

Practical quantum tokens without quantum memories and experimental tests

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


**[1] Centre for Quantum Information and Foundations, DAMTP,
University of Cambridge, UK**

[2] Quantum Engineering Technology Labs, University of Bristol, UK

QCrypt 2021

Quantum tokens: the first invention of quantum information science

- Invented by Wiesner in 1970, but published in 1983 [1].
- The bank gives the user a serial number S and quantum states $|\psi\rangle$ generated randomly from a set of non-mutually orthogonal states (e.g. the BB84 states).
- The user gives S and $|\psi\rangle$ to access a resource.
- Alternatively, a verifier, who knows S and $|\psi\rangle$, asks questions to the user about $|\psi\rangle$. The user measures $|\psi\rangle$ to answer correctly, and in this way accesses the resource.
- The no-cloning theorem and other quantum principles imply that the user cannot forge the quantum tokens.
- Their implementation is not presently practical because they require quantum state storage in quantum memories and/or long distance quantum communication.



$|0\rangle|+\rangle|1\rangle|0\rangle|0\rangle|-\rangle|+\rangle|1\rangle$
 $|-\rangle|1\rangle|0\rangle|-\rangle|+\rangle|1\rangle|+\rangle|0\rangle$
 $|1\rangle|+\rangle|1\rangle|+\rangle|-\rangle|1\rangle|-\rangle|1\rangle$
 $|0\rangle|-\rangle|0\rangle|1\rangle|+\rangle|0\rangle|1\rangle|+\rangle$

