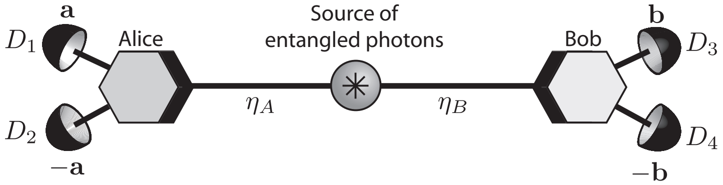
Supplementary Information

Supplementary Figures



Supplementary Figure S1. We consider a source of entangled photon pairs based on spontaneous parametric downconversion (SPDC). The distribution of the number of produced photon pairs per measurement time window follows Poisson statistics. The photons from each pair are coupled into two separate channels. Alice (Bob) then performs projective measurements described by the real Bloch vector $\pm\mathbf{a}$ ($\pm\mathbf{b}$) on her (his) photon. The two possible outcomes of Alice's measurement correspond to clicks at detectors D_1 and D_2, and at detectors D_3 and D_4 for Bob's measurement.

Supplementary Tables

Supplementary Table S1. Estimated experimental parameters. The estimated values of experimental parameters are shown. These estimations are based on previous characterizations of our source [26,19], as well as factory specified values of some of our optical components. All values except d_A and d_B have non-negligible uncertainty and are expressed in terms of their potential minimum and maximum values.

	Minimum value	Maximum value
μ	0.028	0.036
d_A	4×10^{-8}	4×10^{-8}
d_B	2.5×10^{-5}	2.5×10^{-5}
$\mathcal{V}$ (F)	0.96 (0.97)	0.98 (0.985)
η_A	5.35% (12.7 dB loss)	9.79% (10.1 dB loss)
η_B with 10 m link	0.302% (25.2 dB loss)	0.741% (21.3 dB loss)
η_B with 12.4 km link	0.0126% (34.8 dB loss)	0.0331% (30.9 dB loss)

Supplementary Table S2. Elements of M_η.

Transition from	to	Corresponding matrix element
(0000)	(0000)	$M_\eta(1,1) = (1-\eta_A)(1-\eta_B)$
(0000)	(0001)	$M_\eta(2,1) = \frac{1}{2}(1-\eta_A)\eta_B$
(0000)	(0010)	$M_\eta(3,1) = M_\eta(2,1)$
(0000)	(0100)	$M_\eta(5,1) = \frac{1}{2}\eta_A(1-\eta_B)$
(0000)	(0101)	$M_\eta(6,1) = \theta^+\eta_A\eta_B$
(0000)	(0110)	$M_\eta(7,1) = \theta^-\eta_A\eta_B$
(0000)	(1000)	$M_\eta(9,1) = M_\eta(5,1)$
(0000)	(1001)	$M_\eta(10,1) = M_\eta(7,1)$
(0000)	(1010)	$M_\eta(11,1) = M_\eta(6,1)$
(0001)	(0001)	$M_\eta(2,2) = \frac{1}{2}(1-\eta_A)(2-\eta_B)$
(0001)	(0011)	$M_\eta(4,2) = M_\eta(2,1)$
(0001)	(0101)	$M_\eta(6,2) = \eta_A[\theta^+ + \theta^-(1-\eta_B)]$
(0001)	(0111)	$M_\eta(8,2) = M_\eta(7,1)$
(0001)	(1001)	$M_\eta(10,2) = \eta_A[\theta^- + \theta^+(1-\eta_B)]$
(0001)	(1011)	$M_\eta(12,2) = M_\eta(6,1)$
(0010)	(0010)	$M_\eta(3,3) = M_\eta(2,2)$
(0010)	(0011)	$M_\eta(4,3) = M_\eta(2,1)$
(0010)	(0110)	$M_\eta(7,3) = M_\eta(10,2)$
(0010)	(0111)	$M_\eta(8,3) = M_\eta(6,1)$
(0010)	(1010)	$M_\eta(11,3) = M_\eta(6,2)$
(0010)	(1011)	$M_\eta(8,3) = M_\eta(7,1)$
(0011)	(0011)	$M_\eta(4,4) = 1-\eta_A$
(0011)	(0111)	$M_\eta(8,4) = \frac{1}{2}\eta_A$
(0011)	(1011)	$M_\eta(12,4) = M_\eta(8,4)$
(0100)	(0100)	$M_\eta(5,5) = \frac{1}{2}(2-\eta_A)(1-\eta_B)$
(0100)	(0101)	$M_\eta(6,5) = \eta_B[\theta^+ + \theta^-(1-\eta_A)]$
(0100)	(0110)	$M_\eta(7,5) = \eta_B[\theta^- + \theta^+(1-\eta_A)]$
(0100)	(1100)	$M_\eta(13,5) = \frac{1}{2}\eta_A(1-\eta_B)$
(0100)	(1101)	$M_\eta(14,5) = M_\eta(7,1)$
(0100)	(1101)	$M_\eta(15,5) = M_\eta(6,1)$
(0101)	(0101)	$M_\eta(6,6) = 1-\frac{1}{2}(\eta_A+\eta_B)+\theta^+(\eta_A+\eta_B)$
(0101)	(0111)	$M_\eta(8,6) = M_\eta(7,5)$
(0101)	(1101)	$M_\eta(14,6) = M_\eta(10,2)$
(0101)	(1111)	$M_\eta(16,6) = M_\eta(6,1)$

