Science Advances

AAAS

advances.sciencemag.org/cgi/content/full/3/11/e1701491/DC1

Supplementary Materials for

Provably secure and high-rate quantum key distribution with time-bin qudits

Nurul T. Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, Daniel J. Gauthier

Published 24 November 2017, *Sci. Adv.* **3**, e1701491 (2017)
DOI: 10.1126/sciadv.1701491

This PDF file includes:

SUPPLEMENTARY MATERIALS

section S1. Finite-key estimates for the experiment

The quantum key distribution (QKD) system described in the main text is based on the transmission of photonic wavepackets encoded in discrete time bins. The system uses the time basis (denoted by the label T and chosen with probability p_T) for key generation and the phase basis (denoted by the label F and chosen with probability $p_F = 1 - p_T$) for parameter estimation. In the time basis, a state corresponds to a sharply peaked wavepacket in one of the four temporal bins (also called time-bin states), where each time bin represents a distinct communication alphabet. In the phase basis, each wavepacket is randomly prepared in one of the four possible phase states with distinct phase coefficients given by the discrete Fourier transforms of the time states.

To overcome the so-called photon-number splitting attacks, the QKD system uses the decoy-state method to estimate how many of the detected wavepackets are due to single-photon transmissions. Our decoy-state method uses a set of three intensity values $K \coloneqq \{\mu_1, \mu_2, \mu_3\}$ (chosen with probabilities p_{μ_1}, p_{μ_2}, and $p_{\mu_3} := 1 - p_{\mu_1} - p_{\mu_2}$, respectively), where $\mu_1 > \mu_2 + \mu_3$ and $\mu_1 \geq \mu_2 \geq \mu_3 \geq 0$. An important feature of the decoy-state method is that, from the perspective of the eavesdropper, the final prepared state (*i.e.*, with the encoded bit value) appears the same to her regardless of the choice of intensity level (or equivalently, the average photon-number). Therefore, one can imagine an equivalent decoy-state protocol where Alice can send any n-photon state and the choice of intensity is decided after the measurement phase. In the following, we provide the analysis for the T basis; the same analysis applies to the F basis.

Consider the case whereby Alice encodes the states in the T basis and let $s_{T,n}$ be the number of detections observed by Bob given that Alice sent n-photon states. In this case, $\sum_{n=0}^{\infty} s_{T,n} = n_T$ is the total number of detections conditioned on Alice choosing the T basis. In the asymptotic limit, we expect $n_{T,k}$ events from n_T events to be assigned to the intensity k, that is,

$$n_{T,k} \to n_{T,k}^{*} = \sum_{n=0}^{\infty} p_{k|n} s_{T,n}, \ \forall k \in K$$

Here, $p_{k|n}$ is the conditional probability of choosing the intensity k given that Alice prepared a n-photon state. For finite sample sizes, using Hoeffding's inequality for independent events, $n_{T,k}$ satisfies

$$\left|n_{T,k}^{*} - n_{T,k}\right| \leq \delta(n_T, \beta)$$

with probability of at least $1 - 2\beta$, where $\delta(n_T, \beta) := \sqrt{n_T/2 \log(1/\beta)}$. Note that the deviation term $\delta(n_T, \beta)$ is the same for all values of k. These results allow us to establish relations between the asymptotic values and the observed decoy-state statistics (*i.e.*, n_{T,μ_1}, n_{T,μ_2} and n_{T,μ_3}). Moreover, the same relation can also be made for the expected number of errors and the observed number of errors. Let $v_{T,n}$ be the number of errors associated with $s_{T,n}$. In the asymptotic limit, we expect $m_{T,k}$ errors from m_T errors to be assigned to the intensity k, *i.e.*,

$$m_{T,k} \to m_{T,k}^{*} = \sum_{n=0}^{\infty} p_{k|n} v_{T,n}, \ \forall k \in K$$

Likewise, we have

$$\left|m_{T,k}^{*} - m_{T,k}\right| \leq \delta(m_T, \beta)$$

which holds with probability of at least $1 - 2\beta$. Putting everything together, we find that

$$n_{T,k}^{*} \leq n_{T,k} + \ \delta(n_T, \beta) =: \ n_{T,k}^{+}$$

$$n_{T,k}^{*} \geq n_{T,k} - \ \delta(n_T, \beta) =: \ n_{T,k}^{-} \qquad (1)$$

and

$$m_{T,k}^{*} \leq m_{T,k} + \ \delta(m_T, \beta) =: \ m_{T,k}^{+}$$

$$m^*_{T,k} \geq m_{T,k} - \delta(m_T, \beta) =: m^-_{T,k} \tag{2}$$

for all values of k. For the moment, we keep these relations aside; they will be needed later when we derive the bound on the secret key length.

