Supplementary of Source-independent quantum random number generator against detector blinding attacks

I. SI-QRNG protocol treating no-click events as vacua

In the main text, we provide our protocol that resists detector blinding attacks by treating no-click events as error events. Previous SI-QRNG protocols did not consider detector blinding attacks, so they used squashing models to mark the no-click event as a vacuum. Since the vacuum cannot carry information and will not reveal information, they discard no-click events without hesitation. We compare the random number generation rate of our protocol and this kind of protocol. The rate difference implies the security risks caused by the detector blinding attack. To avoid the influence of different squashing model choices and the inconsistency of security parameters under different security frameworks, we use the following protocol as the representative of previous SI-QRNGs.

I.1 Protocol description

State preparation. Alice prepares signals that allow the detector representing $|+\rangle$ to fire. She sends N signals and does not trust the quantum states she prepared. Virtual party Bob guesses that the outcomes of measuring signals in $\mathbb{X}$ basis are always $|+\rangle$.

Two-dimensional measurement. Alice randomly measures signals in basis $\mathbb{X}$ or $\mathbb{Z}$ with probability p_x and $p_z = 1-p_x$, respectively. The no-click events are discarded.

Post-processing. Alice only deals with the click events. In the $\mathbb{X}$ basis, the click events can be divided in two parts: n_x^c and n_x^e. n_x^c is the number of correct events that only the $|+\rangle$ detector fires. Other events, including double-click events and single-click events on the $|-\rangle$ detector, are considered as error results and counted into n_x^e. The error rate is $e_x = n_x^e/n_x$, where n_x is the number of click events in $\mathbb{X}$. In $\mathbb{Z}$ basis, we care only about the single click results n_z^s of all n_z click events. According to the uncertainty relation of entropy, the length of secret random numbers with ε_{sec}-secrecy is given by

$$\ell \geqslant n_z^s[q - h_d(\bar{\phi}_z)] - 2\log_2 \frac{3}{2\varepsilon_{\text{sec}}} - n_{seeds}, \tag{1}$$

where $\bar{\phi}_z = \frac{(e_x+\gamma(n_z,n_x,e_x,\epsilon_{rand}))\times n_z}{n_z^s}$ is the upper bound of the phase error rate in $\mathbb{Z}$ basis, h_d is the d-dimension Shannon entropy, and q is the incompatibility between two measurement bases. The active basis choice consumes some random seeds $n_{seeds} = Np_x \log_2 N$.

I.2 Simulation

In simulation, we assume that the states are coherent states. In the $\mathbb{X}$ basis, the gain of click events is $Q_x = 1-(1-p_d)^2 e^{-\mu\eta}$, where p_d is the dark count, μ is the intensity of light and η is the transmission efficiency. The number of click events is $n_x = Np_xQ_x$. The gain of error events is $Q_x^e = p_d + e_d(Q_x - p_d)$, where e_d is the misalignment error. The error rate is $e_x = Q_x^e/Q_x$.

In the $\mathbb{Z}$ basis, the gain of click events is also $Q_z = 1-(1-p_d)^2e^{-\mu\eta}$. The number of click events is $n_z = Np_zQ_z$. The gain of all single-click events is $Q_z^s = 2(1-p_d)e^{-\mu\eta/2} - 2(1-p_d)^2e^{-\mu\eta}$. The number of single-click events is $n_z^s = Np_zQ_z^s$.

II. Detailed experimental results

In Tab. I, II, III, IV and V we report the detailed results obtained in the experiment. In all the tables, we report the random number generation rate $R := \ell/N$, the number of time windows that Alice choose to measure in Z(X) basis $N_{Z(X)}$, the total number of click events in detector D_H (D_V) in the Z basis, the number of single click events in detector D_H (D_V) in the Z basis, the error rate in the X basis e_x and the upper bound of phase error rate in the Z basis $\bar{\phi}_z$.

Intensity μ	6.32	6.8	7.7	9.6	14.3	18.2
R	0.0531	0.0761	0.0907	0.1010	0.0509	0
N_Z	1064540311	1059470000	999500000	1009708496	99549664	999511985
N_X	532592	530089	500049	505161	500078	500063
Total D_H click in the Z basis	732490456	795307879	792392154	860099255	939175515	968019162
Total D_V click in the Z basis	722825567	750713996	748852702	835145639	919880879	954610805
Single D_H click in the Z basis	235037676	232246534	198791921	148663349	74850323	43486700
Single D_V click in the Z basis	225372787	187652651	155252469	123709733	55555687	30078343
e_x	10.11%	7.69%	5.74%	2.99%	1.10%	2.19%
$\overline{\phi}_z$	23.95%	19.96%	16.76%	11.65%	9.17%	31.49%

TABLE I: Experiment results obtained for various pulse intensities.

Channel loss (dB)	0	1	3	10
R	0.0979	0.0839	0	0
N_Z	1009530770	1149424997	999592872	1229842581
N_X	505067	575054	500083	615245
Total D_H click in the Z basis	826646616	844496091	576423481	143298859
Total D_V click in the Z basis	849768774	861501605	566073702	136472595
Single D_H click in the Z basis	130668741	211532227	249937412	127373092
Single D_V click in the Z basis	153790899	228537741	239587633	120546828
e_x	3.42%	6.91%	19.64%	78.55%
$\overline{\phi}_z$	12.68%	18.57%	40.78%	50%

TABLE II: Experiment results obtained for various channel losses with a fixed intensity.

Channel loss (dB)	0	1	3	10
R	0.220	0.319	0.387	0.171
N_Z	1009530770	1149424997	999592872	1229842581
N_X	505067	575054	500083	615245
Total D_H click in the Z basis	826646616	844496091	576423481	143298859
Total D_V click in the Z basis	849768774	861501605	566073702	136472595
Single D_H click in the Z basis	130668741	211532227	249937412	127373092
Single D_V click in the Z basis	153790899	228537741	239587633	120546828
e_x	0.41%	0.36%	1.01%	0.20%
$\overline{\phi}_z$	1.62%	1.02%	1.86%	0.32%

TABLE IV: Experiment results obtained for various channel losses with a fixed intensity, analysed for the protocol in supplementary.

Channel loss (dB)	1	3	10
R	0.0959	0.0938	0.0995
N_Z	999980222	1009494998	1009882327
N_X	500292	505052	505248
Total D_H click in the Z basis	850571844	822977603	828712721
Total D_V click in the Z basis	835192945	851910282	842746871
Single D_H click in the Z basis	140183635	128031450	137373945
Single D_V click in the Z basis	124804736	156964129	151408095
e_x	3.04%	3.58%	3.47%
$\overline{\phi}_z$	12.05%	13.24%	12.69%

TABLE III: Experiment results obtained for various channel losses with the optimal intensity.

R	0.103
N_Z	1015527087
N_X	508128
Total D_H click in the Z basis	854697340
Total D_V click in the Z basis	824303459
Single D_H click in the Z basis	160570766
Single D_V click in the Z basis	130176885
e_x	3.34%
$\overline{\phi}_z$	12.2%

TABLE V: Experimental results used for final random number generation.