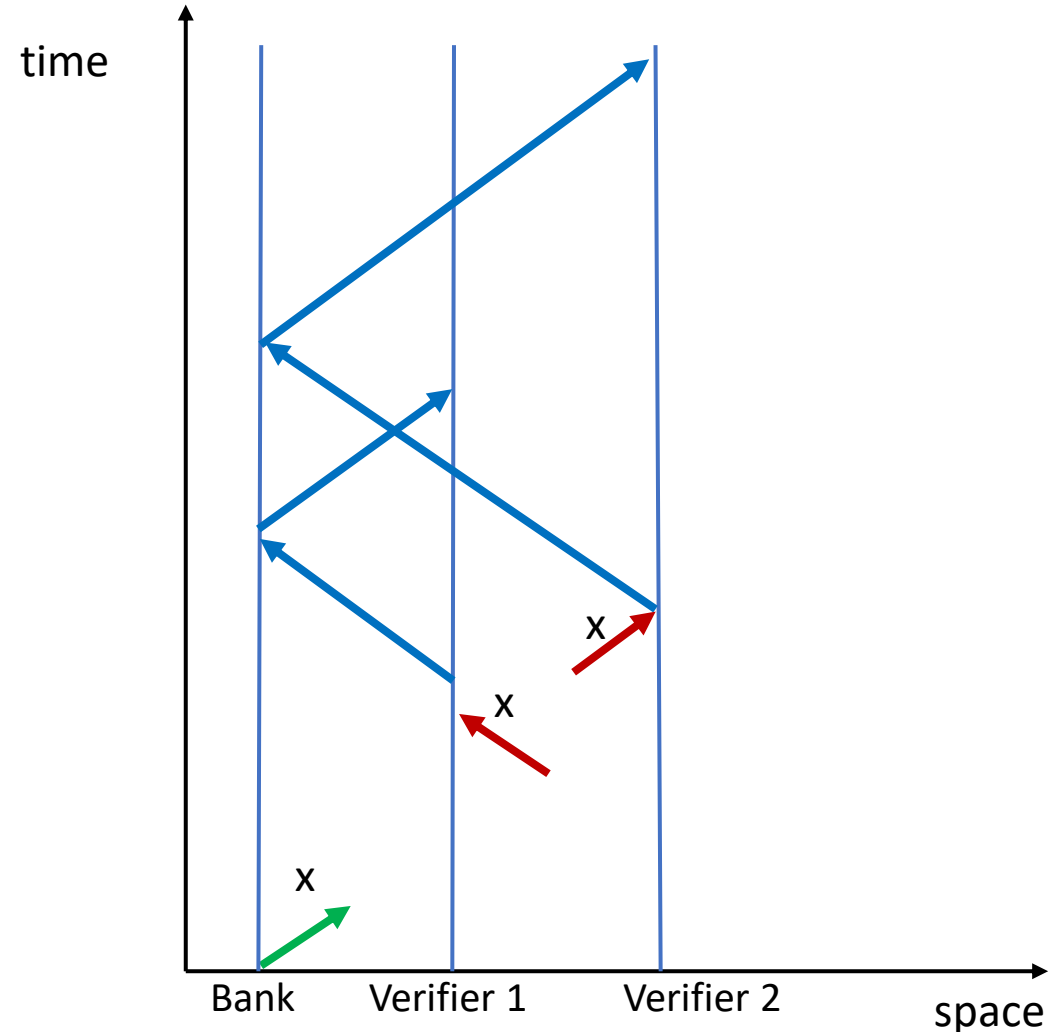
AS974523FT \$ 1000000

[1] Wiesner, Stephen (1983). "Conjugate Coding". *SIGACT News*. **15** (1): 78–88.

The photo of Stephen Wiesner (in 2015) was taken and modified (cut) from Quantumpundit, CC BY-SA 4.0 <<https://creativecommons.org/licenses/by-sa/4.0/>>, via Wikimedia Commons.

Properties of quantum tokens

- **Unforgeability.** The user cannot have a token be validated more than once.
- **User privacy.** The user chooses privately when and where to present the token.
- **Instantaneous validation.** The quantum tokens can be validated near instantly without cross checking.
- There exist simple purely classical token schemes satisfying any two of the three previous properties, but not the three simultaneously.
- **Disadvantage:** they are not practical because they require quantum state storage and/or long distance quantum communication.



Introduction

- Unforgeable quantum tokens were the first invention of quantum information science, by Wiesner in 1970 [1].
- Existing quantum token schemes are not presently practical because they require to store quantum states in quantum memories and/or to transfer quantum states over long-distances.
- **A full experimental demonstration of a quantum token scheme remains an important open problem.**
- ‘S-money’ schemes [2] define secure quantum tokens without needing quantum memories or long distance quantum communication.
- Applications of S-money (like quantum tokens in general) are in scenarios where relativistic constraints are important, for example, in high speed transactions in financial markets.
- **We present theoretical and experimental results suggesting that a full experimental demonstration of quantum S-money tokens can be implemented in practice.**

[1] S. Wiesner, "Conjugate Coding". ACM SIGACT News. **15** (1): 78–88 (1983).

[2] A. Kent, "S-money: virtual tokens for a relativistic economy", Proc. R. Soc. A **475**, 20190170 (2019).

Outline

- A simple quantum S-money token scheme of Ref. [2] **not requiring quantum state storage or long distance quantum communication.**
- **Our extension** of the scheme of Ref. [2]:
 - **Increasing the flexibility in spacetime [3]** for token generation and presentation.
 - **Allowing for various experimental imperfections [4].**
- **Experimental tests [4]** of the quantum stage of our schemes.
- **Conclusions.**

