IOP Publishing Quantum Sci. Technol. 10 (2025) 045043 https://doi.org/10.1088/2058-9565/ae03e7

Quantum Science and Technology

OPEN ACCESS

RECEIVED
17 April 2025

REVISED
1 August 2025

ACCEPTED FOR PUBLICATION
5 September 2025

PUBLISHED
24 September 2025

PAPER

Security analysis of ensemble-based quantum token protocol under advanced attacks

Bernd Bauerhenne[1,*], Lucas Tsunaki[2], Jan Thieme[1], Boris Naydenov[2,3] and Kilian Singer[1,*]

[1] Experimental Physics I, University of Kassel, Heinrich-Plett-Strasse 40, 34132 Kassel, Germany
[2] Department Spins in Energy Conversion and Quantum Information Science (ASPIN), Helmholtz-Zentrum Berlin für Materialien und Energie GmbH, Hahn-Meitner-Platz 1, 14109 Berlin, Germany
[3] Berlin Joint EPR Laboratory, Fachbereich Physik, Freie Universität Berlin, 14195 Berlin, Germany
[*] Authors to whom any correspondence should be addressed.

E-mail: bauerhenne@uni-kassel.de and ks@uni-kassel.de

Keywords: advanced, attacks, qubit, ensembles, quantum, coins

Abstract

We present and characterize advanced attacks on an ensemble-based quantum token protocol that allows for implementing non-clonable quantum coins. Multiple differently initialized tokens of identically prepared qubit ensembles are combined to a quantum coin that can be issued by a bank. A sophisticated attempt to copy tokens can assume that measurements on sub-ensembles can be carried through and that even individual qubits can be measured. Even though such an advanced attack might be perceived as technically unfeasible, we prove the security of the protocol under these conditions. We performed numerical simulations and verified our results by experiments on the IBM quantum platforms for different types of advanced attacks. Finally, we demonstrate that the security of the quantum coin can be made high by increasing the number of tokens. This paper in conjunction with provided numerical simulation tools verified against experimental data from the IBM quantum platforms allows for securely implementing our ensemble-based quantum token protocol with arbitrary quantum systems.

1. Introduction

Quantum tokens [1–11] are proposed as an alternative to classical identification tokens due to improved security guaranteed by the laws of quantum physics. The security is based on the quantum no-cloning theorem, the fact that quantum states cannot be cloned with arbitrary precision. The theorem is a direct consequence of the linearity of quantum mechanics, but its necessity also follows from the fact that measurements on clones of an unknown state could easily violate the Heisenberg-uncertainty relation.

Despite the great potential of the quantum token application, the experimental implementation with single qubits [4] faces many technical challenges. As an example, single qubit control poses typically higher demands on readout, requiring highly sensitive detection techniques to accurately measure the quantum state population. The use of ensembles in a redundant quantum parallelism regime reduces errors and decoherence. To simplify quantum token implementations, we have successfully designed a patented ensemble-based quantum token [12] that is technologically less demanding than conventional single-qubit-based methods. Such a token consists of an ensemble of identical qubits. Using such an implementation would typically render the quantum-no-cloning theorem inapplicable as a protection scheme, because an ensemble already consists of identical qubit copies.

However, the quantum projection noise will be reduced when a measurement of the token is performed in the proper basis, which can be understood by the fact that measurements in the Eigenstate basis are free of quantum projection noise [13, 14]. Thus, the resulting noise reveals a copy operation of a forger, as the cloned token will show increased quantum projection noise when the cloning operation is performed in the wrong basis.

Combining differently initialized tokens to a coin allows to define an ensemble-based quantum token protocol with security against unauthorized coin copying that can be made arbitrarily high. The number of qubits in an ensemble and also the amount of tokens in a coin are crucial design parameters for the security of the protocol. Other important parameters are intrinsically linked to fundamental characteristics of the underlying quantum platform, such as coherence times and qubit lifetimes. We present an optimal copying procedure for the individual tokens of the coin that is more efficient than the tomography methods from the literature based on direct inversion [15] or on the maximum likelihood (ML) method [16] or on Bayesian (Ba) experimental design [17].

Even when using the advanced copying procedure for the individual tokens, the quantum coins can be designed in such a way that the acceptance probabilities of forged coins becomes negligible. For this, numerical simulations of the attack scenarios were performed using C++ programs fully parallelized using the message passing interface. This library called 'DIQTOK-forge' is available on GitHub [18]. These findings are further supported by experimental measurements [13] performed on five IBM superconducting quantum processors of the Eagle family [19–21]: Kyiv, Sherbrooke, Osaka, Brisbane and Kyoto. The experiments were controlled by the Qiskit software [22], the implementations can be accessed through the author's GitHub repository [23]. The detailed analysis presented in this paper combined with the open source tools allow for designing secure quantum coins for any quantum platform, since the protocol is hardware agnostic.

This work is divided as follows. In section 2, we discuss the framework of the ensemble-based quantum token protocol. Then we focus on the individual tokens in the coin. We identified relevant parameters and benchmarked these for the IBMQ hardware. Then in section 3, different attack scenarios are considered and tested on IBMQ, where an attacker attempts to read a token and use different methods to create a forged token. Finally, the safety of the coin as a set of tokens is studied in section 4 and the paper is concluded with a final discussion in section 5.

2. Ensemble-based quantum token protocol

In this section, we discuss in detail the realization of the protocol. In sections 2.1 and 2.2, we describe the mathematical framework for a single qubit and a token composed of identical qubits, respectively. In section 2.3, we discuss how the bank should generate and accepts its own tokes.

A quantum coin contains M quantum tokens, each with N identical qubits prepared in the same quantum state, but different for each token, as can be seen in figure 1.

In order to prepare a coin, a bank randomly selects M secret angle pairs (θ_i, ϕ_i), and initializes the qubits in the ith quantum token with these angles. The prepared quantum coin is then issued to the user, while the set of secret angles is securely kept by the bank. Upon the coin's return for verification, the bank measures each quantum token using the stored angles. The coin is accepted if the number of correctly measured tokens exceeds a predetermined threshold, which is set to ensure that the probability of falsely rejecting a legitimately issued coin remains negligibly small. This normal operation of the protocol is visualized in figure 2. If a forger copies the coin by using sophisticated methods and provides a forged coin to the bank, the bank will again check the coin using the stored angles. Now, by construction, a high number of tokes are not accepted so that the whole coin is rejected with a very high probability. This procedure is shown in figure 3.

2.1. Description of a single qubit

In general, the state of a single qubit or an ensemble can be described by a density matrix [15, 24]

$$\hat{\rho} = \frac{1}{2}\left(\hat{\mathbb{1}} + x\hat{\sigma}_x + y\hat{\sigma}_y + z\hat{\sigma}_z\right)$$

in terms of the Pauli matrices $\hat{\mathbb{1}}, \hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ and the Bloch vector $\mathbf{r} = (x, y, z) \in \mathbb{R}^3$. The eigenvectors of $\hat{\rho}$ are

$$\lambda^{\pm} = \frac{1}{2}\left(1 \pm \sqrt{x^2 + y^2 + z^2}\right)$$

and must be both non-negative, so that $\mathbf{r}$ must fulfill $||\mathbf{r}||^2 \leqslant 1$ for a physical state. Mixed states obey $||\mathbf{r}||^2 < 1$ and pure states have $||\mathbf{r}||^2 = 1$. In order to simplify the model, we only consider pure states, which are represented by the surface of the Bloch sphere, in contrast to mixed states that are located inside the Bloch sphere. Thus, we describe the state $|\theta, \phi\rangle$ of a qubit with the polar angle $\theta \in [0, \pi]$ and the azimuthal angle $\phi \in (-\pi, \pi]$. In the orthonormal basis $|0\rangle$ and $|1\rangle$, we can represent a general state $|\theta_2, \phi_2\rangle$ as

$$|\theta_2,\phi_2\rangle = \mathrm{e}^{-\mathrm{i}\frac{\phi_2}{2}}\cos\left(\frac{\theta_2}{2}\right)|0\rangle + \mathrm{e}^{\mathrm{i}\frac{\phi_2}{2}}\sin\left(\frac{\theta_2}{2}\right)|1\rangle$$
$$= \mathrm{e}^{-\mathrm{i}\frac{\phi_2}{2}\hat{\sigma}_z}\mathrm{e}^{-\mathrm{i}\frac{\theta_2}{2}\hat{\sigma}_y}|0\rangle.$$

Physically, this can be achieved by initializing the qubit in the state $|0\rangle$, performing a rotation around the y-axis by θ_2, followed by a rotation around the z-axis by ϕ_2. We study here only Stern–Gerlach like measurements on the qubit [25]. Such a measurement uses angles θ_1, ϕ_1 for a back rotation around the z-axis with ϕ_1, followed by a back rotation around the y-axis by θ_1. This leads to the final state

$$|\Psi\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{\sigma}_y}\mathrm{e}^{\mathrm{i}\frac{\phi_1}{2}\hat{\sigma}_z}\mathrm{e}^{-\mathrm{i}\frac{\phi_2}{2}\hat{\sigma}_z}\mathrm{e}^{-\mathrm{i}\frac{\theta_2}{2}\hat{\sigma}_y}|0\rangle.$$

Then, the qubit is measured in the orthonormal basis. As a concrete example, we take the readout process to yield photons, which are detected with different probabilities. A photon is measured with a probability $P_0 \in [0,1]$ or $P_1 \in [0,1]$ for state $|0\rangle$ or $|1\rangle$ respectively. Note that P_0 and P_1 are model parameters to be determined for the considered quantum system, which not necessarily add up to 1 in this definition. Furthermore, they should fulfill $P_0 \neq P_1$, otherwise a measurement would not provide any information about the qubit. We assign $|0\rangle$ to the dark state, so that $P_0 < P_1$. An important quality factor of the hardware can be defined from these probabilities described by the normalized contrast

$$c \equiv \frac{P_1 - P_0}{P_1 + P_0}. \tag{1}$$

This value represents how well we can distinguish between dark and bright states upon measurement.

The probability to measure a photon from the qubit in an arbitrary state is given by

$$p_\mathrm{q} = P_0\left|\langle 0|\Psi\rangle\right|^2 + P_1\left|\langle 1|\Psi\rangle\right|^2 = P_1 - (P_1 - P_0)\left|\langle 0|\Psi\rangle\right|^2, \tag{2}$$

where we used $|\langle 0|\Psi\rangle|^2 + |\langle 1|\Psi\rangle|^2 = 1$. We further obtain [13]

$$\begin{aligned}\left|\langle 0|\Psi\rangle\right|^2 &= \left|\langle 0|\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{\sigma}_y}\mathrm{e}^{\mathrm{i}\frac{\phi_1}{2}\hat{\sigma}_z}\mathrm{e}^{-\mathrm{i}\frac{\phi_2}{2}\hat{\sigma}_z}\mathrm{e}^{-\mathrm{i}\frac{\theta_2}{2}\hat{\sigma}_y}|0\rangle\right|^2 \\ &= \left|\langle\theta_1,\phi_1|\theta_2,\phi_2\rangle\right|^2 \\ &= \frac{1}{2}\left(1 + \cos(\theta_1)\cos(\theta_2) + \sin(\theta_1)\sin(\theta_2)\cos(\phi_1 - \phi_2)\right).\end{aligned}$$

Substituting the above result in equation (2), we get

$$\begin{aligned}p_\mathrm{q}(P_0,P_1,\theta_1,\phi_1,\theta_2,\phi_2) = \frac{P_0+P_1}{2} - \frac{P_1-P_0}{2}&(\cos(\theta_1)\cos(\theta_2) \\ &+ \sin(\theta_1)\sin(\theta_2)\cos(\phi_1-\phi_2)).\end{aligned} \tag{3}$$

If we rotate the coordinate system around the z-axis, an offset angle $\Delta\phi$ is added to all angles ϕ. Thus, p_q will not change, since ϕ angles only occur in the term $\cos(\phi_1 - \phi_2)$ in equation (3) and thus the added value of $\Delta\phi$ is canceled.