To model the security of the QKD system, we consider a high dimensional ($d = 4$) QKD protocol with two mutually unbiased bases. Following standard security definitions (*38*), we say that the QKD protocol is ε-secure if it is both ε_{sec}-secret and ε_{cor}-correct. For the first condition, the protocol is called ε_{sec}-secret if the joint state of the output secret key (say on Alice's side) and the adversary's total quantum information is statistically indistinguishable from the ideal output state[1] except with some small probability ε_{sec}. For the second condition, the protocol is called ε_{cor}-correct if the output secret keys on Alice and Bob's sides are identical except with some small probability ε_{cor}.

The starting point of our security analysis is to ask how many secret bits can be extracted from Alice's raw key X given E (Eve's total information about the QKD system). To this end, we use the quantum leftover-hash lemma (*39*) to bound the secret key length (denoted by l), giving

$$l = \max_{\beta \in (0, \frac{\varepsilon_{sec}}{2})} \left\lfloor H_{min}^{\frac{\varepsilon_{sec}}{2} - \beta}(X|E) + 4\log_2 \beta - 2 \right\rfloor \tag{3}$$

where the left-hand term in the floor function is the smooth min-entropy of X given E (see Ref. (*40*) for more details). Then, by using the decomposition result for decoy-state method from Ref. (*27*) and the entropic uncertainty relations for qudits, the smooth min-entropy term is further bounded by

$$H_{min}^{\frac{\varepsilon_{sec}}{2} - \beta}(X|E) \geq 2\tilde{s}_{T,0} + \tilde{s}_{T,1}\left[c - h_2\left(\tilde{Q} + \xi\right) - \left(\tilde{Q} + \xi\right)\log_2 3\right] - leak_{EC} - \log_2 \frac{8}{\beta^4 \varepsilon_{cor}} \tag{4}$$

[1] The ideal output state is an output key which is uniformly random (in the key space) and completely independent of the adversary's total information.

where $leak_{EC}$ is the number of bits published in error correction, $c \coloneqq -\log_2 \max_{i,j} |\langle f_i | t_j \rangle|^2$, and

$$\tilde{Q} = \frac{\tilde{v}_{F,1}}{\tilde{s}_{F,1}},\ \xi \coloneqq \sqrt{\frac{(\tilde{s}_{T,1}+\tilde{s}_{F,1})(\tilde{s}_{F,1}+1)}{\tilde{s}_{T,1}(\tilde{s}_{F,1})^2} \log \frac{2}{\beta}} \tag{5}$$

In the main text, we define $\lambda^U \coloneqq \tilde{Q} + \xi$ and it can be shown that $H(\lambda^U) \coloneqq h_2(\tilde{Q} + \xi) - (\tilde{Q} + \xi)\log_2 3$.

The decoy-state estimates for the *T* basis (replace the statistical quantities accordingly for the *F* basis) are found in Ref. (*27*) and are given by

$$\tilde{s}_{\mathrm{T},0} \coloneqq \max\left\{\left\lfloor \frac{\tau_0}{\mu_2 - \mu_3}\left(\frac{\mu_2 e^{\mu_3} n^-_{\mathrm{T},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^+_{\mathrm{T},\mu_2}}{p_{\mu_2}}\right)\right\rfloor, 0\right\}, \quad \tau_n \coloneqq \sum_{k\in K} e^{-k}\frac{k^n p_k}{n!} \tag{6}$$

$$\tilde{s}_{\mathrm{T},1} \coloneqq \max\left\{\frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3)-(\mu_2^2-\mu_3^2)}\left[\frac{e^{\mu_2} n^-_{\mathrm{T},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^+_{\mathrm{T},\mu_3}}{p_{\mu_3}} + \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(\frac{\tilde{s}_{\mathrm{T},0}}{\tau_0} - \frac{e^{\mu_1} n^+_{\mathrm{T},\mu_1}}{p_{\mu_1}}\right)\right], 0\right\} \tag{7}$$

and

$$\tilde{v}_{\mathrm{F},1} = \frac{\tau_1}{\mu_2 - \mu_3}\left(\frac{e^{\mu_2} m^+_{\mathrm{F},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} m^-_{\mathrm{F},\mu_3}}{p_{\mu_3}}\right) \tag{8}$$