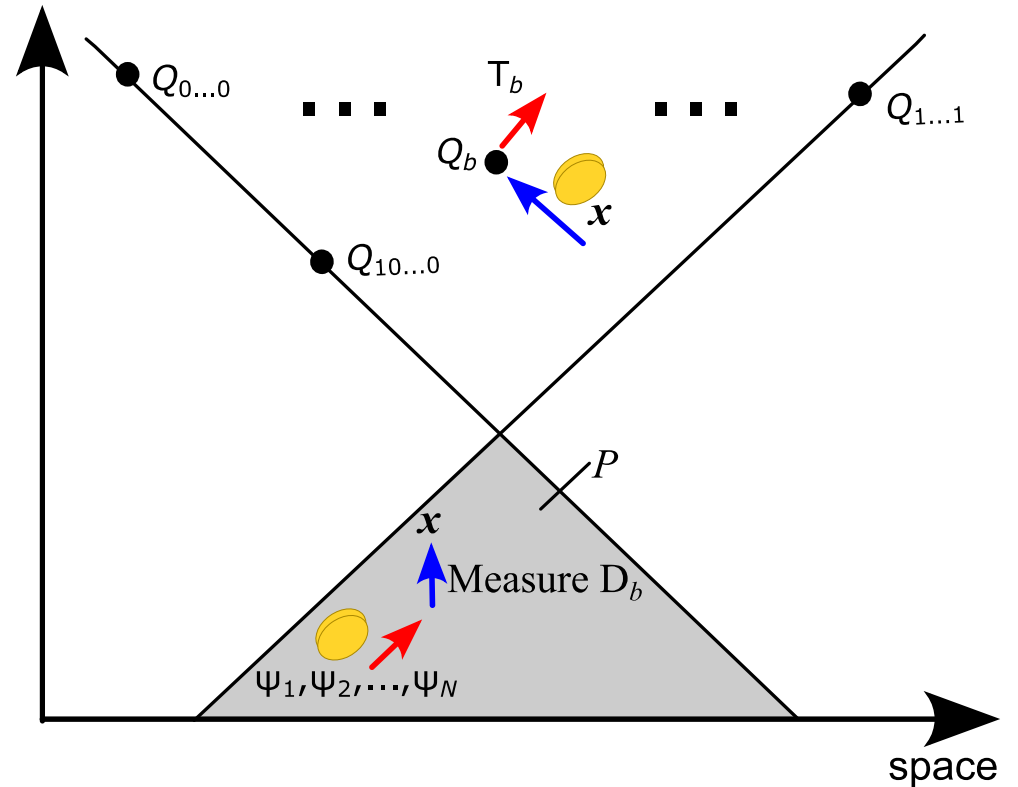
[2] A. Kent, "S-money: virtual tokens for a relativistic economy", Proc. R. Soc. A **475**, 20190170 (2019).

[3] A. Kent and D. Pitalúa-García, "**Flexible quantum tokens in spacetime**", Phys. Rev. A **101**, 022309 (2020).

[4] A. Kent, D. Lowndes, D. Pitalúa-García and J. Rarity, "**Practical quantum tokens without quantum memories and experimental tests**", arXiv: 2104.11717.

A simple quantum S-money token scheme [2]

- Bob (the bank) and Alice (the acquirer or user) agree on spacetime token presentation points Q_i , labelled by M -bit time strings $i = (i_1, \dots, i_M)$. We denote by P the intersection of the causal pasts of all Q_i . Bob (Alice) has secure laboratories communicating with secure classical channels within P and at all Q_i .
- Bob gives Alice a token of $N = nM$ random BB84 states $\psi_1, \psi_2, \dots, \psi_N$, within P .
- Alice chooses to access a resource T_b at Q_b , by measuring within P each of the n systems of M -qubit in a basis D_b (for $k = 1, \dots, M$, the b_k -th qubit is measured in the computational basis $\{|0\rangle, |1\rangle\}$ if $b_k = 0$ or in the Hadamard basis $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ if $b_k = 1$), and by giving Bob the classical outcome x at Q_b .
- Bob validates the token x at Q_b if x is consistent with having measured in basis D_b the states that he gave Alice.