2.2. Description of a token of identical qubits

Now, we consider a quantum token consisting of N such identical qubits. After the measurement using the angles θ_1, ϕ_1 the probability to measure $n \in \{0,1,\ldots,N\}$ photons from these qubits is given by the binomial distribution with probability p_q

$$p_\mathrm{t}(N,n,P_0,P_1,\theta_1,\phi_1,\theta_2,\phi_2) = \binom{N}{n} p_q^n \left(1-p_q\right)^{N-n}. \tag{4}$$

In order to determine the parameters P_0 and P_1, one can drive a Rabi oscillation on the quantum token [26]. This is modeled by preparing the state with different θ_2 settings and keeping $\phi_2 = 0$ fixed. The subsequent measurement is performed using $\theta_1 = \pi$, $\phi_1 = 0$. Averaging over many measurements gives the averaged normalized photon counts $\overline{n}$ and the corresponding standard deviation σ_n as a function of the angle θ_2. From equation (4), we obtain

$$\overline{n} = p_\mathrm{q}, \qquad \sigma_n = p_\mathrm{q}\left(1-p_\mathrm{q}\right). \tag{5}$$

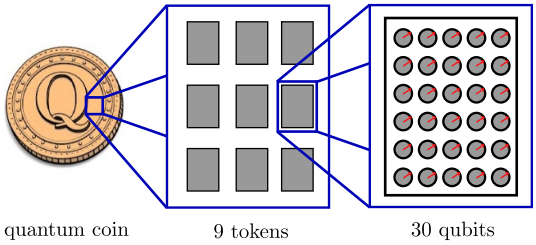

Figure 1. The proposed quantum coin consists of M quantum tokens, each comprising N qubits prepared in the same state. Each quantum token exhibits a distinct qubit state.

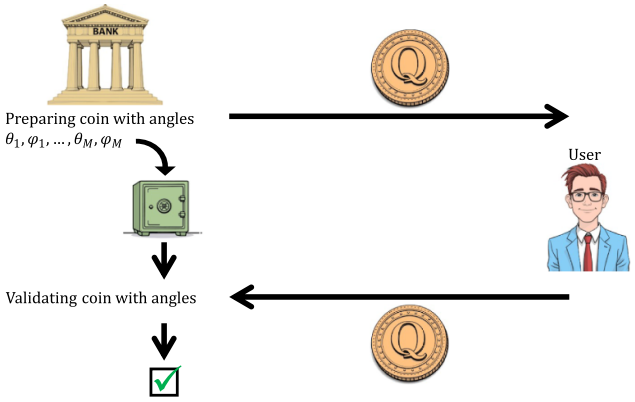

Figure 2. Normal operation of the protocol: the bank selects M secret angle pairs (θ_i, ϕ_i) and prepares a quantum coin by initializing all qubits of the ith quantum token in the state defined by (θ_i, ϕ_i). The coin is provided to the user, while the corresponding angles are securely stored by the bank. Upon return of the coin, the bank verifies its authenticity by measuring each quantum token using the stored angles. The coin is accepted if the number of valid tokens exceeds a predefined threshold. This threshold is chosen such that the probability of the bank accepting its own coin is very high.

The experimental values of $\overline{n}$ and σ_n as a function of θ for 100 qubits were measured with five IBMQ, as shown in figure 4. In the graphs $\overline{n}$ represents the Rabi oscillations for θ from 0 to π. The standard deviation σ_n at $\theta \in \{0, \pi\}$ shows a minimum and ideally a zero value due to the fact that the quantum projection noise vanishes at the poles of the Bloch sphere. One can clearly identify that for the superposition state at $\theta = \pi/2$ the standard deviation becomes maximal due to the fact that this state has the largest projection noise. Depending on the implementation of the qubit, background photons collected during the readout can lead to a reduction of the amplitude of the cosine approaching 0.5. Additionally, increased relative shot noise due to low photon counts during read out leads to a reduction of the amplitude of the cosine for the bright state. If the state at $\theta = 0$ is a dark state then this reduction is only observed at $\theta = \pi$. The fit of the experimental curves permits us to obtain the values of P_0 and P_1 for each hardware, as presented in table 1. Comparing the different IBMQ platforms, Sherbrooke has the best parameters, given by the hardware's longer coherence times and smaller gate and readout errors. Inversely, Kyoto has the worst parameters of the three. Note, in our companion study [13], we used a different model focusing on the noise description in order to model the quantum token. Here, instead, we use a statistical description in order to calculate the probability of acceptance for forged quantum tokens, both representations being in good agreement. The statistical description is better suited for the following derivations.

2.3. Bank generates quantum tokens

A bank generates a quantum token with the angles θ_b, ϕ_b. In order to derive the safety of the token with statistical methods, we consider both angles as independent random variables with a uniform probability distribution on the unit sphere, so that corresponding probability densities are given by

$$f_\theta(\theta) = \frac{\sin(\theta)}{2}, \qquad f_\phi(\phi) = \frac{1}{2\pi}. \tag{6}$$

For verification, the bank measures the token with preparation angles θ_b, ϕ_b. We denote the P_0 and P_1 hardware quality parameters of the bank setup by $P_{0\mathrm{b}}, P_{1\mathrm{b}}$. The bank sets a threshold n_T for maximum photon counts to accept the token. This is because for measuring the token the bank projects it into the dark

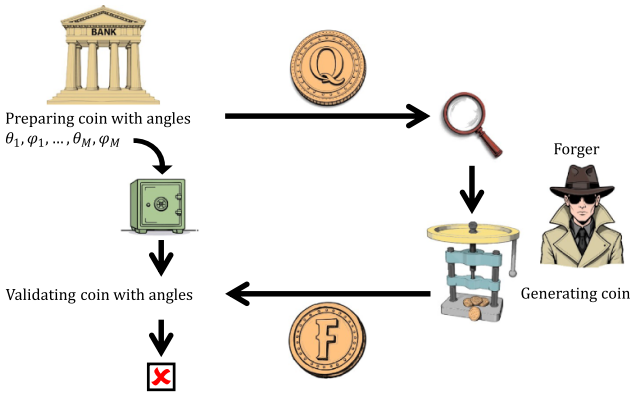

Figure 3. Attack on the protocol: a forger obtains the bank's coin and performs measurements on it to extract information, then uses this information to prepare a forged coin (symbolized by the coin press), which is returned to the bank. The bank attempts to verify the forged coin using the stored secret angles. By design, a larger fraction of quantum tokens in a forged coin are likely to be invalid, resulting in a high probability of rejecting the coin.

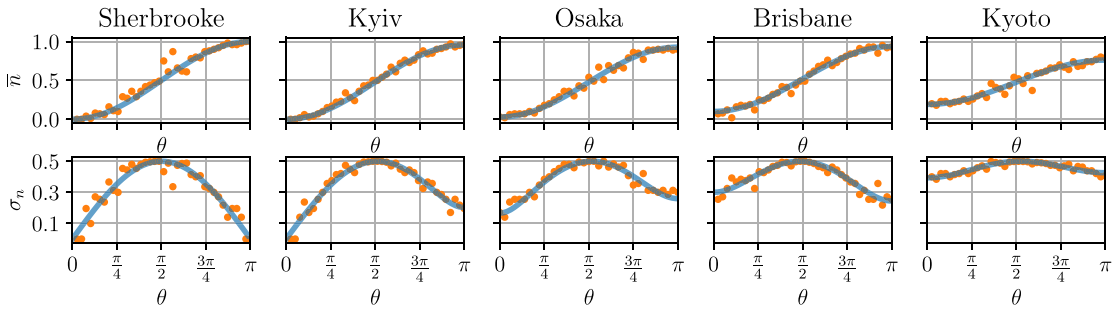

Figure 4. Experimental averaged normalized photon counts $\overline{n}$ and corresponding standard deviations σ_n for 100 qubits as a function of θ for the five IBMQs (data taken from reference [13]). Points correspond to the experimental data and lines correspond to the predictions of our model with parameters P_0, P_1 fitted to the experimental data of σ_n. $\overline{n}$ curves are related through equation (5).

Table 1. Fitted values of P_0 and P_1 from the experimental curves of the average normalized photon counts $\overline{n}$ and their corresponding standard deviation σ_n measured in the IBMQ hardware (figure 4). Additionally, the normalized contrast c is included. Sherbrooke has the best performance among the five hardware platforms, while Kyoto has the worst specifications due to dissimilar coherence times and average errors in readout and gate operations of the qubits. These two parameters are the basis to describe the following development of the quantum coin model.

IBMQ	P_0	P_1	c
Sherbrooke	$2.104 \cdot 10^{-34}$	0.999 999 991	$\sim$1
Kyiv	$7.197 \cdot 10^{-13}$	0.9571	$\sim$1
Osaka	0.028 55	0.9274	0.9403
Brisbane	0.1003	0.9362	0.8065
Kyoto	0.1916	0.7615	0.5979

state $|0\rangle$. Thus, the average probability that the bank accepts a not forged token is given by

$$\overline{p}_\mathrm{b} = \int_0^\pi \mathrm{d}\theta_\mathrm{b} \int_{-\pi}^{\pi} \mathrm{d}\phi_\mathrm{b} f_\theta(\theta_\mathrm{b}) f_\phi(\phi_\mathrm{b}) \sum_{n=0}^{n_\mathrm{T}} p_\mathrm{t}(N, n, P_{0\mathrm{b}}, P_{1\mathrm{b}}, \theta_\mathrm{b}, \phi_\mathrm{b}, \theta_\mathrm{b}, \phi_\mathrm{b}). \tag{7}$$

The acceptance probability is described by the sum of p_t over all n from 0 to n_T, as acceptance requires that the number of detected photons does not exceed n_T. To obtain the average acceptance probability, we integrate the acceptance probability $\sum_{n=0}^{n_\mathrm{T}} p_\mathrm{t}$ over the bank angles $\theta_\mathrm{b}, \phi_\mathrm{b}$ using the angle probability distributions $f_\theta(\theta_\mathrm{b}), f_\phi(\phi_\mathrm{b})$. The acceptance threshold n_T can be chosen in such a way that the average probability for the bank rejecting its own generated quantum tokens is less than ε_b

$$1 - \overline{p}_\mathrm{b} < \varepsilon_\mathrm{b}.$$

In the following we set $\epsilon_\mathrm{b} = 0.0002$ such that $\overline{p}_\mathrm{b}$ of its own token is larger than 0.9998. We considered the test cases with $N = 30$ and $N = 300$ qubits in the token and performed simulations with our model and experiments on the IBMQs (see table 2). As can be seen in table 2, one has to increase the experimental

Table 2. We used $N = 30$ and $N = 300$ qubits in the quantum token and determined the threshold n_T for the different IBMQs such that the averaged bank acceptance $\bar{p}_b$ of its own token is larger than 0.9998. The experimental threshold $n_T^{(e)}$ had to be chosen to be greater than the simulated n_T due to gate errors which are not considered in our model, with only Osaka showing optimal performance ($n_T \simeq n_T^{(e)}$).

