Practical quantum tokens without quantum memories and experimental tests

Adrian Kent, David Lowndes, Damián Pitalúa-García and John Rarity

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.

INTRODUCTION

Quantum tokens, also called quantum money, were invented by Wiesner 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, 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. Intuitively, this follows from the no-cloning theorem, stating that it is impossible to perfectly copy unknown quantum states. Unforgeable quantum token schemes based on computational assumptions have also been investigated (e.g.,), with some of these schemes not requiring communication with the bank for token validation (e.g.,).

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. 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. 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., 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\textsuperscript{16}, 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\textsuperscript{10,13–16}. Recently, a quantum memory of a single qubit with a coherence time of over an hour has been experimentally demonstrated\textsuperscript{17,18}. However, storing large quantum states for more than a fraction of a second remains challenging\textsuperscript{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\textsuperscript{23–27}. References\textsuperscript{25,26} investigated the experimental implementation of forging attacks on quantum token schemes. Reference\textsuperscript{24} presented a simulation of a quantum token scheme in IBM’s five-qubit quantum computer. References\textsuperscript{23,26} 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.\textsuperscript{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”\textsuperscript{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\textsuperscript{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.\textsuperscript{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\textsuperscript{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.\textsuperscript{25}, 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, where a token can be presented by Alice to Bob, for i ∈ {0, 1}\textsuperscript{M} and for some agreed integer M ≥ 1. Bob has trusted agents B and Bi, controlling secure laboratories, and Alice has trusted agents A and Ai, controlling secure laboratories, for i ∈ {0, 1}\textsuperscript{M}. The agent Ai can send messages to Bi in the spacetime region Qi, for i ∈ {0, 1}\textsuperscript{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 A and Bob’s agent B perform the specified actions in a spacetime region P that lies within the intersection of the causal pasts of all Qi, unless otherwise stated.

The token schemes comprise two main stages. Stage I includes the quantum communication between B and 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 Bi from Ai at Qi can be validated by Bi near-instantly at Qi, 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.\textsuperscript{28}, which gives Alice great flexibility in spacetime to choose her presentation point. See Tables 1–3 for details.

In stage I, B generates quantum states randomly from a predetermined set and gives these to A. A measures the received...
Table 1. Ideal quantum token schemes IQT\(_1\) and IQT\(_2\) for two presentation points. Steps 1 to 8 in IQT\(_1\), and 1 to 5 in IQT\(_2\), take place within the intersection of the causal pasts of the presentation points.

| Ideal quantum token scheme IQT\(_1\) | Stage I |
|-------------------------------------|---------|
| 1. For \(k \in [N], B\) generates the qubit state \(|\psi_k\rangle = |\phi_{u_k}\rangle\) randomly from the BB84 set and sends it to \(A\) with its label \(k\). Let the \(N\) – bit strings \(t = (t_1, ..., t_N)\) and \(u = (u_1, ..., u_N)\) denote the states and bases of preparation by \(B\). |
| 2. For \(k \in [N], A\) 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 \(x\). Let the \(N\)-bit string \(y = (y_1, ..., y_N)\) denote Alice’s measurement bases. |
| 3. \(A\) sends \(x\) to \(A_i\), for \(i \in \{0,1\}\). |
| 4. \(A\) chooses a bit \(z\) randomly and gives \(B\) a string \(d\), where \(d = y\) if \(z = 0\), or \(d = \overline{y}\) if \(z = 1\). |
| 5. For \(i \in \{0,1\}, B\) sends \(d\) to \(B_i\), who computes \(d_i\) in the causal past of \(Q_i\), where \(d_0 = d\) and \(d_1 = \overline{d}\). |
| 6. \(B\) sends \(t\) and \(u\) to \(B_i\), for \(i \in \{0,1\}\). |

| Ideal quantum token scheme IQT\(_2\) | Stage I |
|-------------------------------------|---------|
| 1. As step 1 of IQT\(_1\). |
| 2. The step 2 of IQT\(_1\) is replaced by the following. \(A\) chooses a bit \(z\) randomly. \(A\) measures each received qubit in the computational basis if \(z = 0\) or in the Hadamard basis if \(z = 1\). The string \(y \in \{0,1\}^N\) denoting Alice’s measurement bases has bit entries \(y_k = z\) for \(k \in [N]\). |
| 3. As step 3 of IQT\(_1\). The steps 4 and 5 of IQT\(_1\) are discarded. |
| 4. As step 6 of IQT\(_1\). |

| Ideal quantum token scheme IQT\(_2\) | Stage II |
|-------------------------------------|---------|
| 5. As steps 7 and 8 of IQT\(_1\). |
| 6. The step 9 of IQT\(_1\) is replaced by the following. For \(i \in \{0,1\}\), in the causal past of \(Q_i, B\) computes the string \(d_i \in \{0,1\}^N\) with bit entries \(d_{i,k} = i \oplus c\), for \(k \in [N]\). |
| 7. As steps 10 and 11 of IQT\(_1\). |

