npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Practical quantum tokens without quantum memories and experimental tests

Adrian Kent[1,2], David Lowndes[3], Damián Pitalúa-García[1]✉ and John Rarity[3]

Unforgeable quantum money tokens were the first invention of quantum information science, but remain technologically challenging as they require quantum memories and/or long-distance quantum communication. More recently, virtual "S-money" tokens were introduced. These are generated by quantum cryptography, do not require quantum memories or long-distance quantum communication, and yet in principle guarantee many of the security advantages of quantum money. Here, we describe implementations of S-money schemes with off-the-shelf quantum key distribution technology, and analyse security in the presence of noise, losses, and experimental imperfection. Our schemes satisfy near-instant validation without cross-checking. We show that, given standard assumptions in mistrustful quantum cryptographic implementations, unforgeability and user privacy could be guaranteed with attainable refinements of our off-the-shelf setup. We discuss the possibilities for unconditionally secure (assumption-free) implementations.

npj Quantum Information (2022)8:28 ; https://doi.org/10.1038/s41534-022-00524-4

INTRODUCTION

Quantum tokens, also called quantum money, were invented by Wiesner[1] in 1970. In Wiesner's original quantum token scheme Bob (the bank) secretly and securely generates a classical serial number s and a quantum state $|\psi\rangle$ of N qubits, prepared from a set of different bases, gives s and $|\psi\rangle$ to Alice, and stores s and the classical description of $|\psi\rangle$ in a database. Alice presents the token by giving s and $|\psi\rangle$ back to Bob, and Bob validates or rejects the token after measuring the received quantum state in the basis in which $|\psi\rangle$ was prepared. In refinements of this scheme[2–10], Alice can present the token to Bob or to one of a set of verifiers, by communicating the classical outcomes of quantum measurements applied on $|\psi\rangle$, as requested by Bob or the verifier. Alternatively, Alice presents the token by giving s and $|\psi\rangle$ to the verifier, who applies quantum measurements on $|\psi\rangle$. The verifier communicates with Bob to validate or reject the token.

There exist quantum token schemes satisfying *unforgeability*, i.e., they guarantee that a token cannot be validated more than once, with *unconditional security*, i.e., based only on the laws of physics without restricting the technology of dishonest Alice[2–10]. Intuitively, this follows from the no-cloning theorem, stating that it is impossible to perfectly copy unknown quantum states[11,12]. Unforgeable quantum token schemes based on computational assumptions have also been investigated (e.g., [13–16]), with some of these schemes not requiring communication with the bank for token validation (e.g., [15,16]).

However, there exist purely classical token schemes that can also guarantee unforgeability with unconditional security. For example, the token may comprise a classical serial number s and a classical secret password x that Bob gives Alice and that Alice presents by giving to one of a set of verifiers; validation of the token comprises *cross-checking*; for example, the verifier communicates with Bob and validates the token if this has not been presented before and if the given serial number and password correspond to each other.

In addition to unforgeability, some important properties of quantum token schemes are the following. First, quantum tokens can be transferred while keeping Bob's database static. On the other hand, since classical information can be copied perfectly, in order to satisfy unforgeability, when a purely classical token with serial number s is transferred from Alice to another party Charlie, Bob must change the classical data associated to s; for example, Bob must change x to another value x' and give s and x' to Charlie in the example above[2].

Second, some quantum token schemes satisfy *instant validation*. This means that the schemes do not require communication between the verifiers and Bob for validation after Alice presents the token[4]. This implies in particular that the token can be presented by Alice at one of a set of different spacetime points that can be spacelike separated without validation delays by the verifier due to cross-checking with Bob and/or with other verifiers.

Third, quantum token schemes satisfy *future privacy for the user* or simply *user privacy*. That is, neither Bob, nor the verifiers, can know where and when Alice will present the token.

It is not difficult to construct purely classical token schemes that satisfy with unconditional security any two of unforgeability, instant validation, and user privacy. For example, the classical token scheme above satisfies unforgeability and user privacy with unconditional security, but not instant validation. To the best of our knowledge, no purely classical token scheme has been shown to satisfy all three properties simultaneously with unconditional security. Classical variations of the quantum token schemes we consider here, based on classical relativistic bit commitments, whose security is hypothesized but not proven, were proposed in ref. [17], which considers their potential advantages and disadvantages. As far as we are aware, aside from these, there are no known classical schemes that plausibly satisfy all three properties simultaneously with unconditional security.

Among plausible future applications of quantum token schemes are very high value and time-critical transactions

[1]Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, UK. [2]Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo ON N2L 2Y5, Canada. [3]Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol, UK. ✉email: D.Pitalua-Garcia@damtp.cam.ac.uk

requiring very high security, such as financial trading, where many transactions take place within half a millisecond[18], or network control, where semi-autonomous teams need authentication as fast as possible. A reasonable assumption for such applications is that tokens may be transferred a relatively small number of times among a relatively small set of parties—the tokens may be valid for a relatively short time, for example. In this context, Bob having a static database does not seem to be a great advantage of quantum token schemes over classical schemes whose databases must be updated after each transaction, given that processing classical information is much easier and cheaper than processing quantum information. Furthermore, for very high-value transactions one might expect that the communication network among Bob and the verifiers is sufficiently protected that communication among them is very rarely (if ever) interrupted. So, in this context, it appears to be a major advantage of quantum token schemes over classical token schemes that a quantum token can be presented at one of a set of spacelike separated points with near-instant validation without time delays due to cross-checking, while satisfying unforgeability and user privacy with unconditional security.

Standard quantum token schemes satisfying unforgeability, user privacy and instant validation with unconditional security require to store quantum states in quantum memories and/or to transfer quantum states over long distances in order to give Alice enough flexibility in space and time to present the token[1–10,13–16]. Recently, a quantum memory of a single qubit with a coherence time of over an hour has been experimentally demonstrated[19,20]. However, storing large quantum states for more than a fraction of a second remains challenging[21,22]. Furthermore, the transmission of quantum states over long distances in practice comprises the transmission of photons through optical fiber or through the atmosphere via satellites. In both cases a great fraction of the transmitted photons is lost. For these reasons, standard quantum token schemes are impractical for most purposes at present.

Recently, experimental investigations of quantum token schemes have been performed[23–27]. References[23,27] investigated the experimental implementation of forging attacks on quantum token schemes. Reference[24] presented a simulation of a quantum token scheme in IBM's five-qubit quantum computer. References[25,26] reported proof-of-principle experimental demonstrations of the preparation and verification stages of quantum token schemes, by transmitting quantum states encoded in photons over a short distance—for example, ref. [26] reports optical fiber lengths of up to 10 m. A full experimental demonstration of a quantum token scheme that includes storing quantum states in a quantum memory and/or transmitting quantum states over long distances remains an important open problem.

"S-money"[17] is a class of quantum token schemes, which is designed for the settings described above comprising networks with relativistic or other trusted signaling constraints. These schemes can guarantee many of the security advantages of standard quantum token schemes—in particular, instant validation, unforgeability, and user privacy—without requiring either quantum state storage or long-distance transmission of quantum states. Furthermore, S-money tokens that can be transferred among several parties and that give the users great flexibility in space and time to present the token are also possible[28]. In this paper, we begin to investigate how securely S-money schemes can be implemented in practice with current technology.

Our results are twofold. First, we introduce quantum token schemes that extend the quantum S-money scheme of ref. [29] in practical experimental scenarios that consider losses, errors in the state preparations and measurements, and deviations from random distributions; and, in photonic setups, photon sources that do not emit exactly single photons, and single-photon detectors with non-unit detection efficiencies and with nonzero dark count probabilities, which are threshold detectors, i.e., which cannot distinguish the number of photons in detected pulses. In our schemes, Alice can present the token at one of 2^M possible spacetime presentation points, which can have arbitrary timelike or spacelike separation, for any positive integer M. Our schemes satisfy instant validation and comprise Bob transmitting N quantum states to Alice over a distance which can be arbitrarily short, Alice measuring the received quantum states without storing them, and further classical processing and classical communication over distances which can be arbitrarily large. Thus, our schemes are advantageous over standard quantum token schemes because they do not need quantum state storage or transmission of quantum states over long distances. We use the flexible versions of S-money defined in ref. [28], giving Alice the freedom to choose her spacetime presentation point after having performed the quantum measurements. We show that our schemes satisfy unforgeability and user privacy, given assumptions that have been standard in implementations of mistrustful quantum cryptography to date (see Table 6) but are nonetheless idealizations.

Second, we performed experimental tests of the quantum stage of one of our schemes for the case of two presentation points, which show that with refinements of our setup our schemes can be implemented securely, giving guarantees of unforgeability and user privacy, based on the standard assumptions in experimental mistrustful quantum cryptography mentioned above.

RESULTS

Preliminaries and notation

We present below two quantum token schemes that do not require quantum state storage, are practical to implement with current technology, and allow for experimental imperfections. We show that for a range of experimental parameters our token schemes are secure.

In the token schemes below, Bob (the bank) and Alice (the acquirer) agree on spacetime regions Q_i where a token can be presented by Alice to Bob, for $i \in \{0, 1\}^M$ and for some agreed integer $M \geq 1$. Bob has trusted agents $\mathcal{B}$ and $\mathcal{B}_i$ controlling secure laboratories, and Alice has trusted agents $\mathcal{A}$ and $\mathcal{A}_i$ controlling secure laboratories, for $i \in \{0, 1\}^M$. The agent $\mathcal{A}_i$ can send messages to $\mathcal{B}_i$ in the spacetime region Q_i, for $i \in \{0, 1\}^M$. All communications among agents of the same party are performed via secure and authenticated classical channels, which can be implemented with previously distributed secret keys. Alice's agent $\mathcal{A}$ and Bob's agent $\mathcal{B}$ perform the specified actions in a spacetime region P that lies within the intersection of the causal pasts of all Q_i, unless otherwise stated.

The token schemes comprise two main stages. Stage I includes the quantum communication between $\mathcal{B}$ and $\mathcal{A}$, which can take place between adjacent laboratories, and must be implemented within the intersection of the causal pasts of all the presentation points. In particular, this stage can take an arbitrarily long time and can be completed arbitrarily in the past of the presentation points, which is very helpful for practical implementations. Stage II comprises only classical processing and classical communication among agents of Bob and Alice, and must be implemented very fast in order to satisfy some relativistic constraints. A token received by $\mathcal{B}_b$ from $\mathcal{A}_b$ at Q_b can be validated by $\mathcal{B}_b$ near-instantly at Q_b, without the need to cross-check with other agents. We note that Alice chooses her presentation point in stage II, meaning in particular that it can take place after her quantum measurements have been completed. This is basically the application of the refinement of flexible S-money tokens discussed in ref. [28], which gives Alice great flexibility in spacetime to choose her presentation point. See Tables 1–3 for details.

In stage I, $\mathcal{B}$ generates quantum states randomly from a predetermined set and gives these to $\mathcal{A}$. $\mathcal{A}$ measures the received

Table 1. Ideal quantum token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$ for two presentation points. Steps 1 to 8 in $\mathcal{IQT}_1$, and 1 to 5 in $\mathcal{IQT}_2$, take place within the intersection of the causal pasts of the presentation points.

Ideal quantum token scheme $\mathcal{IQT}_1$

Stage I

1. For $k \in [N]$, $\mathcal{B}$ generates the qubit state $|\psi_k\rangle = |\phi_{t_k u_k}\rangle$ randomly from the BB84 set and sends it to $\mathcal{A}$ with its label k. Let the $N-$ bit strings $\mathbf{t} = (t_1, \ldots, t_N)$ and $\mathbf{u} = (u_1, \ldots, u_N)$ denote the states and bases of preparation by $\mathcal{B}$.

2. For $k \in [N]$, $\mathcal{A}$ measures each received qubit randomly in the computational basis ($y_k = 0$) or in the Hadamard basis ($y_k = 1$) and obtains a string of N bit outcomes $\mathbf{x}$. Let the N-bit-string $\mathbf{y} = (y_1, \ldots, y_N)$ denote Alice's measurement bases.

3. $\mathcal{A}$ sends $\mathbf{x}$ to $\mathcal{A}_i$, for $i \in \{0, 1\}$.

4. $\mathcal{A}$ chooses a bit z randomly and gives $\mathcal{B}$ a string $\mathbf{d}$, where $\mathbf{d} = \mathbf{y}$ if $z = 0$, or $\mathbf{d} = \overline{\mathbf{y}}$ if $z = 1$.

5. For $i \in \{0, 1\}$, $\mathcal{B}$ sends $\mathbf{d}$ to $\mathcal{B}_i$, who computes $\mathbf{d}_i$ in the causal past of Q_i, where $\mathbf{d}_0 = \mathbf{d}$ and $\mathbf{d}_1 = \overline{\mathbf{d}}$.

6. $\mathcal{B}$ sends $\mathbf{t}$ and $\mathbf{u}$ to $\mathcal{B}_i$, for $i \in \{0, 1\}$.

Stage II

7. $\mathcal{A}$ chooses the presentation point Q_b for the token, for some $b \in \{0, 1\}$. $\mathcal{A}$ computes the bit $c = b \oplus z$ and sends it to $\mathcal{B}$.

8. $\mathcal{B}$ sends c to $\mathcal{B}_i$, for $i \in \{0, 1\}$.

9. For $i \in \{0, 1\}$, in the causal past of Q_i, $\mathcal{B}_i$ computes the string $\tilde{\mathbf{d}}_i = \mathbf{d}_i$ if $c = 0$, or $\tilde{\mathbf{d}}_i = \overline{\mathbf{d}_i}$ if $c = 1$.

10. $\mathcal{A}$ sends a signal to $\mathcal{A}_b$ indicating to present the token at Q_b, and $\mathcal{A}_b$ presents the token $\mathbf{x}$ to $\mathcal{B}_b$ in Q_b.

11. $\mathcal{B}_b$ validates the token $\mathbf{x}$ received in Q_b if $\mathbf{x}_b = \mathbf{t}_b$, where $\mathbf{a}_v$ is the restriction of a string $\mathbf{a} \in \{\mathbf{x}, \mathbf{t}\}$ to entries a_k with $k \in \Delta_v$, where $\Delta_v = \{k \in [N] | \tilde{d}_{v,k} = u_k\}$, and where $\tilde{d}_{v,k}$ is the kth bit entry of the string $\tilde{\mathbf{d}}_v$, for $k \in [N]$ and for $v \in \{0, 1\}$. That is, Bob validates the token if Alice reports the correct measurement outcome for each qubit that she measured in Bob's preparation basis.