	$N = 30$		$N = 300$		
IBMQ	n_T	$\bar{p}_b$	n_T	$n_T^{(e)}$	$\bar{p}_b$
Sherb.	0	∼1	0	11	∼1
Kyiv	0	0.999 999 999 98	0	10	0.999 999 9998
Osaka	5	0.999 81	20	19	0.999 82
Brisb.	10	0.999 91	50	73	0.999 86
Kyoto	14	0.999 86	83	96	0.999 87

threshold $n_T^{(e)}$ compared to the simulated n_T in order to compensate experimental gate errors that are not considered in our model. In conclusion, we can see that even for the Kyoto platform with lowest contrast a high $\bar{p}_b$ can be achieved by increasing n_T.

3. Attack scenarios

In the following section we describe different attack scenarios together with a description of the methods used and visualizations of the attack on the Bloch-sphere. Our model assumes that a forger tries to copy the quantum token of the bank prepared with the angles θ_b, ϕ_b, which are only known by the bank. The forger has the goal to obtain the highest possible acceptance rate by the bank for the forged token. Forger and bank may have a different measurement setup, so that we denote the parameters of the forger setup by P_{0f}, P_{1f}. In this work, we just assume that the bank has the same setup as the forger, i.e. $P_{0b} = P_{0f}$ and $P_{1b} = P_{1f}$.

3.1. General description of fake token generation

In this section, we provide general statements about the average acceptance probability and the averaged normalized photon count of a forged token that is generated using just a random guess or results from one, two or three measurements on the original token. Finally, we analyze the extent to which the forger is free to choose the coordinate system and visualize the general attack scenarios on the Bloch sphere.

3.1.1. Random guess

We begin with the simplest scenario: the forger does not perform any measurement and just guesses the angles θ_f, ϕ_f for preparing a forged token. We obtain for the average probability that the bank accepts this token as a function of θ_f, ϕ_f:

$$\bar{p}_{f_0}(\theta_f, \phi_f) = \int_0^{\pi} d\theta_b \int_{-\pi}^{\pi} d\phi_b f_\theta(\theta_b) f_\phi(\phi_b) \sum_{n=0}^{n_T} p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b). \tag{8}$$

Note the similarity to equation (7), except that in p_t, the fifth and sixth arguments are replaced by the angles θ_f and ϕ_f. The function is denoted by $\bar{p}_{f_0}$, since the forger performed 0 measurements. Due to the uniform distribution of the bank angles over the Bloch sphere, the above probability does not depend on θ_f, ϕ_f. This acceptance probability depends only on the probability P_{0b} and P_{1b} to measure a photon and the acceptance threshold n_T of the bank (table 1).

For this approach, the numerical results are obtained through integration with Gauss–Legendre quadrature method [27] and the results are presented in section 3.4.

3.1.2. One measurement

Now we consider the case where the forger performs one measurement on the bank's token using the angles θ_{f_1}, ϕ_{f_1} and detects n_{f_1} photons. Using the information from the measurement the forger prepares a token with the angles θ_f, ϕ_f. The average probability that the bank accepts this token is given by

$$\bar{p}_{f_1} = \sum_{n_{f_1}=0}^{N_1} \int_0^{\pi} d\theta_b \int_{-\pi}^{\pi} d\phi_b f_\theta(\theta_b) f_\phi(\phi_b) p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \times \sum_{n=0}^{n_T} p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b). \tag{9}$$

Now we have modified equation (8) by summing the average acceptance probability over all possible single measurement outcomes n_{f_1}, each weighted by the probability of observing that outcome, represented by p_t in the first line. Note, that here $N_1 = N$ and θ_f, ϕ_f are functions of N_1, n_{f_1}, θ_{f_1}, and ϕ_{f_1}. The average normalized photon count $\overline{n}$ measured by the bank as a function of the bank angle θ_b is given by

$$\begin{aligned}\overline{n}(\theta_b) = \frac{1}{N}\sum_{n_{f_1}=0}^{N_1}\int_{-\pi}^{\pi} \mathrm{d}\phi_b f_\phi(\phi_b)\, p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \\ \times \sum_{n=0}^{N} n\, p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b)\,. \end{aligned} \tag{10}$$

The average photon count is calculated as the sum over $n = 0$ to the maximum photon number N, where each photon count n is weighted by its corresponding probability. This probability is obtained by summing over all possible measurement outcomes n_{f_1}; each term is the product of the probability p_t that the forger measures n_{f_1} photons before forging the token (first line) and the probability that the bank measures n photons from the forged token based on n_{f_1} (p_t in the second line). As the average photon count is only a function of θ_b, we further average over ϕ_b by integrating with the weight function f_ϕ. In order to normalize the average photon count, we divide by N.

3.1.3. Two measurements

Now the forger divides the token into several parts and measures each part containing N_j qubits with individual angles θ_{f_j}, ϕ_{f_j} and detects n_{f_j} photons. Using the measurement results, the forger generates a forged token. The average probability that the bank accepts a forged token prepared by the forger from two measurements is given by

$$\begin{aligned}\overline{p}_{f_2} = \sum_{n_{f_1}=0}^{N_1}\sum_{n_{f_2}=0}^{N_2}\int_0^{\pi}\mathrm{d}\theta_b\int_{-\pi}^{\pi}\mathrm{d}\phi_b f_\theta(\theta_b) f_\phi(\phi_b)\, p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \\ \times p_t(N_2, n_{f_2}, P_{0f}, P_{1f}, \theta_{f_2}, \phi_{f_2}, \theta_b, \phi_b)\sum_{n=0}^{n_T} p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b)\,. \end{aligned}$$

In order to account for two measurements equation (9) is modified by now summing over all two possible outcomes n_{f_1} and n_{f_2}, and accounting for the probabilities of both outcomes, as represented by p_t in the first line and in the first term of the second line. Here, θ_f, ϕ_f are functions of N_1, N_2, n_{f_1}, n_{f_2}, θ_{f_1}, ϕ_{f_1}, θ_{f_2}, and ϕ_{f_2}. Now, the average normalized photon count measured by the bank as a function of the bank angle θ_b is given by

$$\begin{aligned}\overline{n}(\theta_b) = \frac{1}{N}\sum_{n_{f_1}=0}^{N_1}\sum_{n_{f_2}=0}^{N_2}\int_{-\pi}^{\pi}\mathrm{d}\phi_b f_\phi(\phi_b)\, p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \\ \times p_t(N_2, n_{f_2}, P_{0f}, P_{1f}, \theta_{f_2}, \phi_{f_2}, \theta_b, \phi_b)\sum_{n=0}^{N} n\, p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b)\,. \end{aligned}$$

Again two measurements are implemented through changing equation (10) by summing over all two possible outcomes n_{f_1} and n_{f_2}, and accounting for the probabilities of both outcomes, as given in line one and in the first term of the second line.

3.1.4. Three measurements

Finally if the forger performs three measurements, the average probability for the bank accepting the forged token is given by

$$\begin{aligned}\overline{p}_{f_3} = \sum_{n_{f_1}=0}^{N_1}\sum_{n_{f_2}=0}^{N_2}\sum_{n_{f_3}=0}^{N_3}\int_0^{\pi}\mathrm{d}\theta_b\int_{-\pi}^{\pi}\mathrm{d}\phi_b f_\theta(\theta_b) f_\phi(\phi_b)\, p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \\ \times p_t(N_2, n_{f_2}, P_{0f}, P_{1f}, \theta_{f_2}, \phi_{f_2}, \theta_b, \phi_b)\, p_t(N_3, n_{f_3}, P_{0f}, P_{1f}, \theta_{f_3}, \phi_{f_3}, \theta_b, \phi_b) \\ \times \sum_{n=0}^{n_T} p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b)\,. \end{aligned}$$

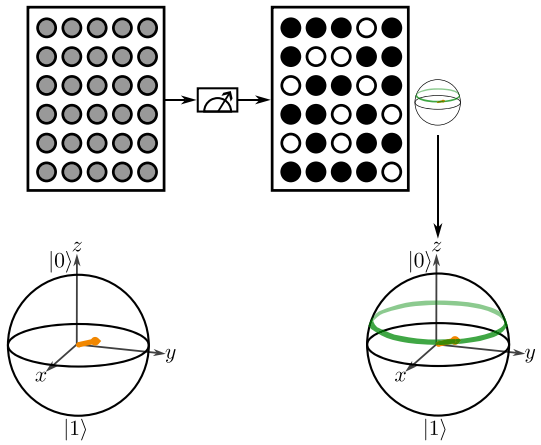

Figure 5. The forger performs a single measurement on the entire quantum token, resulting in some qubits emitting a photon, as indicated by the white filled circles. On the Bloch sphere, the states yielding this measurement outcome with highest probability are distributed along a ring.

By now the extension pattern of equation (9) should be obvious, we now sum over all three possible outcomes n_{f_1}, n_{f_2}, and n_{f_3}, and account for the probabilities of the three outcomes, as represented by p_t in lines one and two. Again, θ_f, ϕ_f are functions of $N_1, N_2, N_3, n_{f_1}, n_{f_2}, n_{f_3}, \theta_{f_1}, \phi_{f_1}, \theta_{f_2}, \phi_{f_2}, \theta_{f_3}$, and ϕ_{f_3}. The choice of the angles θ_{f_j}, ϕ_{f_j} and the number of qubits N_j of the actual measurement may depend on the measurement results of the previous measurements. The average normalized photon count measured by the bank as a function of the bank angle θ_b is denoted by

$$\begin{aligned}\overline{n}(\theta_b) = \frac{1}{N}\sum_{n_{f_1}=0}^{N_1}\sum_{n_{f_2}=0}^{N_2}\sum_{n_{f_3}=0}^{N_3}\int_{-\pi}^{\pi} \mathrm{d}\phi_b f_\phi(\phi_b)\, p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, \theta_{f_1}, \phi_{f_1}, \theta_b, \phi_b) \\ \times p_t(N_2, n_{f_2}, P_{0f}, P_{1f}, \theta_{f_2}, \phi_{f_2}, \theta_b, \phi_b)\, p_t(N_3, n_{f_3}, P_{0f}, P_{1f}, \theta_{f_3}, \phi_{f_3}, \theta_b, \phi_b) \\ \times \sum_{n=0}^{N} n\, p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b)\,.\end{aligned}$$

And as previously we have extended equation (10) by summing over all three possible outcomes n_{f_1}, n_{f_2}, and n_{f_3}, and accounting for the probabilities of the three outcomes, as represented by p_t in lines one and two.