- \(\epsilon_{\text{rob}}\) – robust if the probability that Bob aborts when Alice and Bob follow the token scheme honestly is not greater than \(\epsilon_{\text{rob}}\) 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 \(\epsilon_{\text{cor}}\) 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 \(\frac{1}{2} + \epsilon_{\text{priv}}\). 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 \(\epsilon_{\text{unf}}\). 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 \(\epsilon_{\text{rob}}\) decreasing exponentially with \(N\). |
- correct if it is \(\epsilon_{\text{cor}}\) – correct with \(\epsilon_{\text{cor}}\) decreasing exponentially with \(N\). |
- private if it is \(\epsilon_{\text{priv}}\) – private with \(\epsilon_{\text{priv}}\) approaching zero by increasing some security parameter. |
- unforgeable if it is \(\epsilon_{\text{unf}}\) – unforgeable with \(\epsilon_{\text{unf}}\) 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
probability $1 - \Pi_{\text{nqub}}$ and a quantum state of arbitrary Hilbert space dimension greater than two with probability $\Pi_{\text{nqub}}$, where $\Pi_{\text{nqub}} = 0$ in ideal schemes and $\Pi_{\text{nqub}} > 0$ in practical schemes. In photonic implementations, each pulse transmitted by Bob is either vacuum or one-photon with probability $1 - \Pi_{\text{nqub}}$ and multi-photon with probability $\Pi_{\text{nqub}}$.

Below we present token schemes for two presentation points $(M = 1)$ that satisfy instant validation and that are robust, correct, private, and unforgettable. 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 $IQT_1$ and $IQT_2$ where there are not any losses, errors, or any other experimental imperfections. These are given in Table 1. More realistic quantum token schemes $Q^T_1$ and $Q^T_2$ 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 $\overline{\mathbf{a}}$. The $k$th bit entry of a string $\mathbf{a}$ is denoted by $a_k$. We define the set $\mathcal{N} = \{1, 2, \ldots, N\}$. 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 $\ket{\psi^0} = \ket{0}$, $\ket{\psi^1} = \ket{1}$, $\ket{\psi^+} = \ket{+}$ and $\ket{\psi^-} = \ket{-}$, where $\ket{\pm} = \frac{1}{\sqrt{2}}(\ket{0} \pm \ket{1})$, and where $D_0 = \{\ket{0}, \ket{1}\}$ and $D_1 = \{\ket{+}, \ket{-}\}$ are qubit orthonormal bases, called the computational and Hadamard bases, respectively. The Hamming distance is denoted by $d(\cdot, \cdot)$.

The quantum token schemes $IQT_1$ and $IQT_2$ 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 $IQT_1$ honestly, $d_{ak,b} = d_{ak,b} \oplus c = d_{ak,b} \oplus d_k \oplus c = y_k \oplus z \oplus b \oplus c = y_k \oplus c$ for $k \in \mathcal{N}$. Thus, $d_{ak,b} = y_k$, which means that $y_k = u_k$ for all $k \in \Delta_u$, hence, Alice measures in the same basis of preparation by Bob for all states $\ket{\psi_k}$ with labels $k \in \Delta_u$. Therefore, Alice obtains the correct outcomes for these states: $x_k = t_k$. Similarly, if Alice and Bob follow $IQT_2$ honestly then we have that $d_{ak,b} = c + z = y_k$, for $k \in \mathcal{N}$. Thus, as above, $d_{ak,b} = y_k$. The outcome $d_{ak,b}$ corresponds to the string of measurement basis implemented by Alice. Therefore, in both token schemes $IQT_1$ and $IQT_2$, Alice obtains $x_k = t_k$ 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 $Q^T_1$ and $Q^T_2$ 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
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 \(IQT_1\) and \(IQT_2\) are
\[
\epsilon_{\text{unf}} = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^N.
\]

Fifth, the token schemes satisfy instant validation. We note from step 11 of \(IQT_1\) that a token received by Bob’s agent \(B_0\) from Alice’s agent \(A_0\) at a presentation point \(Q_b\) can be validated by \(B_0\) near-instantly at \(Q_b\). In particular, \(B_0\) 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 \(IQT_1\), step 3 can be discarded, and step 10 can be replaced by the following: after choosing \(b\), \(A\) sends \(x\) to \(A_0\) and \(A_0\) presents the token \(x\) to \(B_0\) in \(Q_b\). In another variation, step 5 in \(IQT_1\) can be modified so that \(B\) computes \(d\), and sends it to \(B_0\); in both versions of step 5, \(B_0\) must have \(d\) in the causal past of \(Q_b\) for \(i \in \{0, 1\}^n\). In another variation, the step 9 in \(IQT_1\) is performed only by Bob’s agent \(B_0\) receiving a token from Alice. The version we have chosen for step 9 allows \(B_0\) 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.