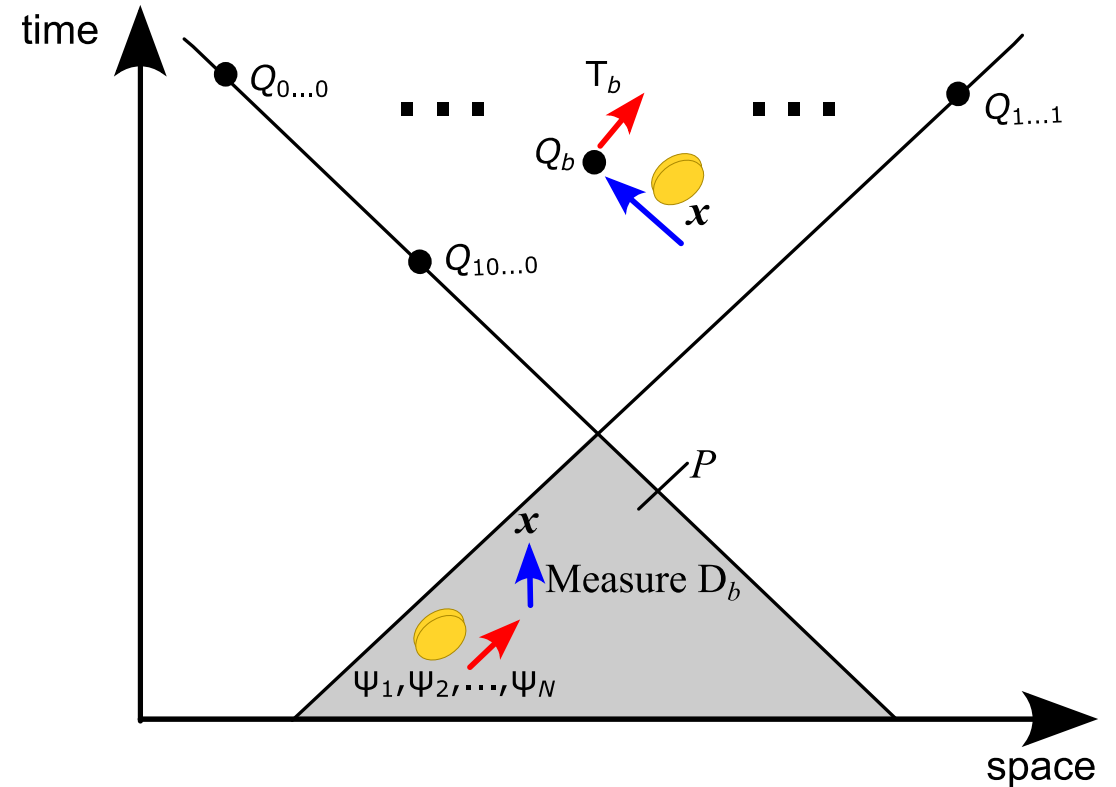
[2] A. Kent, "S-money: virtual tokens for a relativistic economy", Proc. R. Soc. A **475**, 20190170 (2019).

Properties satisfied

- **Unforgeability.** Alice cannot make Bob validate tokens at more than one token presentation point. For example, in the ideal case with BB84 states, Alice's cheating probability P_{forge} is bounded by:

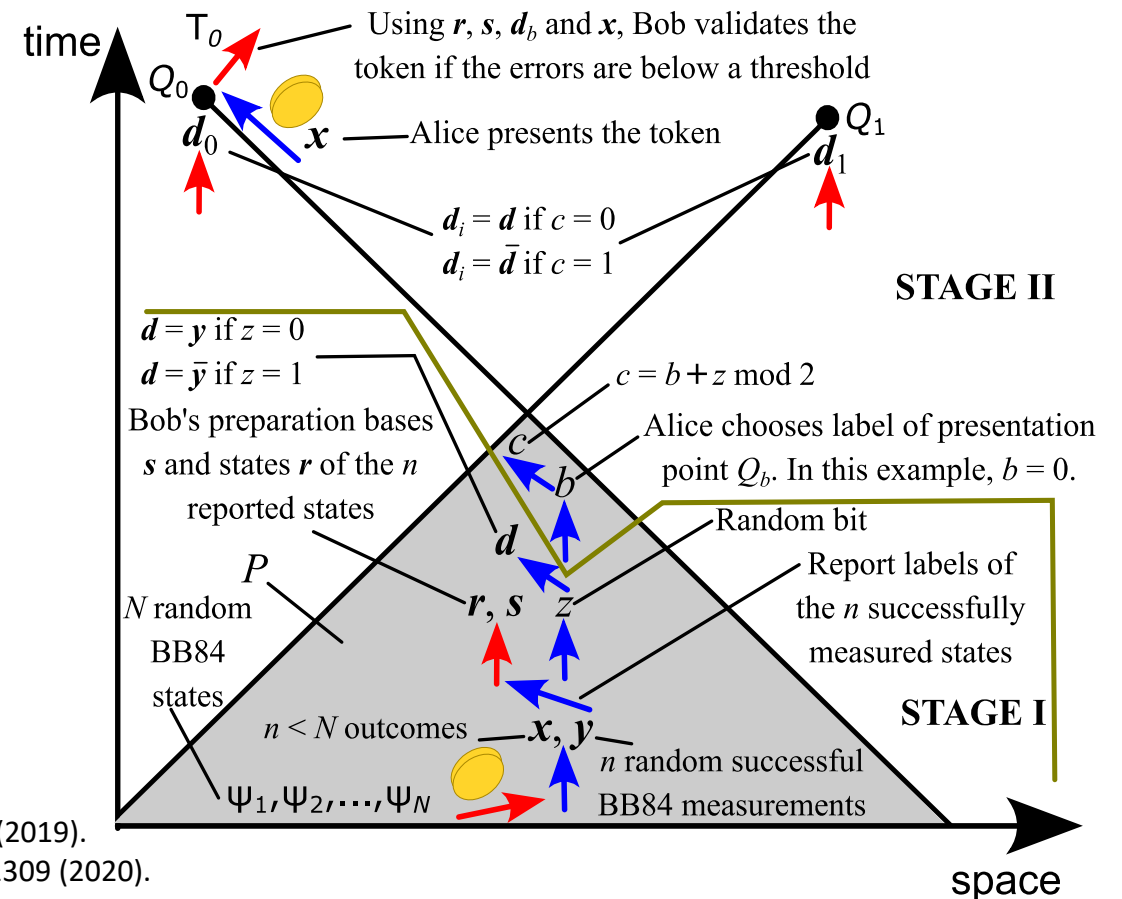
$$P_{\text{forge}} \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n .$$

- **User privacy.** Alice does not give any information until her chosen token presentation point, hence, she is guaranteed privacy of her choice.
- **Instant validation.** Classical tokens are unforgeable with cross-checking, but adding extra delays. S-money tokens can be validated near instantly, not needing to cross check. This is crucial in high-speed transactions (e.g. financial markets).
- Crucially, do not need quantum memories or long-distance quantum communication.



A practical quantum token scheme without quantum memories

- Simple extension of Adrian's scheme [2].
- **Extends the flexibility in spacetime** for token presentation and validation [3].
- **Satisfies unforgeability and privacy, considering various experimental imperfections [4]**, under standard assumptions in practical mistrustful quantum cryptography.
- **Protected against arbitrary multi-photon attacks [5]** to guarantee privacy, *assuming detectors have equal efficiency*.
- We discuss only the case of two presentation points, but **our scheme works for 2^M presentation points and arbitrary M** .



[2] A. Kent, "S-money: virtual tokens for a relativistic economy", Proc. R. Soc. A **475**, 20190170 (2019).

