Supplementary Information for "Enhancing quantum cryptography with quantum dot single-photon sources"

Mathieu Bozzio,[1, *] Michal Vyvlecka,[1, *] * Michael Cosacchi,[2] Cornelius Nawrath,[3] Tim Seidelmann,[2]
Juan C. Loredo,[1, 4] Simone L. Portalupi,[3] Vollrath M. Axt,[2] Peter Michler,[3] and Philip Walther[1, 4]

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), 1090 Vienna, Austria*
[2] *Theoretische Physik III, Universität Bayreuth, 95440 Bayreuth, Germany*
[3] *Institut für Halbleiteroptik und Funktionelle Grenzflächen (IHFG),*
Center for Integrated Quantum Science and Technology (IQST) and SCoPE,
University of Stuttgart, 70569 Stuttgart, Germany
[4] *Christian Doppler Laboratory for Photonic Quantum Computer,*
Faculty of Physics, University of Vienna, 1090 Vienna, Austria

Supplementary Note 1 details the theoretical framework used in our intra-cavity simulations of quantum dot dynamics. The brightness and correlation functions are derived, from which the emitted photon number populations $\{p_n\}$, used in our security analyses, are inferred. Supplementary Note 2 and Supplementary Note 3 show how the collection efficiencies and state encodings are modelled, both in the presence and absence of photon number coherence, for PDS and QDS, respectively. Supplementary Note 4 provides some high-level descriptions of the four main quantum primitives, and displays all results justifying the Main Text claims. Supplementary Note 5 briefly introduces mathematical tools required to understand the security analyses, namely semidefinite programs and Choi's theorem on completely positive maps. Supplementary Note 6 to Supplementary Note 10 provide the practical security analyses of all protocols, and the extensions to account for the presence of coherence in the QDS framework.

Note on security analyses: For all quantum primitives, we make the standard quantum-cryptographic assumption that a dishonest party can replace their lossy channel and detectors by ideal ones, as this only increases their power. Although we take into account experimental imperfections such as channel losses and detector dark counts, we perform all analyses in the asymptotic regime. Our results are designed to illustrate the claims of the Main Text for a handful of protocols, and not to provide a full analysis of quantum primitives with finite-size effects.

SUPPLEMENTARY NOTE 1. QUANTUM DOT DYNAMICS AND SIMULATIONS

A. Model and dynamical equation

We model a quantum-dot–cavity system (QDC) consisting of a laser-driven strongly-confined self-assembled semiconductor quantum dot (QD) coupled to a single-mode microcavity influenced by an environment of longitudinal acoustic phonons (Ph) by the Hamiltonian

$$H = H_{\mathrm{QDC}} + H_{\mathrm{Ph}}\,. \tag{1}$$

1. Two-level model

QDs can often be described as two-level systems, e.g. when one is dealing with trions in charged QDs or, when a circularly polarized laser excites degenerate excitons with vanishing fine-structure splitting [1]. The considered two-level system has an excited state $|X\rangle$ at energy $\hbar\omega_{\mathrm{X}}$ and the energy of the ground state $|G\rangle$ is chosen to be zero. Assuming that the cavity supports only a single mode with nearly resonant coupling to the two-level system, the Jaynes-Cummings Hamiltonian can be used. Denoting the frequency of the microcavity mode by ω_{C} and the coupling strength by $\hbar g$, the QDC Hamiltonian in a frame co-rotating with the laser frequency ω_{L} reads

$$H_{\mathrm{QDC}} = \hbar\Delta\omega_{\mathrm{XL}}|X\rangle\langle X| + \hbar\Delta\omega_{\mathrm{CL}}a^{\dagger}a + \hbar g\left(a\sigma^{\dagger} + a^{\dagger}\sigma\right) - \hbar\frac{f(t)}{2}\left(\sigma^{\dagger} + \sigma\right)\,. \tag{2}$$

[*] Both authors contributed equally.
mathieu.bozzio@univie.ac.at / michal.vyvlecka@univie.ac.at

$\Delta\omega_{\mathrm{XL}} = \omega_{\mathrm{X}} - \omega_{\mathrm{L}}$ is the exciton-laser detuning, $\Delta\omega_{\mathrm{CL}} = \omega_{\mathrm{C}} - \omega_{\mathrm{L}}$ is the cavity-laser detuning, a ($a^\dagger$) annihilates (creates) a cavity photon, $\sigma := |G\rangle\langle X|$ is the QD transition operator, and $f(t)$ is the real envelope of the driving laser. The cavity mode is assumed to be in resonance with the ground state-to-exciton transition, i.e. the cavity-exciton detuning $\Delta\omega_{\mathrm{CX}} = \omega_{\mathrm{C}} - \omega_{\mathrm{X}}$ is zero. We consider pulsed excitations with a train of Gaussian pulses, each of which has the form

$$f(t) = \frac{\mathcal{A}}{\sqrt{2\pi}\tau_{\mathrm{G}}} e^{-\frac{t^2}{2\tau_{\mathrm{G}}{}^2}} \tag{3}$$

with the pulse area $\mathcal{A}$ and width τ_{G}, which is connected to the full width at half maximum by $T_{\mathrm{FWHM}} = 2\sqrt{2\ln 2}\,\tau_{\mathrm{G}}$.

The QD interacts with an environment of longitudinal acoustic (LA) phonons. This interaction is modeled by the Hamiltonian [1–5]

$$H_{\mathrm{Ph}} = \hbar\sum_{\mathbf{q}} \omega_{\mathbf{q}} b^\dagger_{\mathbf{q}} b_{\mathbf{q}} + \hbar\sum_{\mathbf{q}} \left(\gamma^{\mathrm{X}}_{\mathbf{q}} b^\dagger_{\mathbf{q}} + \gamma^{\mathrm{X}*}_{\mathbf{q}} b_{\mathbf{q}}\right) |X\rangle\langle X| \,, \tag{4}$$

where $b_{\mathbf{q}}$ ($b^\dagger_{\mathbf{q}}$) annihilates (creates) a phonon of energy $\hbar\omega_{\mathbf{q}}$ in the mode $\mathbf{q}$. $\gamma^{\mathrm{X}}_{\mathbf{q}}$ is the coupling constant between the QD exciton and the LA phonons. It fully determines the phonon spectral density $J(\omega) = \sum_{\mathbf{q}} |\gamma_{\mathbf{q}}|^2 \delta(\omega - \omega_{\mathbf{q}})$. Assuming harmonic confinement and a linear dispersion $\omega_{\mathbf{q}} = c_s|\mathbf{q}|$ with sound velocity c_s, it becomes

$$J(\omega) = \frac{\omega^3}{4\pi^2\rho_D\hbar c_s^5}\left(D_e e^{-\omega^2 a_e^2/(4c_s^2)} - D_h e^{-\omega^2 a_h^2/(4c_s^2)}\right)^2 \,, \tag{5}$$

where we have considered deformation potential coupling which is usually the dominant coupling mechanism in the type of QDs considered here [4]. ρ_D is the density of the material, D_e (D_h) the electron (hole) deformation potential, and a_e (a_h) the electron (hole) confinement length. We use standard GaAs material parameters listed in [6, 7]. Assuming identical potentials for electrons and holes, the confinement ratio is fixed by the effective masses as $a_h = a_e/1.15$. The electron confinement length a_e as the only free parameter thus becomes a measure for the size of the QD. Choosing a_e between 3 nm and 5 nm has produced results in good agreement with experiment [8–10]. Indeed, both the confinement ratio and the electron confinement length can be considered as fitting parameters when modeling specific samples in experiment. Here, we choose $a_e = 3\,\mathrm{nm}$. Note that the electronic density matrix is affected by phonons only via the phonon spectral density $J(\omega)$. For QDs of any shape, it is always possible to obtain a spherical dot model, which generates the identical $J(\omega)$ [11]. Then, the smallest dimension of the nonspherical QD has the largest influence on the phonon coupling.

Furthermore, we account for the radiative decay of the QD exciton to the free field outside the cavity with rate γ and cavity losses with rate κ. Both processes are well approximated by a phenomenological Markovian description using Lindblad superoperators acting on a density matrix ρ

$$\mathcal{L}_{O,\Gamma}\rho = \Gamma\left(O\rho O^\dagger - \frac{1}{2}\left\{\rho, O^\dagger O\right\}_+\right) \,, \tag{6}$$

where Γ is the decay rate associated with a process described by the operator O. $\{A,B\}_+$ denotes the anti-commutator of operators A and B.

The system dynamics is described by the Liouville-von Neumann equation for the density matrix ρ.

$$\frac{\partial}{\partial t}\rho = -\frac{i}{\hbar}\{H,\rho\}_- + \mathcal{L}_{\sigma,\gamma}\rho + \mathcal{L}_{a,\kappa}\rho \tag{7}$$

with the commutator $\{\cdot,\cdot\}_-$.

2. *Three-level model*

Considering external driving by lasers with well defined linear polarization and again assuming that there is just a single nearly resonant cavity mode, one of the linearly polarized excitons is decoupled from the dynamics. Therefore, including the biexciton state $|B\rangle$ in this situation amounts to the addition of only one further electronic level. The QDC Hamiltonian becomes

$$H_{\mathrm{QDC}} = \hbar\Delta\omega_{\mathrm{XL}}|X\rangle\langle X| + (2\hbar\Delta\omega_{\mathrm{XL}} - E_{\mathrm{B}})|B\rangle\langle B| + \hbar\Delta\omega_{\mathrm{CL}} a^\dagger a + \hbar g\left(a\sigma^\dagger + a^\dagger\sigma\right) - \hbar\frac{f(t)}{2}\left(\sigma^\dagger + \sigma\right) \,, \tag{8}$$

Supplementary Table 1: Phyiscal parameters used in the simulations.

Quantum dot-cavity coupling	$\hbar g$	0.05 meV
Biexciton binding energy	E_B	4 meV
Radiative decay rate	γ	1 ns^{-1}
Cavity loss rate	κ	0.577 ps^{-1}
Temperature	T	4.2 K
Cavity-exciton detuning	$\hbar\Delta\omega_{CX}$	0 meV

where the biexciton binding energy E_B has been introduced. We assume a value of $E_\mathrm{B} = 4\,\mathrm{meV}$ (cf. Supplementary Table 1), which is large for typical QDs, but even if it may be hard to find a naturally grown QD with this value, it can be achieved by applying biaxial stress [12]. Having such a rather large value for E_B means that essentially all collected photons originate from the exciton-to-ground state transition. $\sigma := |G\rangle\langle X| + |X\rangle\langle B|$ now contains both transitions which are optically excited in the QD. The phonon coupling strength of the biexciton state is assumed to be twice the one of the single exciton, i.e.

$$H_\mathrm{Ph} = \hbar\sum_\mathbf{q} \omega_\mathbf{q} b^\dagger_\mathbf{q} b_\mathbf{q} + \hbar\sum_\mathbf{q}\left(\gamma^\mathrm{X}_\mathbf{q} b^\dagger_\mathbf{q} + \gamma^{\mathrm{X}*}_\mathbf{q} b_\mathbf{q}\right)\left(|X\rangle\langle X| + 2|B\rangle\langle B|\right)\ . \tag{9}$$

Finally, the biexciton is assumed to radiatively decay with twice the exciton decay rate γ. Therefore, the dynamical equation becomes

$$\frac{\partial}{\partial t}\rho = -\frac{i}{\hbar}\{H,\rho\}_- + \mathcal{L}_{|G\rangle\langle X|,\gamma}\rho + \mathcal{L}_{|X\rangle\langle B|,2\gamma}\rho + \mathcal{L}_{a,\kappa}\rho \tag{10}$$

3. *Method and parameters*

We employ a numerically exact iterative real-time path integral method to solve the Liouville-von Neumann equation for the QDC's reduced density matrix $\overline{\rho} := \mathrm{Tr}_\mathrm{Ph}[\rho]$, where the phonon subspace is traced out. Details of the method are explained in [7, 13, 14]. This path integral formalism is exact up to the time discretization and the memory truncation length. We call a solution numerically exact, when it does not change noticeably when making the discretization finer or the truncation length longer. All relevant system parameters used for the calculations are listed in Supplementary Table 1.

In the two-level model, we consider two different excitation conditions: (i) resonant π-pulse and (ii) off-resonant phonon-assisted excitation. In the former, the laser is on resonance with the exciton energy, i.e. $\Delta\omega_\mathrm{XL} = 0$ and the excitation pulse has the area $\mathcal{A} = \pi$. In the latter, the laser is detuned above the exciton energy by $\Delta\omega_\mathrm{XL} = -0.9\,\mathrm{meV}$ and the pulse has an area of $\mathcal{A} = 10\pi$.

In the three-level model, we only consider the two-photon resonant excitation of the biexciton state, i.e. $2\hbar\Delta\omega_\mathrm{XL} - E_\mathrm{B} = 0$. For every T_FWHM chosen for the simulation, first, the area $\mathcal{A}$ has to be found, for which the occupation of the biexciton state $|B\rangle$ is unity after the pulse. This calibration is done for a standalone QD, i.e. $g = 0$, and without any losses, i.e. $\gamma = \kappa = 0$.

B. Derivation of photon number populations p_n

1. *Correlation functions*

We calculate second-order two-time correlation functions

$$G^{(2)}(t,\tau) = \langle a^\dagger(t) a^\dagger(t+\tau) a(t+\tau) a(t)\rangle \tag{11}$$

to obtain the multiphoton component of the cavity state. First, we average over the entire pulse sequence to obtain a function of the delay time argument τ only:

$$G^{(2)}(\tau) := \lim_{T\to\infty} \frac{1}{T} \int_0^T dt\, G^{(2)}(t,\tau) \tag{12}$$

Then, we integrate the peak-like structure around $\tau = 0$, which corresponds to the amount of multiphoton contribution within a single pulse of the pulse train, and normalize it to the first uncorrelated side peak. This results in the probability $\mathcal{P}_2$ of having two or more photons during one pulse

$$\mathcal{P}_2 = \frac{\int_{-T_{\mathrm{Pulse}}/2}^{T_{\mathrm{Pulse}}/2} d\tau\, G^{(2)}(\tau)}{\int_{T_{\mathrm{Pulse}}/2}^{3T_{\mathrm{Pulse}}/2} d\tau\, G^{(2)}(\tau)}\,. \tag{13}$$

Here, T_{Pulse} is the separation of two subsequent pulse maxima within the excitation pulse train.

To estimate the probability to obtain three or more photons during one pulse, we evaluate the third-order three-time correlation function

$$G^{(3)}(t,\tau_1,\tau_2) = \langle a^\dagger(t)a^\dagger(t+\tau_1)a^\dagger(t+\tau_1+\tau_2)a(t+\tau_1+\tau_2)a(t+\tau_1)a(t)\rangle\,. \tag{14}$$

Again, it is averaged over the pulse sequence as

$$G^{(3)}(\tau_1,\tau_2) := \lim_{T\to\infty} \frac{1}{T} \int_0^T dt\, G^{(3)}(t,\tau_1,\tau_2)\,. \tag{15}$$

In close analogy to the case above, the probability $\mathcal{P}_3$ of three-photon (or more) coincidence within a single pulse is obtained as

$$\mathcal{P}_3 = \frac{\int_{-T_{\mathrm{Pulse}}/2}^{T_{\mathrm{Pulse}}/2} d\tau_1 \int_{-T_{\mathrm{Pulse}}/2}^{T_{\mathrm{Pulse}}/2} d\tau_2\, G^{(3)}(\tau_1,\tau_2)}{\int_{T_{\mathrm{Pulse}}/2}^{3T_{\mathrm{Pulse}}/2} d\tau_1 \int_{T_{\mathrm{Pulse}}/2}^{3T_{\mathrm{Pulse}}/2} d\tau_2\, G^{(3)}(\tau_1,\tau_2)}\,. \tag{16}$$

Both $G^{(2)}$ and $G^{(3)}$ are then calculated in a numerically exact way following [15]. Finally, note that we define the unnormalized brightness of the QD source as

$$\widetilde{\mathcal{B}} = \kappa \int_{t_0-T_{\mathrm{Pulse}}/2}^{t_0+T_{\mathrm{Pulse}}/2} dt\, \langle a^\dagger(t)a(t)\rangle\,, \tag{17}$$

where t_0 is the center time of the pulse.