**Table 3.** Practical quantum token scheme \(QT_1\) for two presentation points. See Table 4 for a summary of the notation and Fig. 2 for an illustration of the scheme.

| Preparation Stage | Stage I | Stage II |
|-------------------|---------|----------|
| 0. As step 0 of \(QT_1\). | 1. As step 1 of \(QT_1\). | 6. As steps 8 and 9 of \(QT_1\). |
| 2. The step 2 of \(QT_1\) is replaced by the following. \(A\) chooses a bit \(z\) with probability \(P_z(z)\) satisfying \(\frac{1}{2} < P_z(z) < \frac{1}{2} + \beta_z\) for \(z \in \{0, 1\}\) and for a small parameter \(\beta_z \in (0, \frac{1}{2})\). \(A\) measures \(A_z\) in the qubit orthonormal basis \(\mathcal{D}_z\) for all \(k \in \mathbb{N}\). Due to losses, \(A\) only successfully measures quantum states \(\psi_{A_k}\) with labels \(k\) from a proper subset \(\Lambda\) of \(\mathbb{N}\). \(A\) reports \(\Lambda \) for \(\{\Lambda\}\). \(B\) does not abort if and only if \(n \geq \gamma_{\text{det}}N\). | 5. As step 7 of \(QT_1\). | 7. The step 10 of \(QT_1\) is replaced by the following. For \(i \in \{0, 1\}, B_i\) computes the string \(d_i \in \{0, 1\}^n\) with bit entries \(d_{ij} = i \cdot c\), for \(j \in \mathbb{N}\). | 8. As steps 11 and 12 of \(QT_1\). |

The token schemes \(QT_1\) and \(QT_2\) can be modified in various ways, as discussed for the token schemes \(IQT_1\) and \(IQT_2\).

Regarding correctness, we note in the token scheme \(QT_1\) that if Alice follows the token scheme honestly and chooses to present the token in \(Q_b\) then we have that \(d_b\) has bit entries \(d_{b_z} = d_{b_z} \cdot c = d_{ij} \cdot b \cdot c = c = y_f\), for \(j \in \mathbb{N}\). Thus, \(d_b = y_f\), i.e., \(d_b\) corresponds to the string of measurement bases implemented by Alice on the quantum states reported to be successfully measured. Similarly, in the token scheme \(QT_2\), if Alice chooses to present the token in \(Q_b\), then we have that \(d_b\) has bit entries \(d_{b_z} = b \cdot c = z = y_f\), for \(j \in \mathbb{N}\). Thus, as above, \(d_b = y_f\), i.e., \(d_b\) corresponds to the string of measurement bases implemented by Alice on the quantum states reported to be successfully measured. Therefore, in both token schemes \(QT_1\) and \(QT_2\), if Alice can guarantee her error probability to be bounded by \(E < \gamma_{\text{det}}\) then with very high probability she will make less than \(|\Delta_0|\gamma_{\text{det}}\) bit errors in the \(|\Delta_0|\) quantum states that she measured in the basis of preparation by Bob.

Let \(P_{\text{det}}\) be the probability that a quantum state \(\psi_{A_k}\) transmitted by Bob is reported by Alice as being successfully measured, with label \(k \in \Lambda\), for \(k \in \mathbb{N}\). Let \(E\) be the probability that Alice obtains a wrong measurement outcome when she measures a quantum state \(\psi_{A_k}\) in the basis of preparation by Bob; if the error rates \(E_k\) are different for different prepared states, labeled by \(t\), and for different measurement bases, labeled by \(w\), we simply take \(E = \max_{t,w} E_k\).

The robustness, correctness, privacy, and unforgeability of \(QT_1\) and \(QT_2\) are stated by the following lemmas, proven in Supplementary Note V, and theorem, proven in Supplementary Note VII. These lemmas and theorem consider parameters \(Y_{\text{det}}, Y_{\text{err}} \in (0, 1)\), 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
\[
0 < Y_{\text{det}} < P_{\text{det}},
\]
then \(QT_1\) and \(QT_2\) are \(\epsilon_{\text{rob}}\) robust with
\[
\epsilon_{\text{rob}} = e^{-\chi_{\text{rob}}^2\left(1 - \frac{1}{\chi_{\text{rob}}^2}\right)^2}.
\]

**Lemma 3:** If
\[
0 < \frac{\gamma_{\text{det}}}{\gamma_{\text{err}}} < E < Y_{\text{err}},
\]
\[
0 < \nu_{\text{cor}} < \frac{\nu_{\text{cor}}(1 - 2\nu_{\text{cor}})}{2},
\]
\[
0 < Y_{\text{cor}} < \frac{\nu_{\text{cor}}(1 - 2\nu_{\text{cor}})}{2},
\]
Table 4. Summary of notation used for QT1 and QT2.