Ideal quantum token scheme $\mathcal{IQT}_2$

Stage I

1. As step 1 of $\mathcal{IQT}_1$.

2. The step 2 of $\mathcal{IQT}_1$ is replaced by the following. $\mathcal{A}$ chooses a bit z randomly. $\mathcal{A}$ measures each received qubit in the computational basis if $z = 0$ or in the Hadamard basis if $z = 1$. The string $\mathbf{y} \in \{0, 1\}^N$ denoting Alice's measurement bases has bit entries $y_k = z$ for $k \in [N]$.

3. As step 3 of $\mathcal{IQT}_1$. The steps 4 and 5 of $\mathcal{IQT}_1$ are discarded.

4. As step 6 of $\mathcal{IQT}_1$.

Stage II

5. As steps 7 and 8 of $\mathcal{IQT}_1$.

6. The step 9 of $\mathcal{IQT}_1$ is replaced by the following. For $i \in \{0, 1\}$, in the causal past of Q_i, $\mathcal{B}_i$ computes the string $\tilde{\mathbf{d}}_i \in \{0, 1\}^N$ with bit entries $\tilde{d}_{i,k} = i \oplus c$, for $k \in [N]$.

7. As steps 10 and 11 of $\mathcal{IQT}_1$.

states in bases from a predetermined set. $\mathcal{A}$ sends some classical messages to $\mathcal{B}$, mainly to indicate the set of states that she successfully measured. For all $i \in \{0, 1\}^M$, $\mathcal{A}$ communicates her classical outcomes to $\mathcal{A}_i$; $\mathcal{B}$ sends classical messages to $\mathcal{B}_i$, indicating mainly the labels of the states reported by $\mathcal{A}$ to be successfully measured.

In stage II, Alice chooses the label $b \in \{0, 1\}^M$ of her chosen presentation point in the intersection of the causal pasts of the presentation points. Further classical communication steps among agents of Alice and Bob take place. The token schemes conclude by Alice giving a classical message $\mathbf{x}$ (the token) to Bob at her chosen presentation point Q_b and Bob validating the token at Q_b if $\mathbf{x}$ satisfies a mathematical condition.

The main difference between the first and second token schemes below (either in their idealized or realistic version) is that, in the first one, Alice measures each received qubit randomly in one of two predetermined bases, while in the second one Alice measures large sets of qubits in the same basis, which is chosen randomly by Alice from two predetermined bases. The first token scheme is more suitable to implement with setups used for quantum key distribution. The second token scheme requires a slightly different setup.

We say a token scheme satisfies instant validation if, for any presentation point Q_i, an agent of Bob receiving a token from Alice at Q_i can validate or reject the token nearly instantly at Q_i, without the need to wait for any messages from other agents at spacetime points spacelike separated from Q_i.

We say a token scheme is:

- $\epsilon_{\text{rob}}-$ robust if the probability that Bob aborts when Alice and Bob follow the token scheme honestly is not greater than ϵ_{rob}, for any $b \in \{0, 1\}^M$;
- $\epsilon_{\text{cor}}-$ correct if the probability that Bob does not accept Alice's token as valid when Alice and Bob follow the token scheme honestly is not greater than ϵ_{cor}, for any $b \in \{0, 1\}^M$;
- $\epsilon_{\text{priv}}-$ private if the probability that Bob guesses Alice's bit-string b before she presents her token to Bob is not greater than $\frac{1}{2^M} + \epsilon_{\text{priv}}$, if Alice follows the token scheme honestly, for $b \in \{0, 1\}^M$ chosen randomly from a uniform distribution by Alice;
- $\epsilon_{\text{unf}}-$ unforgeable, if the probability that Bob accepts Alice's tokens as valid at any two or more different presentation points is not greater than ϵ_{unf}, if Bob follows the token scheme honestly.

We say a token scheme using N transmitted quantum states is:

- *robust* if it is $\epsilon_{\text{rob}}-$ robust with ϵ_{rob} decreasing exponentially with N.
- *correct* if it is $\epsilon_{\text{cor}}-$ correct with ϵ_{cor} decreasing exponentially with N.
- *private* if it is $\epsilon_{\text{priv}}-$ private with ϵ_{priv} approaching zero by increasing some security parameter.
- *unforgeable* if it is $\epsilon_{\text{unf}}-$ unforgeable with ϵ_{unf} decreasing exponentially with N.

Note that our definition of privacy is different because it depends on different parameters: see Lemma 4 below. In our schemes each of the N quantum states is a qubit state with

Table 2. Practical quantum token scheme $\mathcal{QT}_1$ for two presentation points. Steps 1 to 9 take place within the intersection of the causal pasts of the presentation points. See Table 4 for a summary of the notation and Fig. 2 for an illustration of the scheme.

Preparation Stage

0. Alice and Bob agree on a reference frame, on two presentation points Q_0 and Q_1 in the agreed frame, and on parameters $N \in \mathbb{N}$, $\beta_{\mathrm{PB}} \in (0, \frac{1}{2})$, and γ_{det}, $\gamma_{\mathrm{err}} \in (0, 1)$.

Stage I

1. For $k \in [N]$, $\mathcal{B}$ prepares bits t_k and u_k with respective probability distributions $P^k_{\mathrm{PS}}(t_k)$ and $P^k_{\mathrm{PB}}(u_k)$, satisfying $\frac{1}{2} - \beta_{\mathrm{X}} \leq P^k_{\mathrm{X}}(t) \leq \frac{1}{2} + \beta_{\mathrm{X}}$, where $\beta_{\mathrm{X}} \in (0, \frac{1}{2})$ is a small parameter, for $\mathrm{X} \in \{\mathrm{PS}, \mathrm{PB}\}$, $t \in \{0, 1\}$ and $k \in [N]$. We define $\mathbf{t} = (t_1, \ldots, t_N)$ and $\mathbf{u} = (u_1, \ldots, u_N)$. For $k \in [N]$, $\mathcal{B}$ prepares a quantum system A_k in a quantum state $|\psi_k\rangle$ and sends it to $\mathcal{A}$ with its label k. $\mathcal{B}$ chooses $k \in \Omega_{\mathrm{noqub}}$ with probability $P_{\mathrm{noqub}} > 0$ or $k \in \Omega_{\mathrm{qub}}$ with probability $1 - P_{\mathrm{noqub}}$. For $k \in \Omega_{\mathrm{qub}}$, $|\psi_k\rangle = \left|\phi^k_{t_k u_k}\right\rangle$ is a qubit state, where $\langle \phi^k_{0u} | \phi^k_{1u} \rangle = 0$ for $u \in \{0, 1\}$, where the qubit orthonormal basis $\mathcal{D}^k_u = \{\left|\phi^k_{tu}\right\rangle\}^1_{t=0}$ is the computational (Hadamard) basis up to an uncertainty angle θ on the Bloch sphere if $u = 0$ ($u = 1$). For $k \in \Omega_{\mathrm{noqub}}$, $|\psi_k\rangle = \left|\Phi^k_{t_k u_k}\right\rangle$ is a quantum state of arbitrary finite Hilbert space dimension greater than two. In photonic implementations, a vacuum or one-photon pulse has label $k \in \Omega_{\mathrm{qub}}$, with a one-photon pulse encoding a qubit state, while a multi-photon pulse has label $k \in \Omega_{\mathrm{noqub}}$ and encodes a quantum state of finite Hilbert space dimension greater than two.

2. For $k \in [N]$, $\mathcal{A}$ measures A_k in the qubit orthonormal basis $\mathcal{D}_{w_k}$, for $w_k \in \{0, 1\}$ and $k \in [N]$. Due to losses, $\mathcal{A}$ only successfully measures quantum states $|\psi_k\rangle$ with labels k from a proper subset Λ of $[N]$. Let W be the string of bit entries w_k for $k \in \Lambda$ and let $n = |\Lambda|$. Conditioned on $k \in \Lambda$, the probability that $\mathcal{A}$ measures A_k in the basis $\mathcal{D}_{w_k}$ satisfies $P_{\mathrm{MB}}(w_k) = \frac{1}{2}$, for $w_k \in \{0, 1\}$ and $k \in [N]$. $\mathcal{A}$ reports to $\mathcal{B}$ the set Λ. $\mathcal{B}$ does not abort if and only if $n \geq \gamma_{\mathrm{det}} N$.

3. $\mathcal{A}$ chooses a one-to-one function $g: \Lambda \to [n]$, for example, the numerical ordering, and sends it to $\mathcal{B}$. Let $y_j \in \{0, 1\}$ indicate the basis $\mathcal{D}_{y_j}$ on which the quantum state $|\psi_k\rangle$ is measured by $\mathcal{A}$ and let $x_j \in \{0, 1\}$ be the measurement outcome, where $j = g(k)$, for $k \in \Lambda$ and $j \in [n]$. Let $\mathbf{y} \in \{0, 1\}^n$ and $\mathbf{x} \in \{0, 1\}^n$ denote the strings of Alice's measurement bases and outcomes, respectively.

4. $\mathcal{A}$ sends $\mathbf{x}$ to $\mathcal{A}_i$, for $i \in \{0, 1\}$.

5. $\mathcal{A}$ chooses a bit z with probability $P_{\mathrm{E}}(z)$ that satisfies $\frac{1}{2} - \beta_{\mathrm{E}} \leq P_{\mathrm{E}}(z) \leq \frac{1}{2} + \beta_{\mathrm{E}}$, for $z \in \{0, 1\}$, and for a small parameter $\beta_{\mathrm{E}} \in (0, \frac{1}{2})$. $\mathcal{A}$ computes the string $\mathbf{d} \in \{0, 1\}^n$ with bit entries $d_j = y_j \oplus z$, for $j \in [n]$. $\mathcal{A}$ sends $\mathbf{d}$ to $\mathcal{B}$.

6. For $i \in \{0, 1\}$, $\mathcal{B}$ sends $\mathbf{d}$ to $\mathcal{B}_i$ and $\mathcal{B}_i$ computes the string $\mathbf{d}_i \in \{0, 1\}^n$ with bit entries $d_{i,j} = d_j \oplus i$, for $j \in [n]$.

7. $\mathcal{B}$ uses $\mathbf{t}$, $\mathbf{u}$, Λ, and g to compute the strings $\mathbf{s}, \mathbf{r} \in \{0, 1\}^n$, as follows. We define $r_j = t_k$, and $s_j = u_k$, where $j = g(k)$, for $j \in [n]$ and $k \in \Lambda$. We define $\mathbf{r}$ and $\mathbf{s}$ as the strings with bit entries r_j and s_j, for $j \in [n]$. $\mathcal{B}$ sends $\mathbf{s}$ and $\mathbf{r}$ to $\mathcal{B}_i$, for $i \in \{0, 1\}$.

Stage II

8. $\mathcal{A}$ chooses the presentation point Q_b where to present the token, for some $b \in \{0, 1\}$. $\mathcal{A}$ computes the bit $c = b \oplus z$ and sends it to $\mathcal{B}$.

9. $\mathcal{B}$ sends c to $\mathcal{B}_i$, for $i \in \{0, 1\}$.

10. For $i \in \{0, 1\}$, in the causal past of Q_i, $\mathcal{B}_i$ computes the string $\tilde{\mathbf{d}}_i \in \{0, 1\}^n$ with bit entries $\tilde{d}_{i,j} = d_{i,j} \oplus c$, for $j \in [n]$.

11. $\mathcal{A}$ sends a signal to $\mathcal{A}_b$ indicating to present the token at Q_b, and $\mathcal{A}_b$ presents the token $\mathbf{x}$ to $\mathcal{B}_b$ in Q_b.

12. $\mathcal{B}_b$ validates the token $\mathbf{x}$ received in Q_b if the Hamming distance between the strings $\mathbf{x}_b$ and $\mathbf{r}_b$ satisfies $d(\mathbf{x}_b, \mathbf{r}_b) \leq |\Delta_b| \gamma_{\mathrm{err}}$, where $\Delta_v = \{j \in [n] | \tilde{d}_{v,j} = s_j\}$, and where $\mathbf{a}_v$ is the restriction of a string $\mathbf{a} \in \{\mathbf{x}, \mathbf{r}\}$ to entries a_j with $j \in \Delta_v$, for $v \in \{0, 1\}$.

probability $1 - P_{\mathrm{noqub}}$, and a quantum state of arbitrary Hilbert space dimension greater than two with probability P_{noqub}, where $P_{\mathrm{noqub}} = 0$ in ideal schemes and $P_{\mathrm{noqub}} > 0$ in practical schemes. In photonic implementations, each pulse transmitted by Bob is either vacuum or one-photon with probability $1 - P_{\mathrm{noqub}}$, and multi-photon with probability P_{noqub}.

Below we present token schemes for two presentation points ($M = 1$) that satisfy instant validation and that are robust, correct, private, and unforgeable. The extension to 2^M presentation points for any $M \in \mathbb{N}$ is given in Supplementary Note VIII. For clarity of the presentation, we first present the ideal quantum token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$ where there are not any losses, errors, or any other experimental imperfections. These are given in Table 1. More realistic quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ that allow for various experimental imperfections are presented in Tables 2 and 3, respectively. A summary of the used notation is given in Table 4. An illustration of implementation in a token scheme for the case of two spacelike separated presentation points is given in Fig. 1. A diagram of the schemes is given in Fig. 2.

We use the following notation. We use bold font notation $\mathbf{a}$ for strings of bits. The bit-wise complement of a string $\mathbf{a}$ is denoted by $\bar{\mathbf{a}}$. The kth bit entry of a string $\mathbf{a}$ is denoted by a_k. We define the set $[N] = \{1, 2, \ldots, N\}$. The symbol "$\oplus$" denotes bit-wise sum modulo 2 or sum modulo 2 depending on the context. We write the Bennett-Brassard 1984 (BB84) states[30] as $|\phi_{00}\rangle = |0\rangle$, $|\phi_{10}\rangle = |1\rangle$, $|\phi_{01}\rangle = |+\rangle$ and $|\phi_{11}\rangle = |-\rangle$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, and where $\mathcal{D}_0 = \{|0\rangle, |1\rangle\}$ and $\mathcal{D}_1 = \{|+\rangle, |-\rangle\}$ are qubit orthonormal bases, called the computational and Hadamard bases, respectively. The Hamming distance is denoted by $d(\cdot, \cdot)$.