Supplementary Table S3. Elements of M_η (continuation of Supplementary Table S2).

Transition from	to	Corresponding matrix element
(0110)	(0110)	$M_\eta(7,7) = 1 - \frac{1}{2}(\eta_A + \eta_B) + \theta^-(\eta_A + \eta_B)$
(0110)	(0111)	$M_\eta(8,7) = M_\eta(6,5)$
(0110)	(1110)	$M_\eta(15,7) = M_\eta(6,2)$
(0110)	(1111)	$M_\eta(16,7) = M_\eta(7,1)$
(0111)	(0111)	$M_\eta(8,8) = \frac{1}{2}(2 - \eta_A)$
(0111)	(1111)	$M_\eta(16,8) = M_\eta(8,4)$
(1000)	(1000)	$M_\eta(9,9) = M_\eta(5,5)$
(1000)	(1001)	$M_\eta(10,9) = M_\eta(7,5)$
(1000)	(1010)	$M_\eta(11,9) = M_\eta(6,5)$
(1000)	(1100)	$M_\eta(13,9) = M_\eta(13,5)$
(1000)	(1101)	$M_\eta(14,9) = M_\eta(6,1)$
(1000)	(1110)	$M_\eta(15,9) = M_\eta(7,1)$
(1001)	(1001)	$M_\eta(10,10) = M_\eta(7,7)$
(1001)	(1011)	$M_\eta(12,10) = M_\eta(6,5)$
(1001)	(1101)	$M_\eta(14,10) = M_\eta(6,2)$
(1001)	(1111)	$M_\eta(16,10) = M_\eta(7,1)$
(1010)	(1010)	$M_\eta(11,11) = M_\eta(6,6)$
(1010)	(1011)	$M_\eta(12,11) = M_\eta(7,5)$
(1010)	(1110)	$M_\eta(15,11) = M_\eta(10,2)$
(1010)	(1111)	$M_\eta(16,11) = M_\eta(6,1)$
(1011)	(1011)	$M_\eta(12,12) = M_\eta(8,8)$
(1011)	(1111)	$M_\eta(16,12) = M_\eta(8,4)$
(1100)	(1100)	$M_\eta(13,13) = 1 - \eta_B$
(1100)	(1101)	$M_\eta(14,13) = \frac{1}{2}\eta_B$
(1100)	(1110)	$M_\eta(15,13) = M_\eta(14,13)$
(1101)	(1101)	$M_\eta(14,14) = \frac{1}{2}(2 - \eta_B)$
(1101)	(1111)	$M_\eta(16,14) = M_\eta(14,13)$
(1110)	(1110)	$M_\eta(15,15) = M_\eta(14,14)$
(1110)	(1111)	$M_\eta(16,15) = M_\eta(14,13)$
(1111)	(1111)	$M_\eta(16,16) = 1$

Supplementary Note 1. Modelling the detection statistics of a source of entanglement

To study how noise affects an entanglement-based implementation of our protocol, we developed a model of the detection statistics for a source of entangled photons taking into account loss, dark counts, multi-pair emissions and imperfect optical alignment. This is a generalization of previous work that modelled the detection statistics of a probabilistic source of (unentangled) photon pairs (see Ref. [27] of the main text). We consider a probabilistic source of photonic entanglement, such as one based on spontaneous parametric downconversion, as shown in Supplementary Figure S1.