| Symbol | Brief description |
|--------|-------------------|
| Q |
| A | Alice’s (Bob’s) agent participating in the quantum communication stage |
| A1, A2 | Alice’s (Bob’s) agent by the presentation point Qi |
| N | Number of quantum states that Bob sends Alice |
| Ωqub | Set of labels for prepared qubits states |
| Ωnoqub | Set of labels for prepared quantum states with dimension greater than two |
| P, D | String of bits encoding the states that Alice reports as successfully measured by Alice |
| ΩQb | Set of labels for prepared states (preparation bases) |
| Λ | String of bits encoding the bases of preparation by Bob |
| Λν | Qubit orthonormal bases of measurement by Alice |
| PS | Probability distribution for Alice’s measurement bases |
| det | Minimum rate for states reported by Alice as successfully measured for Bob not aborting |
| err | Maximum error rate allowed by Bob for validating Alice’s token |
| g | One-to-one function g: [1] → [n] |
| y(x) | String of bits encoding Alice’s measurement outcomes (bases) |
| z | Bit chosen by Alice |
| P(z) | Probability distribution for bit z chosen by Alice |
| βE | Bias for the probability distribution P(z) |
| d, di | String with bit entries di = yi ⊕ z that Alice sends Bob |
| 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 ⊕ z, which Alice sends Bob |
| d, di | String with bit entries di = di ⊕ c computed by Bob’s agent B |
| Δν | Set of labels defined by Δν = {j ∈ [n] | dj = sj}, for ν ∈ {0, 1} |
| ai | The substring of a ∈ {x, r} restricted to bit entries ai with k ∈ Δν, for ν ∈ {0, 1} |

then QT1 and QT2 are εcorr – correct with

$$\epsilon_{\text{corr}} = e^{-\frac{\epsilon_{\text{det}}^2}{2}} (1 - 2e^{-\frac{\epsilon_{\text{det}}^2}{2}})^2 + e^{-\frac{\epsilon_{\text{det}}^2}{2}} (1 - 2e^{-\frac{\epsilon_{\text{det}}^2}{2}})^2. \tag{5}$$

Lemma 4: QT1 and QT2 are εpriv – private with

$$\epsilon_{\text{priv}} = \beta_E. \tag{6}$$

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, B0, and B1, controlled by agents B, B0, and B1 (yellow rectangles), and Alice has laboratories A, A0, and A1, controlled by agents A, A0, and A1 (green rectangles), adjacent to Bob’s laboratories. The quantum communication stage takes place within B and A, and can take an arbitrarily long time and can be completed arbitrarily in the past of the presentation points (Q0 and Q1). Alice’s classical measurement outcomes x are kept secret by Alice and communicated to her laboratories A0 and A1 via secure and authenticated classical channels. In this illustrated example, Alice sends classical messages to Bob at laboratory B, and either at B0 or B1. The messages sent to B can take place anywhere in the past of Q0 and Q1 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 B0 and B1 via secure and authenticated classical channels. Alice chooses to present her token at Q0 within the intersection of the causal pasts of Q0 and Q1. The message at either B0 or B1 is the bit c = B ⊕ z, effectively committing Alice to present her token at Q0. Alice presents the token by giving Bob x at Q0. 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 QT, (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 B0 and B1, which could be 10 µs if B0 and B1 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

$$0 < \epsilon_{\text{det}} < \lambda (\theta, \beta_P), \tag{7}$$

$$0 < P_{\text{noqub}} < \epsilon_{\text{det}} < \min\left\{ 2P_{\text{noqub}} Y_{\text{det}} (1 - \frac{\epsilon_{\text{det}}}{\epsilon_{\text{det}}/2}) \right\}. \tag{8}$$

We define the function

$$f(Y_{\text{det}}, \beta_P, \beta_B, \theta, \epsilon_{\text{det}}, \epsilon_{\text{cor}}) = (Y_{\text{det}} - \epsilon_{\text{det}}) \left( 1 - \frac{\epsilon_{\text{det}}}{\epsilon_{\text{det}}/2} \right)^2 - \ln (1 + 2\beta_P) \tag{9}$$

$$- (1 - (Y_{\text{det}} - \epsilon_{\text{det}})) \ln (1 + h(\beta_P, \beta_B, \theta)), \tag{10}$$

where

$$h(\beta_P, \beta_B, \theta) = 2\beta_P \sqrt{1 + 2\beta_P^2 + (1 - 2\beta_B^2) \sin^2(2\theta)}, \tag{11}$$

$$\delta = \frac{\epsilon_{\text{det}}}{\epsilon_{\text{cor}} - \epsilon_{\text{det}}}. \tag{12}$$
Extension of robustness, correctness, and unforgeability. But they must also be good enough to achieve their required degrees of correctness but not in robustness or privacy. Additionally, Alice must choose a suitable mathematical variable $\nu$ 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 $P_{\text{det}}$, $E$, and $\beta_E$ to be good enough. This is independent of any experimental parameters of Bob, except for the previously agreed parameter $\beta_B$, which plays a role in correctness but not in robustness or privacy. Additionally, Alice must choose a suitable mathematical variable $\nu_{\text{det}}$ to compute a guaranteed degree of correctness, as given by the bound of Lemma 3.