The quantum token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$ given in Table 1 have the following properties.

First, the token schemes are correct. Since we assume there are not any errors in the state preparations and measurements, if Alice and Bob follow the token scheme honestly then Bob validates Alice's token at her chosen presentation point Q_b with unit probability. If Alice and Bob follow $\mathcal{IQT}_1$ honestly, $\tilde{d}_{b,k} = d_{b,k} \oplus c = d_k \oplus b \oplus c = y_k \oplus z \oplus b \oplus c = y_k$, for $k \in [N]$. Thus, $\tilde{\mathbf{d}}_b = \mathbf{y}$, which means that $y_k = u_k$ for all $k \in \Delta_b$, hence, Alice measures in the same basis of preparation by Bob for all states $|\psi_k\rangle$ with labels $k \in \Delta_b$. Therefore, Alice obtains the correct outcomes for these states: $\mathbf{x}_b = \mathbf{t}_b$. Similarly, if Alice and Bob follow $\mathcal{IQT}_2$ honestly then we have that $\tilde{\mathbf{d}}_b$ has bit entries $\tilde{d}_{b,k} = b \oplus c = z = y_k$, for $k \in [N]$. Thus, as above, $\tilde{\mathbf{d}}_b = \mathbf{y}$, i.e., $\tilde{\mathbf{d}}_b$ corresponds to the string of measurement basis implemented by Alice. Therefore, in both token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$, Alice obtains $\mathbf{x}_b = \mathbf{t}_b$ and Bob validates Alice's token at Q_b with unit probability.

Second, the token schemes are robust. More precisely, neither Bob nor Alice have the possibility to abort. This is because we assume there are not any losses of the transmitted quantum states and that Alice successfully measures all the received quantum states. Thus, Alice does not need to report to Bob any labels of states that she successfully measured, in contrast to the extended token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ discussed below.

Third, the token schemes are private, i.e., Bob cannot obtain any information about b in the causal past of Q_b. This is because the

Table 3. Practical quantum token scheme $\mathcal{QT}_2$ for two presentation points. See Table 4 for a summary of the notation and Fig. 2 for an illustration of the scheme.

Preparation Stage

0. As step 0 of $\mathcal{QT}_1$.

Stage I

1. As step 1 of $\mathcal{QT}_1$.

2. The step 2 of $\mathcal{QT}_1$ is replaced by the following. $\mathcal{A}$ chooses a bit z with probability $P_E(z)$ satisfying $\frac{1}{2}-\beta_E \le P_E(z) \le \frac{1}{2}+\beta_E$, for $z \in \{0, 1\}$ and for a small parameter $\beta_E \in (0, \frac{1}{2})$. $\mathcal{A}$ measures A_k in the qubit orthonormal basis $\mathcal{D}_z$, for all $k \in [N]$. Due to losses, $\mathcal{A}$ only successfully measures quantum states $|\psi_k\rangle$ with labels k from a proper subset Λ of $[N]$. $\mathcal{A}$ reports to $\mathcal{B}$ the set Λ. Let $n = |\Lambda|$. $\mathcal{B}$ does not abort if and only if $n \ge \gamma_{\text{det}} N$.

3. As step 3 of $\mathcal{QT}_1$. The string $\mathbf{y} \in \{0, 1\}^n$ of Alice's measurement bases has bit entries $y_j = z$ for $j \in [n]$.

4. As step 4 of $\mathcal{QT}_1$. The steps 5 and 6 of $\mathcal{QT}_1$ are discarded.

5. As step 7 of $\mathcal{QT}_1$.

Stage II

6. As steps 8 and 9 of $\mathcal{QT}_1$.

7. The step 10 of $\mathcal{QT}_1$ is replaced by the following. For $i \in \{0, 1\}$, $\mathcal{B}_i$ computes the string $\tilde{\mathbf{d}}_i \in \{0, 1\}^n$ with bit entries $\tilde{d}_{i,j} = i \oplus c$, for $j \in [n]$.

8. As steps 11 and 12 of $\mathcal{QT}_1$.

messages Alice sends Bob in the causal past of Q_b carry no information about b and we assume that Alice's laboratories and communication channels are secure.

Fourth, the token schemes are unforgeable. This follows from the following lemma, which is shown in Supplementary Note IV. Alternative proofs are given in ref. [31], based on quantum state discrimination tasks. We have chosen the proof given in Supplementary Note IV because an extension of it allows us to prove Theorem 1 too.

Lemma 1: The quantum token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$ are $\epsilon_{\text{unf}}-$ unforgeable with

$$\epsilon_{\text{unf}} = \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^N. \tag{1}$$

Fifth, the token schemes satisfy instant validation. We note from step 11 of $\mathcal{IQT}_1$ that a token received by Bob's agent $\mathcal{B}_b$ from Alice's agent $\mathcal{A}_b$ at a presentation point Q_b can be validated by $\mathcal{B}_b$ near-instantly at Q_b. In particular, $\mathcal{B}_b$ does not need to wait for any signals coming from other agents of Bob.

Finally, the token schemes above can be modified in various ways. For example, in $\mathcal{IQT}_1$, step 3 can be discarded, and step 10 can be replaced by the following: after choosing b, $\mathcal{A}$ sends $\mathbf{x}$ to $\mathcal{A}_b$ and $\mathcal{A}_b$ presents the token $\mathbf{x}$ to $\mathcal{B}_b$ in Q_b. In another variation, step 5 in $\mathcal{IQT}_1$ can be modified so that $\mathcal{B}$ computes $\mathbf{d}_i$ and sends it to $\mathcal{B}_i$; in both versions of step 5, $\mathcal{B}_i$ must have $\mathbf{d}_i$ in the causal past of Q_i, for $i \in \{0, 1\}$. In another variation, the step 9 in $\mathcal{IQT}_1$ is performed only by Bob's agent $\mathcal{B}_b$ receiving a token from Alice. The version we have chosen for step 9 allows $\mathcal{B}_b$ to reduce the computation time after receiving a token, hence, allowing faster token validation. Further variations of the token schemes can be devised in order to satisfy specific requirements; for example, some steps might need to be completed within very short times, which might require reducing the computations within these steps, which can be achieved by delegating some computations within some other steps, for instance.

Practical quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ for two presentation points

The quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ presented in Tables 2 and 3 extend the quantum token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$ to allow for various experimental imperfections (see Table 5), and under some assumptions (see Table 6). $\mathcal{QT}_1$ and $\mathcal{QT}_2$ can be implemented in practice with the photonic setups of Fig. 3. The token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ can be modified in various ways, as discussed for the token schemes $\mathcal{IQT}_1$ and $\mathcal{IQT}_2$.

Regarding correctness, we note in the token scheme $\mathcal{QT}_1$ that if Alice follows the token scheme honestly and chooses to present the token in Q_b, then we have that $\tilde{\mathbf{d}}_b$ has bit entries $\tilde{d}_{b,j} = d_{b,j} \oplus c = d_j \oplus b \oplus c = d_j \oplus z = y_j$, for $j \in [n]$. Thus, $\tilde{\mathbf{d}}_b = \mathbf{y}$, i.e., $\tilde{\mathbf{d}}_b$ corresponds to the string of measurement bases implemented by Alice on the quantum states reported to be successfully measured. Similarly, in the token scheme $\mathcal{QT}_2$ if Alice follows the token scheme honestly and chooses to present the token in Q_b, then we have that $\tilde{\mathbf{d}}_b$ has bit entries $\tilde{d}_{b,j} = b \oplus c = z = y_j$, for $j \in [n]$. Thus, as above, $\tilde{\mathbf{d}}_b = \mathbf{y}$, i.e., $\tilde{\mathbf{d}}_b$ corresponds to the string of measurement bases implemented by Alice on the quantum states reported to be successfully measured. Therefore, in both token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$, if Alice can guarantee her error probability to be bounded by $E < \gamma_{\text{err}}$ then with very high probability she will make less than $|\Delta_b|\gamma_{\text{err}}$ bit errors in the $|\Delta_b|$ quantum states that she measured in the basis of preparation by Bob.

Let P_{det} be the probability that a quantum state $|\psi_k\rangle$ transmitted by Bob is reported by Alice as being successfully measured, with label $k \in \Lambda$, for $k \in [N]$. Let E be the probability that Alice obtains a wrong measurement outcome when she measures a quantum state $|\psi_k\rangle$ in the basis of preparation by Bob; if the error rates E_{tu} are different for different prepared states, labeled by t, and for different measurement bases, labeled by u, we simply take $E = \max_{t,u}\{E_{tu}\}$.

The robustness, correctness, privacy, and unforgeability of $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are stated by the following lemmas, proven in Supplementary Note V, and theorem, proven in Supplementary Note VII. These lemmas and theorem consider parameters γ_{det}, $\gamma_{\text{err}} \in (0, 1)$, allow for the experimental imperfections of Table 5, and make the assumptions of Table 6. A diagram presenting the conditions under which robustness, correctness, and unforgeability are satisfied simultaneously is given in Fig. 4.

Lemma 2: If

$$0 < \gamma_{\text{det}} < P_{\text{det}}, \tag{2}$$

then $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are $\epsilon_{\text{rob}}-$ robust with

$$\epsilon_{\text{rob}} = e^{-\frac{P_{\text{det}}N}{2}\left(1-\frac{\gamma_{\text{det}}}{P_{\text{det}}}\right)^2}. \tag{3}$$

Lemma 3: If

$$0 < \tfrac{\gamma_{\text{err}}}{2} < E < \gamma_{\text{err}}, \quad 0 < v_{\text{cor}} < \tfrac{P_{\text{det}}(1-2\beta_{\text{PB}})}{2}, \tag{4}$$

Table 4. Summary of notation used for $\mathcal{QT}_1$ and $\mathcal{QT}_2$.

Symbol	Brief description
Q_i	Presentation points
$\mathcal{A}$ ($\mathcal{B}$)	Alice's (Bob's) agent participating in the quantum communication stage
$\mathcal{A}_i$ ($\mathcal{B}_i$)	Alice's (Bob's) agent by the presentation point Q_i
A_k	Quantum systems sent to Alice by Bob
N	Number of quantum states that Bob sends Alice
Ω_{qub}	Set of labels for prepared qubits states
Ω_{noqub}	Set of labels for prepared quantum states with dimension greater than two
P_{noqub}	Probability that a prepared quantum state has dimension greater than two
t	String of bits encoding the quantum states prepared by Bob
u	String of bits encoding the bases of preparation by Bob
$\mathcal{D}_u^k$	Qubit orthonormal bases of preparation by Bob
$\mathcal{D}_{w_k}$	Qubit orthonormal bases of measurement by Alice
$P_{\text{MB}}(w_k)$	Probability distribution for Alice's measurement bases
β_{PB}	Bias for preparation basis
β_{PS}	Bias for preparation state
Λ	Set of labels for quantum states successfully measured by Alice
W	String of bits encoding the measurement bases for the quantum states successfully measured by Alice
γ_{det}	Minimum rate for states reported by Alice as successfully measured for Bob not aborting
γ_{err}	Maximum error rate allowed by Bob for validating Alice's token
g	One-to-one function g: $\lvert\Lambda\rvert \to [n]$
y (**x**)	String of bits encoding Alice's measurement outcomes (bases)
z	Bit chosen by Alice
$P_{\text{E}}(z)$	Probability distribution for bit z chosen by Alice
β_{E}	Bias for the probability distribution $P_{\text{E}}(z)$
d	String with bit entries $d_j = y_j \oplus z$ that Alice sends Bob
$\mathbf{d}_i$	String with bit entries $d_{i,j} = d_j \oplus i$ computed by Bob's agent $\mathcal{B}_i$
r (**s**)	String of bits encoding Bob's prepared states (preparation bases) for the states that Alice reports as successfully measured
b	Bit encoding Alice's chosen presentation point
c	Bit $c = b \oplus z$, which Alice sends Bob
$\tilde{\mathbf{d}}_i$	String with bit entries $\tilde{d}_{i,j} = d_{i,j} \oplus c$ computed by Bob's agent $\mathcal{B}_i$
Δ_v	Set of labels defined by $\Delta_v = \left\{ j \in [n] \middle\vert \tilde{d}_{v,j} = s_j \right\}$, for $v \in \{0, 1\}$
$\mathbf{a}_v$	The substring of $\mathbf{a} \in \{\mathbf{x}, \mathbf{r}\}$ restricted to bit entries a_k with $k \in \Delta_v$, for $v \in \{0, 1\}$

then $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are $\epsilon_{\text{cor}}-$correct with

$$\epsilon_{\text{cor}} = e^{-\frac{P_{\text{det}}(1-2\beta_{\text{PB}})N}{4}\left(1-\frac{2\nu_{\text{cor}}}{P_{\text{det}}(1-2\beta_{\text{PB}})}\right)^2} + e^{-\frac{E\nu_{\text{cor}}N}{3}\left(\frac{\gamma_{\text{err}}}{E}-1\right)^2}. \tag{5}$$

