(n)}(X|\mathcal{E}) = \max_{\{x_i\}} \left[\max_{\tau^{(n)}} \text{Tr} \left[\left(\hat{\Pi}_{x_1} \otimes \cdots \otimes \hat{\Pi}_{x_n} \right) \tau^{(n)} \right] \right] \quad (15)$$

$$= \max_{\{x_i\}} \left[\max_{\tau_1} \text{Tr} \left[\hat{\Pi}_{x_1} \hat{\tau}_1 \right] \cdots \max_{\tau_n} \text{Tr} \left[\hat{\Pi}_{x_n} \hat{\tau}_n \right] \right] \quad (16)$$

$$= \prod_{i=1}^n \left(\max_{x_i, \tau_i} \text{Tr} \left[\hat{\Pi}_{x_i} \hat{\tau}_i \right] \right) \quad (17)$$

$$= \left[P_{\text{guess}}^{(1)}(X|\mathcal{E}) \right]^n \quad (18)$$

where $P_{\text{guess}}^{(1)}(X|\mathcal{E})$ is the guessing probability for one run of the protocol, derived in the main text. In the above equations the state $\tau^{(n)}$ is a generic n -partite state, whereas τ_i are generic single-party states. The crucial step is going from Eqs. (15) and (16). The argument of the outer maximization in Eq. (15) is given by $\max_{\tau^{(n)}} \text{Tr} \left[\hat{\Pi}_x \tau^{(n)} \right]$ and corresponds to the maximum eigenvalue of the operator $\hat{\Pi}_x$. As $\hat{\Pi}_x$ is the product of Hermitian operators with non-negative eigenvalues, its maximum eigenvalue is equal to the product of their maximum eigenvalues, namely $\max_{\tau_1} \text{Tr} \left[\hat{\Pi}_{x_1} \hat{\tau}_1 \right] \cdots \max_{\tau_n} \text{Tr} \left[\hat{\Pi}_{x_n} \hat{\tau}_n \right]$. This means that Eve's optimal strategy is to generate a n -mode separable state $\tau^{(n)} = \tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_n$.

Therefore, the min-entropy for n runs of the protocol $H_{\text{min}}^{(n)}(X|\mathcal{E})$ can be written as:

$$\begin{aligned} H_{\text{min}}^{(n)}(X|\mathcal{E}) &= -\log_2 P_{\text{guess}}^{(n)}(X|\mathcal{E}) \\ &= -\log_2 \left[\left(P_{\text{guess}}^{(1)}(X|\mathcal{E}) \right)^n \right] \\ &= n H_{\text{min}}^{(1)}(X|\mathcal{E}). \end{aligned} \quad (19)$$

Hence, our bound on the min-entropy is valid not only in the single-shot regime, but also for n repetitions of the protocol and coherent attacks.

Experimental details. We employed a narrow linewidth ECL laser at 1550 nm (Thorlabs SFL1550) followed by an electronically controlled variable optical attenuator and an in-line polarization controller. In this way, we were able to finely control the intensity and the polarization of our LO, besides making the calibration procedure automatized. Before entering the heterodyne measurement, 10% of the LO is sent to a photodetector, for a continuous monitor of its intensity. In such way, any anomaly to the normal functioning of the LO can be noticed in real time, and deviations can be compensated during the post-processing. The optical heterodyne was realized with a commercial fiber integrated "90 degree hybrid": one port is coupled to the LO while from the other is entering the vacuum state. The 90 degree hybrid mixes the signal with the LO and returns two pairs of outputs, featuring a $\pi/2$ phase shift. These optical signals, detected by a couple of high-bandwidth balanced detectors (1.6 GHz Thorlabs-PDB480C), are proportional to the quadratures of the signal, q and p . We sampled both signals coming from the detectors using a fast oscilloscope with 10 bits of resolution (LeCroy HDO 9404). The oscilloscope operated in burst mode, acquiring the analog signal at 10 GSps until the entire memory was completely filled. Then, the data are streamed to the computer via an Ethernet connection where it was post-processed. However, by using high resolution ADC and high throughput FPGA for real time processing, multi GBps real time extraction has been shown³⁴.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 22 February 2018 Accepted: 31 October 2018

Published online: 18 December 2018

References

1. Acn, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213 (2016).
2. König, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**, 4337–4347 (2009).
3. Rarity, J., Owens, P. & Tapster, P. Quantum random-number generation and key sharing. *J. Mod. Opt.* **41**, 2435–2444 (1994).
4. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598 (2000).

5. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
6. Vallone, G., Marangon, D. G., Tomasin, M. & Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A* **90**, 052327 (2014).
7. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
8. Christensen, B. G. et al. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
9. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).
10. Liu, Y. et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **120**, 010503 (2018).
11. Gómez, S. et al. Experimental nonlocality-based randomness generation with non-projective measurements. *Physical Review A* **97.4**, 040102 (2018).
12. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *NPJ Quantum Inf.* **2**, 16021 (2016).
13. Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
14. Cañas, G. et al. Experimental quantum randomness generation invulnerable to the detection loophole. Preprint at <https://arxiv.org/abs/1410.3443> (2014).
15. Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* **118**, 060503 (2017).
16. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016).
17. Xu, F., Shapiro, J. H. & Wong, F. N. C. Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring. *Optica* **3**, 1266–1269 (2016).
18. Cao, Z., Zhou, H. & Ma, X. Loss-tolerant measurement-device-independent quantum random number generation. *New J. Phys.* **17**, 125011 (2015).
19. Himbeek, T. V., Woodhead, E., Cerf, N. J., García-Patrón, R. & Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Quantum* **1**, 33 (2017).
20. Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).
21. Gabriel, C. et al. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **4**, 711–715 (2010).
22. Rehacek, J., Teo, Y. S., Hradil, Z. & Wallentowitz, S. Surmounting intrinsic quantum-measurement uncertainties in Gaussian-state tomography with quadrature squeezing. *Sci. Rep.* **5**, 12289 (2015).
23. Müller, C. R. et al. Evading vacuum noise: wigner projections or husimi samples? *Phys. Rev. Lett.* **117**, 070801 (2016).
24. Arthurs, E. & Kelly, J. L. On the simultaneous measurement of a pair of conjugate observables. *Bell Syst. Tech. J.* **44**, 725–729 (1965).
25. Walker, N. G. Quantum theory of multipoint optical homodyning. *J. Mod. Opt.* **34**, 15–60 (1987).
26. Ma, X. et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).
27. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **06**, 1–127 (2008).
28. Furrer, F., Åberg, J. & Renner, R. Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.* **306**, 165–186 (2011).
29. Furrer, F., Berta, M., Tomamichel, M., Scholz, V. B. & Christandl, M. Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.* **55**, 122205 (2014).
30. Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**, 5524–5535 (2011).
31. Leonhardt, U. *Measuring the quantum state of light* Vol. 22 (Cambridge University Press, Cambridge, UK, 1997).
32. Fiorentino, M., Santori, C., Spillane, S., Beausoleil, R. & Munro, W. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75**, 032334 (2007).
33. Frauchiger, D., Renner, R. & Troyer, M. True randomness from realistic quantum devices. Preprint at <http://arxiv.org/abs/1311.4547> (2013).
34. Zheng, Z., Zhang, Y.-C., Huang, W., Yu, S. & Guo, H. 6 gbps real-time optical quantum random number generator based on vacuum fluctuation. Preprint at <https://arxiv.org/abs/1805.08935> (2018).

Acknowledgements

We thank R. Filip for fruitful discussions. CloudVeneto is acknowledged for the use of computing and storage facilities.

Author contributions

D.G.M., G.V. and P.V. conceived the work. M.A. and D.G.M. realized the experiment. M. A. and D.G.M. analyzed the data. M.A., D.G.M. and G.V. developed the security proof. G.V. and P.V. supervised the experiment. All authors discussed the results and contributed to the final manuscript.

Additional information

Supplementary Information accompanies this paper at <https://doi.org/10.1038/s41467-018-07585-0>.

Competing interests: The authors declare no competing interests.

Reprints and permission information is available online at <http://npg.nature.com/reprintsandpermissions/>

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2018