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

The parameters $N$, $\beta_B$, $\nu_{\text{det}}$, and $\nu_{\text{err}}$ 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 $QT_1$ and $QT_2$ to $2^M$ presentation points**

Extensions of the quantum token schemes $QT_1$ and $QT_2$ 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 $QT_1^M$ and $QT_2^M$ extending $QT_1$ and $QT_2$ to $2^M$ presentation points, in which Bob sends Alice $NM$ quantum states, satisfying instant validation and the following properties:

- Consider parameters $\beta_B$, $\beta_P$, $\beta_E$, $P_{\text{det}}$, $E$, and $\Theta$ satisfying the constraints (2), (4), (7) of Lemmas 2 and 3 and Theorem 1, for which the function $f(y_{\text{err}}, \beta_P, \beta_B, \nu_{\text{err}}, \nu_{\text{det}})$ defined by (8) is positive. For these parameters, $QT_1^M$ and $QT_2^M$ are $\epsilon_{\text{rob}}^M$-robust, $\epsilon_{\text{cor}}^M$-correct, $\epsilon_{\text{priv}}^M$-private, and $\epsilon_{\text{unf}}^M$-unforgeable with

$$
\begin{align*}
\epsilon_{\text{rob}}^M &= M \epsilon_{\text{rob}}, \\
\epsilon_{\text{cor}}^M &= M \epsilon_{\text{cor}}, \\
\epsilon_{\text{priv}}^M &= \frac{1}{2^M} \left[ (1 + 2\epsilon_{\text{priv}})^M - 1 \right], \\
\epsilon_{\text{unf}}^M &= C \epsilon_{\text{unf}},
\end{align*}
$$

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

**Quantum experimental tests**

We performed experimental tests for the quantum stage of the $QT_1$ 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 $P_{\text{det}} = 0.019$, and error rate of $E = 0.058$. We obtained deviations from the random distributions for the basis and state generation of $\beta_B = 2.4 \times 10^{-3}$ and $\beta_P = 3.6 \times 10^{-3}$, respectively. In order to guarantee unforgeability using Theorem 1, we need to improve some experimental parameters (see Fig. 5).

Guaranteeing privacy in our schemes $QT_1$ and $QT_2$ 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 $\epsilon_{\text{priv}}$ 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,
In photonic implementations, the single-photon detectors used in one of two distinct orthogonal qubit basis, $\mathcal{D}_0$ and $\mathcal{D}_1$, which pair of bases is arbitrary.

Because of losses and non-unit detection efficiencies (in photonic setups), $\mathcal{A}$ must report to $\mathcal{B}$ the set $\mathcal{S} \subseteq \mathcal{N}$ of labels of the successfully measured states. $\mathcal{B}$ does not abort if and only if $|\mathcal{S}| \geq \gamma_{\text{ref}} N$, where the subindex “det” stands for “detection”.

$\mathcal{A}$ 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 $\Omega_{\text{noqub}}$ and $\Omega_{\text{qub}}$. 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 $k \in \mathcal{N}$. However, we can include these deviations from the measurement bases $\mathcal{D}_0$ and $\mathcal{D}_1$ of $\mathcal{A}$ in the bases $\mathcal{P}_k$, of preparation by $\mathcal{B}$, and assume that $\mathcal{A}$ applies either $\mathcal{D}_0$ or $\mathcal{D}_1$ to $|\psi_k\rangle$, for $k \in \mathcal{N}$. In other words, the uncertainty angle $\theta$ on the Bloch sphere accounts for both preparation and measurement misalignments. Thus, our analysis is without loss of generality.

Thus, Alice obtains some errors in the measurements that she performs in the same basis $\mathcal{P}_z$. In order to counter multi-photon attacks\textsuperscript{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 $\mathcal{Q}_T_1$ and $\mathcal{Q}_T_2$ 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.\textsuperscript{53}, assumption F (see Table 6) guarantees that these reporting strategies offer perfect protection against arbitrary multi-photon attacks (see Lemma 5 in Methods).
channels, for example in a quantum network envisaged quantum internet, these keys can be expanded discussed, Alice relativistic quantum cryptography relativistic quantum cryptography, and which can operate at daylight conditions. Importantly, Bob key distribution (QKD) that was slightly adapted for our scheme, G. Kent et al. in photonic setups, from the perspective of A, the pulses of B are mixtures of Fock states: in particular, A has no information about relative phases of the components with definite photon number.

synchronized securely to a common reference frame with sufficiently high time precision. This can be implemented using GPS devices and atomic clocks, 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 or in the envisaged quantum internet, these keys can be expanded securely with quantum key distribution. However, it is also possible to distribute the secret keys via secure physical transportation, as implemented in previous demonstrations of relativistic quantum cryptography.