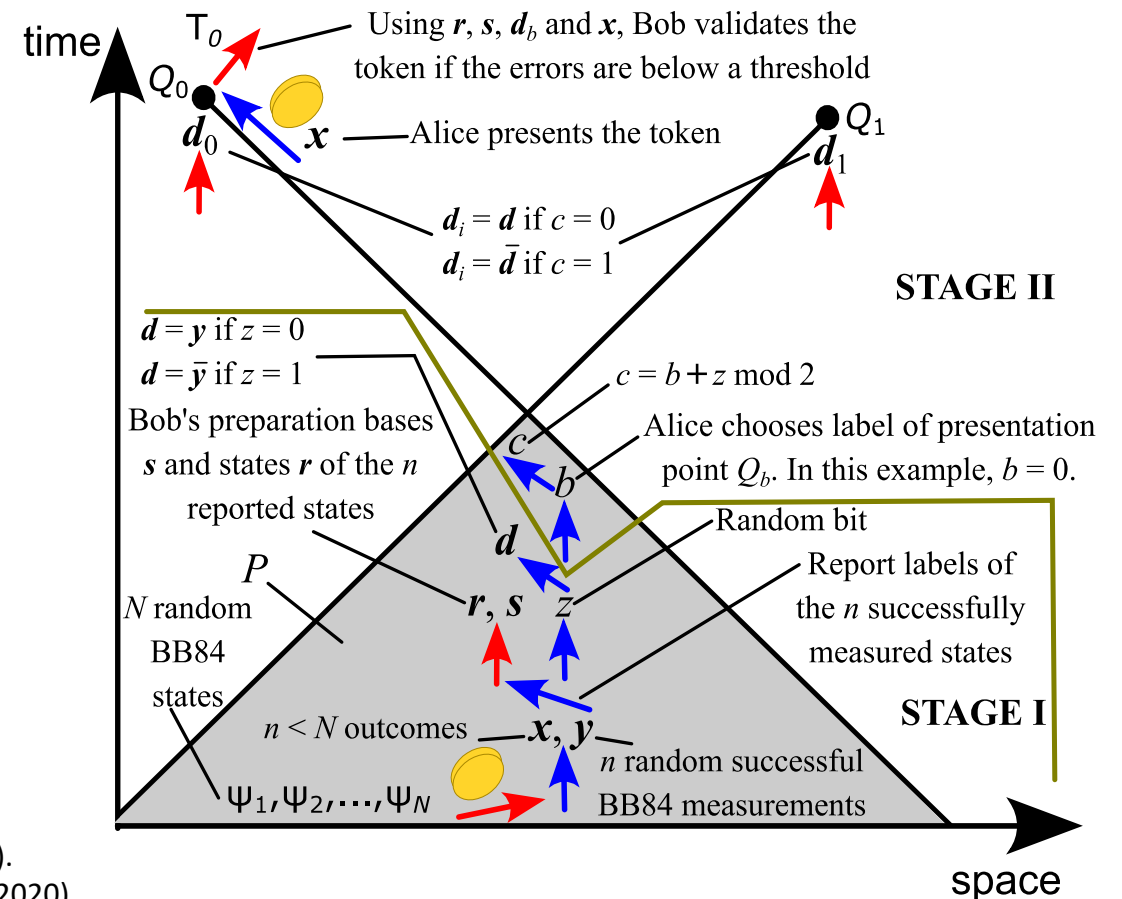
[3] A. Kent and D. Pitalúa-García, "Flexible quantum tokens in spacetime", Phys. Rev. A **101**, 022309 (2020).

[4] A. Kent, D. Lowndes, D. Pitalúa-García and J. Rarity, "Practical quantum tokens without quantum memories and experimental tests", arXiv: 2104.11717.

[5] M. Bozzio, A. Cavailles, E. Diamanti, A. Kent and D. Pitalúa-García, "Multi-photon and side-channel attacks in mistrustful quantum cryptography", arXiv: 2103.06970. To appear in PRX Quantum.

A practical quantum token scheme without quantum memories

- Stage I comprises **short-range quantum communication**, which can be arbitrarily slow, and can be completed arbitrarily in the past of the presentation points.
- **Stage II is purely classical** but must be very fast in order to establish spacelike separated presentation points – and have an advantage over classical schemes. In practice, **we need sufficiently fast FPGAs synchronized to a common reference frame, using GPS devices and atomic clocks, for example.**



[2] A. Kent, "S-money: virtual tokens for a relativistic economy", Proc. R. Soc. A **475**, 20190170 (2019).

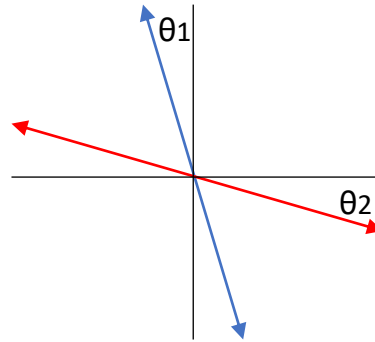
[3] A. Kent and D. Pitalúa-García, "Flexible quantum tokens in spacetime", Phys. Rev. A **101**, 022309 (2020).