Inserting Eq. (4) into Eq. (3), the protocol is able generate an ε_{sec}-secret key of length satisfying

$$l = \max_{\beta\in(0,\frac{\varepsilon_{sec}}{22})} \left\lfloor 2\tilde{s}_{\mathrm{T},0} + \tilde{s}_{\mathrm{T},1}\left[c - h_2(\tilde{Q}+\xi) - (\tilde{Q}+\xi)\log_2 3\right] - leak_{EC} - \log_2 \frac{32}{\beta^8 \varepsilon_{cor}} \right\rfloor$$

section S2. Secret key rate simulation

To simulate the secret key rate, we assume that the quantum channel is described by a loss η_{ch} and that that all detectors used for temporal and phase measurements have an input photon rate-dependent efficiency η_d. The efficiency of the detectors increases as the photon flux decreases. This is discussed in detail in the next section. Thus, the overall system transmittance can be written as $\eta = \eta_{ch}\eta_d$.

The total number of detection events observed in Bob's temporal basis for a given μ_k can be written as

$$n_{T,k} = p_{\mu_k} {p_T}^2 N(1 - e^{-\eta\mu_k} + P_d) \tag{10}$$

where N is the total number of signals transmitted by Alice during a secure communication session, and P_d is the probability of observing a dark count. Similarly, the number of detection events in the phase basis is given by

$$m_{F,k} = p_{\mu_k} {p_F}^2 N(1 - e^{-\eta\eta_i\mu_k} + 0.75P_d) \tag{11}$$

where η_i represents the reduced transmittance due to the insertion loss of the interferometers.

The error events in the temporal basis is given by

$$m_{T,k} = p_{\mu_k} {p_T}^2 N(e_d(1 - e^{-\eta\mu_k}) + 0.75P_d) \tag{12}$$

where e_d is error due to the misalignment, and can be mostly attributed to the finite extinction ratio of the intensity modulator. The coefficient of P_d is set to 3/4 because 75% of the dark count events will result in an incorrect alphabet. The corresponding error in the phase basis is given by

$$m_{F,k} = p_{\mu_k} {p_F}^2 N(e_d(1 - e^{-\eta\eta_i\mu_k}) + 0.75P_d) \tag{13}$$

Using Eqs. 10-13, we determine $\tilde{s}_{T,0}$ $\tilde{s}_{F,0}$, $\tilde{s}_{T,1}$, $\tilde{s}_{F,1}$, ξ and $\tilde{Q}$ and use them to determine l. In all our simulation presented in the main text, we assume $\beta = 1.72 \times 10^{-10}$, $\varepsilon_{cor} = 10^{-12}$, $P_d = 10^{-8}$, $N = 6.25 \times 10^{10}$.

section S3. Detector efficiency calibration

The efficiency of the superconducting nanowire single photon detector (SNSPD) decreases once the photon detection rate exceeds ~2 MHz. We characterize this change in efficiency using two methods. First, we use a continuous wave laser and attenuate the light to the single-photon level and measure the detection rate. From the detection rate and expected count rate, we calculate efficiency as a function of expected count rate. The blue line in fig. S1 shows the efficiency for one of the SNSPD pixels used in the experiment.

Second, we measure the efficiency of the detector with a pulsed source identical to that used in the QKD experiment shown by the red line in fig. S1. It is seen that the two methods are in good agreement with each other and the detection efficiency drops sharply as the rate increases beyond a few MHz, resulting in decreased performance of our QKD system. This also explains why we use four detectors in parallel for measuring the time-basis state, whose rate is higher than the phase-basis measurement system because of the asymmetric basis choice probability.