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 (QT1) using a free space optical setup 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.,). 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 $\beta_{\text{PS}}$ and $\beta_{\text{PS}}$ from random basis and state generation, respectively. In our tests we obtained $\beta_{\text{PS}} = 2.4 \times 10^{-3}$ 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 $\beta_{\text{PS}} = 2.3 \times 10^{-4}$ (about a factor of 10 and 16 lower from $\text{PS}$)}

### Table 6: Assumptions for QT1 and QT2.

| Label | Brief description | Explanation and comments |
|-------|------------------|-------------------------|
| A     | For $k \in \Omega_{\text{QT1}}$, B prepares $|\psi_k\rangle = |\psi_{u_k}\rangle$, where $|\psi_{u_k}\rangle = 0$, defining the qubit orthonormal basis $T^\lambda_k = |\psi_{u_k}\rangle^\dagger$ for $u \in (0, 1)$. | That is, we assume that B prepares each qubit state from exactly two qubit bases. However, in the most general case (not considered here), B prepares each qubit state from a set of four qubit states that does not necessarily define two qubit bases. |
| B     | B generates the bit strings $t = (t_1, ..., t_N)$ and $u = (u_1, ..., u_N)$ with probability distributions that are exactly products of single bit probability distributions. | In the general case (not considered here), the strings $t$ and $u$ could be generated with a probability distribution in which $t$ and $u$, and different bit entries of $t$ and $u$, could be correlated. |
| C     | The set $\Lambda$ of labels transmitted to B in step 2 of QT1 and QT2 gives B no information about the string $W$ and the bit $z$. | In the photonic setups of Fig. 3 to implement QT1 and QT2, with the reporting strategies 1 and 2, respectively, assumption C (and also assumption D for QT1) follows from assumptions E and F (see Lemma 5 in Methods). |
| D     | In QT1, conditioned on reporting the quantum state $|\psi_k\rangle$ as successfully measured, i.e., conditioned on $k \in \Lambda$, A measures $|\psi_k\rangle$ in an orthogonal qubit basis $D_{\text{QT1}}$ with a probability distribution $P_{\text{QT1}}(w_k) = \frac{1}{2}$ 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 QT1 to satisfy assumption C. If this assumption did not hold, there would be at least one label $k' \in A$ for which $P_{\text{QT1}}(w_k = i) = P_{\text{QT1}}(w_k = \bar{i})$, for some $i \in \{0, 1\}$. Thus, $B$ could in principle guess the entry $w_k$ of $W$ with probability greater than $\frac{1}{2}$. This would mean that the set $\Lambda$ reported by $A$ would have given B some information about $W$, in contradiction with assumption C. |
| E     | 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 A. | This assumption guarantees that $A$ is perfectly protected from any side-channel attack by $B$ in any type of physical setup (not necessarily photonic).

In our notation, the term detection efficiency includes the quantum efficiency of the detectors of $A$ and the transmission efficiency from the setup of $B$ to the detectors. We note that the condition $(1 - d_0)(1 - d_1) = (1 - d_2)(1 - d_3)$ can be satisfied if $d_0 = d_1$ and $d_2 = d_3$, or if $d_0 = d_2$ and $d_1 = d_3$, for instance. Exactly equal detection efficiencies cannot be guaranteed in practice. But, attenuators can be used to make the detector efficiencies approximately equal. Furthermore, $A$ 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.

If this assumption is not satisfied, the quantum state received by $A$ 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). This assumption is consistent with our security analysis and is satisfied in practice if $B$ uses a weak coherent source and he uniformly randomizes the phase of each pulse transmitted to $A$; or if $B$ uses an arbitrary photon source with arbitrary signal states and he applies a physical operation to the transmitted pulses with the property that it applies a random phase $\theta$ per photon—i.e., a $\theta$-photons pulse acquires an amplitude $e^{i\theta}$. Alternatively, this condition can be satisfied to a good approximation if $B$ uses a photon source with low spatiotemporal coherence, for example, a source comprising LEDs, as in our experimental tests reported below.

Published in partnership with The University of New South Wales npj Quantum Information (2022) 28
than our values). This highlights that it is crucial to consider the parameters $\beta_{PS}$ and $\beta_{PB}$ 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 $\beta_{PS} = \beta_{PB} = 0$, 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\cite{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\cite{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. 3 Photonic setups to implement the quantum stage of $QT_1$ and $QT_2$. In both $QT_1$ and $QT_2$, the setup of honest $B$ 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 $k \in \mathbb{N}$. a In $QT_1$, the setup of honest $A$ comprises a 50:50 beam splitter, a wave plate, two polarizing beam splitters (PBS$_0$ and PBS$_+$), and four threshold single-photon detectors $D_0$, $D_1$, $D_+$, and $D_-$. In order to counter multi-photon attacks by $B$, $A$ implements the following reporting strategy that we call here reporting strategy 1: $A$ assigns successful measurement outcomes in the basis $D_0$ ($D_1$) 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 $QT_2$, the setup of honest $A$ 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 $B$, $A$ implements the following reporting strategy that we call here reporting strategy 2: $A$ reports to $B$ 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).
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\(^55\).