2. *Population extraction*

To calculate the probabilities of n-photon emission, we used the following assumptions: $\mathcal{P}_{\geqslant 4} = 0$ for two-level systems and $\mathcal{P}_{\geqslant 3} = 0$ for three-level systems. These assumptions are based on n-photon generation probabilities which scale as $(\gamma T_{\mathrm{FWHM}})^{(n-1)}$ for two-level systems [16] and $(\gamma T_{\mathrm{FWHM}})^{2(n-1)}$ for three level systems [17]. Using the correlation functions derived in Eqs. (13) and (16), along with unnormalized brightness from Eq. (17), we inferred the emitted photon number populations $\{p_n\}$ as:

$$\begin{aligned} p_1 &= \widetilde{\mathcal{B}} - 2\mathcal{P}_2 - 3\mathcal{P}_3, \\ p_2 &= \mathcal{P}_2 - \mathcal{P}_3, \\ p_3 &= \mathcal{P}_3, \\ p_{\geqslant 4} &= 0 \\ p_0 &= 1 - p_1 - p_2 - p_3 - p_{\geqslant 4}. \end{aligned} \tag{18}$$

The normalized brightness can now be expressed as:

Supplementary Table 2: Optimal photon number populations derived from Eq. (18).

		RE	**LA-assisted excitation**	**TPE**
Pump pulse length	T_{FWHM}	3 ps	8 ps	12 ps
Pump pulse area	$\mathcal{A}$	π_{RE}	$10\pi_{\mathrm{RE}}$	$\pi_{\mathrm{TPE}} \approx 6.8\pi_{\mathrm{RE}}$
Normalized brightness	$\mathcal{B}$	0.9366	0.8399	0.9526
Single-photon purity	$\mathcal{P}$	0.9903	0.9785	0.9988
Single-photon population	p_1	0.9275	0.8219	0.9514
Two-photon population	p_2	0.0091	0.0180	0.0012
Three-photon population	p_3	10^{-8}	10^{-7}	0

$$\mathcal{B} = \sum_{n \geqslant 1} p_n. \tag{19}$$

The single-photon purity may now be written as:

$$\mathcal{P} = \frac{p_1}{\mathcal{B}}. \tag{20}$$

SUPPLEMENTARY NOTE 2. COLLECTION EFFICIENCY AND STATE ENCODING FOR POISSON-DISTRIBUTED SOURCES

A. With number coherence

Coherent states may be expressed as a Poisson-distributed superposition of photon number states:

$$|\alpha\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = \sum_{n=0}^{\infty} C_\alpha(n) |n\rangle, \tag{21}$$

where $\{|n\rangle\}$ denote the photon number states and α is the coherent state amplitude. Using either polarization, time-bin or path encoding, the two-mode coherent states in all protocols may be expressed as:

$$|\alpha_k\rangle = \left| e^{i\theta} \frac{\alpha}{\sqrt{2}} \right\rangle \otimes \left| e^{i(\theta+\phi_k)} \frac{\alpha}{\sqrt{2}} \right\rangle, \tag{22}$$

where $\theta = 0$ is a global phase and $\phi_k \in \{0, \frac{\pi}{2}, 2\pi, \frac{3\pi}{2}\}$ is the relative phase between the two modes, which can take one of four values depending on $k \in \{0, 1, 2, 3\}$. In quantum cryptography, a potential eavesdropper or adversary must access ϕ_k to unveil the information encoded in the states.

In a similar manner to [18, 19], we may only focus on the second mode which contains the relative phase ϕ_k, and thus rewrite these four encoded states as $|\widetilde{\alpha_k}\rangle = |e^{i\phi_k}\frac{\alpha}{\sqrt{2}}\rangle$, with $k \in \{0, 1, 2, 3\}$. To avoid truncating the infinite-dimensional Fock space in our state expressions, we notice that these four specific states may be expressed in a four-dimensional orthonormal basis $\{|b_i\rangle\}$ as:

$$\begin{aligned}
|\widetilde{\alpha_0}\rangle &= B_0\,|b_0\rangle + B_1\,|b_1\rangle + B_2\,|b_2\rangle + B_3\,|b_3\rangle \\
|\widetilde{\alpha_1}\rangle &= B_0\,|b_0\rangle + iB_1\,|b_1\rangle - B_2\,|b_2\rangle - iB_3\,|b_3\rangle \\
|\widetilde{\alpha_2}\rangle &= B_0\,|b_0\rangle - B_1\,|b_1\rangle + B_2\,|b_2\rangle - B_3\,|b_3\rangle \\
|\widetilde{\alpha_3}\rangle &= B_0\,|b_0\rangle - iB_1\,|b_1\rangle - B_2\,|b_2\rangle + iB_3\,|b_3\rangle
\end{aligned} \tag{23}$$

where

$$\begin{aligned}
B_0 &= \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}+\cos\frac{\alpha^2}{2}} \\
B_1 &= \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}+\sin\frac{\alpha^2}{2}} \\
B_2 &= \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}-\cos\frac{\alpha^2}{2}} \\
B_3 &= \frac{e^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}-\sin\frac{\alpha^2}{2}}
\end{aligned}$$

B. Without number coherence

Phase randomization scrambles the global phase reference from Eq. (22) by allowing θ to take values from $[0, 2\pi]$ uniformly at random instead of a single value. By considering the state $|e^{i\theta}\alpha\rangle$ and integrating over all possible values of θ, the adversary sees a classical mixture of Fock states given by [20]:

$$\frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}e^{i\theta}\rangle\,\langle\sqrt{\mu}e^{i\theta}|\,d\theta = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\,|n\rangle\,\langle n|\,, \tag{24}$$

where $\mu = |\alpha|^2$ is the average photon number, and $|n\rangle$ are the photon number states. As the coherent superpositions of number states vanish, the quantum-cryptographic security proofs may simply proceed according to the result of quantum non-demolition (QND) photon number measurements. If there is no photon in the state, then there is no information content. If there is 1 photon, then the qubit security proof may be applied. If there are more than 2 photons in the pulse, it is assumed that perfect cheating is possible.

One can therefore express the phase randomized states ρ_k in a 7-dimensional orthonormal basis $\{|v\rangle, |q_0\rangle, |q_1\rangle, |m_0\rangle, |m_1\rangle, |m_2\rangle, |m_3\rangle\}$, where $|v\rangle$ is the vacuum state, $|q_0\rangle$ and $|q_1\rangle$ span a qubit space, and $|m_i\rangle$ constitute the four orthogonal outcomes which materialize the four perfectly distinguishable states in the multiphoton subspace. Our four phase-randomized coherent states may then be written as the following density matrices :

$$\begin{aligned}
\rho_0 &= P_\mu(0)\,|v\rangle\langle v| + P_\mu(1)\,|+\rangle\langle +| + P_\mu(\geqslant 2)\,|m_0\rangle\langle m_0| \\
\rho_1 &= P_\mu(0)\,|v\rangle\langle v| + P_\mu(1)\,|+i\rangle\langle +i| + P_\mu(\geqslant 2)\,|m_1\rangle\langle m_1| \\
\rho_2 &= P_\mu(0)\,|v\rangle\langle v| + P_\mu(1)\,|-\rangle\langle -| + P_\mu(\geqslant 2)\,|m_2\rangle\langle m_2| \\
\rho_3 &= P_\mu(0)\,|v\rangle\langle v| + P_\mu(1)\,|-i\rangle\langle -i| + P_\mu(\geqslant 2)\,|m_3\rangle\langle m_3|,
\end{aligned} \tag{25}$$

where $P_\mu(n) = |C_\mu(n)|^2$, $\{|+\rangle, |+i\rangle, |-\rangle, |-i\rangle\}$ are the usual σ_x and σ_y eigenstates in the qubit space spanned by $|q_i\rangle$, and the Poisson distribution coefficients are given by

$$P_\mu(0) = e^{-\mu}, \quad P_\mu(1) = \mu e^{-\mu}, \quad P_\mu(\geqslant 2) = 1-(1+\mu)e^{-\mu}. \tag{26}$$

SUPPLEMENTARY NOTE 3. COLLECTION EFFICIENCY AND STATE ENCODING FOR QUANTUM DOTS

A. Preliminary definitions

Single photons are obtained by the action of the creation operator onto the vacuum. Beam splitters act linearly on creation operators, and leave the vacuum invariant. More precisely, a beam splitter of reflectivity r acting on input modes (k, l) maps the creation operators $\hat{a}_k^\dagger, \hat{a}_l^\dagger$ onto $\hat{b}_k^\dagger, \hat{b}_l^\dagger$ as:

$$\begin{pmatrix} \hat{b}_k^\dagger \\ \hat{b}_l^\dagger \end{pmatrix} = H_{kl}^{(r)} \begin{pmatrix} \hat{a}_k^\dagger \\ \hat{a}_l^\dagger \end{pmatrix}, \tag{27}$$

where

$$H_{kl}^{(r)} = \begin{pmatrix} \sqrt{r} & \sqrt{1-r} \\ \sqrt{1-r} & -\sqrt{r} \end{pmatrix}. \tag{28}$$

We similarly define the phase shift operation $P_{kl}^{(\phi)}$, acting on input modes (k, l), as:

$$P_{kl}^{(\phi)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \tag{29}$$

B. Collection and encoding with number coherence

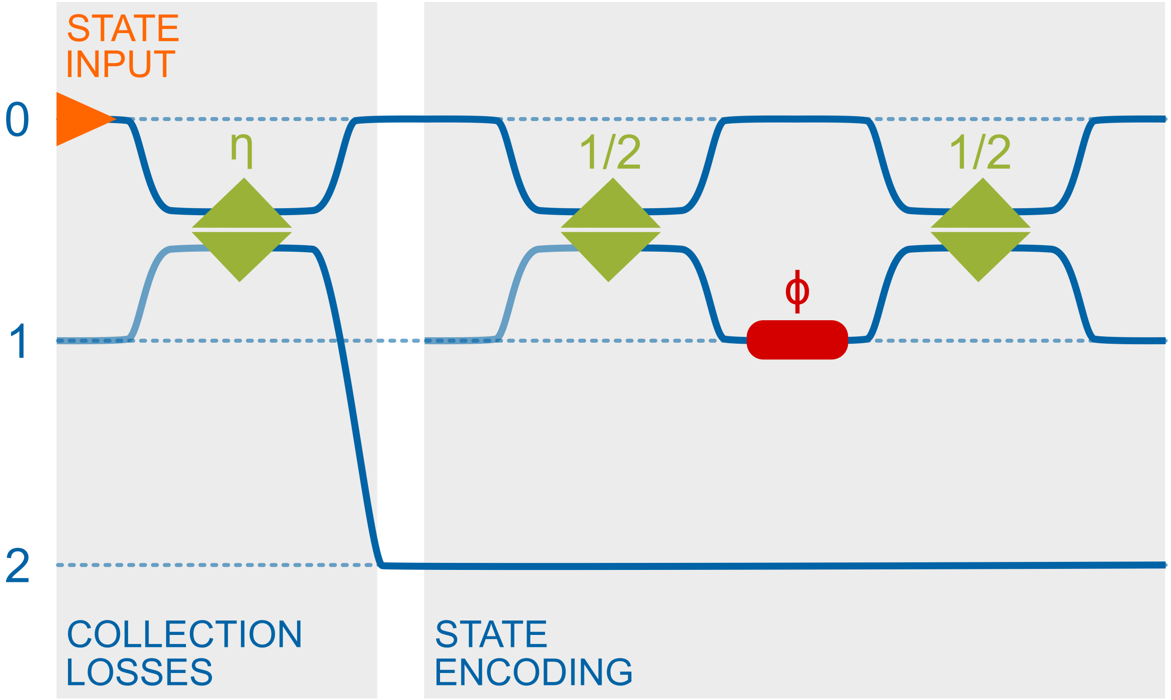
Following Supplementary Figure 1, we model the collection efficiency of the quantum dot as a beamsplitter of reflectivity η, and label the three input spatial modes as 0, 1 and 2. The standard four protocol states are then encoded with a Mach-Zehnder interferometer, consisting of two beamsplitters described by $H_{01}^{(r)}$, with tunable phase $\phi \in \{0, \pi\}$, corresponding to the Pauli Z eigenstates in a two-dimensional Hilbert space, and $\phi \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$, corresponding to the Pauli X eigenstates in a two-dimensional Hilbert space. A general pure photonic state, with photon number distribution given by $\{p_n\}$ and input into spatial mode 0, then evolves as:

$$\begin{aligned}
\sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(a_0^\dagger\right)^n |000\rangle_{012} &\xrightarrow{H_{01}^{(\eta)}} \sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(\sqrt{\eta} a_0^\dagger + \sqrt{1-\eta} a_2^\dagger\right)^n |000\rangle_{012} \\
&\xrightarrow{H_{01}^{(1/2)}} \sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(\sqrt{\frac{\eta}{2}} a_0^\dagger + \sqrt{\frac{\eta}{2}} a_1^\dagger + \sqrt{1-\eta} a_2^\dagger\right)^n |000\rangle_{012} \\
&\xrightarrow{P_{01}^{(\phi)}} \sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(\sqrt{\frac{\eta}{2}} a_0^\dagger + \sqrt{\frac{\eta}{2}} e^{i\phi} a_1^\dagger + \sqrt{1-\eta} a_2^\dagger\right)^n |000\rangle_{012} \\
&\xrightarrow{H_{01}^{(1/2)}} \sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(\sqrt{\frac{\eta}{4}} \left(1+e^{i\phi}\right) a_0^\dagger + \sqrt{\frac{\eta}{4}} \left(1-e^{i\phi}\right) a_1^\dagger + \sqrt{1-\eta} a_2^\dagger\right)^n |000\rangle_{012} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sqrt{\frac{p_n}{n!}} \binom{n}{k} \binom{k}{l} \left(\sqrt{\frac{\eta}{4}} \left(1+e^{i\phi}\right) a_0^\dagger\right)^{k-l} \left(\sqrt{\frac{\eta}{4}} \left(1-e^{i\phi}\right) a_1^\dagger\right)^{l} \left(\sqrt{1-\eta} a_2^\dagger\right)^{n-k} |000\rangle_{012} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sqrt{\frac{p_n}{n!}} \binom{n}{k} \binom{k}{l} \left(\frac{\eta}{4}\right)^{\frac{k}{2}} (1-\eta)^{\frac{n-k}{2}} \left(1+e^{i\phi}\right)^{k-l} \left(1-e^{i\phi}\right)^{l} \left(a_0^\dagger\right)^{k-l} \left(a_1^\dagger\right)^{l} \left(a_2^\dagger\right)^{n-k} |000\rangle_{012}
\end{aligned} \tag{30}$$

The encoded state then reads:

$$|\psi_{\eta,\phi}\rangle_{012} = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} c_{nkl}(\eta, \phi) \left(a_0^\dagger\right)^{k-l} \left(a_1^\dagger\right)^{l} \left(a_2^\dagger\right)^{n-k} |000\rangle_{012}, \tag{31}$$

where



Supplementary Figure 1: **Collection efficiency modeling and state encoding.** The collection efficiency of the quantum dot is modelled as a beamsplitter of reflection η, with two input spatial modes as 0 and 1. The quantum information is then encoded with a Mach-Zehnder interferometer, with tunable phase $\phi \in \{0, \pi\}$ for Z eigenstates and $\phi \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ for X eigenstates.

$$c_{nkl}(\eta, \phi) = \sqrt{\frac{p_n}{n!}} \binom{n}{k} \binom{k}{l} \left(\frac{\eta}{4}\right)^{\frac{k}{2}} (1-\eta)^{\frac{n-k}{2}} \left(1+e^{i\phi}\right)^{k-l} \left(1-e^{i\phi}\right)^{l}. \tag{32}$$

and $\{p_n\}$ take the values of Eq. (18) in our work.