[4] A. Kent, D. Lowndes, D. Pitalúa-García and J. Rarity, "Practical quantum tokens without quantum memories and experimental tests", arXiv: 2104.11717.

[5] M. Bozzio, A. Cavailles, E. Diamanti, A. Kent and D. Pitalúa-García, "Multi-photon and side-channel attacks in mistrustful quantum cryptography", arXiv: 2103.06970. To appear in PRX Quantum.

Considered experimental imperfections

- We allow that Bob's states are not perfect BB84 states. ***But we restrict them to define two orthogonal qubit bases.***

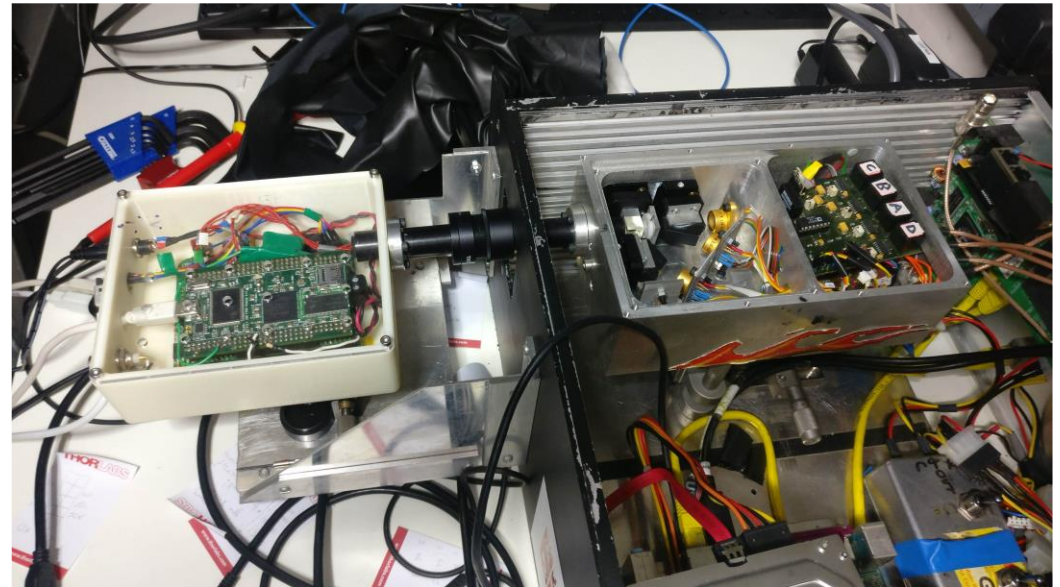


- A fraction of Bob's states may have arbitrarily high finite dimension, instead of being qubits (non-ideal single photon sources emitting multi-photon pulses with non-zero probability).
- We assume that bit probability distributions for Bob's bases and states, for Alice's measurement bases, etc., are not perfectly random. ***But we assume bit string probability distributions are products of bit probability distributions.***
- We allow losses of the transmitted quantum states.
- We allow a fraction of errors in Alice's measurement outcomes.
- In photonic setups, the single photon detectors are threshold and have non-zero dark count probabilities.

Quantum experimental tests

- Bob sends BB84 states in polarized light pulses (mean photon number $\mu = 0.09$).
- Alice measures using 50:50 and polarizing beam splitters, and single photon detectors with $\eta = 21\%$ detection efficiency.
- At frequency of 10 MHz, we generated a token of $N = 4 \times 10^7$ in 4 seconds, with error rate of $E = 5.8\%$ and detection probability of $P_{\text{det}} = 1.9\%$. We obtained deviations from the random distributions for the basis and state generation of $\beta_{\text{PB}} = 2.4 \times 10^{-3}$ and $\beta_{\text{PS}} = 3.6 \times 10^{-3}$, respectively.