3.1.5. Forger's measurement process

Since the bank chooses the angles θ_b, ϕ_b uniformly distributed on the Bloch sphere, as described in equation (6), there are no preferred directions and the forger has the free choice of setting the measurement basis. Thus, the forger chooses the basis in such a way that the angles $\theta_{f_1} = 0$, $\phi_{f_1} = 0$ are used in the first measurement and the angle $\phi_{f_2} = 0$ with arbitrary θ_{f_2} is used in the second measurement. In the last case $\phi_{f_2} = 0$ is no restriction of generality because the value of ϕ_{f_1} does not play any role when measured at the pole with $\theta_{f_1} = 0$ (see equation (3)). In figures 5–7, we visualize the measurement process for one, two and three measurements.

3.2. Quantum state tomography

In the general description of fake token generation, the forger has to concretely choose the measurement angles of the second and third measurement and has to define the preparation angles of the forged token θ_f, ϕ_f from the measurement results. In this section, we describe several strategies determining these angles depending on the measurement result using state-of-the art quantum state tomography methods. Here, the forger tries to determine θ_f, ϕ_f from the measurements trying to reach values as close as possible to the unknown bank angles θ_b, ϕ_b. We compare three different methods for quantum state tomography: direct inversion tomography (DIT), maximum likelihood (ML) method and Bayesian (Ba) method.

3.2.1. Direct Inversion Tomography (DIT)

The simplest method providing in principle the complete information of the bank state θ_b, ϕ_b is performing three measurements, one in each of the dimensions on the Bloch sphere using $N_j = N/3$ qubits. In detail, the forger measures n_{f_1} photons using $\theta_{f_1} = 0$, $\phi_{f_1} = 0$, n_{f_2} photons using $\theta_{f_2} = \frac{\pi}{2}$, $\phi_{f_2} = 0$ and n_{f_3} photons using $\theta_{f_3} = \frac{\pi}{2}$, $\phi_{f_3} = \frac{\pi}{2}$. This corresponds to a measurement along the z-, x- and y-axis, as shown in figure 8(a).

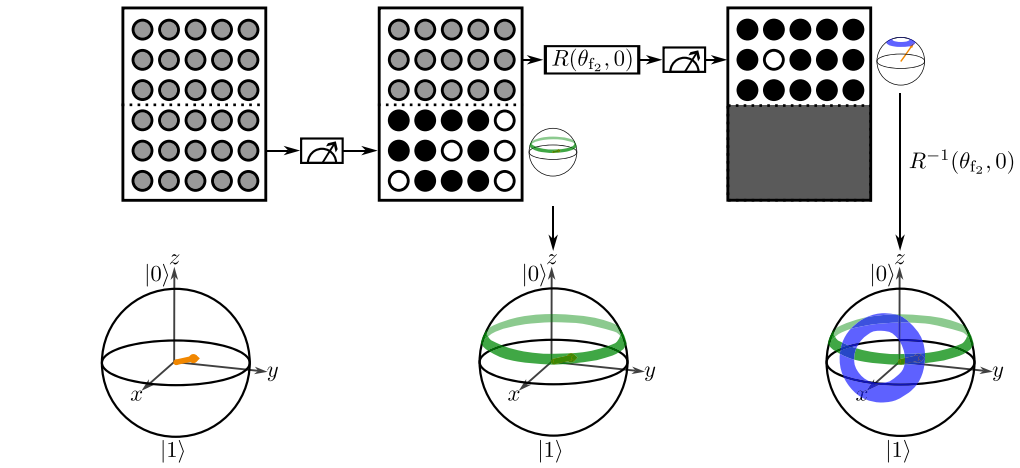

Figure 6. An improved measurement scheme consists of two measurements. Now the forger divides the token into two parts. First, one part is measured as in figure 5. Note that the width of the ring is now larger as compared to a single measurement due to the reduced ensemble size. The forger then measures the second part of the token after applying a rotation by θ_{f_2}, leading now to a typically different positioned ring (see top blue ring). By applying the inverse rotation $-\theta_{f_2}$, this second result can be visualized together with the first measurement. The intersection of the two rings generally consists of two distinct regions, which represent the states on the Bloch sphere most likely to produce both measurement outcomes. Even though the area of possible angles was reduced compared to a single measurement, there still exists an ambiguity.

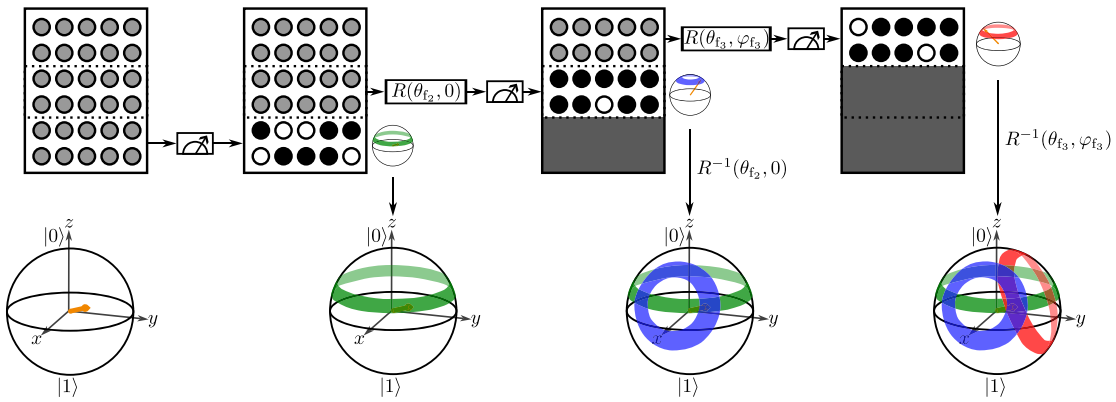

Figure 7. With three measurements typically an unambiguous result is obtained. Now the forger divides the token into three parts. The forger measures each part but he rotates the second and third sub-ensembles by angles θ_{f_2} and θ_{f_3}, ϕ_{f_3} respectively. Note that the width of the ring is now larger as compared to a single and two measurements due to the reduced ensemble size. But after undoing the rotation by θ_{f_3} and ϕ_{f_3}, typically, only a single distinct intersection region exists, which contains the states most likely to produce all three measurement outcomes. With this method typically an unambiguous result with minimal area of possible angles is obtained.

Using equation (3) for the ideal case where $P_0 = 0$ and $P_1 = 1$, $\overline{n}$ can be calculated for this measurement scheme as a function of the bank angles θ_b and ϕ_b. These results plotted over the Bloch sphere are shown in figure 8(a). We observe that the number of detected counts decreases as the measurement angles chosen by the attacker approach the secret angles used by the bank. To further test the model, this measurement procedure was performed with IBMQ Brisbane for three ensemble sizes of $N = 300$, 100 and 10, as shown in figure 8(b). The Bloch sphere is projected into a 2D-plane for better visualization, where we observe a good agreement with the experimental data for the largest ensemble size. As the ensemble size decreases to $N = 10$, the measurement becomes increasingly noisy. Therefore, we chose an intermediate ensemble size of $N = 300$ allowing for low noise state estimation if we take 100 measurements in each axis. Additionally, we realized that the photon counts are independent of ϕ_b for the measurement in the z-axis, as expected. In the following, the forger uses this measurement results to forge the fake tokens.

From the three results n_{f_1}, n_{f_2}, n_{f_3}, the forger obtains the following guess of the bank's state Bloch vector [15]

$$\mathbf{R}_d = \left(\frac{N_2 - 2n_{f_2}}{N_2}, \frac{N_3 - 2n_{f_3}}{N_3}, \frac{N_1 - 2n_{f_1}}{N_1} \right).$$

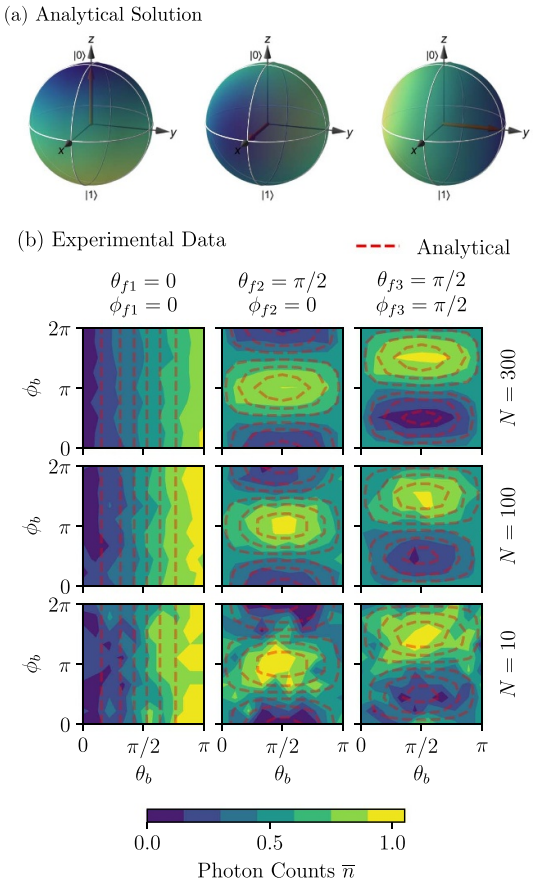

Figure 8. (a) Analytic solution from equation (3) for the averaged normalized photon counts $\overline{n}$ which an attacker obtains by measuring a bank token along the z, x and y axes. As the bank's angles approach the attacker's angles in the Bloch sphere, the photon counts get smaller. (b) Measurements performed by the attacker on IBMQ Brisbane with $N = 300$, 100 and 10 qubits along the three axes on the Bloch sphere and projected on a 2D-plane. The data is compared with the analytic solution for the fitted value of P_0 and P_1 obtained from the Rabi measurement in figure 4. As the ensemble size approaches a small value of $N = 10$, the measurement becomes noisy and deviates from theory. Whereas at $N = 100$ and 300, a good agreement is observed.

In general, $||\mathbf{R}_\mathrm{d}|| \neq 1$, so that the forger has to perform a normalization in order to obtain a physically reasonable guess of the bank's state

$$\mathbf{r}_\mathrm{d} = \frac{\mathbf{R}_\mathrm{d}}{||\mathbf{R}_\mathrm{d}||}.$$

Finally, the forger obtains the angles $\theta_\mathrm{f}^{(\mathrm{DIT})}, \phi_\mathrm{f}^{(\mathrm{DIT})}$ for the best guess of the bank's angles from

$$\theta_\mathrm{f}^{(\mathrm{DIT})} = \arccos\left(r_\mathrm{d}^{(z)}\right), \tag{11}$$

where arccos denotes the inverse cosine function and $r_\mathrm{d}^{(z)}$ is the z-component of the vector $\mathbf{r}_\mathrm{d}$. If $\theta_\mathrm{f}^{(\mathrm{DIT})} \in \{0, \pi\}$, we can set $\phi_\mathrm{f}^{(\mathrm{DIT})} = 0$, since the value of $\phi_\mathrm{f}^{(\mathrm{DIT})}$ does not play any role. Otherwise, we obtain

$$\phi_\mathrm{f}^{(\mathrm{DIT})} = \mathrm{atan2}\left(\frac{r_\mathrm{d}^{(\mathrm{x})}}{\sin\left(\theta_\mathrm{f}^{(\mathrm{DIT})}\right)}, \frac{r_\mathrm{d}^{(\mathrm{y})}}{\sin\left(\theta_\mathrm{f}^{(\mathrm{DIT})}\right)}\right), \tag{12}$$

where atan2 is the 2-argument arctangent function. Note that $\theta_\mathrm{f}^{(\mathrm{DIT})}, \phi_\mathrm{f}^{(\mathrm{DIT})}$ are functions of n_{f_1}, n_{f_2} and n_{f_3}. We denote the average probability for the bank accepting this forged token by $\overline{p}_{\mathrm{f}_3}^{(\mathrm{DIT})}$ and present our numerical results in section 3.4.