To account for the rate-dependent detection efficiency in our simulations, we fit the data shown in fig. S1 with a hyperbolic tangent function $a\tanh x/d + c$. We then use this function to determine $n_{T,k}$ and $n_{F,k}$. The expected rate is given by

$$R_{exp} = 625\text{MHz} \sum_{k=1}^{3} p_{\mu_k}(1 - e^{-\eta_{ch}\mu_k}) \tag{14}$$

where the first term on the right-hand side is the state preparation rate.

section S4. Numerically optimized secret key rate

In the simulation presented in the main text, we use experimentally determined system parameters to calculate the expected secret key rate. Here, we show the secret key rates that can be achieved in an improved system where the intrinsic error rate in the time and phase bases are decreased to 1% and 2%, respectively, and the efficiency is increased to 80% for all detectors (their nominal efficiency at low count rates). We also optimize the secret key rate over the probability of sending of time and phase basis, and the signal and decoy intensities, $\{\mu_1, \mu_2\}$ and set $\mu_3 = 0$.

The optimized secret key rate for $N = 6.25 \times 10^9$ and $N = 6.25 \times 10^{10}$ are shown in fig. S2A. As expected, we observe that a non-zero secret key can be generated at longer distances for larger N. In this case, for $N = 6.25 \times 10^{10}$, the secret key rate drops at a loss greater than 35 dB, which corresponds to a 175 km in standard fiber with a loss coefficient 0.2 dB/km. Figure S2B shows the optimized parameters p_T, μ_1, μ_2 as a function of distance. For relatively short distance ($<$ 20 dB), all the optimized quantities are relatively constant.

section S5. Experimental parameters

Based on the optimized parameters, we choose to randomly direct 90% of the incoming states to temporal basis and 10% to phase basis, and set μ_1 and μ_2 to 0.66 and 0.16, respectively, for all channel losses, except for a channel loss of 4 dB where we set it to 0.45 and 0.12, respectively. The reason for setting lower mean photon numbers at 4 dB is that there are spurious events due to ringing of the read-out electronics that occur between the detector pulses. These events cause errors when the event threshold is kept constant, and we minimize the effect of these events using a read-out voltage threshold equal to ~90% of the peak voltage for all detectors. However, this method fails at the extremely high detection rates for the 4 dB channel loss, and therefore we lower μ_1 for this case. We also estimate that μ_3 = 0.002 for all losses, mainly due to finite extinction ratio of the intensity modulators.

The experimentally determined sifted counts and the corresponding error rates for all channel losses observed during 100 seconds of data collection are presented in table SI, where we denote the error rates in time (phase) basis corresponding to mean photon number μ_k as $e_{T,k}$ ($e_{F,k}$).

section S6. Generation of the phase states

The phase states used in this experiment, illustrated in fig. S3, have a repeated pattern, which simplifies their generation. The phase between successive peaks of $|f_1\rangle$ increases in steps of π/2. Similarly, the phase difference between successive peaks in $|f_2\rangle$ and $|f_3\rangle$ are π and 3π/2, respectively.

To create these phases, we combine three independent, equal-amplitude signals from the FPGA as shown in fig. S4A. As an example, to create the state $|f_1\rangle$ the signal going into amplifier 1 (Amp1) is set to ‘on’ (high) between time bins 2 and 4. Similarly, the signal going into Amp2 is set to ‘on’ between time bins 3 and 4, and the signal going into Amp.3 is ‘on’ only during time bin 4. The combined signal at the output of the 3x1 combiner is a step-like function, where each

step corresponds to a π/2 phase shift. When this signal temporally overlaps with the four-peaked wavepacket from the intensity modulator, it creates the phase state $|f_1\rangle$. The states $|f_2\rangle$ and $|f_3\rangle$ are generated in a similar way as shown in fig. S4B. Conveniently, the step-like signal required to create $|f_3\rangle$ is just the inverse of the signal required to create $|f_1\rangle$.

In principle, the setup can be simplified and only one amplifier can be placed after the combiner. However, we find that most variable-gain amplifiers cannot take the combined power of the signals and saturates.

table S1. Length of sifted data. Number of sifted events observed during 100 seconds of data collection, and the corresponding error rates for both time and phase states as a function of loss.