Lemma 4: $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are $\epsilon_{\text{priv}}-$private with

$$\epsilon_{\text{priv}} = \beta_{\text{E}}. \tag{6}$$

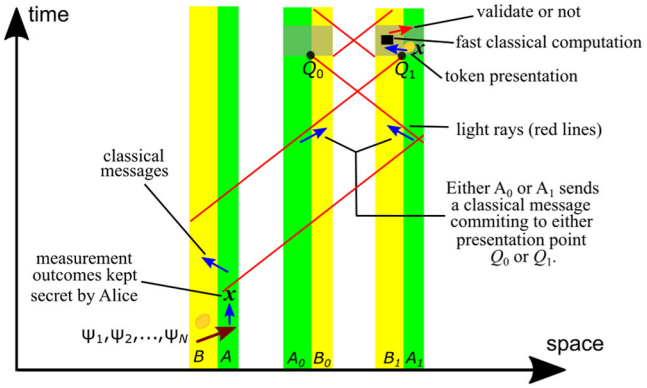

Fig. 1 Illustration of implementation in a quantum token scheme. A case of two presentation points in a Minkowski spacetime diagram in $1+1$ dimensions is illustrated. Bob has laboratories B, B_0, and B_1, controlled by agents $\mathcal{B}$, $\mathcal{B}_0$, and $\mathcal{B}_1$ (yellow rectangles), and Alice has laboratories A, A_0, and A_1, controlled by agents $\mathcal{A}$, $\mathcal{A}_0$, and $\mathcal{A}_1$ (green rectangles), adjacent to Bob's laboratories. The quantum communication stage takes place within B and A, can take an arbitrarily long time and can be completed arbitrarily in the past of the presentation points (Q_0 and Q_1). Alice's classical measurement outcomes **x** are kept secret by Alice and communicated to her laboratories A_0 and A_1 via secure and authenticated classical channels. In this illustrated example, Alice sends classical messages to Bob at laboratory B, and either at B_0 or B_1. The messages sent to B can take place anywhere in the past of Q_0 and Q_1 after the quantum communication stage and includes a message indicating the labels of the quantum states successfully measured by Alice. These messages are communicated from B to B_0 and B_1 via secure and authenticated classical channels. Alice chooses to present her token at Q_b within the intersection of the causal pasts of Q_0 and Q_1. The message at either B_0 or B_1 is the bit $c = b \oplus z$, effectively committing Alice to present her token at Q_b. Alice presents the token by giving Bob **x** at Q_b. The case $b = 1$ is illustrated. The small black box represents a fast classical computation performed at Bob's laboratory receiving the token, to validate or reject Alice's token, as described in step 12 of the scheme $\mathcal{QT}_1$ (see Table 2), for instance. As illustrated, this would require this computation to be completed within a time shorter than the time that light takes to travel between the locations of laboratories B_0 and B_1, which could be 10 μs if B_0 and B_1 are separated by 3 km, for example. This is because, as discussed in the introduction, we require presentation and acceptance to be completed within spacelike separated regions in order to achieve an advantage over purely classical token schemes.

Theorem 1: Consider the constraints

$$\begin{aligned} &0 < \gamma_{\text{err}} < \lambda(\theta, \beta_{\text{PB}}), \\ &0 < P_{\text{noqub}} < \nu_{\text{unf}} < \min\left\{ 2P_{\text{noqub}}, \gamma_{\text{det}}\left(1 - \tfrac{\gamma_{\text{err}}}{\lambda(\theta,\beta_{\text{PB}})}\right) \right\}, \\ &0 < \beta_{\text{PS}} < \tfrac{1}{2}\left[e^{\frac{\lambda(\theta,\beta_{\text{PB}})}{2}\left(1-\frac{\delta}{\lambda(\theta,\beta_{\text{PB}})}\right)^2} - 1 \right]. \end{aligned} \tag{7}$$

We define the function

$$\begin{aligned} &f(\gamma_{\text{err}}, \beta_{\text{PS}}, \beta_{\text{PB}}, \theta, \nu_{\text{unf}}, \gamma_{\text{det}}) \\ &\quad = (\gamma_{\text{det}} - \nu_{\text{unf}})\left[\tfrac{\lambda(\theta,\beta_{\text{PB}})}{2}\left(1 - \tfrac{\delta}{\lambda(\theta,\beta_{\text{PB}})}\right)^2 - \ln(1 + 2\beta_{\text{PS}}) \right] \\ &\qquad - (1 - (\gamma_{\text{det}} - \nu_{\text{unf}}))\ln[1 + h(\beta_{\text{PS}}, \beta_{\text{PB}}, \theta)], \end{aligned} \tag{8}$$

where

$$\begin{aligned} h(\beta_{\text{PS}}, \beta_{\text{PB}}, \theta) &= 2\beta_{\text{PS}}\sqrt{\tfrac{1}{2} + 2\beta_{\text{PB}}^2 + \left(\tfrac{1}{2} - 2\beta_{\text{PB}}^2\right)\sin(2\theta)}, \\ \delta &= \tfrac{\gamma_{\text{det}}\gamma_{\text{err}}}{\gamma_{\text{det}} - \nu_{\text{unf}}}. \end{aligned} \tag{9}$$

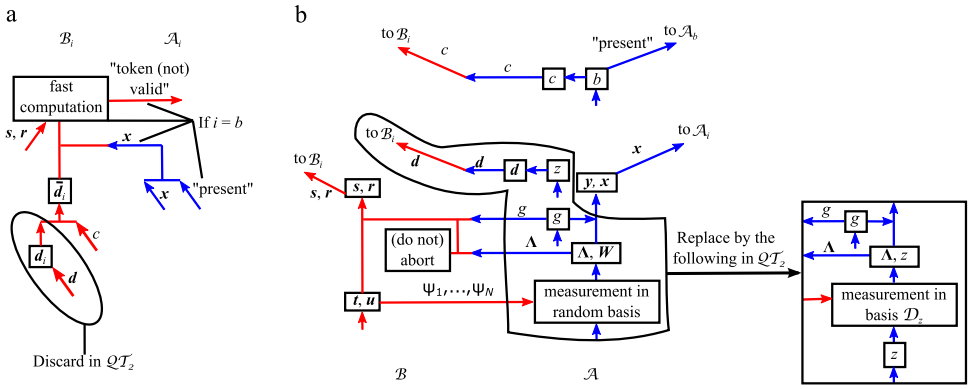

Fig. 2 Diagram of the quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$. Alice's (Bob's) steps are indicated with the blue (red) arrows. The differences between $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are shown. **b** The steps perfomed by Alice's and Bob's agents $\mathcal{A}$ and $\mathcal{B}$ in $\mathcal{QT}_1$ are illustrated. **a** The steps of Alice's and Bob's agents $\mathcal{A}_i$ and $\mathcal{B}_i$ in $\mathcal{QT}_1$ are shown, for $i \in \{0, 1\}$. The case $i = b$ represents Alice's token presentation and Bob's validation/rejection.

There exist parameters satisfying the constraints (7), for which $f(\gamma_{\mathrm{err}}, \beta_{\mathrm{PS}}, \beta_{\mathrm{PB}}, \theta, v_{\mathrm{unf}}, \gamma_{\mathrm{det}}) > 0$. For these parameters, $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are $\epsilon_{\mathrm{unf}}-$ unforgeable with

$$\epsilon_{\mathrm{unf}} = e^{-\frac{P_{\mathrm{noqub}}N}{3}\left(\frac{v_{\mathrm{unf}}}{P_{\mathrm{noqub}}}-1\right)^2} + e^{-Nf(\gamma_{\mathrm{err}},\beta_{\mathrm{PS}},\beta_{\mathrm{PB}},\theta,v_{\mathrm{unf}},\gamma_{\mathrm{det}})}. \tag{10}$$

We note in step 0 of $\mathcal{QT}_1$ and $\mathcal{QT}_2$ that Alice and Bob agree on parameters N, β_{PB}, γ_{det}, and γ_{err}. As follows from Lemmas 2–4, in order for Alice to obtain a required degree of correctness, robustness, and privacy, she must guarantee her experimental parameters P_{det}, E, and β_{E} to be good enough. This is independent of any experimental parameters of Bob, except for the previously agreed parameter β_{PB}, which plays a role in correctness but not in robustness or privacy. Additionally, Alice must choose a suitable mathematical variable v_{cor} to compute a guaranteed degree of correctness, as given by the bound of Lemma 3.

On the other hand, as follows from Theorem 1, in order for Bob to obtain a required degree of unforgeability, he must guarantee his experimental parameters P_{noqub}, θ, β_{PB}, and β_{PS} to be good enough. This is independent of any experimental parameters of Alice. Additionally, Bob must choose a suitable mathematical variable v_{unf} to compute a guaranteed degree of unforgeability, as given by the bound of Theorem 1.

Furthermore, as follows from Lemma 4, in order for Alice to obtain a required degree of privacy, she must guarantee her experimental parameter β_{E} to be small enough.

The parameters N, β_{PB}, γ_{det}, and γ_{err} agreed by Alice and Bob must be good enough to achieve their required degrees of robustness, correctness, and unforgeability. But they must also be achievable given their experimental setting.

Extension of $\mathcal{QT}_1$ and $\mathcal{QT}_2$ to 2^M presentation points

Extensions of the quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ to 2^M presentation points, for any integer $M \geq 1$, and the proof of the following theorem are given in Supplementary Note VIII.

Theorem 2: For any integer $M \geq 1$, there exist quantum token schemes $\mathcal{QT}_1^M$ and $\mathcal{QT}_2^M$ extending $\mathcal{QT}_1$ and $\mathcal{QT}_2$ to 2^M presentation points, in which Bob sends Alice NM quantum states, satisfying instant validation and the following properties. Consider parameters β_{PB}, β_{PS}, β_{E}, P_{det}, P_{noqub}, E, and θ satisfying the constraints (2), (4), (7) of Lemmas 2 and 3 and Theorem 1, for which the function $f(\gamma_{\mathrm{err}}, \beta_{\mathrm{PS}}, \beta_{\mathrm{PB}}, \theta, v_{\mathrm{unf}}, \gamma_{\mathrm{det}})$ defined by (8) is positive. For these parameters, $\mathcal{QT}_1^M$ and $\mathcal{QT}_2^M$ are $\epsilon_{\mathrm{rob}}^M-$robust, $\epsilon_{\mathrm{cor}}^M-$correct, $\epsilon_{\mathrm{priv}}^M-$private, and $\epsilon_{\mathrm{unf}}^M-$unforgeable with

$$\begin{aligned}
\epsilon_{\mathrm{rob}}^M &= M\epsilon_{\mathrm{rob}},\\
\epsilon_{\mathrm{cor}}^M &= M\epsilon_{\mathrm{cor}},\\
\epsilon_{\mathrm{priv}}^M &= \tfrac{1}{2^M}\left[(1+2\epsilon_{\mathrm{priv}})^M - 1\right],\\
\epsilon_{\mathrm{unf}}^M &= C\epsilon_{\mathrm{unf}},
\end{aligned} \tag{11}$$

where C is the number of pairs of spacelike separated presentation points, and where ϵ_{rob}, ϵ_{cor}, ϵ_{priv}, and ϵ_{unf} are given by (3), (5), (6), and (10).

Quantum experimental tests

We performed experimental tests for the quantum stage of the $\mathcal{QT}_1$ scheme for the case of two presentation points ($M = 1$), using the photonic setup of Fig. 3 and reporting strategy 1 (see Methods for details). Using a photon source with Poissonian distribution of average photon number $\mu = 0.09$, and a repetition rate of 10 MHz, we generated a token of $N = 4 \times 10^7$ photon pulses, with detection efficiency of $\eta = 0.21$, detection probability of $P_{\mathrm{det}} = 0.019$, and error rate of $E = 0.058$. We obtained deviations from the random distributions for the basis and state generation of $\beta_{\mathrm{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\mathrm{PS}} = 3.6 \times 10^{-3}$, respectively. In order to guarantee unforgeability using Theorem 1, we need to improve some experimental parameters (see Fig. 5).

Guaranteeing privacy in our schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ can be satisfied with good enough random number generators, as follows from Lemma 4. Due to the piling-up lemma, by using a large number of close-to-random bits, we can guarantee ϵ_{priv} to be arbitrarily small in practice.

DISCUSSION

We have presented two quantum token schemes that do not require either quantum state storage or long-distance quantum communication and are practical with current technology. Our schemes allow for losses, errors in the state preparations and measurements, and deviations from random distributions; and, in photonic setups, photon sources that do not emit exactly single photons, and threshold single-photon detectors with non-unit detection efficiencies and with nonzero dark count probabilities (see Table 5).

Our analyses follow much of the literature on practical mistrustful quantum cryptography (e.g., [32–36]) in making the assumptions of Table 6. Under these assumptions, we have shown that there exist attainable experimental parameters for which our schemes can satisfy instant validation, correctness, robustness,

Table 5. Allowed experimental imperfections for $\mathcal{QT}_1$ and $\mathcal{QT}_2$.