Forged tokens were experimentally prepared with this method based on the attacker measurements from figure 8(b) for $N = 300$, with 100 qubits measured in each axis. Subsequently these forged tokens are passed to the bank, where the photons counts are measured with the original angles $\theta_\mathrm{b}, \phi_\mathrm{b}$. These normalized photon counts obtained with IBMQ Brisbane as a function of the preparation angle θ_b and averaged over ϕ_b are shown in figure 9.

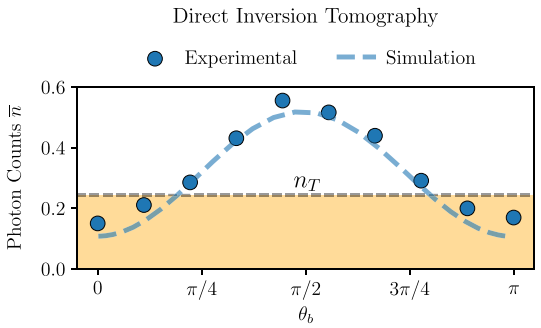

Figure 9. IBMQ Brisbane simulated and experimental normalized photon counts measured by the bank from tokens forged with direct inversion tomography. Using the measurement results from figure 8, the attacker sets the forged angles $\theta_f^{(\mathrm{DITe})}$ and $\phi_f^{(\mathrm{DITe})}$ for the token, which is then passed to the bank. The photon counts measured by the bank and averaged over ϕ_b show a maximum at $\theta_b = \pi/2$, due to the larger distribution of states at the equator of the Bloch sphere. The token is accepted if the photon counts are smaller than the threshold $\overline{n} < n_T$, where $n_T^{(e)}$ is taken from table 2. Averaging over θ_b according to the distribution of equation (6), we obtain an acceptance probability of $\overline{p}_{f_3}^{(\mathrm{DITe})} = 0.3769$ for tokens forged by DIT.

As discussed in section 2.3, the token is accepted if the photon counts are smaller than the threshold $\overline{n} < n_T^{(e)}$, where $n_T^{(e)}$ is taken from table 2. Due to smaller density of states at the poles we observe that the acceptance probability is larger, in agreement with equation (6). The experimental data agrees well with the numerical values. Averaging over θ_b weighted according to the spherical distribution (equation (6)), we obtain the experimental acceptance probability of $\overline{p}_{f_3}^{(\mathrm{DITe})} = 0.3769$, which is higher than the numerical value $\overline{p}_{f_3}^{(\mathrm{DIT})} = 0.2770$, due to the different acceptance thresholds $n_T^{(e)} > n_T$. We will present in section 3.4 a detailed analysis of the numerical results.

3.2.2. Maximum Likelihood (ML) method

The above method has the disadvantage that the forger has to divide the quantum token into three parts and has to perform a measurement with different angles on each part. This may be technically unfeasible for some quantum systems like NV-centers, where the ensemble inseparability is guaranteed by the diffraction limited area of the optical initialization and readout [28], as well as the non-local microwave state manipulation [29]. Another approach is using the ML method, which can also be used with only one measurement on the entire token. In this method, the forger tries to determine θ_f, ϕ_f in such a way that these angles most likely generate the observed measurement results. The forger performs N_m measurements and obtains n_{f_j} photons in the jth measurement with the angles θ_{f_j}, ϕ_{f_j} on N_j qubits. The likelihood function, which describes the probability of the total experimental outcomes, is given by [16]

$$\mathcal{L}\left(\{n_{f_j}\}\,|\theta_b,\phi_b\right) = \prod_{j=1}^{N_m} p_t\left(N_j, n_{f_j}, P_{0f}, P_{1f}, \theta_{f_j}, \phi_{f_j}, \theta_b, \phi_b\right). \tag{13}$$

The forger searches for the angles θ_b, ϕ_b that maximize the likelihood function, which can be found through the conditions

$$\frac{\partial \mathcal{L}}{\partial \theta_b} = 0, \qquad \frac{\partial \mathcal{L}}{\partial \phi_b} = 0.$$

The solution provides the ML estimation $\theta_f^{(\mathrm{ML})}$, $\phi_f^{(\mathrm{ML})}$ for the unknown bank angles θ_b, ϕ_b. Thus, in order to determine the solution, we formally exchange θ_b, ϕ_b with $\theta_f^{(\mathrm{ML})}$, $\phi_f^{(\mathrm{ML})}$ in equation (13).

Firstly, we consider the case of $N_m = 1$ measurement. Here, we have

$$\mathcal{L}\left(n_{f_1}\,|\theta_f^{(\mathrm{ML})}, \phi_f^{(\mathrm{ML})}\right) = p_t\left(N_1, n_{f_1}, P_{0f}, P_{1f}, 0, 0, \theta_f^{(\mathrm{ML})}, \phi_f^{(\mathrm{ML})}\right)$$

using $\theta_{f_1} = 0$, $\phi_{f_1} = 0$, and $N_1 = N$. Since p_t is a binomial distribution with probability $p_q\left(P_{0f}, P_{1f}, 0, 0, \theta_f^{(\mathrm{ML})}, \phi_f^{(\mathrm{ML})}\right)$, the likelihood function is maximal for [30]

$$\frac{n_{f_1}}{N} = p_q\left(P_{0f}, P_{1f}, 0, 0, \theta_f^{(\mathrm{ML})}, \phi_f^{(\mathrm{ML})}\right).$$

Using equation (3), one obtains further

$$\frac{n_{\mathrm{f}_1}}{N_1} = \frac{P_0 + P_1}{2} - \frac{P_1 - P_0}{2} \cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right).$$

A rearrangement yields

$$\underbrace{\frac{2\,\frac{n_{\mathrm{f}_1}}{N_1} - P_0 - P_1}{P_0 - P_1}}_{=:a_{\mathrm{f}_1}} = \cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right), \tag{14}$$

where we get

$$\theta_{\mathrm{f}}^{(\mathrm{ML})} = \arccos\left(a_{\mathrm{f}_1}\right). \tag{15}$$

Due to noise in a real world measurement, one may obtain a value of a_{f_1} that is outside of the interval $[-1,1]$. In order to obtain a physically meaningful value for $\theta_{\mathrm{f}}^{(\mathrm{ML})}$ in these cases, a_{f_1} must be constrained to lie within the interval $[-1,1]$. For $\phi_{\mathrm{f}}^{(\mathrm{ML})}$, the forger can choose any value in the interval $(-\pi,\pi]$. We choose the value $\phi_{\mathrm{f}}^{(\mathrm{ML})} = 0$ without restriction of generality.

Now we consider $N_{\mathrm{m}} = 2$ measurements with $\theta_{\mathrm{f}_2} \notin \{0,\pi\}$. Note, for $\theta_{\mathrm{f}_2} \in \{0,\pi\}$, the second measurement is equivalent to the first measurement, so that one effectively performs one measurement on the whole quantum token as described above. We have

$$\begin{aligned}\mathcal{L}\left(n_{\mathrm{f}_1}, n_{\mathrm{f}_2} \middle| \theta_{\mathrm{f}}^{(\mathrm{ML})}, \phi_{\mathrm{f}}^{(\mathrm{ML})}\right) = {} & p_{\mathrm{t}}\left(N_1, n_{\mathrm{f}_1}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, 0, 0, \theta_{\mathrm{f}}^{(\mathrm{ML})}, \phi_{\mathrm{f}}^{(\mathrm{ML})}\right) \\ & \times p_{\mathrm{t}}\left(N_2, n_{\mathrm{f}_2}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_2}, 0, \theta_{\mathrm{f}}^{(\mathrm{ML})}, \phi_{\mathrm{f}}^{(\mathrm{ML})}\right).\end{aligned}$$

Using $\theta_{\mathrm{f}_1} = 0$, $\phi_{\mathrm{f}_1} = 0$, and $\phi_{\mathrm{f}_2} = 0$. The likelihood function is maximal, if the two factors are maximal. This generates directly the conditions

$$\frac{n_{\mathrm{f}_1}}{N_1} = p_{\mathrm{q}}\left(P_{0\mathrm{f}}, P_{1\mathrm{f}}, 0, 0, \theta_{\mathrm{f}}^{(\mathrm{ML})}, \phi_{\mathrm{f}}^{(\mathrm{ML})}\right), \tag{16}$$

$$\frac{n_{\mathrm{f}_2}}{N_2} = p_{\mathrm{q}}\left(P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_2}, 0, \theta_{\mathrm{f}}^{(\mathrm{ML})}, \phi_{\mathrm{f}}^{(\mathrm{ML})}\right). \tag{17}$$

From equation (16), we can directly derive $\theta_{\mathrm{f}}^{(\mathrm{ML})}$ via equation (15). Using $\theta_{\mathrm{f}}^{(\mathrm{ML})}$, we obtain from equation (17)

$$a_{\mathrm{f}_2} = \cos\left(\theta_{\mathrm{f}_2}\right) \cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right) + \sin\left(\theta_{\mathrm{f}_2}\right) \sin\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right) \cos\left(\phi_{\mathrm{f}}^{(\mathrm{ML})}\right), \tag{18}$$

if we define a_{f_2} as a function of N_2 and n_{f_2} by replacing the corresponding variables in a_{f_1} following equation (14). If $\theta_{\mathrm{f}}^{(\mathrm{ML})} \in \{0,\pi\}$, then $\sin\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right) = 0$ and the value of $\phi_{\mathrm{f}}^{(\mathrm{ML})}$ does not play any role, so that we can set $\phi_{\mathrm{f}}^{(\mathrm{ML})} = 0$. Otherwise, a rearrangement yields

$$\frac{a_{\mathrm{f}_2} - \cos\left(\theta_{\mathrm{f}_2}\right) \cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right)}{\sin\left(\theta_{\mathrm{f}_2}\right) \sin\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right)} = \cos\left(\phi_{\mathrm{f}}^{(\mathrm{ML})}\right).$$

Since we have $\cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right) = a_{\mathrm{f}_1}$ and

$$\sin\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right) = \sqrt{1 - \cos\left(\theta_{\mathrm{f}}^{(\mathrm{ML})}\right)^2} = \sqrt{1 - a_{\mathrm{f}_1}^2},$$

we obtain

$$\phi_{\mathrm{f}}^{(\mathrm{ML}\pm)} = \pm\arccos\left(\frac{a_{\mathrm{f}_2} - \cos\left(\theta_{\mathrm{f}_2}\right) a_{\mathrm{f}_1}}{\sin\left(\theta_{\mathrm{f}_2}\right) \sqrt{1 - a_{\mathrm{f}_1}^2}}\right). \tag{19}$$

Again, one has to adapt the argument of the arccos function so that it is located in the interval $[-1,1]$ in order to obtain real solutions. In general, there are two solutions for $\phi_{\mathrm{f}}^{(\mathrm{ML})}$, from which the forger has to

choose one. Due to symmetry properties, both solutions are equivalent, such that we can choose the '+' solution without restriction of generality.