To obtain the actual collected state $\rho^{(c)}_{\eta,\phi}$ used in our security analyses (where the (c) superscript denotes coherence in Fock basis for further convenience), we simply trace out over spatial mode 2:

$$\begin{aligned} \rho^{(c)}_{\eta,\phi} &= \mathrm{Tr}_2 \left(|\psi_{\eta,\phi}\rangle_{012} \langle\psi_{\eta,\phi}|_{012} \right) \\ &= \mathrm{Tr}_2 \left(\sum_{n,m=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sum_{p=0}^{m} \sum_{q=0}^{p} c_{nkl}(\eta,\phi) c^*_{mpq}(\eta,\phi) \left(a_0^\dagger\right)^{k-l} \left(a_1^\dagger\right)^{l} \left(a_2^\dagger\right)^{n-k} |000\rangle_{012} \langle 000|_{012}\, a_0^{p-q} a_1^q a_2^{m-p} \right). \end{aligned} \tag{33}$$

C. Collection and encoding without number coherence

Similar calculations lead to the expression for the collected state $\rho^{(nc)}_{\eta,\phi}$, where the superscript (nc) this time accounts for "no coherence" in Fock basis. In essence, we set $n = m$ in Eq. (33) and obtain the following state:

$$\rho^{(nc)}_{\eta,\phi} = \mathrm{Tr}_2 \left(\sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sum_{p=0}^{n} \sum_{q=0}^{p} c_{nkl}(\eta,\phi) c^*_{npq}(\eta,\phi) \left(a_0^\dagger\right)^{k-l} \left(a_1^\dagger\right)^{l} \left(a_2^\dagger\right)^{n-k} |000\rangle_{012} \langle 000|_{012}\, a_0^{p-q} a_1^q a_2^{n-p} \right). \tag{34}$$

SUPPLEMENTARY NOTE 4. QDS PERFORMANCE FOR QUANTUM PRIMITIVES

A. BB84 quantum key distribution

1. *Brief introduction*

Quantum key distribution (QKD) is one of the most mature quantum-cryptographic primitives implemented so far. In its simplest form, it allows two parties, Alice and Bob, to establish a secret key over a public quantum channel, provided that a public, authenticated classical channel is available. The parties must ensure that the unwanted presence of an eavesdropper, Eve, on the channel is detected with arbitrarily high probability. Once a secret key has successfully been established, Alice and Bob may use it to encrypt a secret message through one-time padding [21]. This encryption technique requires a secret key whose length is at least equal to the message length.

In a standard protocol, Alice encodes N bits of the secret key she wishes to share into N qubit states. She randomly picks the encoding basis for each qubit (σ_z or σ_x), and stores this classical information. Bit 0 is therefore randomly encoded in either $|0\rangle$ or $|+\rangle$, while bit 1 is randomly encoded in $|1\rangle$ or $|-\rangle$. The states are sent over a quantum channel to distant Bob, who does not know the encoding basis, and thus randomly measures each qubit in either σ_z or σ_x. He records each qubit's measurement basis, along with the associated measurement outcomes. Once the quantum communication stage is over, Alice and Bob proceed to a classical reconciliation stage: Bob communicates his sequence of measurement bases (without the measurement outcomes) to Alice. After comparing it with her stored sequence, Alice reports to Bob the elements for which her preparation basis does not match Bob's measurement basis. They both agree to dismiss all bits which correspond to a basis mismatch from the final key. After basis reconciliation, Alice and Bob then compare a pre-agreed random subset of their corrected key to ensure that all bits match. If any of the bits disagree, they may conclude on the presence of Eve and abort the protocol. If all bits agree, the key has then successfully been established, and they may use it to encrypt a secret message. Note that an additional stage, known as privacy amplification, is required in the noisy setting, in order to decrease the amount of information that Eve acquires from Alice and Bob's classical error correction routine [22].

2. *Results*

In order to compare the performance of all sources for BB84 QKD, we study the protocol with and without the decoy state countermeasure (see Supplementary Note 6 for details), assuming one-way classical post-processing [23]. Without decoy states, we plot the secure key rate per pulse as a function of source efficiency, collection efficiency, and distance in Supplementary Figure 2. We then display the performance of QDS pumping schemes for collection efficiencies ranging from 1% to 100% in Supplementary Figure 3, and compare these to the best performance of randomized-phase PDS. We then proceed to similar plots for BB84 QKD with decoy states, in Supplementary Figure 4 and Supplementary Figure 5. In general, the secure key rate as a function of source efficiency reaches a maximum for PDS, after which the multiphoton component becomes too significant. Regarding QDS, the key rate evolves almost linearly with source efficiency, since the vacuum and single photon components dominate at all source efficiencies.

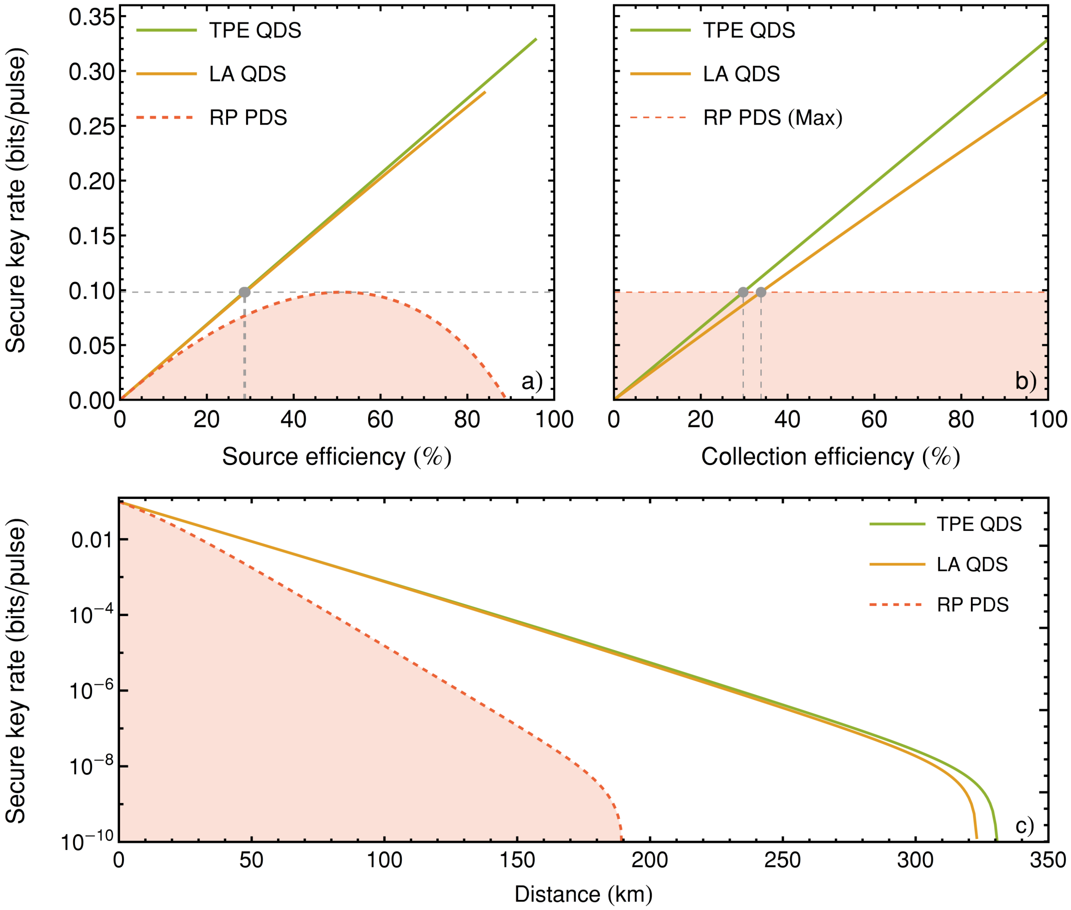
B. Twin-field quantum key distribution

1. *Brief introduction*

Twin-field QKD (TF-QKD) was proposed as a new protocol configuration to overcome the repeaterless rate-distance limit of standard QKD [24]. By delegating the measurement setup to a third untrusted party situated halfway between Alice and Bob, the optical fields sent by each party travel only half the communication distance of standard QKD. Since the key bits are extracted from the resulting single-photon interference at Charlie's station, the secure key rate scales with the square root of the channel transmittance instead of scaling linearly.

2. *Results*

In order to compare the performance of all sources for twin-field QKD, we plot the secure key rate from Eq. (54) as a function of source efficiency, collection efficiency, and distance in Supplementary Figure 6. We then display the



Supplementary Figure 2: **Source comparison for BB84 QKD without decoy states.** (a) Simulated secret key rates from Eq. (48) as a function of source efficiency for LA and TPE QDS, along with randomized-phase (RP) PDS. Source efficiency is defined as $1 - e^{-\mu}$ for PDS and $1 - \sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. (b) Simulated secret key rates as a function of QDS collection efficiency, compared to the best performance of RP PDS sources (dashed line). (c) Simulated secret key rates as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from Fig (b). Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

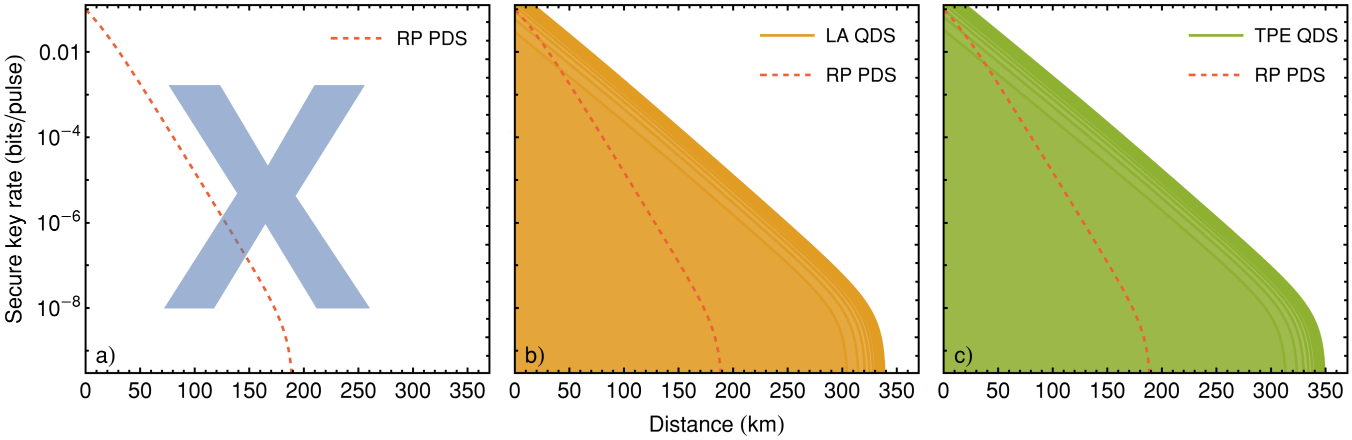
performance of QDS pumping schemes for collection efficiencies ranging from 1% to 100% in Supplementary Figure 7, and compare these to the best performance of randomized-phase PDS.

C. Unforgeable quantum tokens

1. *Brief introduction*

This primitive, in its private-key form, allows a central authority to issue tokens comprising of quantum states, whose unforgeability is intrinsically guaranteed by the no-cloning theorem. One famous application is quantum money, which can prevent banknote forgery [25], double-spending with credit cards [19, 26], and also guarantee features such as user privacy [27].

In a private-key scheme, the quantum state is encoded according to a secret pre-shared classical key, which is known by the central authority and the verifier(s) only. The key contains a sequence of secret information bits, as well as a



Supplementary Figure 3: **Collection efficiency comparison for BB84 QKD without decoy states.** Simulated secret key rates from Eq. (48) as a function of distance for (a) RE QDS (b) LA QDS (c) TPE QDS, with collection efficiencies ranging from $\eta = 1\%$ (bottom curves) to $\eta = 100\%$ (top curves), in steps of 10%. The optimal performance of randomized-phase (RP) PDS is also plotted in dashed lines, in order to identify which QDS collection efficiencies are required to overcome PDS for each pumping. Single mode telecom fiber losses of 0.21 dB/km are assumed. Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

sequence of secret basis bits, which indicate the random preparation basis of each information bit (the states used are the standard BB84 states from QKD). This ensures that a dishonest client willing to duplicate the money state will introduce errors in at least one of two states, due to no-cloning. Upon verification, these errors will be detected by the verifier(s), who measure(s) each sub-system of the money state in the correct basis and compares the measurement outcomes with the secret key.

There exist different forms of quantum token protocols, from private-key to public-key, with quantum verification [25] or classical verification [19]. Some schemes require quantum storage [26, 28], while others replace this requirement with no-signalling constraints [27]. Here, we focus on private-key quantum token schemes with quantum verification that assume quantum storage, which can provide information-theoretic security for unforgeability.

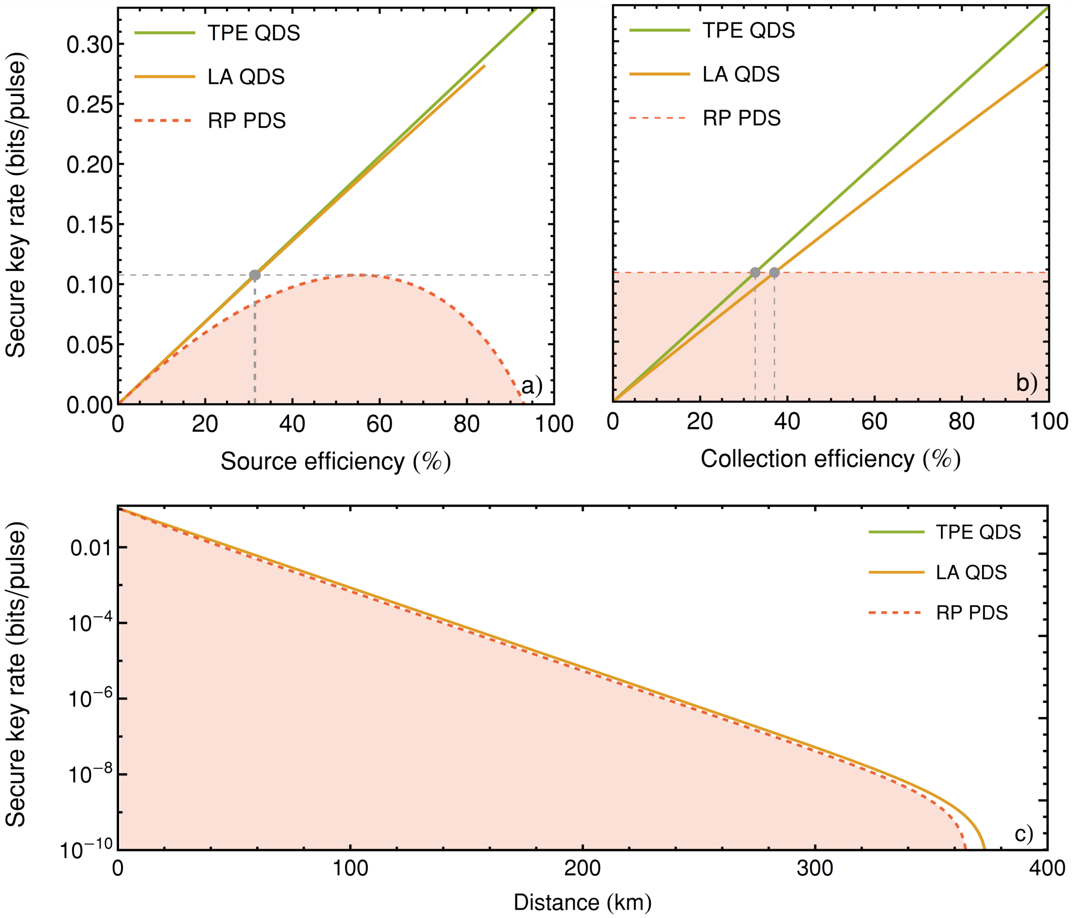
2. Results

The exact protocol considered here is described in [19], and we extend its security analysis to the quantum dot framework in Supplementary Note 8.