To model the detection statistics of this experimental setup we construct a 16 × 1 column vector $\mathbf{P}$, as shown in Eq. (S1), that describes the joint state of the four detectors:

$$\mathbf{P} = \left(P_{0000}\ P_{0001}\ P_{0010}\ P_{0011}\ P_{0100}\ \ldots\ P_{1111}, \right)^{\mathrm{T}}. \tag{S1}$$

The enumeration of the indices of the elements of the state vector $\mathbf{P}$ follows the binary counting order, from '0000' to '1111', with the rightmost bit being the least significant. For example, the 11th element is labelled as P_{1010}. Each element of $\mathbf{P}$ describes the probability that a set of detectors clicked or not per measurement time window, which is defined as a window centred on a pump pulse and for which detections are considered for statistical analysis. We use the notation $(ijkl)$, where $i, j, k, l \in \{0, 1\}$, to describe the state of detectors D_1 through D_4, respectively. Hence, probability P_{ijkl} denotes the probability to find the detectors in state $ijkl$ after the measurement. For example, P_{0101} is the probability that detectors D_2 and D_4 clicked, and that D_1 and D_3 did not.

The goal is to determine how this state vector, initially described by $\mathbf{P}_0 = \left(1\ 0\ \ldots\ 0 \right)^{\mathrm{T}}$, is affected by single and multiple photon pair emissions, as well as detector dark counts, after one measurement time window. Photons from different pairs are assumed to be independent of each other and cannot, for example, bunch. This is the case when the source follows Poisson statistics as pairs are distinguishable in their emission time within the pump pulse duration. This condition is well satisfied by the source used in our experiment [27] as the coherence time of the photons, 0.27 ps, is much smaller than the pump pulse duration, 50 ps.

Transitions caused by entangled photon pairs

First, we describe the interaction of *one* entangled photon pair with the system. We assume the pair is emitted in a Werner state:

$$\rho = \mathcal{V}|\Phi^+\rangle\langle\Phi^+| + \frac{1-\mathcal{V}}{4}\mathbb{I}, \tag{S2}$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\mathcal{V} \in]0, 1]$ is called the intrinsic visibility of the state, and $\mathbb{I}$ is the 4 × 4 identity matrix. It is maximally entangled if and only if $\mathcal{V} = 1$. The fidelity of ρ with $|\Phi^+\rangle$ is given by $F = \langle\Phi^+|\rho|\Phi^+\rangle = \frac{3\mathcal{V}+1}{4}$.

Let us assume that Alice and Bob each perform their projective measurements described by real Bloch vectors $\pm\mathbf{a}$ and $\pm\mathbf{b}$, respectively. Hence, a click at detector D_1 (D_2) projects on the state corresponding to $\mathbf{a}$ ($-\mathbf{a}$). Similarly, a click at D_3 (D_4) corresponds to a projection on $\mathbf{b}$ ($-\mathbf{b}$). Let 2θ be the angle (on the Bloch sphere) between $\mathbf{a}$ and $\mathbf{b}$. Assuming the qubits do not decohere during transmission from the source to the detectors (this is a very good approximation for time-bin entangled qubits), then the probability for a given pair to create a two-fold coincidence between D_1 and D_3 is given by $\theta^+\eta_A\eta_B$, where $\theta^+ = \frac{1}{4}(1+\mathcal{V}\cos\theta)$, and where η_A (η_B) denotes the overall transmission from the source (i.e., from the SPDC medium) to D_1 (D_3). Similarly, the two-fold coincidence probability between D_2 and D_4 is also $\theta^+\eta_A\eta_B$. Coincidences between D_1 and D_4, as well as between D_2 and D_3, each happen with a probability $\theta^-\eta_A\eta_B$, where $\theta^- = \frac{1}{4}(1-\mathcal{V}\cos\theta)$. Note that we are assuming that both of Alice's (Bob's) detectors are identical, and that transmissions η_A and η_B include all optical losses, fibre coupling losses, detector inefficiencies, spectral and temporal filtering losses.