At last, we consider $N_\mathrm{m} = 3$ measurements with $\theta_{\mathrm{f}_2} \notin \{0, \pi\}$ and $\theta_{\mathrm{f}_3} \notin \{0, \pi\}$ and $\phi_{\mathrm{f}_3} \notin \{0, \pi\}$. The constraints $\theta_{\mathrm{f}_2} \notin \{0, \pi\}$ and $\theta_{\mathrm{f}_3} \notin \{0, \pi\}$ are responsible for all measurements being different. The constraint $\phi_{\mathrm{f}_3} \notin \{0, \pi\}$ takes care that the third measurement is not equivalent to the second measurement. We have

$$\begin{aligned}\mathcal{L}\left(n_{\mathrm{f}_1}, n_{\mathrm{f}_2}, n_{\mathrm{f}_3} \middle| \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right) = {} & p_\mathrm{t}\left(N_1, n_{\mathrm{f}_1}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, 0, 0, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right) \\ & \times p_\mathrm{t}\left(N_2, n_{\mathrm{f}_2}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_2}, 0, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right) \\ & \times p_\mathrm{t}\left(N_3, n_{\mathrm{f}_3}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_3}, \phi_{\mathrm{f}_3}, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right),\end{aligned}$$

using $\theta_{\mathrm{f}_1} = 0$, $\phi_{\mathrm{f}_1} = 0$, and $\phi_{\mathrm{f}_2} = 0$. The likelihood function is maximal, if the three factors are maximal, which produces the conditions

$$\frac{n_{\mathrm{f}_1}}{N_1} = p_\mathrm{q}\left(P_{0\mathrm{f}}, P_{1\mathrm{f}}, 0, 0, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right), \tag{20}$$

$$\frac{n_{\mathrm{f}_2}}{N_2} = p_\mathrm{q}\left(P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_2}, 0, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right), \tag{21}$$

$$\frac{n_{\mathrm{f}_3}}{N_3} = p_\mathrm{q}\left(P_{0\mathrm{f}}, P_{1\mathrm{f}}, \theta_{\mathrm{f}_3}, \phi_{\mathrm{f}_3}, \theta_\mathrm{f}^{(\mathrm{ML})}, \phi_\mathrm{f}^{(\mathrm{ML})}\right). \tag{22}$$

From equation (20) we obtain $\theta_\mathrm{f}^{(\mathrm{ML})}$ using equation (15). Combining this result with equation (21) we derive the two solutions $\phi_\mathrm{f}^{(\mathrm{ML}\pm)}$ for $\phi_\mathrm{f}^{(\mathrm{ML})}$ using equation (19). We obtain further from equation (22)

$$\frac{a_{\mathrm{f}_3} - \cos\left(\theta_{\mathrm{f}_3}\right)\cos\left(\theta_\mathrm{f}^{(\mathrm{ML})}\right)}{\sin\left(\theta_{\mathrm{f}_3}\right)\sin\left(\theta_\mathrm{f}^{(\mathrm{ML})}\right)} = \cos\left(\phi_{\mathrm{f}_3} - \phi_\mathrm{f}^{(\mathrm{ML})}\right).$$

Using

$$\cos\left(\phi_{\mathrm{f}_3} - \phi_\mathrm{f}^{(\mathrm{ML})}\right) = \cos\left(\phi_{\mathrm{f}_3}\right)\cos\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right) + \sin\left(\phi_{\mathrm{f}_3}\right)\sin\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right)$$

we further obtain

$$\frac{a_{\mathrm{f}_3} - \cos\left(\theta_{\mathrm{f}_3}\right)\cos\left(\theta_\mathrm{f}^{(\mathrm{ML})}\right)}{\sin\left(\theta_{\mathrm{f}_3}\right)\sin\left(\phi_{\mathrm{f}_3}\right)\sin\left(\theta_\mathrm{f}^{(\mathrm{ML})}\right)} - \frac{\cos\left(\phi_{\mathrm{f}_3}\right)\cos\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right)}{\sin\left(\phi_{\mathrm{f}_3}\right)} = \sin\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right)$$

and finally

$$\sin\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right) = \frac{a_{\mathrm{f}_3} - \cos\left(\theta_{\mathrm{f}_3}\right)a_{\mathrm{f}_1}}{\sin\left(\theta_{\mathrm{f}_3}\right)\sin\left(\phi_{\mathrm{f}_3}\right)\sqrt{1 - a_{\mathrm{f}_1}^2}} - \frac{\cos\left(\phi_{\mathrm{f}_3}\right)\cos\left(\phi_\mathrm{f}^{(\mathrm{ML})}\right)}{\sin\left(\phi_{\mathrm{f}_3}\right)}.$$

In contrast to the cosine function, the sine function is sensitive to the sign of the argument, so that one can determine the final solution $\phi_\mathrm{f}^{(\mathrm{ML})}$ with the correct sign by inserting the two solutions $\phi_\mathrm{f}^{(\mathrm{ML}\pm)}$ in the above equation.

Similar to the direct inversion tomography, the forger obtains a clear estimate of the unknown bank angles using three measurements with the ML method. Using two measurements, the forger obtains two possible points on the Bloch sphere and using one measurement, the forger obtains a circle on the Bloch sphere as possible solutions for the bank angles (see figures 5 and 6). We denote the average probability that the bank accepts the forged tokens generated by the ML method using one, two, or three measurements as $\overline{p}_{\mathrm{f}_1}^{(\mathrm{ML})}$, $\overline{p}_{\mathrm{f}_2}^{(\mathrm{ML})}$ and $\overline{p}_{\mathrm{f}_3}^{(\mathrm{ML})}$, respectively. For Brisbane and $N = 300$, we obtain $\overline{p}_{\mathrm{f}_1}^{(\mathrm{ML})} = 0.2835$, $\overline{p}_{\mathrm{f}_2}^{(\mathrm{ML})} = 0.6404$ and $\overline{p}_{\mathrm{f}_3}^{(\mathrm{ML})} = 0.9803$. In section 3.4, we present and discuss all numerical results in detail.

These values were also measured experimentally with IBMQ Brisbane using $N = 300$, as shown in figure 10. As in the case of the DIT method, the normalized counts are maximal at $\theta_\mathrm{b} = \pi/2$. As the number of measurement axes are increased, the counts get lower at the equator resulting in a better estimation of the state by the forger. By averaging over θ_b, weighted by equation (6) and assuming the experimental benchmarked threshold of $n_\mathrm{T}^{(\mathrm{e})}$ from table 2, we get the acceptance probabilities of $\overline{p}_{\mathrm{f}_1}^{(\mathrm{MLe})} = 0.4698$, $\overline{p}_{\mathrm{f}_2}^{(\mathrm{MLe})} = 0.6688$ and $\overline{p}_{\mathrm{f}_3}^{(\mathrm{MLe})} = 0.9847$. From this results one can clearly see that the acceptance probability of the forged token increases substantially with the number of measurements. Note that several measurements might not be physically realizable on every quantum platform.

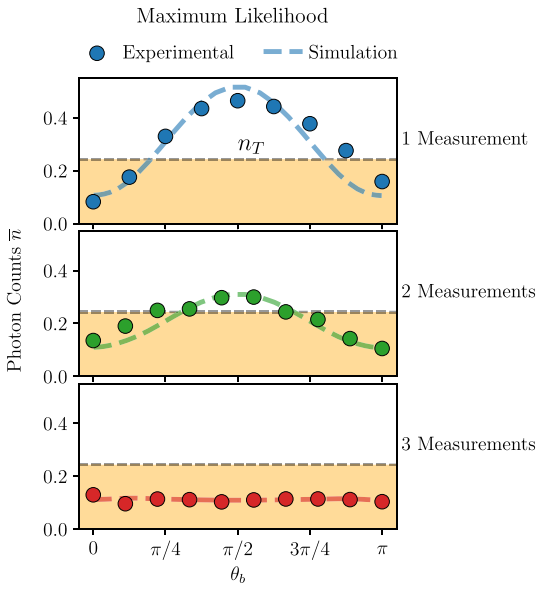

Figure 10. Simulated and experimental averaged photon counts of IBMQ Brisbane for tokens forged by maximum likelihood method for 1, 2 and 3 measurement axes performed by the forger. As in figure 9 for the DIT method, the forger uses the results from his measurements to forge fake tokens for many combinations of bank angles θ_b and ϕ_b of the token, which is then passed to the bank and verified. The photon counts are maximal at $\theta_b = \pi/2$ for 1 and 2 measurements, due to the larger density of states at this point. While for 3 measurements, the attacker can efficiently forge fake tokens over the whole Bloch sphere. The corresponding experimental acceptance probabilities are $\overline{p}_{f_1}^{(MLe)} = 0.4698$, $\overline{p}_{f_2}^{(MLe)} = 0.6688$ and $\overline{p}_{f_3}^{(MLe)} = 0.9847$.