In order to compare the performance of all sources for unforgeable quantum tokens, we solve problem (62) from Supplementary Note 8 numerically using the MATLAB cvx package with solver SDPT3. In this way, we plot the evolution of the noise tolerance as a function of source efficiency, collection efficiency, and distance in Supplementary Figure 8. We then display the performance of all three QDS pumping schemes for collection efficiencies ranging from 1% to 100% in Supplementary Figure 9, and compare these to the best performance of randomized-phase PDS.

Naturally, PDS reach a maximal noise tolerance for source efficiencies around 63%, corresponding to $\mu \approx 1$, before dropping again when the multiphoton contribution becomes too significant. For QDS, we notice a striking difference between schemes with coherence (RE) and those without (LA and TPE): the latters give an overhead of almost 2% on the noise tolerance with respect to RE at high source efficiencies. This difference is crucial in making implementations feasible, since boosting the fidelity of quantum state preparation and quantum storage by a few percent can be extremely challenging. These differences are also reflected in Supplementary Figure 8.b., which identifies the collection efficiencies at which QDS can outperform the best PDS performance: while LA and TPE require 44% and 38%, respectively, RE must be pushed to 47% to beat PDS. For information purposes, we also select three state-of-the art experimental QDS, and show how they would perform in such a beyond-QKD protocol with their reported values of brightness and single-photon purity.

Supplementary Figure 8.c. finally compares the performance of each source as a function of distance. Once again,



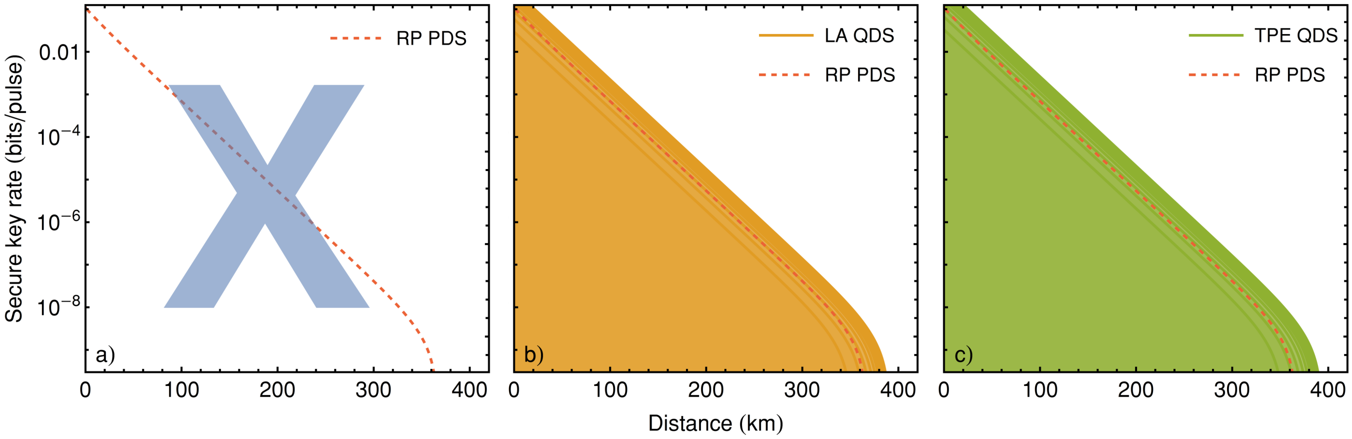
Supplementary Figure 4: **Source comparison for BB84 QKD with decoy states.** (a) Simulated secret key rates from Eq. (48) as a function of source efficiency for LA and TPE QDS, along with randomized-phase (RP) PDS. Source efficiency is defined as $1 - e^{-\mu}$ for PDS and $1 - \sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. (b) Simulated secret key rates as a function of QDS collection efficiency, compared to the best performance of RP PDS sources (dashed line). (c) Simulated secret key rates as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from Fig (b). Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

the difference between LA/TPE and RE is significant due to the coherence feature. We notice here that the maximal distance for all sources is much shorter than in QKD schemes, since our selected quantum token scheme bears a maximal loss tolerance of 50%: above this limit, an adversary can clone the quantum token without introducing any errors [19].

D. Quantum strong coin flipping

1. *Brief introduction*

Strong coin flipping (SCF) allows two distant parties, Alice and Bob, to generate and agree on a random bit. They do not trust each other and wish to ensure that the bit is truly random. We call the coin flip *fair* when two honest parties each win with probability 1/2. On the other hand, security for this task must guarantee that none of the two parties can force the other to declare outcome $i \in \{0, 1\}$ with probability higher than $P = \frac{1}{2} + \epsilon^{(i)}$, where $\epsilon^{(i)}$ is



Supplementary Figure 5: **Collection efficiency comparison for BB84 QKD with decoy states.** Simulated secret key rates from Eq. (48) as a function of distance for (a) RE QDS (b) LA QDS (c) TPE QDS, with collection efficiencies ranging from $\eta = 1\%$ (bottom curves) to $\eta = 100\%$ (top curves), in steps of 10%. The optimal performance of randomized-phase (RP) PDS is also plotted in dashed lines, in order to identify which QDS collection efficiencies are required to overcome PDS for each pumping. Single mode telecom fiber losses of 0.21 dB/km are assumed. Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

the protocol *bias*. In its most general form, SCF does not necessarily involve equal cheating probabilities for both parties, but when it does, the protocol is labelled *balanced*. We define the following upper bounds on Alice and Bob's probabilities of forcing their opponent to declare outcome i:

$$\begin{aligned} P_A^{(i)} &\leqslant \frac{1}{2} + \epsilon_A^{(i)} \qquad \text{Alice forces Bob to declare } i \\ P_B^{(i)} &\leqslant \frac{1}{2} + \epsilon_B^{(i)} \qquad \text{Bob forces Alice to declare } i \end{aligned} \tag{35}$$

The bias ϵ of a given SCF protocol is then defined as the highest of all four biases:

$$\epsilon = \max\left\{\epsilon_A^{(0)}, \epsilon_A^{(1)}, \epsilon_B^{(0)}, \epsilon_B^{(1)}\right\}. \tag{36}$$

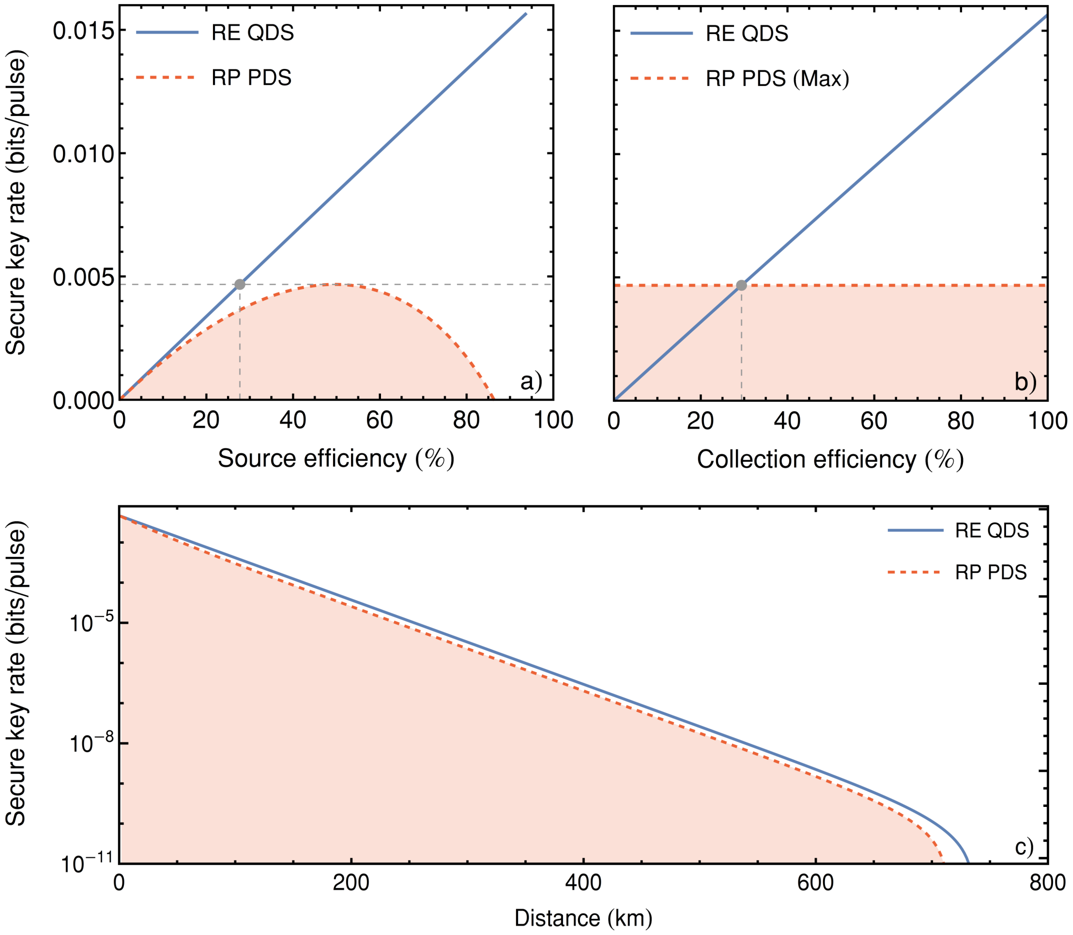
Information-theoretic strong coin flipping with arbitrarily small bias cannot be reached with quantum mechanics alone [29, 30], but requires additional space-time constraints [31], which can be experimentally challenging. It was shown, however, that even without such constraints, quantum mechanics can provide strong coin flipping protocols that perform better than any classical coin flipping protocol with information-theoretic security (in terms of bias) [32]. This led to experimental demonstrations of quantum strong coin flipping, namely [33–35].

In quantum coin flipping, the states generated by Alice are usually not encoded in the standard way of Supplementary Figure 1 (i.e. they are not an extension of the BB84 states $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ to infinite Hilbert spaces). Instead, the four coin flipping states must allow for an extra free parameter y, which will be varied to guarantee a fair (resp. balanced) coin flip, i.e. a coin flip in which Alice and Bob have equal honest (resp. dishonest) winning probabilities.

The required states in a two-dimensional qubit space spanned by $\{|v_0\rangle, |v_1\rangle\}$ are the following:

$$\begin{aligned} |\Phi_{\alpha,0}^{(y)}\rangle &= \sqrt{y}\,|v_0\rangle + (-1)^\alpha\sqrt{1-y}\,|v_1\rangle\,, \\ |\Phi_{\alpha,1}^{(y)}\rangle &= \sqrt{1-y}\,|v_0\rangle - (-1)^\alpha\sqrt{y}\,|v_1\rangle\,, \end{aligned} \tag{37}$$

where $\alpha \in \{0, 1\}$ denotes the encoding basis. In order to extend them to the full Hilbert space required in photonic setups, we simply change the two $H_{01}^{(1/2)}$ beamsplitter transformations from Supplementary Figure 1 to $H_{01}^{(y)}$. We



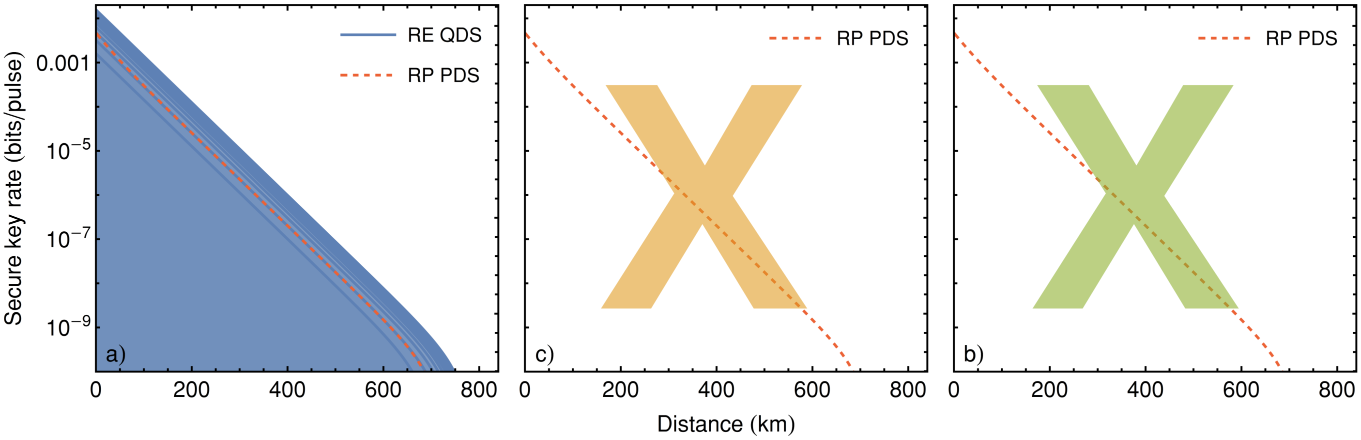
Supplementary Figure 6: **Source comparison for twin-field QKD.** (a) Simulated secret key rates from Eq. (54) as a function of source efficiency for RE QDS, along with randomized-phase (RP) PDS. Source efficiency is defined as $1 - e^{-\mu}$ for PDS and $1 - \sum_{n=0}^{\infty} p_n (1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. (b) Simulated secret key rates as a function of QDS collection efficiency, compared to the best performance of RP PDS sources (dashed line). (c) Simulated secret key rates as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from Fig (b). Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

then reproduce the workings from Eqs. (30), (33) and (34) with these new coefficients. The resulting coin flipping states are labelled as $\{\sigma_{\alpha,0}^{(y,\eta,\phi)}, \sigma_{\alpha,1}^{(y,\eta,\phi)}\}$, to account for PDS average photon number or QDS collection efficiency η, and phase encoding ϕ.

2. Results

We focus here on the quantum protocol from [33], and additionally study the effect of photon number coherence on the protocol bias in the security proof (see Supplementary Note 9 for details).