To see how the state vector is affected by a single entangled pair, we construct a 16 × 16 matrix M_η such that its elements give the probabilities of the possible transitions, i.e. transitions from state $(ijkl)$ to $(i'j'k'l')$, where $i, j, k, l, i', j', k', l' \in \{0, 1\}$. Specifically, the matrix element of row 1 and column 1, $M_\eta(1,1)$, gives the probability to transit from state (0000) to (0000), that is, the probability that none of the photons are detected. This term is given by

$$M_\eta(1,1) = 2\theta^+(1-\eta_A)(1-\eta_B) + 2\theta^-(1-\eta_A)(1-\eta_B) = (1-\eta_A)(1-\eta_B). \tag{S3}$$

Similarly, element $M_\eta(2,1)$ give the probability to transit from (0000) to (0001), and is given by

$$M_\eta(2,1) = \theta^+(1-\eta_A)\eta_B + \theta^-(1-\eta_A)\eta_B = \frac{1}{2}(1-\eta_A)\eta_B. \tag{S4}$$

The rest of the matrix is constructed following the same physical reasoning. All elements above the diagonal of the matrix are equal to 0 as photons cannot make detectors "unclick". Furthermore, to conserve the total probability, each column of M_η sums to 1. The result of one pair interacting with the system is thus given by $M_\eta \mathbf{P}_0$. The matrix M_η is too large to be written explicitly here, but all the elements are written in supplementary Tables S2 and S3.

Second, we describe the interaction of i pairs created during the same measurement time window. Because the pairs are assumed to be independent of each other, the result is simply given by $(M_\eta)^i \mathbf{P}_0$.

Transitions caused dark counts

In addition to the absorption of a photon, thermal excitations can also cause detectors to click. These dark counts can be taken into account by constructing another matrix M_{dc}. Let d_A denote the dark count probability per measurement time window of D_1 and D_2 (we assume both of Alice's detectors are identical). Similarly, d_B denotes the dark count probability per measurement time window of D_3 and D_4. Let us first consider D_1 only. Following the same reasoning as before, the transition matrix due to dark counts is

$$M_{dc}^{(1)} = \begin{pmatrix} 1-d_A & 0 \\ d_A & 1 \end{pmatrix}. \tag{S5}$$

For D_2, we get $M_{dc}^{(2)} = M_{dc}^{(1)}$. The matrices for D_3 and D_4 are the same as D_1 but with d_A replaced by d_B.

Now, because dark counts happen independently on all detectors, the transition matrix of all four detectors is simply given by

$$M_{dc} = M_{dc}^{(1)} \otimes M_{dc}^{(2)} \otimes M_{dc}^{(3)} \otimes M_{dc}^{(4)}, \tag{S6}$$

where $\otimes$ is the Kronecker product of the matrices. Here again, M_{dc} is too large to be written explicitly, but it is trivial to construct.

Transitions caused by entangled photon pairs and dark counts

When the number of incident photons follows an arbitrary, known distribution, it is possible to calculate the final state vector $\mathbf{P}$ through

$$\mathbf{P} = M_{dc} \sum_{i=0}^{\infty} p_i (M_\eta)^i \mathbf{P}_0, \tag{S7}$$

where p_i is the probability that i photon pairs are incident per measurement time window. For a Poisson distribution, we have $p_i = \mathrm{e}^{-\mu}\mu^i/i!$, where μ is the mean number of photon pairs created per pump pulse. Note that all matrices commute, so the order in which they are applied does not matter. The construction of the matrices ensures that all elements of $\mathbf{P}$ are bounded individually between 0 and 1 and that the elements of $\mathbf{P}$ sum to 1, i.e. the total probability is conserved.

Supplementary Note 2. Application to our loss-tolerant quantum coin-flipping protocol

We now show how one can apply this model of the detection statistics to assess the performance of our quantum coin-flipping protocol in the presence of varying loss and with the fair states. We first discuss how one can calculate the intrinsic error probability P^* as well as the probability P_A (P_B) for a cheating Alice (Bob) to fix the outcome to the bit of her (his) liking. All these calculations neglect cases with more than one click at Alice's and/or at Bob's. This approximation is valid as the probability of such events is much smaller than the one of events with one click at Alice's and one at Bob's. Hence, neglecting multiple clicks in the simulation has no impact on the comparison with our experimental data.