Loss (dB)	**4**	**8**	**10**	**14**	**16.6**
n_{T,μ_1}	3.13×10^9	1.98×10^9	1.21×10^9	5.63×10^8	2.49×10^8
n_{T,μ_2}	1.22×10^8	7.61×10^7	4.66×10^7	2.16×10^7	9.54×10^6
n_{T,μ_3}	1.58×10^7	7.15×10^6	4.46×10^6	1.67×10^6	5.83×10^5
n_{F,μ_1}	7.26×10^6	5.48×10^6	3.66×10^6	1.63×10^6	1.05×10^6
n_{F,μ_2}	4.97×10^5	3.69×10^5	2.45×10^5	1.10×10^5	4.58×10^4
n_{F,μ_3}	1.44×10^4	8.17×10^3	4.75×10^3	1.62×10^3	6.61×10^2
$e_{T,1}$	0.0447	0.0383	0.0373	0.0355	0.0336
$e_{T,2}$	0.0664	0.0521	0.0510	0.0450	0.0430
$e_{F,1}$	0.0478	0.0435	0.0402	0.0369	0.0485
$e_{F,2}$	0.0607	0.0498	0.0446	0.0488	0.0555

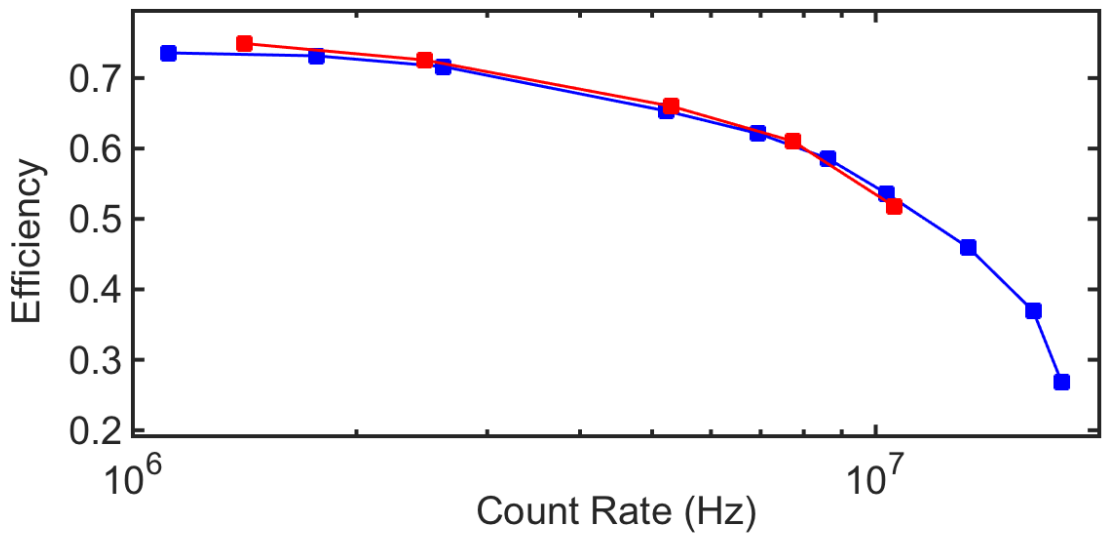

fig. S1. Efficiency of single-photon detectors. Experimentally determined efficiencies of a superconducting nanowire single-photon detector as a function of input count rate for a pulsed source (red) and a continuous-wave source (blue) at a wavelength of 1550 nm.