We show in Supplementary Figure 10 how the cheating probability evolves as a function of source and collection efficiencies in a balanced protocol (i.e., a protocol in which Alice and Bob have equal cheating probabilities). For the purpose of this example, we fix the number of states to $N = 1000$, and calculate the subsequent honest abort probability:



Supplementary Figure 7: **Collection efficiency comparison for twin-field QKD.** Simulated secret key rates from Eq. (54) as a function of distance for (a) RE QDS (b) LA QDS (c) TPE QDS, with collection efficiencies ranging from $\eta = 1\%$ (bottom curves) to $\eta = 100\%$ (top curves), in steps of 10%. The optimal performance of randomized-phase (RP) PDS is also plotted in dashed lines, in order to identify which QDS collection efficiencies are required to overcome PDS for each pumping. Single mode telecom fiber losses of 0.21 dB/km are assumed. Parameters for all plots are: alignment error rate $e_d = 2\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\%$, and error-correcting code inefficiency $f = 1.2$.

$$\mathcal{P}_{ab} = Z + (1 - Z)\,\frac{e}{2}, \tag{38}$$

where Z is the probability that Honest Bob does not register any click after the N states have been sent, and e is the quantum error rate. Using the results derived in [32, 36], we deduce the best achievable classical bound, thus identifying where QDS and PDS allow for quantum advantage in terms of cheating probability. For balanced, strong coin flipping protocols, the optimal classical bound reads:

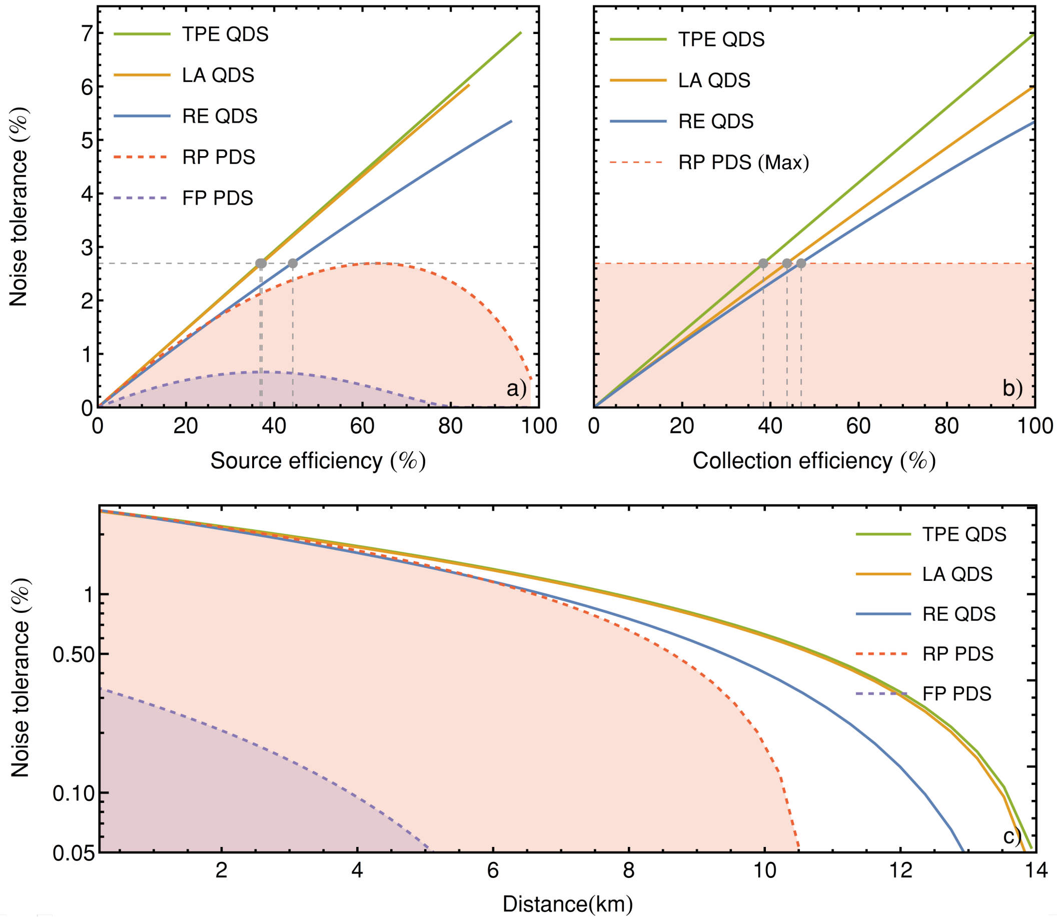
$$\mathcal{P}_c = 1 - \sqrt{\frac{\mathcal{P}_{ab}}{2}}. \tag{39}$$

As can be seen from Supplementary Figure 10, the cheating probability for RE is under-estimated, since we have only considered a specific discrimination attack in our security proof (Supplementary Note 9). The bounds for no coherence (LA/TPE), on the other hand, are over-estimated, since we have used the framework from [33], which does not provide tight bounds on the cheating probability. The combination of both features does not allow us to directly conclude that LA performs better than RE. However, for comparable brightness and purity, we know that it should perform better than RE, since the optimal attacks in quantum strong coin flipping protocols involve some form of discrimination, which is always more successful in the presence of photon-number coherence.

Note that we have not plotted the curves for fixed-phase PDS. For LA, TPE, and RE QDs, the dimension of the Hilbert space is upper-bounded (since $p_n = 0$ for $n >= 3$). For randomized-phase PDS, the required dimension is also upper-bounded, since perfect cheating is assumed for higher photon number terms. On the other hand, deriving the bounds for fixed-phase PDS would imply solving the semidefinite program from Eq. (66) in an infinite-dimensional Hilbert space.

In Supplementary Figure 11, we show how the cheating probability evolves as a function of distance for various collection efficiencies and a fixed honest abort probability of $\mathcal{P}_{ab} = 2.5\%$. Since, for PDS, a given abort probability can be achieved by varying either the number of states N or the average photon number per pulse μ, we choose N to be equal to the number of states required for the best performing quantum dot scheme (TPE). Essentially, the number of states N dictates the time duration of the protocol (for a fixed repetition rate), so the plots compare QDS to PDS performance for a fixed protocol duration, and fixed abort probability.

Here, we note the striking feature that QDS perform better at lower collection efficiencies, due to lower multiphoton component. This is in contrast with QKD, in which the main figure of merit is key rate, and the trade-off between brightness and single-photon purity is more crucial.



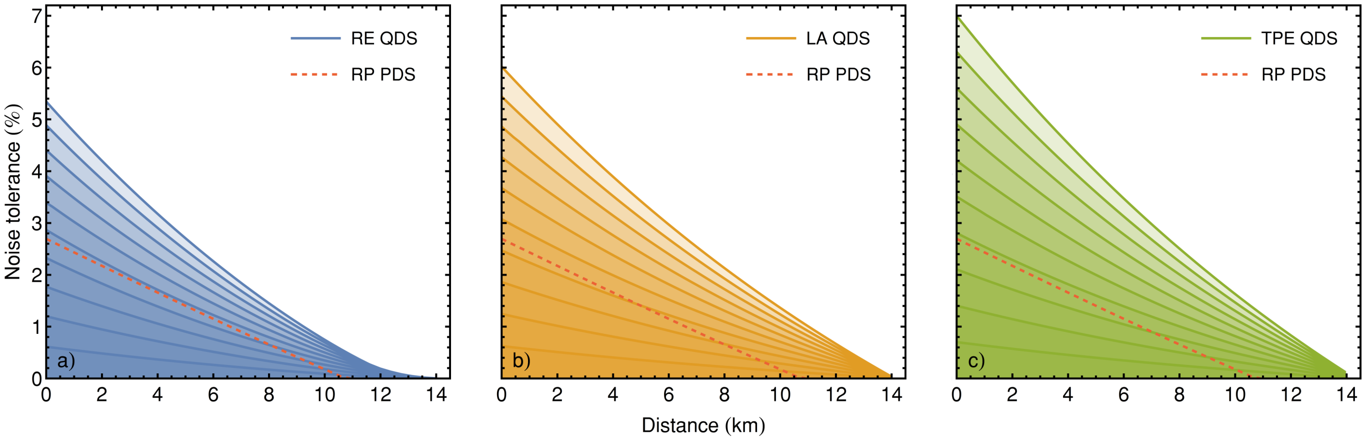
Supplementary Figure 8: **Source comparison for unforgeable quantum tokens.** (a) Numerical optimal noise tolerance from Eq. (62) as a function of source efficiency for RE, LA and TPE QDS, along with fixed-phase (FP) and randomized-phase (RP) PDS. Source efficiency is defined as $1 - e^{-\mu}$ for PDS and $1 - \sum_{n=0}^{\infty} p_n (1 - \eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. RE photonic states were assumed to be maximally pure in number basis, expressed as $\sum_{n=0}^{\infty} \sqrt{p_n} \, |n\rangle$, while LA states were expressed as diagonal states $\sum_{n=0}^{\infty} p_n \, |n\rangle \langle n|$. (b) Numerical noise tolerance as a function of QDS collection efficiency, compared to the best performance of PDS sources (dashed line). (c) Numerical noise tolerance plotted as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from Fig (b).

Interestingly, we have not considered the weak coin flipping protocol from [37] in our work, since the information there is not encoded onto the phase between various photon number terms (as is the case in our polarization, time-bin or path-encoded primitives), but rather onto the photon number itself. This means that having a phase reference between the photon number terms should not leak any information to an adversary, since it does not reveal whether the state was a vacuum state or a 1-photon Fock state. It therefore should not matter whether one uses RE, LA or TPE pumping schemes.

E. Quantum bit commitment

1. *Brief introduction*

A bit commitment protocol consists of two phases: the *commit* phase and the *open* phase. In the commit phase, Honest Alice chooses a bit $b \in \{0, 1\}$ and provides Honest Bob with some form of evidence that she has committed to



Supplementary Figure 9: **Collection efficiency comparison for unforgeable quantum tokens.** Numerical optimal noise tolerance from Eq. (62) as a function of distance for (a) RE QDS (b) LA QDS (c) TPE QDS, with collection efficiencies ranging from $\eta = 10\%$ (bottom curves) to $\eta = 100\%$ (top curves), in steps of 10%. The optimal performance of randomized-phase (RP) PDS is also plotted in dashed lines, in order to identify which QDS collection efficiencies are required to overcome PDS for each pumping. Single mode telecom fiber losses of 0.21 dB/km are assumed.

this choice. In the open phase, which happens some time after the commit phase, Honest Alice reveals b to Honest Bob. The desired security features are the following:

- Dishonest Alice cannot change b after the commit phase,

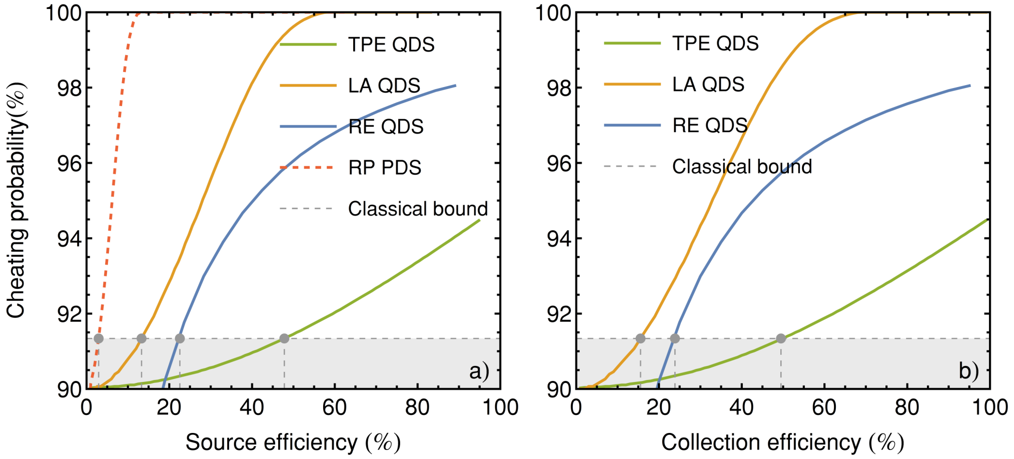
- Dishonest Bob cannot access b before the open phase.

Just like its strong coin flipping counterpart, the quantum version of bit commitment cannot provide perfect information-theoretic security for both parties without additional spacetime constraints [38, 39]. However, it is possible to circumvent this no-go theorem for two-party computations [38, 39] by placing restrictions on Dishonest Bob's storage capabilities.

We focus on the quantum protocol from [40], secure under a bounded storage assumption. During the commit phase, Honest Alice generates N BB84 states similarly to the QKD and quantum token protocols from Supplementary Note 4, and Honest Bob performs random X or Z measurements on each state. Both parties wait a pre-agreed amount of time Δt, during which it is assumed that a Dishonest Bob may only store and retrieve S of the N quantum states sent by Alice. After waiting Δt, Honest Alice sends her preparation basis for each of the N states to Honest Bob, who compares them with his measurement basis choices. An error correction and privacy amplification subroutine is then performed between the two parties. During the open phase, Honest Alice reveals the encoding of each of the N states, along with her committed bit b. Honest Bob performs consistency checks and accepts or rejects the commitment depending on the outcome.

2. Results

In Supplementary Figure 12 and Supplementary Figure 13, we plot the security condition from Eq. (70) presented in Supplementary Note 10. Similarly to [40], we assume that Alice sends $N = 10^8$ states, and that Dishonest Bob's storage size is $S = 972$. Once again, the security condition as a function of source efficiency reaches a maximum for PDS, after which the multiphoton component becomes too significant. Regarding QDS, the condition evolves almost linearly with source efficiency, since the vacuum and single photon components dominate at all source efficiencies.



Supplementary Figure 10: **Source comparison for quantum strong coin flipping.** Cheating probability as a function of (a) source efficiency and (b) collection efficiency for a balanced protocol with number of states $N = 1000$, using RE, LA, TPE QDS, and randomized-phase (RP) PDS. The best achievable classical bound from Eq. (39) is plotted in gray dashed lines, for an error rate of $e = 1.5\%$. Source efficiency is defined as $1 - e^{-\mu}$ for PDS and $1 - \sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. RE photonic states were assumed to be maximally pure in number basis, expressed as $\sum_{n=0}^{\infty} \sqrt{p_n}\,|n\rangle$, while LA states were expressed as diagonal states $\sum_{n=0}^{\infty} p_n\,|n\rangle\,\langle n|$. As discussed in Supplementary Note 9, note that the upper bounds on the cheating probability for LA and TPE are general and may be over-estimated, while the upper bound for RE considers a specific attack only (i.e., the cheating probability may in fact be higher).

SUPPLEMENTARY NOTE 5. MATHEMATICAL TOOLS FOR QUANTUM CRYPTOGRAPHY

A. Semidefinite programming

Quantum theory relies on linear algebra. In quantum cryptography, security analyses often involve optimizing over semidefinite positive objects to find the adversary's optimal cheating strategy. Most of the time, these objects are density matrices, measurement operators, or more general completely positive trace-preserving (CPTP) maps. Semidefinite programming provides a suitable framework for this, as it allows to optimize over semidefinite positive variables, given linear constraints.

A semidefinite program may be defined as a triple (Λ, F, C) where Λ is a Hermitian-preserving CPTP map, and F and C are Hermitian operators living in complex Hilbert spaces $\mathcal{H}_F$ and $\mathcal{H}_C$, respectively.

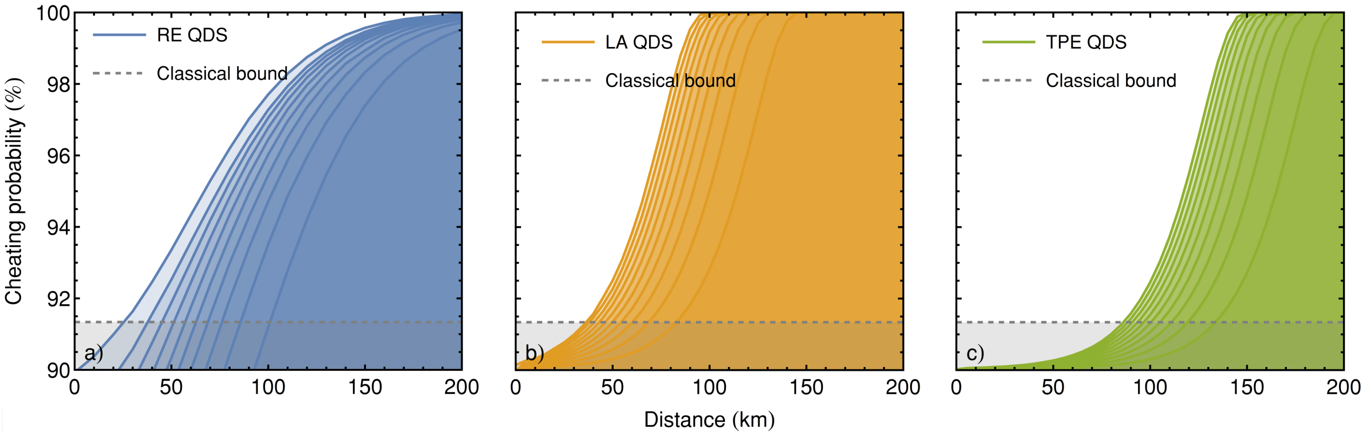
We start by defining a maximization problem, which will serve as our *primal problem*. The primal problem maximizes a *primal objective function*, $\mathrm{Tr}\left(F^\dagger X\right)$, over all positive semidefinite variables X, given a set of linear constraints expressed as a function of C:

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}\left(F^\dagger X\right) \\ \text{s.t.} \quad & \Lambda(X) = C \\ & X \geqslant 0. \end{aligned} \tag{40}$$

If it exists, the operator X which maximizes $\mathrm{Tr}\left(F^\dagger X\right)$ given these constraints is the *primal optimal solution*, and the corresponding value of $\mathrm{Tr}\left(F^\dagger X\right)$ is the *primal optimal value*.