3.2.3. Bayesian (Ba) method

If the forger performs multiple measurements on the token, the outcomes of previous measurements can be used to optimize subsequent measurement settings via the Ba update rule. For this the ensemble should be split into sub-ensembles. Before the jth measurement, the knowledge of the forger is described by a prior probability distribution $p^{(j-1)}(\theta_b, \phi_b)$ of the bank angles. In detail, before any measurement, the forger can only assume uniform distribution of the bank angles from equation (6), i.e.

$$p^{(0)}(\theta_b, \phi_b) = f_\theta(\theta_b) f_\phi(\phi_b).$$

Now the forger performs the jth measurement on N_j qubits using the angles θ_{f_j}, ϕ_{f_j} and measures n_{f_j} photons. From the result n_{f_j}, the forger can derive the posterior probability distribution of the bank angles from the Ba update rule [31] via

$$\begin{aligned} p^{(j)}(\theta_b, \phi_b) &:= p\left((\theta_b, \phi_b) \middle| n_{f_j}, (\theta_{f_j}, \phi_{f_j})\right) \\ &= \frac{p\left(n_{f_j} \middle| (\theta_b, \phi_b), (\theta_{f_j}, \phi_{f_j})\right) p^{(j-1)}(\theta_b, \phi_b)}{p\left(n_{f_j} \middle| (\theta_{f_j}, \phi_{f_j})\right)}, \end{aligned}$$

where $p(n_{f_j}|(\theta_b, \phi_b), (\theta_{f_j}, \phi_{f_j}))$ is the conditional probability of observing n_{f_j} photons, if one measures in the basis θ_{f_j}, ϕ_{f_j} a token that is prepared with angles θ_b, ϕ_b, which is given by

$$p\left(n_{f_j} \middle| (\theta_b, \phi_b), (\theta_{f_j}, \phi_{f_j})\right) = p_t\left(N_j, n_{f_j}, P_{0f}, P_{1f}, \theta_{f_j}, \phi_{f_j}, \theta_b, \phi_b\right).$$

$p\left(n_{f_j} \middle| (\theta_{f_j}, \phi_{f_j})\right)$ denotes the marginal probability of observing n_{f_j} photons, if one measures with angles θ_{f_j}, ϕ_{f_j}, which is defined as

$$p\left(n_{f_j} \middle| (\theta_{f_j}, \phi_{f_j})\right) = \int_0^\pi d\theta_b \int_{-\pi}^{\pi} d\phi_b\, p^{(j-1)}(\theta_b, \phi_b)\, p_t\left(N_j, n_{f_j}, P_{0f}, P_{1f}, \theta_{f_j}, \phi_{f_j}, \theta_b, \phi_b\right).$$

The information gain through the j-th experiment is given by the utility function $U(n_{f_j}, (\theta_{f_j}, \phi_{f_j}))$, which is the difference of the Shannon entropies between the posterior and the prior probability distributions:

$$U\left(n_{f_j}, (\theta_{f_j}, \phi_{f_j})\right) = \int_0^\pi d\theta_b \int_{-\pi}^{\pi} d\phi_b\, p\left((\theta_b, \phi_b) \middle| n_{f_j}, (\theta_{f_j}, \phi_{f_j})\right) \ln\left(p\left((\theta_b, \phi_b) \middle| n_{f_j}, (\theta_{f_j}, \phi_{f_j})\right)\right)$$

$$-\int_0^{\pi} \mathrm{d}\theta_\mathrm{b} \int_{-\pi}^{\pi} \mathrm{d}\phi_\mathrm{b}\, p^{(j-1)}\left(\theta_\mathrm{b},\phi_\mathrm{b}\right) \ln\left(p^{(j-1)}\left(\theta_\mathrm{b},\phi_\mathrm{b}\right)\right).$$

Averaging over all possible outcomes, n_{f_j} provides a quantity independent of the hitherto unknown measurement result:

$$\overline{U}\left(\theta_{\mathrm{f}_j},\phi_{\mathrm{f}_j}\right) = \sum_{n_{\mathrm{f}_j}=0}^{N_j} U\left(n_{\mathrm{f}_j},\left(\theta_{\mathrm{f}_j},\phi_{\mathrm{f}_j}\right)\right) p\left(n_{\mathrm{f}_j}\middle|\left(\theta_{\mathrm{f}_j},\phi_{\mathrm{f}_j}\right)\right).$$

In order to optimize the jth experiment using the knowledge of the prior probability distribution $p^{(j-1)}(\theta_\mathrm{b},\phi_\mathrm{b})$ of the bank angles, the forger determines the optimal measurement angles θ_{f_j}, ϕ_{f_j} by maximizing $\overline{U}(\theta_{\mathrm{f}_j},\phi_{\mathrm{f}_j})$. These angles can then be used for the jth measurement. In this way, the forger obtains a series of probability distributions $p^{(j)}(\theta_\mathrm{b},\phi_\mathrm{b})$ for the bank angles. The forger gains in each individual measurement the maximum information due to the optimization using the information from the previous results. After performing N_m measurements, the forger takes the angles with the maximum value of the probability distribution $p^{(N_\mathrm{m})}(\theta_\mathrm{b},\phi_\mathrm{b})$ as the optimal guess for the angles of the forged token:

$$\left(\theta_\mathrm{f}^{(\mathrm{Ba})},\phi_\mathrm{f}^{(\mathrm{Ba})}\right) = \mathrm{argmax}\left(p^{(N_\mathrm{m})}\left(\theta_\mathrm{b},\phi_\mathrm{b}\right)\right).$$

We only consider the case of two and three measurements. In both cases, there is no need for optimization of the first measurement due to the freedom of choice of the coordinate system. Before the second measurement, the forger optimizes the angle θ_{f_2} using the first outcome. For three measurements, the angles θ_{f_3} and ϕ_{f_3} are subsequently optimized based on the outcomes of the first two measurements. We denote the average probability that the bank accepts the forged tokens generated by the Ba method using two, or three measurements as $\overline{p}_{\mathrm{f}_2}^{(\mathrm{Ba})}$ and $\overline{p}_{\mathrm{f}_3}^{(\mathrm{Ba})}$, respectively. In our numerical calculations, we perform the search for the optimal measurement angle θ_{f_2} after the first measurement using a brute force search with 2000 values in the interval $[0,\pi)$. In the three measurements scenario, we also determine the optimal measurement angle $\theta_{\mathrm{f}_2}, \theta_{\mathrm{f}_3}, \phi_{\mathrm{f}_3}$ using a similar brute force scan. We present the numerical results in section 3.4.

Due to similar performance of this method when compared to the ML method, we did not perform any experimental verification due to the increased complexity caused by its iterative nature.

3.3. Optimal forged quantum tokens

Now we present the forger's strategy to generate quantum tokens that show the highest possible acceptance rate by the bank after one, two or three measurements. For this, the forger needs to know the parameters $P_{0\mathrm{b}}$, $P_{1\mathrm{b}}$ of the bank setup and the acceptance threshold n_T of the bank. If this knowledge is not available to the forger, the following methods are not applicable. This shows the advantage of keeping the quantum token implementation of the bank setup secret.

3.3.1. One measurement

Firstly, we consider the case that the forger performs one measurement on all of the $N_1 = N$ qubits of the quantum token using the measurement angles θ_{f_1}, ϕ_{f_1} and detecting n_{f_1} photons. Using this result, the forger has to determine the angles θ_f, ϕ_f of the forged token in such a way that the average probability

$$\begin{aligned}\overline{p}_{\mathrm{f}_1}\left(\left(\theta_\mathrm{f},\phi_\mathrm{f}\right)\middle|n_{\mathrm{f}_1}\right) = &\int_0^{\pi} \mathrm{d}\theta_\mathrm{b} \int_{-\pi}^{\pi} \mathrm{d}\phi_\mathrm{b} f_\theta\left(\theta_\mathrm{b}\right) f_\phi\left(\phi_\mathrm{b}\right) p_\mathrm{t}\left(N_1, n_{\mathrm{f}_1}, P_{0\mathrm{f}}, P_{1\mathrm{f}}, 0, 0, \theta_\mathrm{b}, \phi_\mathrm{b}\right)\\ &\times \sum_{n=0}^{n_\mathrm{T}} p_\mathrm{t}\left(N, n, P_{0\mathrm{b}}, P_{1\mathrm{b}}, \theta_\mathrm{f}, \phi_\mathrm{f}, \theta_\mathrm{b}, \phi_\mathrm{b}\right)\end{aligned} \tag{23}$$

of the bank accepting this forged token is maximum. Since the measurement is performed at $\theta_{\mathrm{f}_1} = 0$, the above probability does not depend on ϕ_f, so that the forger may set $\phi_\mathrm{f} = 0$ and we can write $\overline{p}_{\mathrm{f}_1}(\theta_\mathrm{f}|n_{\mathrm{f}_1})$. The optimal value of the angle

$$\theta_\mathrm{f}^{(\mathrm{opt})} = \mathrm{argmax}\left(\overline{p}_{\mathrm{f}_1}\left(\theta_\mathrm{f}|n_{\mathrm{f}_1}\right)\right) \tag{24}$$

for the forged token must be obtained by brute force numerical methods. The average probability for the bank accepting this forged token can be calculated by

$$\overline{p}_{\mathrm{f}_1}^{(\mathrm{opt})} = \sum_{n_{\mathrm{f}_1}=0}^{N_1} \overline{p}_{\mathrm{f}_1}\left(\theta_\mathrm{f}^{(\mathrm{opt})}\middle|n_{\mathrm{f}_1}\right).$$

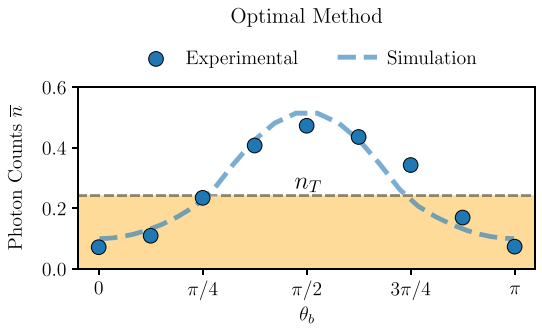

Figure 11. Experimental and simulated normalized counts measured by the bank from a token forged with the optimal method for one measurement axis. As for the other methods, the counts are higher at $\theta_b = \pi/2$, with strong agreement between simulation and experimental data from IBMQ Brisbane. The resulting acceptance probability is $\overline{p}_{f_1}^{(opte)} = 0.4937$.

The optimal method for 1 measurement was experimentally measured with IBMQ Brisbane, as shown in figure 11. As in DIT and ML, the method has better chances of success at the poles than at the equator, also showing a great correspondence to the numerical results. Overall, the resulting acceptance probability is $\overline{p}_{f_1}^{(opte)} = 0.4937$.

In order to numerically derive the average acceptance probability of the forged tokens $\overline{p}_{f_1}^{(opt)}$, we calculate the optimal angle $\theta_f^{(opt)}$ from equation (24) using Newton's method [27], starting with an initial guess obtained by a brute force scan of all θ angles. In detail, we deployed the Newton's method for searching for θ_f such that the derivative of $\overline{p}_{f_1}^{(opt)}$ with respect to θ_f is zero. Towards this goal, we analytically derive the second derivatives with respect to θ_f and obtained for $N = 300$ with Brisbane $\overline{p}_{f_1}^{(opt)} = 0.3258$, which is lower than the experimental value due to the lower acceptance threshold n_T in the numerical calculations. All numerical results are presented and discussed in section 3.4.