No	Brief description	Explanation and comments
1	For $k \in [N]$, there is a small probability $P_{\text{noqub}} > 0$ for $\mathcal{B}$ to prepare a quantum state $\|\psi_k\rangle$ of arbitrary finite Hilbert space dimension greater than two.	In photonic implementations, we define P_{noqub} and $\Omega_{\text{noqub}} \subseteq [N]$ as the probability that a pulse is multi-photon and as the set of labels for multi-photon pulses (see Methods). We define $\Omega_{\text{qub}} = [N] \setminus \Omega_{\text{noqub}}$ as the set of labels for vacuum or one-photon pulses, where the subindex refers to "qubit". When showing unforgeability, we treat vacuum pulses as one-photon pulses encoding the qubit state Bob attempted to send. Since this gives Alice extra options that cannot make it more difficult for her to cheat, the deduced unforgeability bound holds in general. A Poissonian photon source (e.g. weak coherent) with average photon number $\mu << 1$ gives $P_{\text{noqub}} = 1 - (1+\mu)e^{-\mu} = \frac{\mu^2}{2} + O(\mu^3)$, while a heralded single-photon source can give extremely small values for P_{noqub}, of the order of 10^{-10} for usual experimental parameters.
2	For $k \in \Omega_{\text{qub}}$, $\mathcal{B}$ prepares $\|\psi_k\rangle = \left\|\phi^k_{t_k u_k}\right\rangle$ in a qubit orthonormal basis $\mathcal{D}^k_{u_k}$ that is the computational (Hadamard) basis within an uncertainty angle $\theta \in (0, \frac{\pi}{4})$ on the Bloch sphere if $u_k = 0$ ($u_k = 1$).	Thus, the angle on the Bloch sphere between the states $\|\phi^k_{t0}\rangle$ and $\|\phi^k_{t1}\rangle$ is guaranteed to be within the range $[\frac{\pi}{2} - 2\theta, \frac{\pi}{2} + 2\theta]$, for $k \in \Omega_{\text{qub}}$. We define $O(\theta) = \frac{1}{\sqrt{2}}(\cos\theta + \sin\theta)$, where the notation refers to "overlap" on the Bloch sphere. It follows that $\|\langle\phi^k_{t0}|\phi^k_{t'1}\rangle\| \leq O(\theta)$, for some $O(\theta) \in (\frac{1}{\sqrt{2}}, 1)$, for $t, t' \in \{0, 1\}$ and $k \in \Omega_{\text{qub}}$.
3	For $k \in [N]$, $\mathcal{B}$ generates the bits t_k and u_k with probability distributions $P^k_{\text{PS}}(t_k)$ and $P^k_{\text{PB}}(u_k)$ that have small deviations from the random distributions given by biases β_{PS}, $\beta_{\text{PB}} > 0$.	That is, we have $\frac{1}{2} - \beta_{\text{X}} \leq P^k_{\text{X}}(t) \leq \frac{1}{2} + \beta_{\text{X}}$, with $0 < \beta_{\text{X}} < \frac{1}{2}$, for $t \in \{0, 1\}$, $k \in [N]$ and $\text{X} \in \{\text{PS}, \text{PB}\}$. The subindices "PS" and "PB" refer to "preparation state" and "preparation basis", respectively. It is useful for our security analysis to define: $\lambda(\theta, \beta_{\text{PB}}) = \frac{1}{2}\left(1 - \sqrt{1 - [1 - (O(\theta))^2](1 - 4\beta^2_{\text{PB}})}\right)$. It follows from $0 < \beta_{\text{PB}} < \frac{1}{2}$ and $\frac{1}{\sqrt{2}} < O(\theta) < 1$ that $0 < \lambda(\theta, \beta_{\text{PB}}) < \frac{1}{2}(1 - O(\theta)) < \frac{1}{2}(1 - \frac{1}{\sqrt{2}})$.
4	A fraction of the quantum states transmitted from $\mathcal{B}$ to $\mathcal{A}$ is lost. In photonic setups, $\mathcal{A}$ has single-photon detectors with non-unit detection efficiencies.	Because of losses and non-unit detection efficiencies (in photonic setups), $\mathcal{A}$ must report to $\mathcal{B}$ the set $\Lambda \subset [N]$ of labels of the successfully measured states. $\mathcal{B}$ does not abort if and only if $\|\Lambda\| \geq \gamma_{\text{det}} N$, where the subindex "det" stands for "detection".
5	For $k \in [N]$, $\mathcal{A}$ measures the received state $\|\psi_k\rangle$ in one of two distinct orthogonal qubit basis, $\mathcal{D}_0$ and $\mathcal{D}_1$, where this pair of bases is arbitrary.	$\mathcal{A}$ applying a measurement on a qubit basis $\mathcal{D}_0$ ($\mathcal{D}_1$) on a received quantum state that is not a qubit, i.e., for $k \in \Omega_{\text{noqub}}$, means that $\mathcal{A}$ sets her devices as she would do to apply a measurement in the qubit basis $\mathcal{D}_0$ ($\mathcal{D}_1$)—we note that $\mathcal{A}$ does not know the sets Ω_{qub} and Ω_{noqub}. For photonic setups, this may include arranging a set of wave plates, polarizing beam splitters and single-photon detectors in a particular setting. If $\mathcal{D}_0$ and $\mathcal{D}_1$ are very different from the computational and Hadamard bases, the number of measurement errors in Alice's outcomes is high. But, this is considered in our security analysis via Alice's error rate. Moreover, the set of two measurement bases applied by $\mathcal{A}$ could vary slightly for different quantum states $\|\psi_k\rangle$, i.e., for different $k \in [N]$. However, we can include these deviations from the measurement bases $\mathcal{D}_0$ and $\mathcal{D}_1$ of $\mathcal{A}$ in the bases $\mathcal{D}^k_{u_k}$ of preparation by $\mathcal{B}$, and assume that $\mathcal{A}$ applies either $\mathcal{D}_0$ or $\mathcal{D}_1$ to $\|\psi_k\rangle$, for $k \in [N]$. In other words, the uncertainty angle θ on the Bloch sphere accounts for both preparation and measurement misalignments. Thus, our analysis is without loss of generality.
6	There are errors in Alice's quantum measurements.	Thus, Alice obtains some errors in the measurements that she performs in the same basis of preparation by Bob. For this reason, in the validation stage, Bob allows a fraction of bit errors in Alice's reported measurement outcomes, up to a predetermined small threshold $\gamma_{\text{err}} > 0$, where "err" stands for "errors".
7	$\mathcal{A}$ generates the bit z with probability distribution $P_{\text{E}}(z)$ that has small deviation from the random distribution given by a bias $\beta_{\text{E}} > 0$.	That is, we have that $\frac{1}{2} - \beta_{\text{E}} \leq P_{\text{E}}(z) \leq \frac{1}{2} + \beta_{\text{E}}$, for $z \in \{0, 1\}$. The subindex "E" refers to "encoding". $\mathcal{A}$ can guarantee the parameter β_{E} to decrease exponentially with a number N_{CRB} of close-to-random bits with biases not greater than $\beta_{\text{CRB}} \in (0, \frac{1}{2})$, as follows from the Piling-up Lemma[56].
8	In photonic setups, the single-photon detectors used by $\mathcal{A}$ are threshold, i.e., they cannot distinguish the number of photons activating a detection. Moreover, the detectors have nonzero dark count probabilities.	Thus, for some photon pulses received from $\mathcal{B}$, more than one of the detectors of $\mathcal{A}$ click. In order to counter multi-photon attacks[53], in which $\mathcal{B}$ sends and tracks multi-photon pulses to obtain information about the measurement bases of $\mathcal{A}$, and guarantee privacy, $\mathcal{A}$ must carefully choose how to report multiple clicks to $\mathcal{B}$, i.e., how to define successful measurements. For this reason, in the second step of our token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ with the photonic setups of Fig. 3, $\mathcal{A}$ implements the reporting strategies 1 and 2, respectively. As follows from straightforward extensions of Lemmas 1 and 12 of ref. [53], assumption F (see Table 6) guarantees that these reporting strategies offer perfect protection against arbitrary multi-photon attacks (see Lemma 5 in Methods).

unforgeability, and user privacy. Importantly, Theorem 2 shows that this holds, in principle, for 2^M presentation points with arbitrary M. As in the schemes of ref. [28], our schemes allow the user to choose her presentation point Q_b after her quantum measurements are completed, as long as she chooses Q_b within the intersection of the causal past of all the presentation points. This means that the quantum communication stage of our schemes can take an arbitrarily long time and can be implemented arbitrarily in the past of the presentation points, which is very convenient for practical implementations.

We note that the security of our quantum token schemes does not rely on any spacetime constraints. In principle, all presentation points could be timelike separated, for example. However, as discussed in the introduction, in order for our quantum token schemes to have an advantage over purely classical schemes, some spacetime presentation points need to be spacelike separated.

In practice, this means that some classical processing and classical communication steps in our schemes must be implemented sufficiently fast. This is in general feasible with current technology (for example, using field programmable gate arrays), if the presentation points are sufficiently far apart, as demonstrated by previous implementations of relativistic cryptographic protocols[33,34,37–39]. Furthermore, Alice's and Bob's laboratories must be

Table 6. Assumptions for $\mathcal{QT}_1$ and $\mathcal{QT}_2$.

Label	Brief description	Explanation and comments
A	For $k \in \Omega_{\text{qub}}$, $\mathcal{B}$ prepares $\|\psi_k\rangle = \left\|\phi^k_{t_k u_k}\right\rangle$, where $\langle\phi^k_{0u}\|\phi^k_{1u}\rangle = 0$, defining the qubit orthonormal basis $\mathcal{D}^k_u = \{\|\phi^k_{tu}\rangle\}^1_{t=0}$, for $u \in \{0, 1\}$.	That is, we assume that $\mathcal{B}$ prepares each qubit state from exactly two qubit bases. However, in the most general case (not considered here), $\mathcal{B}$ prepares each qubit state from a set of four qubit states that does not necessarily define two qubit basis.
B	$\mathcal{B}$ generates the bit strings $\mathbf{t} = (t_1, \ldots, t_N)$ and $\mathbf{u} = (u_1, \ldots, u_N)$ with probability distributions that are exactly products of single bit probability distributions.	In the general case (not considered here), the strings $\mathbf{t}$ and $\mathbf{u}$ could be generated with a probability distribution in which $\mathbf{t}$ and $\mathbf{u}$, and different bit entries of $\mathbf{t}$ and $\mathbf{u}$, could be correlated.
C	The set Λ of labels transmitted to $\mathcal{B}$ in step 2 of $\mathcal{QT}_1$ and $\mathcal{QT}_2$ gives $\mathcal{B}$ no information about the string W and the bit z.	In the photonic setups of Fig. 3 to implement $\mathcal{QT}_1$ and $\mathcal{QT}_2$, with the reporting strategies 1 and 2, respectively, assumption C (and also assumption D for $\mathcal{QT}_1$) follows from assumptions E and F (see Lemma 5 in Methods).
D	In $\mathcal{QT}_1$, conditioned on reporting the quantum state $\|\psi_k\rangle$ as successfully measured, i.e., conditioned on $k \in \Lambda$, $\mathcal{A}$ measures $\|\psi_k\rangle$ in an orthogonal qubit basis $\mathcal{D}_{w_k}$ with a probability distribution $P_{\text{MB}}(w_k) = \frac{1}{2}$, for $w_k \in \{0, 1\}$ and $k \in [N]$, where the subindex denotes "measurement basis".	This is a necessary, but in general not sufficient, condition for $\mathcal{QT}_1$ to satisfy assumption C. If this assumption did not hold, there would be at least one label $k' \in \Lambda$ for which $P_{\text{MB}}(w_{k'} = i) > P_{\text{MB}}(w_{k'} = i \oplus 1)$, for some $i \in \{0, 1\}$. Thus, $\mathcal{B}$ could in principle guess the entry $w_{k'}$ of W with probability greater than $\frac{1}{2}$. This would mean that the set Λ reported by $\mathcal{A}$ would have given $\mathcal{B}$ some information about W, in contradiction with assumption C.
E	$\mathcal{B}$ cannot use degrees of freedom not previously agreed for the transmission of the quantum states to affect, or obtain information about, the statistics of the quantum measurement devices of $\mathcal{A}$.	This assumption guarantees that $\mathcal{A}$ is perfectly protected from any side-channel attack by $\mathcal{B}$ in any type of physical setup (not necessarily photonic)[53].
F	In the photonic setup of Fig. 3, the detectors D_0, D_1, D_+ and D_- of $\mathcal{A}$ have equal detection efficiencies $\eta \in (0, 1)$, and respective dark count probabilities d_0, d_1, d_+, $d_- \in (0, 1)$ satisfying $(1 - d_0)(1 - d_1) = (1 - d_+)(1 - d_-)$, for $k \in [N]$. In the photonic setup of Fig. 3, the detectors D_0 and D_1 of $\mathcal{A}$ satisfy that: (1) their detection efficiencies have the same value $\eta \in (0, 1)$, for $k \in [N]$; and (2) their dark count probabilities have values $d_0 \in (0, 1)$ and $d_1 \in (0, 1)$, for $k \in [N]$. Dark counts and each photo-detection are independent random events, for $k \in [N]$.	In our notation, the term 'detection efficiency' includes the quantum efficiency of the detectors of $\mathcal{A}$ and the transmission efficiency from the setup of $\mathcal{B}$ to the detectors. We note that the condition $(1 - d_0)(1 - d_1) = (1 - d_+)(1 - d_-)$ can be satisfied if $d_0 = d_+$ and $d_1 = d_-$, or if $d_0 = d_-$ and $d_1 = d_+$, for instance. Exactly equal detection efficiencies cannot be guaranteed in practice. But, attenuators can be used to make the detector efficiencies approximately equal. Furthermore, $\mathcal{A}$ can effectively make the dark count probabilities of her detectors approximately equal by simulating dark counts in the detectors with lower dark count probabilities so that they approximate the dark count probability of the detector with the highest dark count probability. To our knowledge, that dark count and each photo-detection are independent random events is a valid assumption.
G	In photonic setups, from the perspective of $\mathcal{A}$, the pulses of $\mathcal{B}$ are mixtures of Fock states: in particular $\mathcal{A}$ has no information about relative phases of the components with definite photon number.	If this assumption is not satisfied, the quantum state received by $\mathcal{A}$ could not be described by our analysis, opening the possibility to attacks more powerful than the ones considered in our security proof (e.g., more powerful state discrimination attacks[57]). This assumption is consistent with our security analysis and is satisfied in practice if $\mathcal{B}$ uses a weak coherent source and he uniformly randomizes the phase of each pulse transmitted to $\mathcal{A}$; or if $\mathcal{B}$ uses an arbitrary photonic source with arbitrary signal states and he applies a physical operation to the transmitted pulses with the property that it applies a random phase φ per photon—i.e., an l-photon pulse acquires an amplitude $e^{il\varphi}$[58]. Alternatively, this condition can be satisfied to a good approximation if $\mathcal{B}$ uses a photonic source with low spatiotemporal coherence, for example, a source comprising LEDs[59], as in our experimental tests reported below.

synchronized securely to a common reference frame with sufficiently high time precision. This can be implemented using GPS devices and atomic clocks[33,34,37–39], for example. A detailed analysis of these experimental challenges is left for future work.

Using quantum key distribution for secure communications in our quantum token schemes can be useful, but it is not crucial. As discussed, Alice's and Bob's agents must communicate via secure and authenticated classical channels, which can be implemented with previously distributed secret keys. In an ideal situation where Alice's and Bob's agents have access to enough quantum channels, for example in a quantum network[40–43] or in the envisaged quantum internet[44,45], these keys can be expanded securely with quantum key distribution[30,46,47]. However, it is also possible to distribute the secret keys via secure physical transportation, as implemented in previous demonstrations of relativistic quantum cryptography[33,34,37–39].

We note that in our proof of unforgeability, our only potential restriction on the technology and capabilities of dishonest Alice is indirectly made through assumption G in photonic setups (see Table 6), in the case where Bob's photon source does not perfectly conceal phase information. In fact, we believe that assumptions A, B, and G can be significantly weakened. Investigating unforgeability for realistic weaker forms of these assumptions is left as an open problem.