Semidefinite programs present an elegant dual structure, which associates a dual minimization problem to each primal maximization problem. Effectively, the new variable(s) of the dual problem may be understood as the Lagrange multipliers associated with the constraints of the primal problem (one for each constraint).

The dual problem associated with (40) reads:



Supplementary Figure 11: **Collection efficiency comparison for quantum strong coin flipping.** Cheating probability as a function of distance for a balanced protocol using (a) RE, (b) LA, and (c) TPE QDS. The honest abort probability $\mathcal{P}_{ab} = 2.5\%$ (of which 1.5% come from the error rate), and the number of states N are varied for each point to achieve $\mathcal{P}_{ab}$. The best achievable classical bound from Eq. (39) is plotted in gray dashed lines. Collection efficiencies ranging from $\eta = 10\%$ to $\eta = 100\%$ are plotted from right to left, in steps of 10%. Single mode telecom fiber losses of 0.21dB/km are assumed.

$$\begin{aligned} \text{minimize} \quad & \operatorname{Tr}\left(C^{\dagger}Y\right) \\ \text{s.t.} \quad & \Lambda^{*}(Y) - F \geqslant 0 \\ & Y = Y^{\dagger}. \end{aligned} \tag{41}$$

Similarly to the primal problem, the operator Y which minimizes $\operatorname{Tr}\left(C^{\dagger}Y\right)$ given these constraints, if it exists, is the *dual optimal solution*, and the corresponding value of $\operatorname{Tr}\left(C^{\dagger}Y\right)$ is the *dual optimal value*.

The Lagrange multiplier method allows to find the local extremum of a constrained function. The optimal value s_p of the primal problem therefore upper bounds the optimal value s_d of the dual problem, while the optimal value of the dual lower bounds that of the primal. This property is known as *weak duality*, and may be simply expressed as:

$$s_p \leqslant s_d. \tag{42}$$

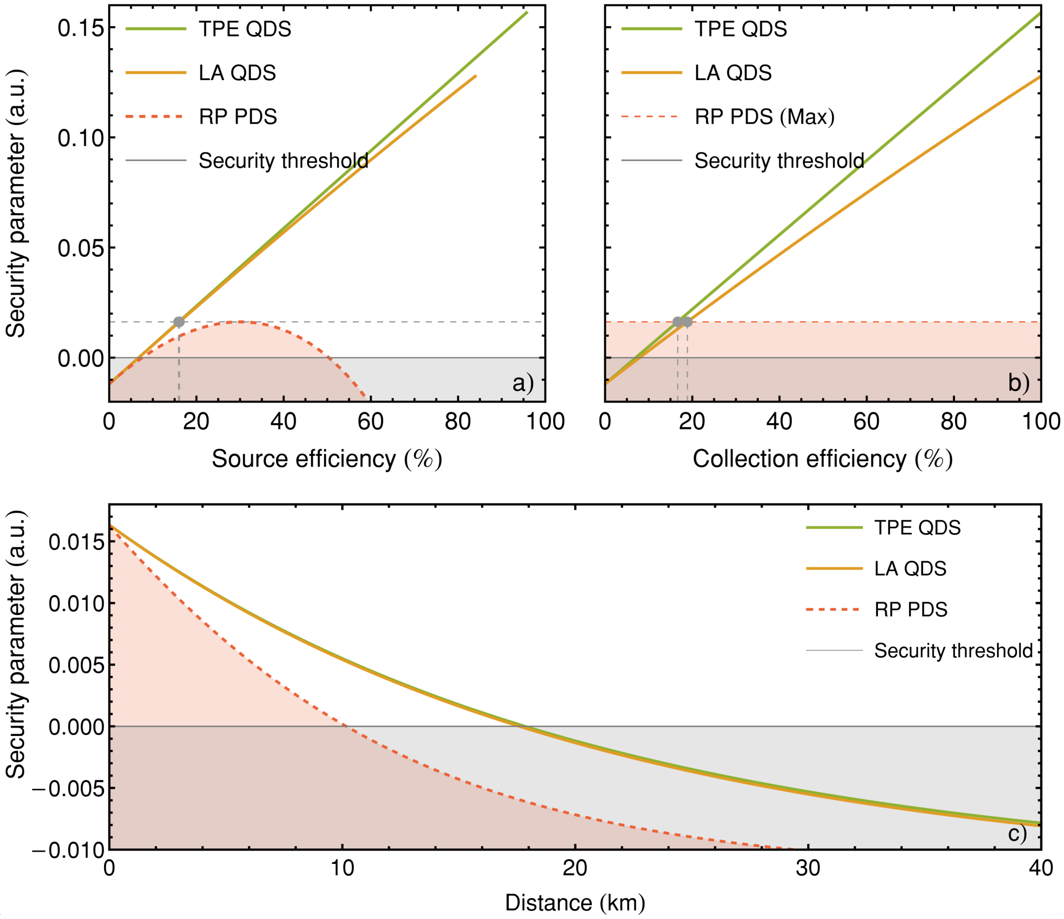
In many quantum-cryptographic applications however, we wish to ensure that the upper bound derived in the primal problem is *tight*, i.e. that the local maximum is in fact a global maximum for the objective function. The dual problem will help to prove this when there exists *strong duality*:

$$s_p = s_d. \tag{43}$$

B. Choi's theorem on completely positive maps

Let us consider a tensor product of two d-dimensional Hilbert spaces $\mathcal{H} = \mathcal{H}_1^d \otimes \mathcal{H}_2^d$, and then define the maximally entangled state $|\Phi^+\rangle\langle\Phi^+|$ on $\mathcal{H}$ as

$$|\Phi^+\rangle\langle\Phi^+| = \frac{1}{d}\sum_{i,j=1}^{d} |i\rangle\langle j| \otimes |i\rangle\langle j| \tag{44}$$

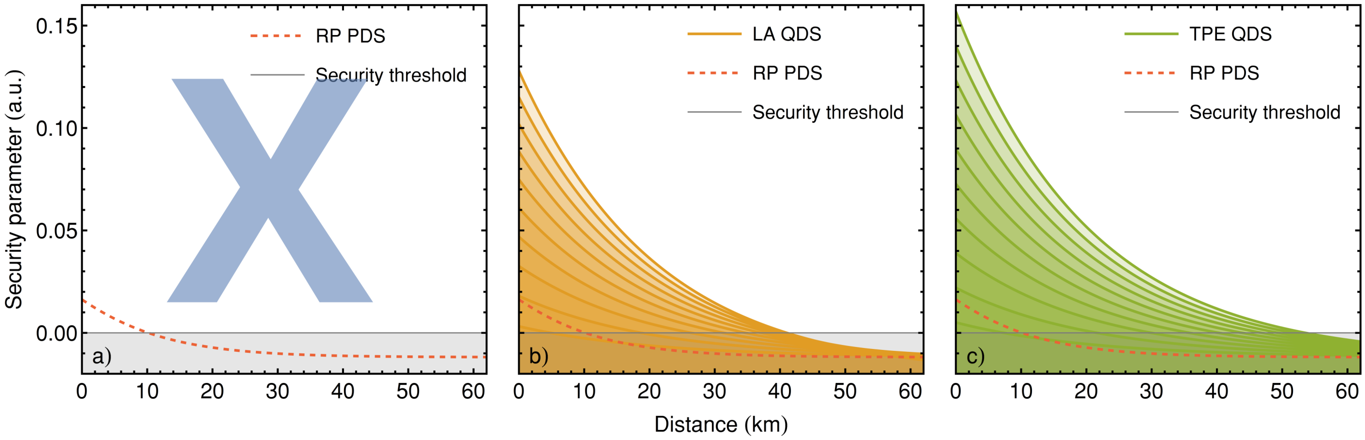


Supplementary Figure 12: **Source comparison for quantum bit commitment under the bounded storage assumption.** (a) Security condition from Eq. (70) as a function of source efficiency for LA and TPE QDS, along with randomized-phase (RP) PDS. Source efficiency is defined as $1-e^{-\mu}$ for PDS and $1-\sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDS, where η is the QDS collection efficiency. Chosen pulse lengths, pulse areas, and photon number populations $\{p_n\}$ are displayed in Supplementary Table 2. (b) Security condition from Eq. (70) as a function of QDS collection efficiency, compared to the best performance of RP PDS sources (dashed line). (c)Security condition from Eq. (70) as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDS collection efficiencies were chosen as the intersection points from Fig (b). The error rate is $e = 2\%$, detection efficiency $\eta_d = 100\%$, and the chosen parameters for Eq. (70) are $\epsilon = 2\times10^{-5}$, $\beta = 0.007$ and $\gamma = 0.008$.

We introduce a completely positive linear map $\Lambda : \mathcal{H}_1^d \to \mathcal{H}_3^{d'}$, and define the Choi-Jamiolkowski operator $J(\Lambda) : \mathcal{H}_1^d \otimes \mathcal{H}_2^d \to \mathcal{H}_3^{d'} \otimes \mathcal{H}_2^d$ as the operator which applies Λ to the first half of the maximally entangled state $|\Phi^+\rangle\langle\Phi^+|$:

$$J(\Lambda) = \frac{1}{d}\sum_{i,j=1}^{d} \Lambda(|i\rangle\langle j|) \otimes |i\rangle\langle j|\,. \tag{45}$$

Choi's theorem then states that Λ is completely positive if and only if $J(\Lambda)$ is positive semidefinite. We also have that Λ is a trace-preserving map if and only if $\mathrm{Tr}_{\mathcal{H}_3^{d'}}(J(\Lambda)) = \mathbb{1}_{\mathcal{H}_2^d}$ [41–43]. These properties are implemented as constraints in the optimization problem from Eq. (62).



Supplementary Figure 13: **Collection efficiency comparison for quantum bit commitment under the bounded storage assumption.** Security condition from Eq. (70) as a function of distance for (a) RE QDS (b) LA QDS (c) TPE QDS, with collection efficiencies ranging from $\eta = 1\%$ (bottom curves) to $\eta = 100\%$ (top curves), in steps of 10%. The optimal performance of randomized-phase (RP) PDS is also plotted in dashed lines, in order to identify which QDS collection efficiencies are required to overcome PDS for each pumping. Single mode telecom fiber losses of 0.21 dB/km are assumed. The error rate is $e = 2\%$, detection efficiency $\eta_d = 100\%$, and the chosen parameters for Eq. (70) are $\epsilon = 2 \times 10^{-5}$, $\beta = 0.007$ and $\gamma = 0.008$.

SUPPLEMENTARY NOTE 6. SECURITY OF BB84 QUANTUM KEY DISTRIBUTION

A. With Poisson-distributed sources

In the majority of QKD implementations so far, highly attenuated laser states are used instead of single photons [44]. New techniques, such as the insertion of decoy states into the protocol, have been developed to provide significant secure key rates despite the presence of multiphoton noise [45, 46]. We note that the derivation of the secure key rate in this setting assumes that the states sent by Alice bear no coherence in Fock basis, in order to satisfy the photon number channel assumption [46, 47]. This implies that the global phase of each state must be actively randomized, where the random phases are chosen from a given set of m phases $\mathcal{S}_m \in [0, 2\pi)$. In this work, we assume $m \to \infty$, but note that security proofs with discrete phase randomization also exist [48].

We briefly recall the workings from [45–47] for practical BB84 QKD without and with infinite decoy states, respectively. Let us define the yield Y_k of a k-photon state, which gives the conditional probability of a detection on Bob's detector given that Alice generates a k-photon state:

$$Y_k = Y_0 + (1 - Y_0)\left[1 - (1 - \eta_d \eta_t)^k\right], \tag{46}$$

where η_d is Bob's detection efficiency, η_t is the channel transmission, and Y_0 is the dark count probability. We may then define the gain Q_k of a k-photon state as the probability that Alice sends a k-photon state *and* Bob gets a detection:

$$Q_k = Y_k P_\mu(k), \tag{47}$$

where $P_\mu(k)$ are the Poisson distributed coefficients from Eq. (26) with average photon number μ. From [47], the secure key rate R after privacy amplification and error correction may be lower-bounded as:

$$R \geqslant \frac{1}{2}\left[Q_1\left(1 - H_2(e_1)\right) - f Q_\mu H_2\left(E_\mu\right)\right], \tag{48}$$

where Q_μ and E_μ are the gain and quantum bit error rate (QBER) of the signal state, respectively, e_1 is the QBER generated by single-photon states only, f is the error correcting code inefficiency assuming one-way classical post-processing, and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function for $0 < x \leqslant 1$. The first term states that only single-photon states contribute positively to the secure key rate, since multi-photon pulses leak information on lossy channels [49]. The second term materializes the cost of error correction.

In practical BB84 QKD without decoy states, Alice and Bob cannot estimate Q_1 and e_1 from their eavesdropped channel, as an eavesdropper may influence the photon number statistics observed by Alice and Bob. In order to nevertheless estimate the secure key rate from Eq. (48), we use the GLLP reasoning and make the pessimistic (yet secure) assumption that *all* losses and error come from single-photon states [46, 47]:

$$\begin{cases} Y_k = 1 \\ e_k = 0 \end{cases} \quad \text{for} \quad k \geqslant 2 \tag{49}$$

In other words, we separate the tagged qubits (i.e. multiphoton states that leak information to Eve) from the untagged qubits (i.e. single-photon states that do not leak information to Eve). We may then estimate the required single-photon parameters as:

$$\begin{cases} Q_1 \geqslant Q_\mu - \sum\limits_{k=2}^{\infty} P_\mu(k) \\ e_1 \leqslant \frac{E_\mu Q_\mu}{Q_1} \end{cases} \tag{50}$$

where $Q_\mu = \sum\limits_{k=0}^{\infty} Q_k$ and $E_\mu = \frac{1}{Q_\mu} \sum\limits_{k=0}^{\infty} e_k Q_k$ and $e_k = \frac{e_0 Y_0 + e_d \left[1-(1-\eta_d \eta_t)^k\right]}{Y_k}$. The parameter e_d characterizes the detection error probability, which depends on the optical alignment of the entire system.

In practice, this pessimistic assumption places a limit on the secure communication distance between Alice and Bob: since single-photon states are the only signals that contribute positively to the secret key rate from (48), assuming that all channel losses come from these effectively reduces the key rate.

Decoy state QKD [46], on the other hand, fixes this issue by proposing that Alice varies the average photon number μ of her signal. Some pulses are then used as decoy states to estimate the channel statistics, while the others are used as true signal states for the protocol. In the limit of infinite decoy states, since the eavesdropper cannot differentiate between the two, the estimation of Q_1 and e_1 can be performed much more accurately, as:

$$\begin{cases} Q_1 = Y_1 P_\mu(1) \\ e_1 = \frac{e_0 Y_0 + e_d \eta_d \eta_t}{Y_1} \end{cases} \tag{51}$$

B. With quantum dot sources

For QDS with collection efficiency η, we simply replace the $P_\mu(k)$ photon number coefficients in Eqs. (47), (50) and (51) by the following $P_\eta(k)$ coefficients:

$$\begin{aligned} P_\eta(0) &= p_0 + p_1 (1-\eta) + p_2 (1-\eta)^2 \\ P_\eta(1) &= p_1 \eta + p_2 \left[1 - \eta^2 - (1-\eta)^2\right] \\ P_\eta(k \geqslant 2) &= 1 - P_\eta(0) - P_\eta(1), \end{aligned} \tag{52}$$

where $\{p_n\}$ are the photon number populations from Eq. (18).

SUPPLEMENTARY NOTE 7. SECURITY OF TWIN-FIELD QUANTUM KEY DISTRIBUTION

A. With Poisson-distributed sources

The decoy method presented in Supplementary Note 6 can also be applied in TF-QKD, which implies that Alice and Bob must both randomize their pulses' global phase. However, a global phase reference must be shared between the two parties at some stage of the protocol, without leaking any information to Charlie. In [24], the proposed method is for Alice and Bob to agree on a fixed number of global phase slices m, equally splitting the interval $[0, 2\pi)$, from which they uniformly sample a global phase for each state. After Charlie's announcement of the measurement outcomes, they reveal which phase slice was chosen, and sift the raw key in such a way that they keep only the elements for which their chosen phase slices match. This method can potentially leak information to eavesdroppers, and variants that offer alternative methods have been proposed [50, 51].