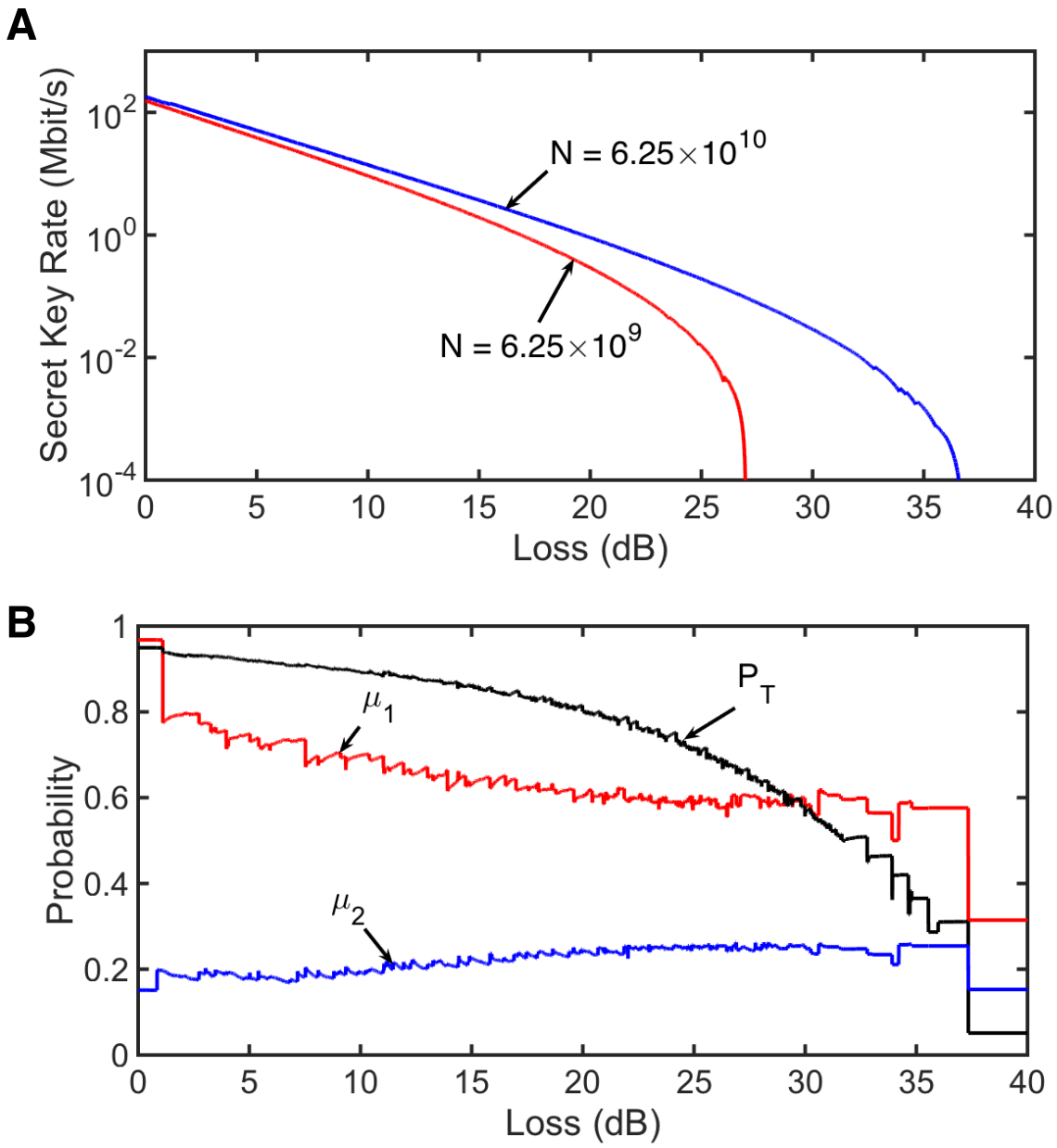

fig. S2. Numerical simulation. (**A**), Optimized secret key rate as a function of loss corresponding to $N = 6.25 \times 10^9$ (red) and $N = 6.25 \times 10^{10}$ (blue). (**B**), The optimized parameters p_T , μ_1 , and μ_2 for $N = 6.25 \times 10^{10}$ plotted as a function of quantum channel loss.

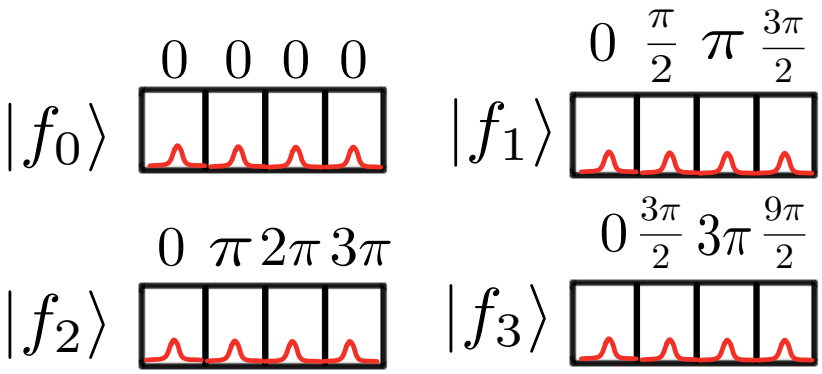

fig. S3. Graphical illustration of all phase states in *d* = 4. The phase values between successive time bins in the state $|f_1\rangle$ increases in steps of $\pi/2$. Correspondingly, the phase values between successive time bins in $|f_2\rangle$ ($|f_3\rangle$) increases in steps of π ($3\pi/2$).