We implemented experimental tests of the quantum part of our scheme ($\mathcal{QT}_1$) using a free space optical setup[48,49] for quantum key distribution (QKD) that was slightly adapted for our scheme, and which can operate at daylight conditions. Importantly, Bob's transmission device is small, hand-held, and low cost. These type of QKD setups are designed for future daily-life applications, for example with mobile devices (see e.g., [50–52]).

Experiments with our relatively low precision devices do not guarantee unforgeability, but show it can be guaranteed with refinements. Crucial experimental parameters that we need to improve to achieve this are the deviations β_{PB} and β_{PS} from random basis and state generation, respectively. In our tests we obtained $\beta_{\text{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\text{PS}} = 3.6 \times 10^{-3}$. An implementation in which the uncertainty in basis choices was bounded by $\theta = 5^\circ$ and the error rate by $E = 0.03$ would guarantee unforgeability if $\beta_{\text{PB}} \approx \beta_{\text{PS}} \approx 2.3 \times 10^{-4}$ (about a factor of 10 and 16 lower

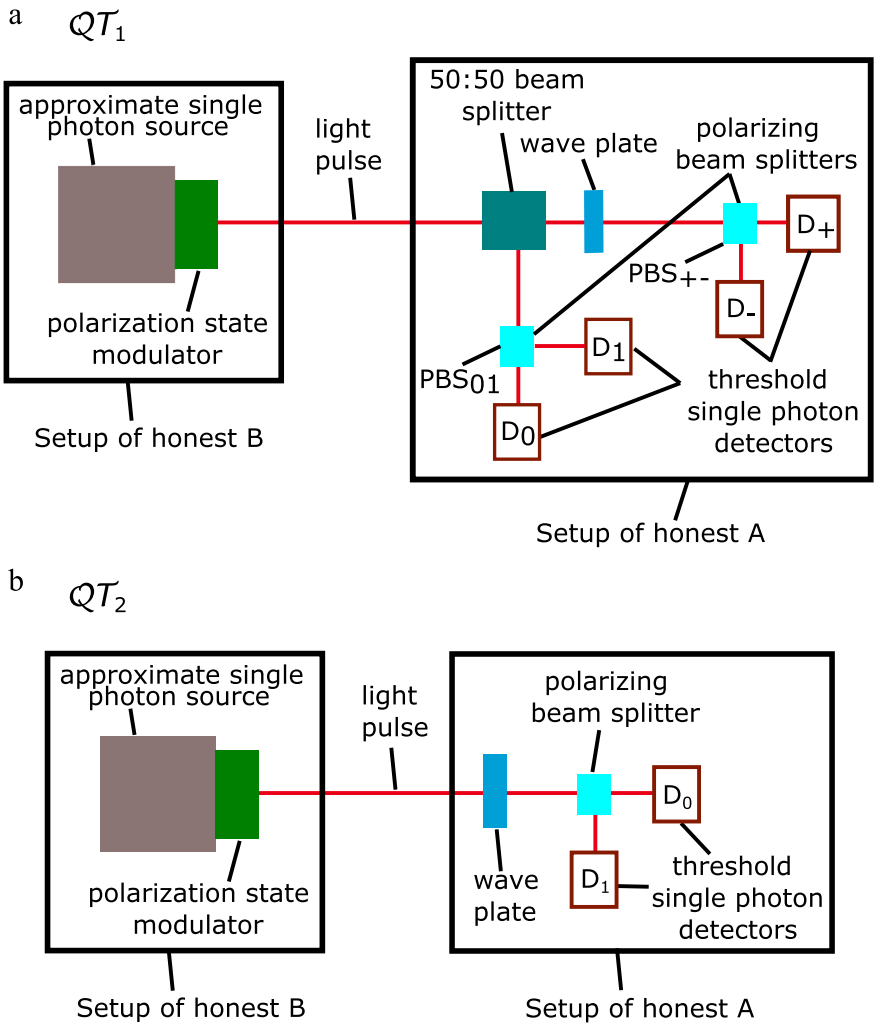

Fig. 3 Photonic setups to implement the quantum stage of $\mathcal{QT}_1$ and $\mathcal{QT}_2$. In both $\mathcal{QT}_1$ and $\mathcal{QT}_2$, the setup of honest $\mathcal{B}$ comprises an approximate single-photon source and a polarization state modulator, encoding the quantum state $|\psi_k\rangle$ in the polarization degrees of freedom of a photon pulse labeled by k, for $k \in [N]$. **a** In $\mathcal{QT}_1$, the setup of honest $\mathcal{A}$ comprises a 50:50 beam splitter, a wave plate, two polarizing beam splitters (PBS_{01} and PBS_{+-}), and four threshold single-photon detectors D_0, D_1, D_+, and D_-. In order to counter multi-photon attacks by $\mathcal{B}$,$\mathcal{A}$ implements the following reporting strategy that we call here reporting strategy 1: $\mathcal{A}$ assigns successful measurement outcomes in the basis $\mathcal{D}_0$ ($\mathcal{D}_1$) with unit probability for the pulses in which at least one of the detectors D_0 and D_1 (D_+ and D_-) click and D_+ and D_- (D_0 and D_1) do not click. As follows from ref. [53], this reporting strategy offers perfect protection against arbitrary multi-photon attacks, given assumption F (see Table 6, and Lemma 5 in Methods). **b** In $\mathcal{QT}_2$, the setup of honest $\mathcal{A}$ comprises a wave plate set in one of two positions, according to the value of her bit z, a polarizing beam splitter, and two threshold single-photon detectors D_0 and D_1. In order to counter multi-photon attacks by $\mathcal{B}$, $\mathcal{A}$ implements the following reporting strategy that we call here *reporting strategy 2*: $\mathcal{A}$ reports to $\mathcal{B}$ as successful measurements those in which at least one of her two detectors click. As follows from ref. [53], this reporting strategy offers perfect protection against arbitrary multi-photon attacks, given assumption F (see Table 6, and Lemma 5 in Methods).

than our values). This highlights that it is crucial to consider the parameters β_{PS} and β_{PB} in practical security proofs. For example, if we simply assumed $\beta_{PS} = \beta_{PB} = 0$ as our experimental values then our results would imply that we had attained unforgeability, even for $\theta = 10^\circ$ (see Fig. 5). Taking $\beta_{PS} = \beta_{PB} = \theta = 0$, as implicitly assumed in some previous analyses of practical mistrustful quantum cryptography (e.g., [33,34,36]), is unsafe.

User privacy can also be guaranteed by using good enough random number generators. However, further security issues arise from the assumptions that Bob cannot use degrees of freedom not previously agreed for the transmission of the quantum states to affect, or obtain information about, the statistics of Alice's quantum measurement devices; and, in photonic setups, that Alice's single-photon detectors have equal efficiencies and equal dark count probabilities (assumptions E and F in Table 6). These issues are not specific to our implementations or to quantum token schemes: they arise quite generally in practical mistrustful quantum cryptographic schemes in which one party measures states sent by the other. The attacks they allow and defences against these (such as requiring single-photon sources and using attenuators to equalize detector efficiencies) are analysed in detail elsewhere[53]. As noted in ref. [53], further options, such as iterating the scheme and using the XOR of the bits generated, also merit investigation. Importantly, our analyses here take into account multi-photon attacks[53] in photonic setups, and the reporting strategies we have considered offer perfect protection against arbitrary multi-photon attacks, given our assumptions (see Fig. 3, and Lemma 5 in Methods).

In conclusion, our theoretical and experimental results give a proof of principle that quantum token schemes are implementable with current technology, and that, conditioned on standard technological assumptions, security can be maintained in the presence of the various experimental imperfections we have considered (see Table 5). As with other practical implementations

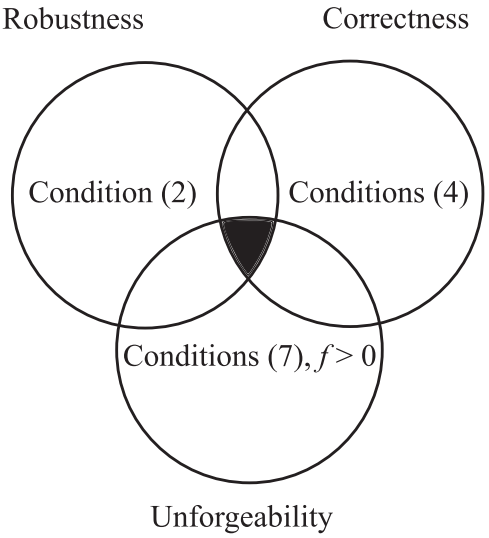

Fig. 4 Illustration of security conditions for $\mathcal{QT}_1$ and $\mathcal{QT}_2$. A diagram presenting the conditions under which robustness, correctness, and unforgeability of the quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are satisfied simultaneously is illustrated (see Lemmas 2 and 3 and Theorem 1). The function f is defined by (8). If all the conditions are satisfied (filled area) then there exist a sufficiently large integer N such that $\mathcal{QT}_1$ and $\mathcal{QT}_2$ are ϵ_{rob}-robust, ϵ_{cor}-correct and ϵ_{unf}-unforgeable, for desired values of ϵ_{rob}, ϵ_{cor}, $\epsilon_{\text{unf}} > 0$.

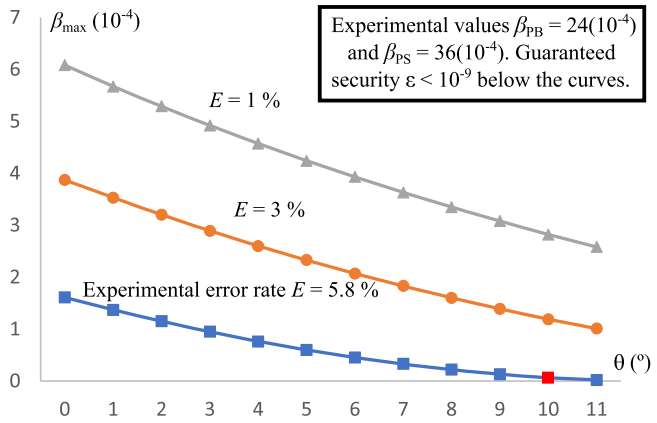

Fig. 5 Numerical example. The plots denote the maximum value $\beta_{\max}$ for β_{PB} and β_{PS} that our bounds can allow to guarantee correctness, robustness, and unforgeability simultaneously in a numerical example with the allowed experimental imperfections of Table 5 and under the assumptions of Table 6 for our quantum token schemes $\mathcal{QT}_1$ and $\mathcal{QT}_2$. The region below the plotted curves denotes the secure region in which we have set $\epsilon_{\text{rob}} = \epsilon_{\text{cor}} = \epsilon_{\text{unf}} = 10^{-9}$ in Lemmas 2 and 3 and in Theorem 1. The plotted values keep all parameters fixed to the experimental values reported above, except for the deviations from the random distributions for basis and state generation, β_{PB} and β_{PS}, the uncertainty θ on the Bloch sphere in the state generation, and the error rate E. The blue curve denotes the values obtained for the experimentally obtained value $E = 0.058$. The red square denotes the assumed upper bound for our experimental values of $\theta \leq 10^{\circ}$, and corresponds to a value of $\beta_{\max} = 6 \times 10^{-6}$, which is about 400 and 600 times smaller than the obtained experimental values of $\beta_{\text{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\text{PS}} = 3.6 \times 10^{-3}$, respectively. The orange and gray curves plot the values of $\beta_{\max}$ assuming $E = 0.03$ and $E = 0.01$, respectively. In an ideal case in which $\theta = 0^{\circ}$ and $E = 0.01$, the value for $\beta_{\max}$ would be $\sim 6 \times 10^{-4}$, which is about four and six times smaller than our obtained experimental values for β_{PB} and β_{PS}, respectively. In a more realistic case, with $\theta = 5^{\circ}$ and $E = 0.03$, our numerical example gives approximately $\beta_{\max} = 2.3 \times 10^{-4}$; meaning that with these experimental values, by reducing our obtained experimental values for β_{PB} and β_{PS} by respective factors of ~10 and 16, we could guarantee correctness, robustness, and unforgeability simultaneously in our schemes.

of mistrustful quantum cryptography (and indeed quantum key distribution), completely unconditional security would require defences against every possible collection of physical systems Bob might transmit to Alice, including programmed nano-robots that could enter and reconfigure her laboratory[54]. Attaining this is beyond current technology, but such far-fetched possibilities also illustrate that security based on suitable technological assumptions (which may depend on the context) may suffice for practical purposes. More work on attacks and defences in practical mistrustful quantum cryptography is undoubtedly needed to reach a consensus on trustworthy technologies. That said, as our schemes are built on simple mistrustful cryptographic primitives, we expect they can be refined to incorporate any agreed practical defences[53].

METHODS

Protection against multi-photon attacks in photonic implementations

The following lemma is a straightforward extension of Lemmas 1 and 12 of ref. [53] to the case of $N > 1$ transmitted photon pulses. Note that Alice (Bob) in our notation refers to Bob (Alice) in the notation of ref. [53]. The proof is given in Supplementary Note VI.

Lemma 5. Suppose that Bob sends Alice N photon pulses, labeled by $k \in [N]$. Let the kth pulse have L_k photons. Let ρ be an arbitrary quantum state prepared by Bob in the polarization degrees of freedom of the photons sent to Alice, which can be arbitrarily entangled among all photons in all pulses and can also be arbitrarily entangled with an ancilla held by Bob. Let $\mathcal{D}_0$ and $\mathcal{D}_1$ be two arbitrary qubit orthogonal bases. Suppose that either Alice uses the setup of Fig. 3 with reporting strategy 1 to implement the quantum token scheme $\mathcal{QT}_1$ (see Table 2), or Alice uses the setup of Fig. 3 with reporting strategy 2 to implement the quantum token scheme $\mathcal{QT}_2$ (see Table 3). Suppose also that assumptions E and F (see Table 6) hold. For $k \in [N]$, let $m_k = 1$ if Alice assigns a successful measurement to the kth pulse and $m_k = 0$ otherwise; let $w_k = 0$ ($w_k = 1$) if Alice assigns a measurement basis to the kth pulse in the basis $\mathcal{D}_0$ ($\mathcal{D}_1$). If Alice uses the setup of Fig. 3 and reporting strategy 1 to implement the scheme $\mathcal{QT}_1$, without loss of generality, suppose also that Alice sets $w_k = 0$ with unit probability, if $m_k = 0$, for $k \in [N]$. Let $m = (m_1, \ldots, m_N)$, $w = (w_1, \ldots, w_N)$ and $L = (L_1, \ldots, L_N)$.