In this setting, the secret key rate for TF-QKD resembles that derived in Eq. (48) for standard decoy QKD, with a few amendments. First, the channel transmittance η_t presented in Eq. (46) must be corrected to $\sqrt{\eta_t}$, since each optical pulse travels only half the distance between Alice and Bob. This gives the following expression for the yield:

$$Y_k^{(TF)} = Y_0 + (1 - Y_0)\left[1 - (1 - \eta_d\sqrt{\eta_t})^k\right]. \tag{53}$$

Then, an extra factor, dependent on the number m of chosen phase slices and the duty cycle d of quantum vs. classical signals, must be added to correct the key rate. This factor reads d/m. Finally, the intrinsic error rate e_s generated by the finite phase slicing must be taken into account on top of the overall setup alignment error e_d. For illustration purposes, we here assume that the setup alignment error $e_d = 2\%$, and, for $d = 1$ and $m = 16$, that the error due to phase slicing is $e_s = 1.275\%$ [24]. Following the workings from [24] with optimal $\mu = 0.765$, this provides the following modified expression for the TF key rate :

$$R^{(TF)} \geqslant \frac{d}{2m}\left[Q_1^{(TF)}\left(1 - H_2\left(e_1^{(TF)}\right)\right) - fQ_\mu^{(TF)}H_2\left(E_\mu^{(TF)}\right)\right], \tag{54}$$

where

$$\begin{cases} Q_k^{(TF)} &= Y_k^{(TF)}P_\mu(k), \\ Q_\mu^{(TF)} &= \sum\limits_{k=0}^{\infty} Q_k^{(TF)} \\ e_k^{(TF)} &= \frac{e_0 Y_0 + (e_d + e_s)\left[1 - \left(1 - \eta_d\sqrt{\eta_t}\right)^k\right]}{Y_k^{(TF)}} \\ E_\mu^{(TF)} &= \frac{1}{Q_\mu^{(TF)}}\sum\limits_{k=0}^{\infty} e_k^{(TF)}Q_k^{(TF)} \end{cases} \tag{55}$$

B. With quantum dot sources

For QDS with collection efficiency η, we simply replace the $P_\mu(k)$ photon number coefficients in Eq. (55) by the following $P_\eta(k)$ coefficients:

$$\begin{aligned} P_\eta(0) &= p_0 + p_1(1-\eta) + p_2(1-\eta)^2 \\ P_\eta(1) &= p_1\eta + p_2\left[1 - \eta^2 - (1-\eta)^2\right] \\ P_\eta(k \geqslant 2) &= 1 - P_\eta(0) - P_\eta(1), \end{aligned} \tag{56}$$

where $\{p_n\}$ are the photon number populations from Eq. (18).

SUPPLEMENTARY NOTE 8. SECURITY OF UNFORGEABLE QUANTUM TOKENS (OR MONEY)

We start with a brief introduction to the semidefinite programming techniques required for this security analysis, followed by Choi's theorem on completely positive maps, before deriving the unforgeability regions of the protocol.

A. Unforgeability analysis for quantum tokens

The exact protocol considered here is described in [19], and we extend its security analysis to the quantum dot framework. A successful forging attack is one in which two copies of the quantum token state are simultaneously accepted at two spatially separated verification points. Let Λ be the optimal adversarial map which produces two copies (living in $\mathcal{H}_1 \otimes \mathcal{H}_2$) of the following original quantum token state living in $\mathcal{H}_{\text{ini}}$:

$$\rho_{\text{ini}} = \frac{1}{4}\sum_{k=0}^{3} \sigma_k^{(\eta,\phi)}. \tag{57}$$

Here, the set $\{\sigma_k^{(\eta,\phi)}\}$ contains either the fixed-phase coherent states from Eq. (23), the randomized phase coherent states from Eq. (25), the quantum dot states exhibiting number coherence from Eq. (33), or the quantum dot states without number coherence from Eq. (34). The superscripts (η, ϕ) serve as a reminder that these states depend on the PDS average photon number or QDS collection efficiency η, and encoding phase ϕ.

This proof makes use of the existence of a squashing model for the measurement setup [52]. Essentially, this model allows to express the infinite-dimensional measurement operators in a 3-dimensional space spanned by $\{|0\rangle, |1\rangle, |\varnothing\rangle\}$, by imposing a condition on the terminal's postprocessing, consisting of assigning a random measurement outcome $|0\rangle$ or $|1\rangle$ to any double click, and declaring a $|\varnothing\rangle$ flag when no detection is registered. The probability that a verifier declares an incorrect measurement outcome for token 1 is given by:

$$V_1 = \operatorname{Tr}\sum_{k=0}^{3}\left(\frac{1}{2}|\beta_k^{\perp}\rangle\langle\beta_k^{\perp}| \otimes \mathbb{1}\right)\Lambda\left(\frac{1}{4}\sigma_k^{(\eta,\phi)}\right), \tag{58}$$

while that for token 2 reads:

$$V_2 = \operatorname{Tr}\sum_{k=0}^{3}\left(\mathbb{1} \otimes \frac{1}{2}|\beta_k^{\perp}\rangle\langle\beta_k^{\perp}|\right)\Lambda\left(\frac{1}{4}\sigma_k^{(\eta,\phi)}\right), \tag{59}$$

where $|\beta_k\rangle$ is the squashed qubit associated with the original state $\sigma_k^{(\eta,\phi)}$, i.e. $|\beta_0\rangle = |+\rangle$, $|\beta_1\rangle = |+i\rangle$, $|\beta_2\rangle = |-\rangle$, $|\beta_3\rangle = |-i\rangle$, and $|\beta_k^{\perp}\rangle$ is its orthogonal qubit state. The factor 1/4 indicates that each σ_k is equally likely to occur, while 1/2 accounts for the verifier's random measurement basis choice. Using Eq. (45), we may rewrite these expressions as $V_1 = \operatorname{Tr}(E_1(\mu)J(\Lambda))$ and $V_2 = \operatorname{Tr}(E_2(\mu)J(\Lambda))$, where $E_1(\mu)$ and $E_2(\mu)$ are the *error operators*:

$$\begin{aligned} E_1(\mu) =& \frac{1}{4}\sum_{k=0}^{3}\frac{1}{2}|\beta_k^{\perp}\rangle\langle\beta_k^{\perp}| \otimes \mathbb{1} \otimes \overline{\sigma_k^{(\eta,\phi)}}, \\ E_2(\mu) =& \frac{1}{4}\sum_{k=0}^{3}\mathbb{1} \otimes \frac{1}{2}|\beta_k^{\perp}\rangle\langle\beta_k^{\perp}| \otimes \overline{\sigma_k^{(\eta,\phi)}}. \end{aligned} \tag{60}$$

Following a similar method, the probability that verifier 1 (resp. 2) registers a no-detection event for token 1 (resp. 2) reads $\operatorname{Tr}(L_1(\mu)J(\Lambda))$ (resp. $\operatorname{Tr}(L_2(\mu)J(\Lambda))$), where $L_1(\mu)$ and $L_2(\mu)$ are the *loss operators*, which contain the projection onto the state $|\varnothing\rangle$:

$$\begin{aligned} L_1(\mu) &= \frac{1}{4}\sum_{k=0}^{3}|\varnothing\rangle\langle\varnothing| \otimes \mathbb{1} \otimes \overline{\sigma_k^{(\eta,\phi)}}, \\ L_2(\mu) &= \frac{1}{4}\sum_{k=0}^{3}\mathbb{1} \otimes |\varnothing\rangle\langle\varnothing| \otimes \overline{\sigma_k^{(\eta,\phi)}}. \end{aligned} \tag{61}$$

We now search for the optimal cloning map Λ that minimizes the noise that the adversary must introduce for both tokens given a fixed combined channel and detection losses l. We cast this problem in the following SDP for a card with a single state,

$$\begin{aligned} \min \quad & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathcal{H}_1\otimes\mathcal{H}_2}\left(J(\Lambda)\right) = \mathbb{1}_{\mathcal{H}_{\mathrm{ini}}} \\ & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) \geqslant \mathrm{Tr}\left(E_2(\mu)J(\Lambda)\right) \\ & \mathrm{Tr}\left(L_1(\mu)J(\Lambda)\right) \leqslant l \\ & \mathrm{Tr}\left(L_2(\mu)J(\Lambda)\right) \leqslant l \\ & J(\Lambda) \geqslant 0 \end{aligned} \tag{62}$$

The first constraint imposes that Λ is trace-preserving, the second imposes that the error rate measured for token 1 is at least equal to the one measured for token 2, the third and fourth impose that the losses measured for tokens 1 and 2 do not exceed the expected honest losses, and the fifth imposes that Λ is completely positive.

Using similar techniques to [19], it can be shown that this lower bound is in fact optimal, and that the adversary does not succeed better by performing a general attack on the full tensor product of the N states contained in the token.

SUPPLEMENTARY NOTE 9. SECURITY OF QUANTUM STRONG COIN FLIPPING

We focus here on the quantum protocol from [33], and additionally study the effect of photon number coherence on the protocol bias in the security proof.

A. Dishonest Alice

Since Dishonest Alice can send any arbitrary quantum state to Honest Bob, the corresponding security proof does not depend on the emitted PDS or QDS state, but depends only on the parameter y imposed by the protocol. Using the notations from [33], we assume here that Dishonest Alice wishes to bias the outcome towards $x = 0$, corresponding to $b = c$. Note that the security analysis proceeds similarly for outcome $x = 1$ with $b \neq c$.

From [33], Dishonest Alice's optimal strategy consists in sending the state that maximizes the average probability of revealing $(\alpha = 0, c = 0)$ and $(\alpha = 1, c = 1)$ or of revealing $(\alpha = 1, c = 0)$ and $(\alpha = 0, c = 1)$. Note that these four pairs yield a better cheating strategy than the other pairs, since the states in the pairs $\{|\Phi_{00}^{(y)}\rangle, |\Phi_{11}^{(y)}\rangle\}$ and $\{|\Phi_{10}^{(y)}\rangle, |\Phi_{01}^{(y)}\rangle\}$ have a larger overlap than the states in the pairs $\{|\Phi_{00}^{(y)}\rangle, |\Phi_{01}^{(y)}\rangle\}$ and $\{|\Phi_{10}^{(y)}\rangle, |\Phi_{11}^{(y)}\rangle\}$.

Following the arguments from [31, 33], Dishonest Alice's optimal cheating strategy is to create an entangled state, of which she sends one half to Bob, waits for his measurement and declaration of classical data, and finally performs a measurement on her part of the state to decide which outcome she reveals. This yields the following upper-bound on Alice's cheating probability:

$$\mathcal{P}_A^{bias} \leqslant \frac{3}{4} + \frac{1}{2}\sqrt{y(1-y)}. \tag{63}$$

B. Dishonest Bob

1. *Without photon number coherence*

In general, Dishonest Bob's optimal cheating strategy involves some form of discrimination problem, in which he tries to identify which state was sent by Alice from a known and pre-agreed set of states. The works from [33–35] provided a practical security analysis for PDS (either SPDC or attenuated laser states), with the crucial assumption that *no coherence* is present in the photon number basis. Thus, we can use these security analyses for phase-randomized PDS, as well as for LA and TPE QDS. For RE QDS however, we must extend the security analysis to incorporate the presence of photon number coherence in the states generated by Alice, which is performed in the next section.

To upper bound Bob's cheating probability without photon number coherence, we use the expression derived in [53], noting that it may not be a tight upper bound. However, this does not compromise the security of the protocol, as it only increases Dishonest Bob's power. Similarly to Dishonest Alice, we assume that Dishonest Bob wishes to bias the flip outcome towards $x = 0$, corresponding to $b = c$. Note that the security analysis proceeds similarly for outcome $x = 1$ with $b \neq c$. As a brief summary, the cases in which Bob *cannot* perfectly cheat, considered in [53], are the following:

- A_1: Alice sends only vacuum states, with probability $\mathcal{P}(A_1) = P_x^N(0)$.
- A_2: Alice sends at least one single-photon pulse, and vacuum states, with probability $\mathcal{P}(A_2) = (P_x(0) + P_x(1))^N - P_x^N(0)$.
- A_3: Alice sends one two-photon pulse, and vacuum states, with probability $\mathcal{P}(A_3) = NP_x(k \geqslant 2)P_x^{N-1}(0)$.
- A_4: Alice sends one two-photon pulse, at least one single-photon pulse, and vacuum states, with probability $\mathcal{P}(A_4) = NP_x(k \geqslant 2)\left((P_x(0) + P_x(1))^{N-1} - P_x^{N-1}(0)\right)$

where $\{P_x(k)\}$ are the PDS coefficients from Eq. (26) for $x = \mu$ or the QDS coefficients from Eq. (52) for $x = \eta$.

Assuming no coherence in photon number basis, Bob's cheating probability can be upper-bounded individually for each of the four cases [33]. In case A_1, Bob's optimal strategy involves declaring a random bit b', which will make him successfully bias the coin towards his desired outcome with probability $\mathcal{P}(b'|A_1) = 1/2$. In case A_2, Bob's optimal strategy consists in performing a Helstrom measurement, which is successful with probability $\mathcal{P}(b'|A_2) = y$. In case A_3, Bob's optimal cheating strategy also reads $\mathcal{P}(b'|A_3) = y$. In case A_4, an optimization must be performed to find the best set of discrimination measurement operators within the full spectrum of conclusive and inconclusive measurements. This allows to upper bound his cheating probability as $\mathcal{P}(b'|A_4) \leqslant -2y^2 + 4y - 1$ [33].

Summing the contributions from all four cases, and assuming that Bob can cheat with probability 1 in all other cases, provides the final upper bound:

$$\mathcal{P}_B^{bias} \leqslant \sum_{i=1}^{4} \mathcal{P}(A_i)\,\mathcal{P}(b'|A_i) + \left[1 - \sum_{i=1}^{4} \mathcal{P}(A_i)\right] \times 1. \tag{64}$$

2. *With photon number coherence*

Extending the security proof to account for photon number coherence in the RE-pumped QDS is challenging: unlike in the previous subsection, the security analysis cannot be decomposed into independent security analyses that are conditioned on the outcome of a photon number measurement. Dishonest Bob can indeed exploit the presence of coherence to perform more general discrimination attacks.

We note that Bob's aim is to discriminate between the following two states sent by Honest Alice with equal probabilities, in such a way that the outcome of the flip is optimally biased towards $x = 0$:

$$\begin{aligned} \sigma_0^{(y,\eta,\phi)} &= \frac{1}{2}\left(\sigma_{00}^{(y,\eta,\phi)} + \sigma_{10}^{(y,\eta,\phi)}\right) \\ \sigma_1^{(y,\eta,\phi)} &= \frac{1}{2}\left(\sigma_{01}^{(y,\eta,\phi)} + \sigma_{11}^{(y,\eta,\phi)}\right). \end{aligned} \tag{65}$$

There exists a broad spectrum of discrimination measurements, which may be characterized by a set of parameters $\{p_{conc}, p_{corr}\}$ [31]. The first parameter p_{conc} gives the probability that implementing the POVM will yield a conclusive outcome, i.e. that one state from the pre-agreed set of states will be identified. The second parameter p_{corr} gives the probability that this outcome is correct, i.e. that the identified state is indeed the one that was sent. Fully conclusive measurements have $p_{conc} = 1$, but usually display a non-unit probability of being correct $p_{corr} < 1$ (depending on the set of states). Other measurements will increase p_{corr} by allowing some probability of the measurement being inconclusive, i.e. $p_{conc} < 1$.