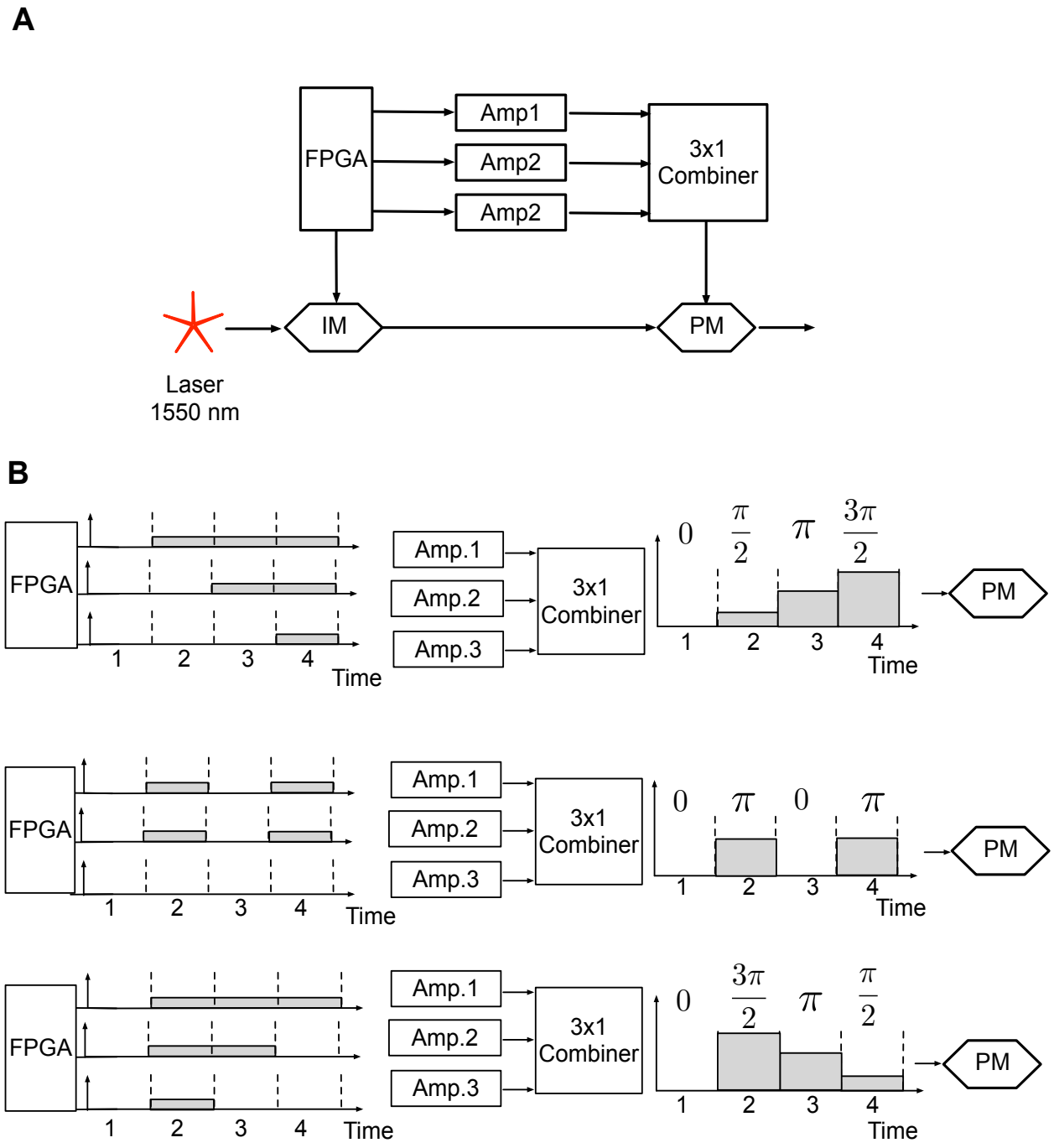

fig. S4. Generation of phase states. (**A**), Experimental setup used to create the phase states. (**B**), A detailed illustration of how the signals are combined to create the phase state $|f_1\rangle, |f_2\rangle$, and $|f_3\rangle$.