If Alice uses the setup of Fig. 3 with reporting strategy 1 to implement the scheme $\mathcal{QT}_1$, then the probability that Alice reports the string m to Bob and assigns the string of measurement bases w, given ρ and L, is

$$P^{(1)}_{\text{rep}}(m, w|\rho, L) = \prod_{k=1}^{N} G^{(1)}_{m_k, w_k}(d_0, d_1, \eta, L_k), \tag{12}$$

where

$$\begin{aligned} G^{(1)}_{1,b}(d_0, d_1, \eta, a) &= (1-d_0)(1-d_1)\left(1-\tfrac{\eta}{2}\right)^a - (1-d_0)^2(1-d_1)^2(1-\eta)^a, \\ G^{(1)}_{0,0}(d_0, d_1, \eta, a) &= 1 - 2G^{(1)}_{1,0}(d_0, d_1, \eta, a), \\ G^{(1)}_{0,1}(d_0, d_1, \eta, a) &= 0, \end{aligned} \tag{13}$$

for $b \in \{0, 1\}$, $m, w \in \{0, 1\}^N$ and $a, L_1, \ldots, L_N \in \{0, 1, 2, \ldots\}$. Furthermore, the probability $P_{\text{MB}}(w_k)$ that Alice assigns a measurement in the basis $\mathcal{D}_{w_k}$, conditioned on the value $m_k = 1$, for the kth pulse, satisfies

$$P_{\text{MB}}(w_k) = \frac{1}{2}, \tag{14}$$

for $w_k \in \{0, 1\}$ and $k \in [N]$.

If Alice uses the setup of Fig. 3 with reporting strategy 2 to implement the scheme $\mathcal{QT}_2$, then the probability that Alice reports the string m to

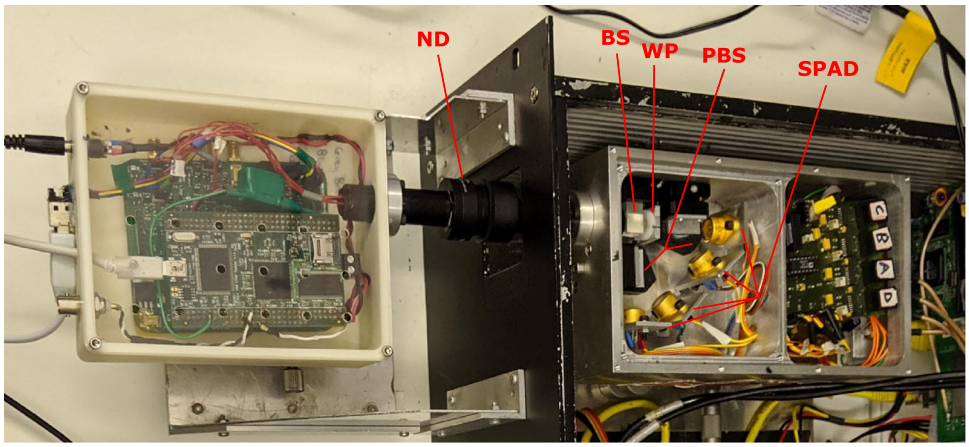

Fig. 6 Photograph of the experimental setup. Bob's quantum transmitter (white box in the left) is a small and low-cost hand-held device of ~20 cm × 15 cm × 5 cm. Alice's quantum receiver is contained within a box of ~20 cm × 12 cm × 5 cm (grey box on the right), with further electronics contained within another box of ~30 cm × 50 cm × 15 cm (bigger black box). At Bob's site, the QKD transmitter comprises a field programmable gate array (FPGA) which pulses 4 LEDs, each polarized in one of the horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A) states, corresponding to the $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ BB84 states, respectively. The light from the LEDs is collimated by a diffraction grating and pinholes. The statistics of Bob's photon source is assumed Poissonian[49,55]. Neutral-density (ND) filters (small black cylinders) are used to attenuate the pulses down to the required mean photon number, which in our experiment was $\mu = 0.09$. Since Bob's photon source consists of LEDs, and LEDs have low spatiotemporal coherence[59], no phase randomization is required to satisfy assumption G to a good approximation (see Table 6). At Alice's site, the received light pulses from Bob are focused from the transmitter pinhole, through a 50:50 beam splitter (BS, small transparent cube) which performs basis selection, and wave plate (WP, thin white cylinder), and polarizing beam splitters (PBS, small black boxes) which perform the measurement of the polarization. The photons are detected with single-photon avalanche diodes (SPAD, small golden cylinders), which are threshold single-photon detectors with efficiency $\eta = 0.21$, including the quantum efficiency of the detectors and the transmission efficiency from Bob's setup to the detectors. An FPGA time tags the detections with 52 bit precision, equivalent to 30.5 ps[60], and sends them to a PC for processing. Alice's grey and black boxes are closed during operation to decrease noise due to environment light. But they are shown open here for illustration.

Bob, given ρ, w, and L, is

$$P^{(2)}_{\mathrm{rep}}(m|w,\rho,L) = \prod_{k=1}^{N} G^{(2)}_{m_k}(d_0,d_1,\eta,L_k), \tag{15}$$

where

$$\begin{aligned} G^{(2)}_0(d_0,d_1,\eta,a) &= (1-d_0)(1-d_1)(1-\eta)^a, \\ G^{(2)}_1(d_0,d_1,\eta,a) &= 1-(1-d_0)(1-d_1)(1-\eta)^a, \end{aligned} \tag{16}$$

for m, $w \in \{0,1\}^N$ and a, L_1, …, $L_N \in \{0, 1, 2, \ldots\}$.

In any of the two cases, the message m gives Bob no information about the bit entries w_k for which $m_k = 1$. Equivalently, the set $\Lambda \subset [N]$ of labels transmitted to Bob in step 2 of $\mathcal{QT}_1$ and $\mathcal{QT}_2$ gives Bob no information about the string W and the bit z.

Clarification about unforgeability in photonic implementations

A subtle technical issue when implementing our quantum token schemes with photonic setups is that in our schemes we have assumed the quantum systems A_k that Bob transmits to Alice to have finite Hilbert space dimension, for $k \in [N]$. However, some light sources, like weak coherent sources, or other photon sources with Poissonian statistics, can emit pulses with a number of photons J, where J can tend to infinity, although with a probability tending to zero. This issue is easily solved by fixing a maximum number of photons $J_{\max}$ and assuming that unforgeability is not guaranteed whenever Bob's photon source emits a pulse with more than $J_{\max}$ photons. By fixing $J_{\max}$ to be arbitrarily large, but finite, the probability that among the N emitted pulses there is at least one pulse with more than $J_{\max}$ photons can be made arbitrarily small. Thus, with probability arbitrarily close to unity, honest Bob is guaranteed that each of his N emitted pulses does not have more than $J_{\max}$ photons, i.e., the internal degrees of freedom—like the polarization degrees of freedom— of each pulse, represented by the quantum system A_k, have a finite Hilbert space dimension.

Experimental setup

Our experimental setup is based on a free space optical quantum key distribution (QKD) system, which can operate at daylight conditions. This setup was developed by one of us (DL) during his PhD[49], based upon the work of ref. [48]. The main features of our experimental setup are illustrated in Figs. 3 and 6.

Only minor changes to our quantum setup are needed to implement the quantum stage of $\mathcal{QT}_2$. For example, the 50:50 beam splitter in Alice's site can be replaced by a suitably placed mirror directing the received photon pulses to one of the two polarizing beam splitters. This mirror can be set in a movable arm, which positions the mirror in place if z has a specific value (e.g., if $z = 1$) and out of place, letting the photon pulses reach the other polarizing beam splitter, if z takes the other value (e.g., $z = 0$). The movable arm putting the mirror in place or out of place does not need to move very fast, as it remains in the same position during the transmission of all N pulses from Bob in the case of two presentation points, or during the transmission of each set of N pulses from the total of NM in the case of 2^M presentation points (see quantum token scheme $\mathcal{QT}_2^M$ in Supplementary Note VIII).

Experimental tests and numerical example

The quantum stage of the token scheme $\mathcal{QT}_1$ was implemented with the experimental setup described above. Below we describe our experiment and the numerical example of Fig. 5. Unless we consider it necessary or helpful, all values smaller than unity obtained in our experiment and numerical example are given below rounded to two significant figures.

As we explain below, our obtained experimental values for the parameters in Lemmas 2 and 3 and in Theorem 1 are $N = 4 \times 10^7$, $P_{\mathrm{det}} = 0.019$, $E = 0.058$, $\beta_{\mathrm{PB}} = 2.4 \times 10^{-3}$, $\beta_{\mathrm{PS}} = 3.6 \times 10^{-3}$, $P_{\mathrm{noqub}} = 3.8 \times 10^{-3}$. We assume an angle $\theta \leq 10^\circ$ in our experiment.

In the numerical example of Fig. 5 we used the previous experimental values, except for θ and E, which were varied as shown in the plots, and for β_{PB} and β_{PS}. In the plots of Fig. 5, if $\beta_{\mathrm{PB}} \leq \beta_{\max}$ and $\beta_{\mathrm{PS}} \leq \beta_{\max}$ hold, then we obtain from Lemmas 2 and 3 and from Theorem 1 that ϵ_{rob}, ϵ_{cor}, $\epsilon_{\mathrm{unf}} \leq 10^{-9}$. We do not claim that our numerical example is optimal. In other words, we do not claim that with our experimental parameters every point above the curves of Fig. 5 is insecure, in the sense that the conditions ϵ_{rob}, ϵ_{cor}, $\epsilon_{\mathrm{unf}} \leq 10^{-9}$ do not hold. Our claim is only that given our experimental parameters, the regions of points below the curves of Fig. 5 satisfy the conditions ϵ_{rob}, ϵ_{cor}, $\epsilon_{\mathrm{unf}} \leq 10^{-9}$.

For the three curves of Fig. 5, we set $\gamma_{\mathrm{det}} = 0.018$. Thus, condition (2) of Lemma 2 is satisfied, and from (3), we have $\epsilon_{\mathrm{rob}} = e^{-1052} < 10^{-9}$.

For the three curves of Fig. 5, we set $v_{\mathrm{unf}} = 3.9 \times 10^{-3}$. This is the minimum value for which the first term of ϵ_{unf} in (10) equals $\frac{10^{-9}}{2}$. This is because, as we describe below, we also chose the parameters satisfying that the second term of ϵ_{unf} in (10) equals $\frac{10^{-9}}{2}$, from which we have $\epsilon_{\mathrm{unf}} = 10^{-9}$. We recognize that although this particular choice seems natural, it probably does not optimize our results.

Then, for each of the three considered error rates $E = 0.01$, $E = 0.03$, and $E = 0.058$, and for each of the angles $\theta = 0°, 1°, \ldots, 11°$, we set $\beta_{\mathrm{PB}} = \beta_{\mathrm{PS}} = \beta_{\max}$ and varied $\beta_{\max}$, v_{cor}, and γ_{err} trying to find the maximum value of $\beta_{\max}$ for which both terms of ϵ_{cor} in (5) and the second term of ϵ_{unf} in (10) were as close as possible to $\frac{10^{-9}}{2}$, but not bigger than $\frac{10^{-9}}{2}$, while guaranteeing that the constraints (4) and (7) were satisfied. Our results for $\beta_{\max}$ are plotted in Fig. 5.

We describe how we obtained the experimental parameters presented above. At a repetition rate of 10 MHz, Bob transmitted photon pulses to Alice during 4 s. Thus, the number of transmitted pulses was $N = 4 \times 10^7$.

Since the photon statistics of Bob's source is assumed Poissonian[49,55], the probability that a photon pulse has two or more photons is $P_{\mathrm{noqub}} = 1 - (1+\mu)e^{-\mu}$. Since in our experiment $\mu = 0.09$, we obtain $P_{\mathrm{noqub}} = 3.8 \times 10^{-3}$.

As discussed below, Alice assigned successful measurements using reporting strategy 1. The number of pulses for which Alice assigned successful measurement was $n = 742{,}491$. The obtained estimation for the probability P_{det}, was obtained as $P_{\mathrm{det}} = \frac{n}{N} = 0.019$.

The measured detection efficiency, including the quantum efficiency of the detectors and the transmission probability from Bob's setup to the detectors, was $\eta = 0.21$. We note that our obtained value of $P_{\mathrm{det}} = 0.01856$, which we reported above with the less precise value $P_{\mathrm{det}} = 0.019$, is a good approximation to the theoretical prediction in which the photon statistics of Bob's source follow a Poisson distribution with average photon number $\mu = 0.09$, Alice uses reporting strategy 1 with her four detectors having the same efficiency $\eta = 0.21$, and the dark count probabilities are assumed to be zero. As follows from (12) and (13) in Lemma 5, this theoretical prediction for P_{det} is given by

$$\begin{aligned} P_{\mathrm{det}}^{\mathrm{theo}} &= \sum_{k=0}^{\infty} \frac{e^{-\mu}\mu^k}{k!} \left(G_{1,0}^{(1)}(0,0,\eta,k) + G_{1,1}^{(1)}(0,0,\eta,k) \right) \\ &= 2 \sum_{k=0}^{\infty} \frac{e^{-\mu}\mu^k}{k!} \left[\left(1 - \tfrac{\eta}{2}\right)^k - (1-\eta)^k \right] \\ &= 2\left(e^{-\frac{\mu\eta}{2}} - e^{-\mu\eta} \right) \\ &= 0.01863, \end{aligned} \tag{17}$$

where in the last line we used our experimental parameters $\mu = 0.09$ and $\eta = 0.21$. This gives a ratio $\frac{P_{\mathrm{det}}}{P_{\mathrm{det}}^{\mathrm{theo}}} = 0.996$.