**METHODS**

**Protection against multi-photon attacks in photonic implementations**

The following lemma is a straightforward extension of Lemmas 1 and 12 of ref. \(^5\) 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. \(^5\). 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 \(k\)th pulse have \(L_k\) photons. Let \(\rho\) 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 \(\mathcal{D}_L\) and \(\mathcal{D}_T\) be two arbitrary quibit orthogonal bases. Suppose that either Alice uses the setup of Fig. 3 with reporting strategy 2 to implement the quantum token scheme \(\mathcal{Q}T_2\) (see Table 3), or suppose that the conditions listed in Table 2 are satisfied simultaneously. 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 \(\mathcal{Q}T_1\) and \(\mathcal{Q}T_2\) are \(e_{\text{rob}}\)-robust, \(e_{\text{cor}}\)-correct and \(e_{\text{unf}}\)-unforgeable, for desired values of \(e_{\text{rob}}, e_{\text{cor}}\) and \(e_{\text{unf}}\).

| Robustness | Correctness |
|------------|-------------|
| Condition (2) | Conditions (4) |
| Conditions (7), \(f > 0\) |

Unforgeability

**Fig. 4 Illustration of security conditions for \(\mathcal{Q}T_1\) and \(\mathcal{Q}T_2\).** A diagram presenting the conditions under which robustness, correctness, and unforgeability of the quantum token schemes \(\mathcal{Q}T_1\) and \(\mathcal{Q}T_2\) 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 \(\mathcal{Q}T_1\) and \(\mathcal{Q}T_2\) are \(e_{\text{rob}}\)-robust, \(e_{\text{cor}}\)-correct and \(e_{\text{unf}}\)-unforgeable, for desired values of \(e_{\text{rob}}, e_{\text{cor}}\) and \(e_{\text{unf}}\).

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 \(\mathcal{Q}T_1\), then the probability that Alice reports the string \(m\) to Bob and assigns the string of measurement bases \(w\) given \(\rho\) and \(L\), is

\[
P_{\text{rob}}^{(1)}(m, w|\rho, L) = \prod_{k=1}^{N} G_{m_k w_k}^{(1)}(d_k, d_1, \eta, L_k),
\]

where

\[
G_{m_k w_k}^{(1)}(d_k, d_1, \eta, a) = \left(1 - d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right) - \left(1 - d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right),
\]

\[
G_{m_k w_k}^{(1)}(d_k, d_1, \eta, a) = \left(1 - 2d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right),
\]

\[
G_{m_k w_k}^{(1)}(d_k, d_1, \eta, a) = 0,
\]

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 \(P_{\text{rob}}(w_k)\) that Alice assigns a measurement in the basis \(\mathcal{D}_{w_k}\) conditioned on the value \(m_k = 1\), for the \(k\)th pulse, satisfies

\[
P_{\text{rob}}(w_k) = \frac{1}{2^N},
\]

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 \(\mathcal{Q}T_2\), then the probability that Alice reports the string \(m\) to Bob and assigns the string of measurement bases \(w\) given \(\rho\) and \(L\), is

\[
P_{\text{rob}}^{(2)}(m, w|\rho, L) = \prod_{k=1}^{N} G_{m_k w_k}^{(2)}(d_k, d_1, \eta, L_k),
\]

where

\[
G_{m_k w_k}^{(2)}(d_k, d_1, \eta, a) = \left(1 - d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right) - \left(1 - d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right),
\]

\[
G_{m_k w_k}^{(2)}(d_k, d_1, \eta, a) = \left(1 - 2d_k^2\right)\left(1 - d_1^2\right)\left(1 - \eta^2\right),
\]

\[
G_{m_k w_k}^{(2)}(d_k, d_1, \eta, a) = 0,
\]

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 \(P_{\text{rob}}(w_k)\) that Alice assigns a measurement in the basis \(\mathcal{D}_{w_k}\) conditioned on the value \(m_k = 1\), for the \(k\)th pulse, satisfies

\[
P_{\text{rob}}(w_k) = \frac{1}{2^N},
\]

for \(w_k \in \{0, 1\}\) and \(k \in [N]\).
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⟩, |1⟩, |+⟩ and |−⟩ 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. 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 μ = 0.09. Since Bob’s photon source consists of LEDs, and LEDs have low spatiotemporal coherence, 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 η = 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, and sends them to a PC for processing. Alice’s grey and black boxes are closed during operation to decrease noise due to light environment. But they are shown open here for illustration.

Bob, given p, w, and L, is
\[ P_{\text{rep}}^{|w|p}(m, w, p, L) = \prod_{k=1}^{N} G_{m}^{L}(d_{o}, d_{i}, \eta, L_{s}), \]  
where
\[ G_{m}^{L}(d_{o}, d_{i}, \eta, a) = (1 - d_{o})(1 - d_{i})/(1 - \eta)^{a}, \]
\[ G_{m}^{L}(d_{o}, d_{i}, \eta, a) = (1 - d_{o})(1 - d_{i})/(1 - \eta)^{a}, \]
for m, w ∈ {0, 1}^n and a, L_s ∈ {0, 1, 2, ...}.

In any of the two cases, the message m gives Bob no information about the bit entries w_i for which m_i = 1. Equivalently, the set Λ ∈ [N] of labels transmitted to Bob in step 2 of QT_1 and 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 ∈ [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_k where J_k 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, 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 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 QT_2 in Supplementary Note VIII).