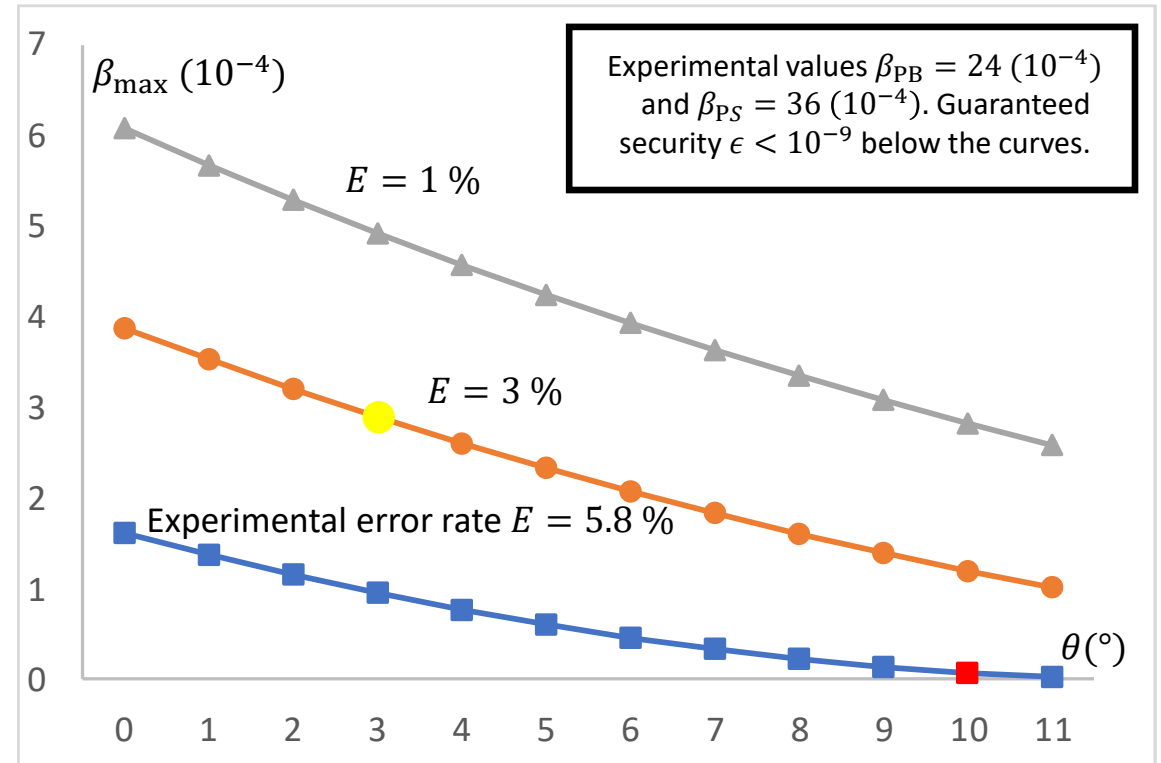
- Experimental setting (implemented by David Lowndes):



[4] A. Kent, D. Lowndes, D. Pitalúa-García and J. Rarity, "Practical quantum tokens without quantum memories and experimental tests", ArXiv: 2104.11717.

Experimental results

- To guarantee unforgeability, we need to improve some parameters. In a numerical example, we plot the required maximum deviation β_{\max} from random state generation vs. uncertainty θ in the Bloch sphere for a security bound of 10^{-9} .
- User privacy is not considered in the plots. But this can be made arbitrarily good in practice using good random number generators.



[4] A. Kent, D. Lowndes, D. Pitalúa-García and J. Rarity, "Practical quantum tokens without quantum memories and experimental tests", ArXiv: 2104.11717.

Conclusions

- S-money token schemes provide instant validation, user privacy, and unforgeability, and they do not require quantum-state storage or long-distance quantum communication.
- We extended a previous quantum S-money scheme to a practical setting considering errors, losses and other experimental imperfections, and we proved its security.
- We performed experimental tests of the quantum communication stage using handheld optical QKD devices. Refinements are needed to ensure full security for our scheme.
- Our analysis shows β_{PB} , β_{PS} and θ are crucial in practical security proofs.
- Some applications are authentication in high-speed transactions (e.g financial markets) and in communication networks.
- We are assessing the practicality of a full experimental demonstration of the scheme with spacelike separated token presentation points using FPGAs, etc.