As mentioned in Fig. 3, Alice applies reporting strategy 1, in order to protect against multi-photon attacks[53] (see Lemma 5). That is, Alice assigns successful measurement outcomes in the basis $\mathcal{D}_0$ ($\mathcal{D}_1$) with unit probability for the pulses in which at least one of the detectors D_0 and D_1 (D_+ and D_-) click and D_+ and D_- (D_0 and D_1) do not click. It is clear that when only the detector D_i clicks, Alice associates the measurement outcome to the BB84 state $|i\rangle$, for $i \in \{0, 1, +, -\}$. However, it is not clear how Alice should assign measurement outcomes to the cases in which both D_0 and D_1 (D_+ and D_-) click and D_+ and D_- (D_0 and D_1) do not click. The results of Lemma 5 are independent of how Alice assigns these outcomes. In order to make clear this generality of the results of Lemma 5, we have not included how these outcomes are assigned by Alice in the definition of reporting strategy 1 in Fig. 3. Nevertheless, how these outcomes are assigned by Alice plays a role in the error rate E, and thus also in the degrees of correctness and unforgeability that can be guaranteed (see Lemma 3 and Theorem 1). In our experiment, Alice assigns a random measurement outcome associated to the state $|0\rangle$ and $|1\rangle$ ($|+\rangle$ and $|-\rangle$) when both D_0 and D_1 (D_+ and D_-) click and D_+ and D_- (D_0 and D_1) do not click.

As mentioned above, in our experiment we obtained Alice's error rate $E = 0.058$, and deviations from the random distributions for basis and state generation by Bob of $\beta_{\mathrm{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\mathrm{PS}} = 3.6 \times 10^{-3}$, respectively. These values were computed as we describe below.

Statistical information

In our experimental tests, the number of photon pulses transmitted from Bob to Alice was $N = 4 \times 10^7$. The number of pulses for which Alice assigned successful measurement was $n = 742{,}491$. The obtained estimation for the probability P_{det}, was obtained as $P_{\mathrm{det}} = \frac{n}{N} = 0.019$.

The error rate $E = 0.058$ was computed as follows. From the n pulses that Alice assigned as successful measurements, n_{tu}^{same} pulses were prepared by Bob with polarization given by the qubit state $|\phi_{tu}\rangle$ and were measured by Alice in the same basis of preparation by Bob ($\mathcal{D}_u = \{|\phi_{tu}\rangle\}_{t=0}^{1}$), from which n_{tu}^{error} gave Alice the outcome opposite to the state prepared by Bob, i.e., an error, for $t, u \in \{0, 1\}$. We computed $E_{tu} = \frac{n_{tu}^{\mathrm{error}}}{n_{tu}^{\mathrm{same}}}$, for $t, u \in \{0, 1\}$. The estimation for the error rate E was taken as $E = \max\{E_{00}, E_{10}, E_{01}, E_{11}\}$. We obtained $n_{00}^{\mathrm{same}} = 80786$, $n_{10}^{\mathrm{same}} = 121159$, $n_{01}^{\mathrm{same}} = 93618$, $n_{11}^{\mathrm{same}} = 80653$, $n_{00}^{\mathrm{error}} = 4725$, $n_{10}^{\mathrm{error}} = 2250$, $n_{01}^{\mathrm{error}} = 1602$, and $n_{11}^{\mathrm{error}} = 3851$. From these values, we obtained $E_{00} = 0.058$, $E_{10} = 0.019$, $E_{01} = 0.017$, $E_{11} = 0.048$, and $E = 0.058$.

Our experimentally obtained estimations $\beta_{\mathrm{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\mathrm{PS}} = 3.6 \times 10^{-3}$ were obtained from the number n of pulses that Alice reported as successfully measured. We did not use the whole number N of transmitted pulses for these estimations, because the software integrated into our experimental setup is configured to output data for the pulses that produce a detection event in at least one detector. From the $n = 742{,}491$ pulses reported above, Bob produced n_{tu} pulses in the state $|\phi_{tu}\rangle$, for $t, u \in \{0, 1\}$. We note that $n = n_{00} + n_{10} + n_{01} + n_{11}$. We computed $\beta_{\mathrm{PB}} = \left| \frac{n_{00}+n_{10}}{n} - \frac{1}{2} \right|$ and $\beta_{\mathrm{PS}} = \max\left\{ \left| \frac{n_{00}}{n_{00}+n_{10}} - \frac{1}{2} \right|, \left| \frac{n_{01}}{n_{01}+n_{11}} - \frac{1}{2} \right| \right\}$. We obtained $n_{00} = 185{,}166$, $n_{10} = 187842$, $n_{01} = 184251$, $n_{11} = 185232$, $\beta_{\mathrm{PB}} = 2.4 \times 10^{-3}$, and $\beta_{\mathrm{PS}} = 3.6 \times 10^{-3}$.

DATA AVAILABILITY

The datasets generated and analysed during the current study are available from the corresponding author on reasonable request.

Received: 21 April 2021; Accepted: 11 January 2022;
Published online: 11 March 2022

REFERENCES

1. Wiesner, S. Conjugate coding. *ACM Sigact News* **15**, 78 (1983).
2. D., Gavinsky, Quantum money with classical verification. in *Proc. 2012 IEEE 27th Annual Conference on Computational Complexity* (CCC) 42–52 (IEEE, 2012).
3. Molina, A., Vidick, T. & Watrous, J. in *Theory of Quantum Computation, Communication, and Cryptography* (eds Iwama, K., Kawano, Y. & Murao, M.) 45–64. (Springer, 2012).
4. Pastawski, F., Yao, N. Y., Jiang, L., Lukin, M. D. & Cirac, J. I. Unforgeable noise-tolerant quantum tokens. *Proc. Natl. Acad. Sci. USA* **109**, 16079 (2012).
5. Georgiou, M. & Kerenidis, I. New constructions for quantum money. in *LIPIcs-Leibniz International Proceedings in Informatics* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015).
6. Moulick, S. R. & Panigrahi, P. K. Quantum cheques. *Quantum Inf. Process.* **15**, 2475–2486 (2016).
7. Amiri, R. & Arrazola, J. M. Quantum money with nearly optimal error tolerance. *Phys. Rev. A* **95**, 062334 (2017).
8. Bozzio, M., Diamanti, E. & Grosshans, F. Semi-device-independent quantum money with coherent states. *Phys. Rev. A* **99**, 022336 (2019).
9. Kumar, N. Practically feasible robust quantum money with classical verification. *Cryptography* **3**, 26 (2019).
10. Horodecki, K. & Stankiewicz, M. Semi-device-independent quantum money. *New J. Phys.* **22**, 023007 (2020).
11. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802 (1982).
12. Dieks, D. Communication by EPR devices. *Phys. Lett. A* **92**, 271 (1982).
13. Bennett, C. H., Brassard, G., Breidbart, S. & Wiesner, S. in *Advances in Cryptology* (eds Chaum, D., Rivest, R. & Sherman, A.) 267–275 (Springer, 1983).
14. Mosca, M. & Stebila, D. Quantum coins. Error-Correcting Codes, Finite Geometries and Cryptography **523**, 35 (2010).
15. Aaronson, S. & Christiano, P. Quantum money from hidden subspaces. in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '12. 41–60 (Association for Computing Machinery, 2012).
16. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A. & Shor, P. Quantum money from knots. in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12. 276–289 (Association for Computing Machinery, 2012).
17. Kent, A. S-money: virtual tokens for a relativistic economy. *Proc. R. Soc. A* **475**, 20190170 (2019).
18. Wissner-Gross, A. D. & Freer, C. E. Relativistic statistical arbitrage. *Phys. Rev. E* **82**, 056104 (2010).

19. Wang, Y. et al. Single-qubit quantum memory exceeding ten-minute coherence time. *Nat. Photonics* **11**, 646 (2017).
20. Wang, P. et al. Single ion qubit with estimated coherence time exceeding one hour. *Nat. Commun.* **12**, 233 (2021).
21. Wang, Y. et al. Efficient quantum memory for single-photon polarization qubits. *Nat. Photonics* **13**, 346 (2019).
22. Wallucks, A., Marinković, I., Hensen, B., Stockill, R. & Gröblacher, S. A quantum memory at telecom wavelengths. *Nat. Phys.* **16**, 772 (2020).
23. Bartkiewicz, K. et al. Experimental quantum forgery of quantum optical money. *npj Quantum Inf.* **3**, 7 (2017).
24. Behera, B. K., Banerjee, A. & Panigrahi, P. K. Experimental realization of quantum cheque using a five-qubit quantum computer. *Quantum Inf. Process.* **16**, 312 (2017).
25. Bozzio, M. et al. Experimental investigation of practical unforgeable quantum money. *npj Quantum Inf.* **4**, 5 (2018).
26. Guan, J.-Y. et al. Experimental preparation and verification of quantum money. *Phys. Rev. A* **97**, 032338 (2018).
27. Jiráková, K., Bartkiewicz, K., Černoch, A. & Lemr, K. Experimentally attacking quantum money schemes based on quantum retrieval games. *Sci. Rep.* **9**, 16318 (2019).
28. Kent, A. & Pitalúa-García, D. Flexible quantum tokens in spacetime. *Phys. Rev. A* **101**, 022309 (2020).
29. Kent, A. Quantum tokens, US patent 10,790,972 (2020).
30. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. 175–179 (IEEE, 1984).
31. Croke, S. & Kent, A. Security details for bit commitment by transmitting measurement outcomes. *Phys. Rev. A* **86**, 052309 (2012).
32. Ng, N., Joshi, S., Chen Ming, C., Kurtsiefer, C. & Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **3**, 1326 (2012).
33. Lunghi, T. et al. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111**, 180504 (2013).
34. Liu, Y. et al. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.* **112**, 010504 (2014).
35. Pappa, A. et al. Experimental plug and play quantum coin flipping. *Nat. Commun.* **5**, 3717 (2014).
36. Erven, C. et al. An experimental implementation of oblivious transfer in the noisy storage mode. *Nat. Commun.* **5**, 3418 (2014).
37. Lunghi, T. et al. Practical relativistic bit commitment. *Phys. Rev. Lett.* **115**, 030502 (2015).
38. Verbanis, E. et al. 24-hour relativistic bit commitment. *Phys. Rev. Lett.* **117**, 140506 (2016).
39. Alikhani, P. et al. Experimental relativistic zero-knowledge proofs. *Nature* **599**, 47 (2021).
40. Elliott, C. et al. Current status of the DARPA quantum network. In *Quantum Information and Computation III* (eds Donkor, E. J., Pirich, A. R. & Brandt, H. E.) 138–149 (SPIE, 2005).
41. Simon, C. Towards a global quantum network. *Nat. Photonics* **11**, 678 (2017).
42. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
43. Dynes, J. F. et al. Cambridge quantum network. *npj Quantum Inf.* **5**, 101 (2019).
44. Kimble, H. J. The quantum internet. *Nature* **453**, 1023 (2008).
45. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
46. Fröhlich, B. et al. Long-distance quantum key distribution secure against coherent attacks. *Optica* **4**, 163 (2017).
47. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
48. Duligall, J. L., Godfrey, M. S., Harrison, K. A., Munro, W. J. & Rarity, J. G. Low cost and compact quantum key distribution. *New J. Phys.* **8**, 249 (2006).
49. Lowndes, D. L. D. *Low Cost, Short Range Free Space Quantum Cryptography for Consumer Applications: Pocket Size for Pocket Change*. Ph.D. thesis, University of Bristol (2014).
50. Mélen, G. et al. Integrated quantum key distribution sender unit for daily-life implementations, in *Advances in Photonics of Quantum Computing, Memory, and Communication IX* (eds Hasan, Z. U., Hemmer, P. R., Lee, H. & Migdall, A. L.) 31–36 (SPIE, 2016).
51. Mélen, G. et al. Handheld quantum key distribution. in *Quantum Information and Measurement (QIM)* QT6A.57 (Optical Society of America, 2017).
52. Chun, H. et al. Handheld free space quantum key distribution with dynamic m otion compensation. *Opt. Express* **25**, 6784 (2017).
53. Bozzio, M., Cavaillès, A., Diamanti, E., Kent, A. & Pitalúa-García, D. Multiphoton and side-channel attacks in mistrustful quantum cryptography. *PRX Quantum* **2**, 030338 (2021).
54. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999).
55. Hu, Y., Peng, X., Li, T. & Guo, H. On the Poisson approximation to photon distribution for faint lasers. *Phys. Lett. A* **367**, 173 (2007).
56. Matsui, M. Linear cryptanalysis method for DES cipher, in Advances in Cryptology — EUROCRYPT '93, (eds Helleseth, T) 386–397 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994).
57. Dušek, M., Jahma, M. & Lütkenhaus, N. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A* **62**, 022306 (2000).
58. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **41**, 599 (2007).
59. Mehta, D. S., Saxena, K., Dubey, S. K. & Shakher, C. Coherence characteristics of light-emitting diodes. *J. Lumin.* **130**, 96 (2010).
60. Nock, R., Dahnoun, N. & Rarity, J. Low cost timing interval analyzers for quantum key distribution. In *2011 IEEE International Instrumentation and Measurement Technology Conference*. 1–5 (IEEE, 2011).

ACKNOWLEDGEMENTS

The authors acknowledge financial support from the UK Quantum Communications Hub grants no. EP/M013472/1 and EP/T001011/1, and thank Siddarth Koduru Joshi for helpful conversations. A.K. and D.P.-G. also thank Sarah Croke for helpful conversations. A.K. is partially supported by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

AUTHOR CONTRIBUTIONS

A.K and J.R. conceived the project. D.P.-G. did the majority of the theoretical work, with input from A.K. D.L. devised the experimental setup and took the experimental data. D.P.-G. analysed the experimental data and did the numerical work. A.K. and D.P.-G. wrote the manuscript with input from D.L.

COMPETING INTERESTS

A.K. jointly owns the patent "A. Kent, Quantum tokens, US Patent No. 10,790,972 (2020)" and similar patents in other jurisdictions, and has consulted for and owns shares in a corporate co-owner.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00524-4.

Correspondence and requests for materials should be addressed to Damián Pitalúa-García.

Reprints and permission information is available at http://www.nature.com/reprints

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