Experimental tests and numerical example
The quantum stage of the token scheme QT_1 was implemented with the experimental setup described above. Below we describe our experimental 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 × 10^5, P_{\text{det}} = 0.019, E = 0.056, β_{\text{PP}} = 2.4 × 10^{-3}, β_{\text{PS}} = 3.8 × 10^{-3}, P_{\text{phot}} = 3.8 × 10^{-3}. We assume an angle θ ≤ 10° in our experiment.

In the numerical example of Fig. 5, we used the previous experimental values, except for E and β_{\text{PS}}, which were varied as shown in the plots, and for β_{\text{PP}} and β_{\text{PS}}. In the plots of Fig. 5, if β_{\text{PP}} ≤ β_{\text{max}} and β_{\text{PS}} ≤ β_{\text{max}} hold, then we obtain from Lemmas 2 and 3 and from Theorem 1 that ε_{\text{rob}, \text{can}} ≤ 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_{\text{rob}, \text{can}} ≤ 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_{\text{rob}, \text{can}} ≤ 10^{-9}.

For the three curves of Fig. 5, we set Y_{\text{det}} = 0.018. Thus, condition (2) of Lemma 2 is satisfied, and from (3), we have ε_{\text{rob}} = e^{-1052} < 10^{-9}.
For the three curves of Fig. 5, we set \( \nu_{\text{con}} = 3.9 \times 10^{-3} \). This is the minimum value for which the first term of \( \nu_{\text{con}} \) in (10) equals \( \frac{19}{20} \). This is because, as we describe below, we also chose the parameters satisfying that the second term of \( \nu_{\text{con}} \) in (10) equals \( \frac{19}{20} \) from which we have \( \nu_{\text{con}} = 10^{-9} \). 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 \( \theta = 0^\circ, 1^\circ, \ldots, 11^\circ \), we set \( \beta_{\min} = \beta_{\max} \) and varied \( \beta_{\max} \), \( \nu_{\text{con}} \), and \( \nu_{\text{det}} \) trying to find the maximum value of \( \beta_{\max} \) for which both terms of \( \nu_{\text{con}} \) in (5) and the second term of \( \nu_{\text{con}} \) in (10) were as close as possible to \( \frac{19}{20} \), but not bigger than \( \frac{19}{20} \) while guaranteeing that the constraints (4) and (7) were satisfied. Our results for \( \beta_{\max} \) are plotted in Fig. 5.

We describe below 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\(^{4,50,51}\), the probability that a photon pulse has two or more photons is \( P_{\text{two photon}} = 1 - \left( 1 + \mu \right)^{-\mu} \). Since in our experiment \( \mu = 0.09 \), we obtain \( P_{\text{two photon}} = 3.8 \times 10^{-3} \).

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 \( \nu_{\text{det}} \) was obtained as \( \nu_{\text{det}} = 0.019 \).

The measured detection efficiency, including the quantum efficiency of the detectors and the transmission probability from Bob, was 0.09. Alice used 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 \( \nu_{\text{det}} \) is given by

\[
\nu_{\text{det}} = \sum_{\nu_{\text{con}} = 0}^{\nu_{\text{det}}} \nu_{\text{con}} \left( G_1^1(0, 0, \eta, \theta, k) + G_1^1(0, 0, \eta, \theta) \right) \\
= 2 \sum_{\nu_{\text{con}} = 0}^{\nu_{\text{det}}} \nu_{\text{con}} \left( 1 - \left( \frac{\nu_{\text{con}}}{\nu_{\text{det}}} \right)^2 \right)^\theta - (1 - \eta)^\theta \\
= 2 \left( e^{-\eta} - e^{-\nu_{\text{det}}} \eta \right) \\
= 0.01863,
\]

where in the last line we used our experimental parameters \( \mu = 0.09 \) and \( \eta = 0.21 \). This gives a ratio \( \nu_{\text{det}} / \nu_{\text{con}} = 0.996 \).

As mentioned in Fig. 3, Alice applies reporting strategy 1, in order to protect against multi-photon attacks\(^{35,36} \) (see Lemma 5). That is, Alice assigns successful measurement outcomes in the basis \( \{ \mathcal{O}_i \} \) with unit probability for the pulses in which at least one of the detectors \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) click and \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) do not click. It is clear that when only the detector \( D_0 \) clicks, Alice associates the measurement outcome to the BB84 state \( |j \rangle \), for \( j = 0, 1, \pm \). However, it is not clear how Alice should assign measurement outcomes to the cases in which both \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) click and \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) 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 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 \( |1 \rangle \) \( \{ \mathcal{O}_i \} \) when both \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) click and \( D_0 \) and \( D_1 \) \( \{ \mathcal{D}_0 \} \) and \( \{ \mathcal{D}_1 \} \) 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 \( \beta_{\min} = 2.4 \times 10^{-3} \) and \( \beta_{\max} = 3.6 \times 10^{-3} \), 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 \( \nu_{\text{det}} \) was obtained as \( \nu_{\text{det}} = 0.019 \).