Intrinsic error probability

Let us consider P^* first. When both Alice and Bob are honest, a mismatch can occur only when both Alice and Bob measure in the same basis, which happens with probability $\frac{1}{2}$. When this is the case, the state vector $\mathbf{P}$ is calculated using $\theta = 0$. Overall, P^* is given by

$$P^* = \frac{1}{2}\left(\frac{P_{0110} + P_{1001}}{P_{0110} + P_{1001} + P_{1010} + P_{0101}}\right). \tag{S8}$$

The two terms in the numerator correspond to a mismatch associated with a two-fold coincidence between one of Alice's detector and one of Bob's. To obtain the value of P^* per coin-flip instance, we normalize by the probability of an instance.

Error probabilities in the presence of a cheater

Let us now consider P_A. When Alice cheats, she succeeds in fixing the outcome of the coin-flip instance in two possible ways. She either declares a basis different from Bob's with probability $\frac{1}{2}$ and he is forced to accept her bit, or she declares the same basis as Bob, with probability $\frac{1}{2}$, and succeeds in fixing the bit with conditional probability P'_A, which is obtained from $\mathbf{P}$ using $\theta = \frac{\pi}{2} - \arccos(4/5)$. Specifically, we have

$$P_A = \frac{1}{2}\left(1 + P'_A\right) \tag{S9}$$

where

$$P'_A = \frac{P_{1010} + P_{0101}}{P_{1010} + P_{0101} + P_{0110} + P_{1001}}. \tag{S10}$$

When Bob cheats, he succeeds whenever he correctly identified Alice's bit by measuring in a basis satisfying $\theta = \arccos(4/5)$. Hence, probability P_B is given by

$$P_B = \frac{P_{1010} + P_{0101}}{P_{1010} + P_{0101} + P_{0110} + P_{1001}}. \tag{S11}$$

Using the calculated values of P_A and P_B, we can also calculate the lower bound

$$P_C^* = 2(1 - P_A)(1 - P_B) \tag{S12}$$

on the intrinsic error probability of any classical protocol for noisy coin flipping [22].

Supplementary Note 3. Estimation of the experimental parameters

We now detail our estimation of the experimental parameters μ, η_A, η_B, d_A, d_B and $\mathcal{V}$, where μ corresponds to the mean number of photon pairs created per pump pulse. This estimation is based on previous characterizations of our source [20,27] as well as factory specified values of some of our optical components. We obtained the values presented on Supplementary Table S1.

The loss over the 12.4 km link includes the optical loss of the fibre and the loss of all optical components [20]. It also includes additional loss caused by the temporal widening of the wave packets due to chromatic dispersion in the fibre. Indeed, the 5 nm spectral width of Bob's photons is sufficient to considerably widen the wavepackets. Considering that we used a 400 ps detection window, and that the jitter of Bob's detectors was equal to 200 ps, we calculated an additional loss of 2.3 dB. Globally, the 12.4 km link increases the loss by 9.6 dB.

Using these parameters, we can estimate the expected performance of our protocol. Specifically, using values of Supplementary Table S1 and eq. S8 through S12, we can produce lower and upper bounds for P^* and P_C^*, as shown on Fig. 4-a of the main text.

We can also produce another curve of P^* assuming slightly improved, but realistic, experimental parameters, as explained in the main text. The parameters are $\mu = 0.005$, $\eta_A = 9.79\%$, $d_A = 4\times10^{-8}$, $d_B = 10\ \text{Hz}\times400\ \text{ps} = 4\times10^{-9}$ and $F = 99.25\%$. To obtain this μ, one would have to lower the pump power by a approximately factor of 6 with respect to the value we used in our experiment. The improved value of d_B corresponds to the dark count probability per 400 ps of a free-running detector having a 10 Hz dark count rate. Finally, the improved value of F corresponds to an intrinsic visibility of $\mathcal{V} = 99\%$ and is achievable through better optical alignment. The expected value of P^* as a function of η_B is shown on Fig. 4-b in the main text.