Of course, Bob's optimal discrimination strategy will involve optimizing over these parameters for all N states, which is beyond the scope of this paper. Nevertheless, we show here how one powerful attack exploiting inconclusive measurement operators, known as unambiguous state discrimination (USD) [54, 55], can already provide Dishonest Bob with a cheating advantage over states which do not exhibit photon number coherence under TPE pumping. Intuitively, a USD POVM will return an outcome that is always correct ($p_{corr} = 1$), at the risk of getting an inconclusive outcome with some probability $p_{conc} < 1$. Since this attack yields inconclusive outcomes instead of erroneous ones, Bob can repeatedly perform the same attack on each state until the outcome is conclusive, in which case he has identified Alice's state without any error. If, after $(N-1)$ states, the attack is still inconclusive, he may then perform a conclusive minimum-error discrimination measurement on the last state, with $p_{corr} < 1$ and $p_{conc} = 1$, whose maximum success probability is given by the Helstrom bound [56].

To derive Bob's cheating probability in this case, we must first justify that USD is possible for our set of states (i.e., that there exists a USD attack which yields a non-zero probability of successfully identifying which state was sent by Alice). For this, it suffices to note that the kernels associated with the states $\sigma_0^{(y,\eta,\phi)}$ and $\sigma_1^{(y,\eta,\phi)}$ living in the full photon space are both non-zero [54]. Although this is enough to derive an upper bound on the success of the USD measurement, i.e. on the value of p_{conc}, we must find a bound that is *tight* in order to provide a meaningful comparison with the over-estimated bounds from Eq. (64). For this, we once again use the semidefinite programming techniques introduced in Supplementary Note 5. We extend the pure state treatment from [57] and the discrimination problem from [58] to recast Dishonest Bob's search for the optimal USD strategy:

$$\begin{aligned} \max \quad & \frac{1}{2}\left[\mathrm{Tr}\left(M_0\sigma_0^{(y,\eta,\phi)}\right) + \mathrm{Tr}\left(M_1\sigma_1^{(y,\eta,\phi)}\right)\right] \\ \text{s.t.} \quad & \mathrm{Tr}\left(M_0\sigma_1^{(y,\eta,\phi)}\right) = 0 \\ & \mathrm{Tr}\left(M_1\sigma_0^{(y,\eta,\phi)}\right) = 0 \\ & M_0 + M_1 + M_{inc} = \mathbb{1} \\ & M_0, M_1, M_{inc} \geqslant 0, \end{aligned} \tag{66}$$

where M_0 and M_1 are the POVM operators which identify the states $\sigma_0^{(y,\eta,\phi)}$ and $\sigma_1^{(y,\eta,\phi)}$, respectively, and M_{inc} is the POVM operator yielding an inconclusive outcome. All three operators serve as the optimization variables. The first two constraints ensure that the optimal POVM operators identify the correct state with zero error probability. Similarly to unforgeable quantum tokens, the tightness of this upper bound can be shown by using strong duality (see Supplementary Note 5 and [58]).

We label the optimal value to problem (66), i.e. Bob's optimal USD cheating probability, as $\mathcal{P}_{USD}$. On the other hand, the probability of a successful Helstrom measurement is given by [56]:

$$\mathcal{P}_{HEL} = \frac{1}{2} + \frac{1}{4}||\sigma_0^{(y,\eta,\phi)} - \sigma_1^{(y,\eta,\phi)}||_1, \tag{67}$$

where $|| \odot ||_1$ denotes the Schatten 1-norm.

Since Bob performs the same attack on each of the $(N-1)$ states sent by Alice, followed by a Helstrom measurement on the Nth state, we can finally upper-bound his cheating probability as:

$$\mathcal{P}_B^{bias} \leqslant \left[1 - (1-\mathcal{P}_{USD})^{N-1}\right] \times 1 + (1-\mathcal{P}_{USD})^{N-1} \times \mathcal{P}_{HEL}. \tag{68}$$

SUPPLEMENTARY NOTE 10. SECURITY OF QUANTUM BIT COMMITMENT

We focus on the quantum protocol from [40], under the bounded storage assumption. This assumption circumvents the no-go theorem for two-party computations [38, 39] by placing restrictions on Dishonest Bob's storage capabilities: he may store only S of the N quantum states sent by Honest Alice, over a time duration no longer than Δt. Similarly to BB84 QKD in Supplementary Note 6, the practical security analysis assumes that states emitted by Honest Alice bear no coherence in the photon number basis. We therefore consider only phase-randomized PDS, and LA/TPE QDS. We adapt here the conditions provided in the Supplementary Information of [40] for a 3ϵ-secure quantum bit commitment implementation. Here, ϵ is a fixed parameter which upper-bounds the occurrence of bad events, governed by the Hoeffding inequality.

In a nutshell, the practical bit commitment protocol is constructed from a weak string erasure sub-routine with errors (WSEE) [59]. An $(N, \lambda, \epsilon, e)$-WSEE provides Alice with a string X_N and Bob with a randomly chosen subset $I \in [N]$, as well as a substring $\widetilde{X}_I$. This substring is given by the substring X_I (the bits of X_N corresponding to the indices in I) passed through a binary symmetric channel that flips each bit of X_I with probability e. The security statements then read as follows:

- If Alice is honest, then the amount of information a Dishonest Bob holds about X_N is limited, i.e. the ϵ-smooth min entropy of X_N conditioned on a Dishonest Bob's information is lower bounded by a value λ.
- If Bob is honest, then Alice does not have any information I. That is, Alice does not learn which bits of X_N are known to Bob.

Essentially, losses allow Dishonest Bob to discard a fraction of single-photon detection events, and keep more multiphoton events so that his chance of guessing X_N correctly is increased. The resulting min-entropy rate λ can thereby be calculated as a function of experimental parameters $\{P_x(k)\}$ and $\{P_{(x\eta_c)}(k)\}$, where $\{P_x(k)\}$ are the PDS coefficients from Eq. (26) for $x = \mu$ or the QDS coefficients from Eq. (52) for $x = \eta$, and $\{P_{(x\eta_c)}(k)\}$ are defined similarly, only with an extra channel transmission factor η_c multiplying x to account for honest losses.

Following Lemma 12 from the Supplementary Information of [40], given an experimental error rate e, channel losses η_c, fixed parameters ϵ and $(\beta, \gamma) \in (0, 0.01]$, and considering a Dishonest Bob with bounded storage size S, we define the following parameters:

$$\begin{aligned}
m_2 &= P_x(1) - P_{(x\eta_c)}(0) + P_x(0) - 3\gamma \\
m_3 &= 1 - P_{(x\eta_c)}(k) \\
L' &= \max_{s\in(0,1]} -\frac{1}{s}\left[\log\left(1+2^s\right) - 1 - s\right] - \frac{3\epsilon}{s} \\
\delta &= 2\,\frac{e + \frac{\beta}{\sqrt{1-2\beta}}}{1-4\sqrt{5}\beta} \\
\lambda &= H_2(\delta) + 3\beta^2 \\
M_1 &= \frac{1}{2\gamma^2}\log\frac{2}{\epsilon} \\
M_2 &= \frac{\log\frac{1}{\epsilon}}{\epsilon\, m_2} \\
M_3 &= \frac{\log\frac{2}{\epsilon}}{(m_3-\gamma)\,\beta^2} \\
M_4 &= \frac{S}{m_2 L' - m_3\lambda}
\end{aligned} \tag{69}$$

where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function for $0 < x \leqslant 1$. For security to hold in a practical implementation, the following condition must hold:

$$m_2 L' - m_3\lambda > 0. \tag{70}$$

If Eq. (70) is true, then quantum bit commitment under the bounded storage model can be implemented 3ϵ-securely by using a randomly constructed error-correcting code, whenever the number of states sent by Alice:

$$N > \max\{M_1, M_2, M_3, M_4\}. \tag{71}$$

[1] D. E. Reiter, T. Kuhn, and V. M. Axt, Advances in Physics: X **4**, 1655478 (2019), URL https://doi.org/10.1080/23746149.2019.1655478.

[2] L. Besombes, K. Kheng, L. Marsal, and H. Mariette, Phys. Rev. B **63**, 155307 (2001), URL https://link.aps.org/doi/10.1103/PhysRevB.63.155307.

[3] P. Borri, W. Langbein, S. Schneider, U. Woggon, R. L. Sellin, D. Ouyang, and D. Bimberg, Phys. Rev. Lett. **87**, 157401 (2001), URL https://link.aps.org/doi/10.1103/PhysRevLett.87.157401.

[4] B. Krummheuer, V. M. Axt, and T. Kuhn, Phys. Rev. B **65**, 195313 (2002), URL https://link.aps.org/doi/10.1103/PhysRevB.65.195313.

[5] V. M. Axt, T. Kuhn, A. Vagov, and F. M. Peeters, Phys. Rev. B **72**, 125309 (2005), URL https://link.aps.org/doi/10.1103/PhysRevB.72.125309.

[6] B. Krummheuer, V. M. Axt, T. Kuhn, I. D'Amico, and F. Rossi, Phys. Rev. B **71**, 235329 (2005), URL https://link.aps.org/doi/10.1103/PhysRevB.71.235329.

[7] M. Cygorek, A. M. Barth, F. Ungar, A. Vagov, and V. M. Axt, Phys. Rev. B **96**, 201201(R) (2017), URL https://link.aps.org/doi/10.1103/PhysRevB.96.201201.

[8] S. Bounouar, M. Müller, A. M. Barth, M. Glässl, V. M. Axt, and P. Michler, Phys. Rev. B **91**, 161302 (2015), URL https://link.aps.org/doi/10.1103/PhysRevB.91.161302.

[9] J. H. Quilter, A. J. Brash, F. Liu, M. Glässl, A. M. Barth, V. M. Axt, A. J. Ramsay, M. S. Skolnick, and A. M. Fox, Phys. Rev. Lett. **114**, 137401 (2015), URL https://link.aps.org/doi/10.1103/PhysRevLett.114.137401.

[10] T. Kaldewey, S. Lüker, A. V. Kuhlmann, S. R. Valentin, J.-M. Chauveau, A. Ludwig, A. D. Wieck, D. E. Reiter, T. Kuhn, and R. J. Warburton, Phys. Rev. B **95**, 241306 (2017).

[11] S. Lüker, T. Kuhn, and D. E. Reiter, Phys. Rev. B **96**, 245306 (2017), URL https://link.aps.org/doi/10.1103/PhysRevB.96.245306.

[12] F. Ding, R. Singh, J. D. Plumhof, T. Zander, V. Křápek, Y. H. Chen, M. Benyoucef, V. Zwiller, K. Dörr, G. Bester, et al., Phys. Rev. Lett. **104**, 067405 (2010), ISSN 0031-9007, 1079-7114, URL https://link.aps.org/doi/10.1103/PhysRevLett.104.067405.

[13] A. Vagov, M. D. Croitoru, M. Glässl, V. M. Axt, and T. Kuhn, Phys. Rev. B **83**, 094303 (2011), URL https://link.aps.org/doi/10.1103/PhysRevB.83.094303.

[14] A. M. Barth, A. Vagov, and V. M. Axt, Phys. Rev. B **94**, 125439 (2016), URL https://link.aps.org/doi/10.1103/PhysRevB.94.125439.

[15] M. Cosacchi, M. Cygorek, F. Ungar, A. M. Barth, A. Vagov, and V. M. Axt, Phys. Rev. B **98**, 125302 (2018), URL https://link.aps.org/doi/10.1103/PhysRevB.98.125302.

[16] K. A. Fischer, L. Hanschke, M. Kremser, J. J. Finley, K. Müller, and J. Vučković, Quantum Science and Technology **3**, 014006 (2017), ISSN 2058-9565, URL http://dx.doi.org/10.1088/2058-9565/aa9269.

[17] L. Hanschke, K. A. Fischer, S. Appel, D. Lukin, J. Wierzbowski, S. Sun, R. Trivedi, J. Vučković, J. J. Finley, and K. Müller, npj Quantum Information **4** (2018), ISSN 2056-6387, URL http://dx.doi.org/10.1038/s41534-018-0092-0.

[18] M. D. sek, M. Jahma, and N.Lütkenhaus, Phys. Rev. A **62**, 022306 (2000), quant-ph/9910106.

[19] M. Bozzio, E. Diamanti, and F. Grosshans, Phys. Rev. A **99**, 022336 (2019), URL https://link.aps.org/doi/10.1103/PhysRevA.99.022336.

[20] H.-K. Lo and J. Preskill (2005), quant-ph/0504209.

[21] F. Miller, *Telegraphic code to ensure privacy and secrecy in the transmission of telegrams* (C.M. Cornwell, 1882).

[22] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996), URL https://link.aps.org/doi/10.1103/PhysRevLett.77.2818.

[23] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005), URL https://link.aps.org/doi/10.1103/PhysRevLett.95.080501.

[24] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400–403 (2018), ISSN 1476-4687, URL http://dx.doi.org/10.1038/s41586-018-0066-6.

[25] S. Wiesner, ACM Sigact News **15**, 78 (1983).

[26] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, npj Quantum Information **4**, 5 (2018), 1705.01428.

[27] A. Kent and D. Pitalúa-García, Phys. Rev. A **101**, 022309 (2020), URL https://link.aps.org/doi/10.1103/PhysRevA.101.022309.

[28] J.-Y. Guan, J.-M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. A **97**, 032338 (2018), 1709.05882.

[29] A. Kitaev, 6th Workshop on Quantum Information Processing (2003).

[30] A. Chailloux and I. Kerenidis, 50th Annual IEEE Symposium on Foundations of Computer Science pp. 527–533 (2009).

[31] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, Phys. Rev. A **80**, 062321 (2009).

[32] E. Hänggi and J. Wullschleger, Proceedings of TCC pp. 468–485 (2011).

[33] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nature Commun. **5**, 3717 (2014).

[34] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).

[35] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Phys. Rev. Lett. **94**, 040501 (2005).

[36] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nature Communications **5** (2014), ISSN 2041-1723, URL http://dx.doi.org/10.1038/ncomms6480.

[37] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, Phys. Rev. A **102**, 022414 (2020), URL https://link.aps.org/doi/10.1103/PhysRevA.102.022414.

[38] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997), URL https://link.aps.org/doi/10.1103/PhysRevLett.78.3414.

[39] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997), URL https://link.aps.org/doi/10.1103/PhysRevLett.78.3410.

[40] S. K. Ng, N. Huei Y.and Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner, Nature Communications **3** (2012), ISSN 2041-1723.

[41] A. Molina, T. Vidick, and J. Watrous, in *TQC 2012: Theory of Quantum Computation, Communication, and Cryptography*, edited by K. Iwama, Y. Kawano, and M. Murao (Springer, 2013), vol. 7582 of *Lecture Notes in Computer Science*, 1202.4010.

[42] J. Watrous, *Semidefinite Programming* (University of Waterloo, 2011), chap. 7, URL https://cs.uwaterloo.ca/~watrous/LectureNotes.html.

[43] L. Vandenberghe and S. Boyd, SIAM Review **38**, 49 (1996).

[44] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020), URL https://link.aps.org/doi/10.1103/RevModPhys.92.025002.

[45] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Info. Comput. **4**, 325 (2004), ISSN 1533-7146.

[46] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005), URL https://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[47] X. Ma, *Quantum cryptography: theory and practice* (2008), 0808.1385.

[48] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New Journal of Physics **17**, 053014 (2015).

[49] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000), URL https://link.aps.org/doi/10.1103/PhysRevLett.85.1330.

[50] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Physical Review Applied **11** (2019), ISSN 2331-7019, URL http://dx.doi.org/10.1103/PhysRevApplied.11.034053.

[51] M. Curty, K. Azuma, and H.-K. Lo, npj Quantum Information **5**, 64 (2019).

[52] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008), 0804.3082.

[53] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).

[54] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301 (2003), URL https://link.aps.org/doi/10.1103/PhysRevA.68.010301.

[55] X. Lü, Phys. Rev. A **103**, 022216 (2021), URL https://link.aps.org/doi/10.1103/PhysRevA.103.022216.

[56] S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009), URL http://www.osapublishing.org/aop/abstract.cfm?URI=aop-1-2-238.

[57] Y. Eldar, IEEE Transactions on Information Theory **49**, 446 (2003).

[58] Y. Eldar, A. Megretski, and G. Verghese, IEEE Transactions on Information Theory **49**, 1007 (2003).

[59] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).