3.3.2. Two measurements

Precisely determining both token angles with a single measurement is in general not possible. Thus, splitting the quantum token into two parts is a more robust attack scenario. The first part contains $N_1 \geqslant 1$ qubits and the second part $N_2 = N - N_1 \geqslant 1$ qubits. Due to the freedom of choice of the coordinate system, the forger again performs the first measurement with $\theta_{f_1} = 0$ and $\phi_{f_1} = 0$, detecting n_{f_1} photons. In the second measurement, the forger uses the angles $\theta_{f_2} \notin \{0, \pi\}$ and $\phi_{f_2} = 0$, detecting n_{f_2} photons. Remember, if $\theta_{f_2} \in \{0, \pi\}$, then the second measurement is equivalent to the first one. We want to point out that the forger may choose θ_{f_2} depending on the first measurement result n_{f_1}. Using both measurement results n_{f_1} and n_{f_2}, the forger prepares the angles to θ_f, ϕ_f of the forged token. The average probability that the bank accepts these forged tokens, generated from the two measurement results n_{f_1} and n_{f_2}, is given by

$$\overline{p}_{f_2}\left((\theta_f, \phi_f)\,\middle|N_1, n_{f_1}, \theta_{f_2}, n_{f_2}\right) = \int_0^{\pi} d\theta_b \int_{-\pi}^{\pi} d\phi_b f_\theta(\theta_b) f_\phi(\phi_b) p_t(N_1, n_{f_1}, P_{0f}, P_{1f}, 0, 0, \theta_b, \phi_b) \times p_t(N_2, n_{f_2}, P_{0f}, P_{1f}, \theta_{f_2}, 0, \theta_b, \phi_b) \sum_{n=0}^{n_T} p_t(N, n, P_{0b}, P_{1b}, \theta_f, \phi_f, \theta_b, \phi_b).$$

This scenario has the parameters N_1 and $\theta_{f_2}(n_{f_1})$ that have to be optimized. The optimal angles for the forged token are

$$\left(\theta_f^{(opt)}, \phi_f^{(opt)}\right) = \text{argmax}\left(\overline{p}_{f_2}\left((\theta_f, \phi_f)\,\middle|N_1, n_{f_1}, \theta_{f_2}, n_{f_2}\right)\right), \tag{25}$$

and must be obtained by brute force numerical methods. The average probability for the bank to accept these forged tokens can be calculated by

$$\overline{p}_{f_2}^{(opt)} = \sum_{n_{f_1}=0}^{N_1} \sum_{n_{f_2}=0}^{N_2} \overline{p}_{f_2}\left(\left(\theta_f^{(opt)}, \phi_f^{(opt)}\right)\,\middle|N_1^{(opt)}, n_{f_1}, \theta_{f_2}^{(opt)}, n_{f_2}\right).$$

Instead of optimizing the parameters N_1 and θ_{f_2}, we also consider a simpler scenario where $N_1 = N_2 = \frac{N}{2}$ and $\theta_{f_2} = \frac{\pi}{2}$, so that the measurements are performed in the z- and x-direction. We denote the average acceptance

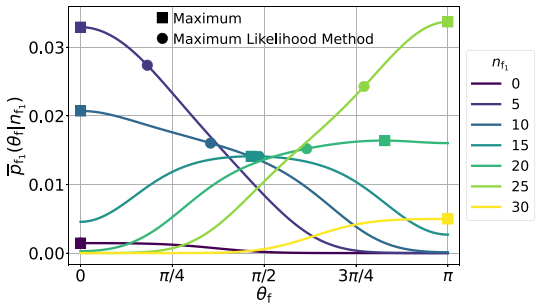

Figure 12. Average acceptance probability $\overline{p}_{f_1}(\theta_f|n_{f_1})$ of the bank accepting the forged tokens as a function of θ_f for different measurement results n_{f_1} of one measurement on the quantum token for IBMQ Brisbane with $N = 30$ qubits. The squares indicate the maximum and the dots show the results from the maximum likelihood method. It is clearly visible that the maximum likelihood method is suboptimal. This can be also deduced from table 3 where we have compared the different methods with corresponding acceptance probabilities.

probability of the forged tokens for this scenario by $\overline{p}_{f_2}^{(\mathrm{fix})}$. In the numerical calculations, we derive the optimal angles $\theta_f^{(\mathrm{opt})}$, $\phi_f^{(\mathrm{opt})}$ from equation (25) using the two dimensional Newton's method starting from an initial guess obtained by a brute force scan. For this, we derive all necessary derivatives analytically. In addition, we optimize N_1 and the optimal measurement angle $\theta_{f_2}(n_{f_1})$ as a function of n_{f_1} by performing a brute force scan using $N_1 = 1, 2, \ldots, 29$ and 2000 points of θ_{f_2} in the interval $[0, \pi)$. We present the optimal acceptance probability of this scenario $\overline{p}_{f_2}^{(\mathrm{opt})}$ together with the corresponding optimal N_1 in table 3 in section 3.4.

3.3.3. Three measurements

Now the forger divides the quantum token into three parts. The first part contains $N_1 \geqslant 1$ qubits, the second part $N_2 \geqslant 1$ and the third part $N_3 = N - N_1 - N_2$ qubits. Again, due to the freedom choice of the coordinate system, the forger performs the first measurement with $\theta_{f_1} = 0$ and $\phi_{f_1} = 0$, detecting n_{f_1} photons. In the second measurement, the forger uses the angles $\theta_{f_2} \notin \{0, \pi\}$ and $\phi_{f_2} = 0$ and detects n_{f_2} photons. In the third measurement, the forger uses the angles θ_{f_3} and ϕ_{f_3}, detecting n_{f_3} photons. Using the three measurement results n_{f_1}, n_{f_2} and n_{f_3}, the forger sets the angles θ_f, ϕ_f of the forged token. The average probability that the bank accepts these forged tokens generated from the measurement results n_{f_1}, n_{f_2} and n_{f_3} is given by

$$\begin{aligned}\overline{p}_{f_3}\left((\theta_f,\phi_f)\,\middle|N_1,n_{f_1},N_2,\theta_{f_2},n_{f_2},\theta_{f_3},\phi_{f_3},n_{f_3}\right) = &\int_0^{\pi} \mathrm{d}\theta_b \int_{-\pi}^{\pi} \mathrm{d}\phi_b f_\theta(\theta_b) f_\phi(\phi_b) p_t(N_1,n_{f_1},P_{0f},P_{1f},0,0,\theta_b,\phi_b)\\ &\times p_t(N_2,n_{f_2},P_{0f},P_{1f},\theta_{f_2},0,\theta_b,\phi_b)\, p_t(N_3,n_{f_3},P_{0f},P_{1f},\theta_{f_3},\phi_{f_3},\theta_b,\phi_b)\\ &\times \sum_{n=0}^{n_T} p_t(N,n,P_{0b},P_{1b},\theta_f,\phi_f,\theta_b,\phi_b)\,.\end{aligned}$$

The measurement scheme in this scenario has the parameters N_1, $N_2(n_{f_1})$, $\theta_{f_2}(n_{f_1})$, $\theta_{f_3}(n_{f_1}, n_{f_2})$ and $\phi_{f_3}(n_{f_1}, n_{f_2})$ that have to be optimized. Since numerically determining the optimal parameters is quite demanding, we only consider the simpler scenario where the token is divided in equal parts with $N_1 = N_2 = N_3 = \frac{N}{3}$ qubits and the angles $\theta_{f_2} = \frac{\pi}{2}$, $\phi_{f_2} = 0$, $\theta_{f_3} = \frac{\pi}{2}$, $\phi_{f_3} = \frac{\pi}{2}$, so that the measurements are performed in the z-, x- and y-direction. We denote the average probability for the bank to accept the forged tokens in this measurement procedure by $\overline{p}_{f_3}^{(\mathrm{fix})}$ and present the results in section 3.4.

3.4. Token security

Now we discuss the numerical results of the different attack methods with regard to the acceptance probability. We first simulate attacks using one measurement on the whole quantum token. In figure 12 we show the average probability for the bank to accept the forged tokens $\overline{p}_{f_1}(\theta_f|n_{f_1})$ from equation (23) for various measurement results n_{f_1} as a function of θ_f derived for the IBMQ Brisbane with $N = 30$ qubits. In addition, we indicate the results of the ML method via dots and the optimal solutions as crosses. One can clearly see that the ML method does not provide optimal results in all cases. If n_{f_1} changes, the qubit is with high probability in a different state, thus the probability distribution is modified as can be seen in figure 12. The probability distribution becomes broader for $n_{f_1} \to N/2 = 15$, since the qubit state is more probably initialized in the equatorial plane, where the density of states is higher.

In table 3, we present all numerical and experimental results for the average acceptance probability of the differently generated forged tokens for $N = 30$ and $N = 300$ qubits in the different IBMQs. One can clearly

Table 3. (top) Average acceptance probability of the bank and forged tokens generated from various attack scenarios for $N = 30$ and $N = 300$ qubits in a quantum token on the five IBMQs with $P_{0b} = P_{0f}$ and $P_{1b} = P_{1f}$. For $N = 300$, the stars indicate the attack scenarios that were not simulated due to the very high computational cost. Note that the numerical brute force methods with $\overline{p}_{f_1}^{(opt)}$, $\overline{p}_{f_2}^{(opt)}$ and $\overline{p}_{f_3}^{(fix)}$ achieve always larger acceptance values than the state estimation methods with biggest advantages for three measurements. The values are also visualized in figure 13. (bottom) For direct comparison we have repeated the experimental values for the Brisbane IBMQ with $N = 300$.

IBMQ	N	n_T	$\overline{p}_b$	$\overline{p}_{f_0}$	$\overline{p}_{f_1}^{(ML)}$	$\overline{p}_{f_1}^{(opt)}$	$\overline{p}_{f_2}^{(Ba)}$	$\overline{p}_{f_2}^{(ML)}$	$\overline{p}_{f_2}^{(fix)}$	N_1	$\overline{p}_{f_2}^{(opt)}$	$\overline{p}_{f_3}^{(DIT)}$	$\overline{p}_{f_3}^{(Ba)}$	$\overline{p}_{f_3}^{(ML)}$	$\overline{p}_{f_3}^{(fix)}$
Sherb.	30	0	~ 1	0.032 26	0.1393	0.1409	0.2992	0.2969	0.3196	15	0.3196	0.1094	0.4655	0.3474	0.4832
Kyiv	30	0	~ 1	0.033 70	0.1383	0.1408	0.2923	0.2879	0.3094	15	0.3099	0.1091	0.4496	0.3423	0.4651
Osaka	30	5	0.999 81	0.1836	0.4169	0.4726	0.6664	0.6797	0.7372	15	0.7372	0.3847	0.9291	0.8592	0.9384
Brisb.	30	10	0.999 91	0.3045	0.5450	0.6475	0.7552	0.7693	0.8537	15	0.8537	0.5183	0.9731	0.9356	0.9776
Kyoto	30	14	0.999 86	0.5128	0.7077	0.8367	0.8260	0.8454	0.9112	14	0.9192	0.6707	0.9546	0.9299	0.9583
Sherb.	300	0	~ 1	0.003 322	0.042 68	0.044 03	0.2780	0.2299	0.2815	*	*	0.042 83	*	0.3357	0.5589
Kyiv	300	0	~ 1	0.003 471	0.041 57	0.042 73	0.2594	0.2165	0.2630	*	*	0.037 75	*	0.3139	0.5299
Osaka	300	20	0.999 82	0.045 86	0.2094	0.2307	0.5863	0.5945	0.6326	*	*	0.1962	*	0.9473	0.9954
Brisb.	300	50	0.999 86	0.082 71	0.2835	0.3258	0.6340	0.6404	0.7104	*	*	0.2770	*	0.9803	0.9990
Kyoto	300	83	0.999 87	0.1535	0.3869	0.4591	0.6792	0.6905	0.7812	*	*	0.3757	*	0.9758	0.9982

IBMQ	N	$n_T^{(e)}$	$\overline{p}_{f_1}^{(MLe)}$	$\overline{p}_{f_1}^{(opte)}$	$\overline{p}_{f_2}^{(MLe)}$	$\overline{p}_{f_3}^{(DITe)}$	$\overline{p}_{f_3}^{(MLe)}$
Brisbane	300	73	0.4698	0.4937	0.6688	0.3769	0.9847

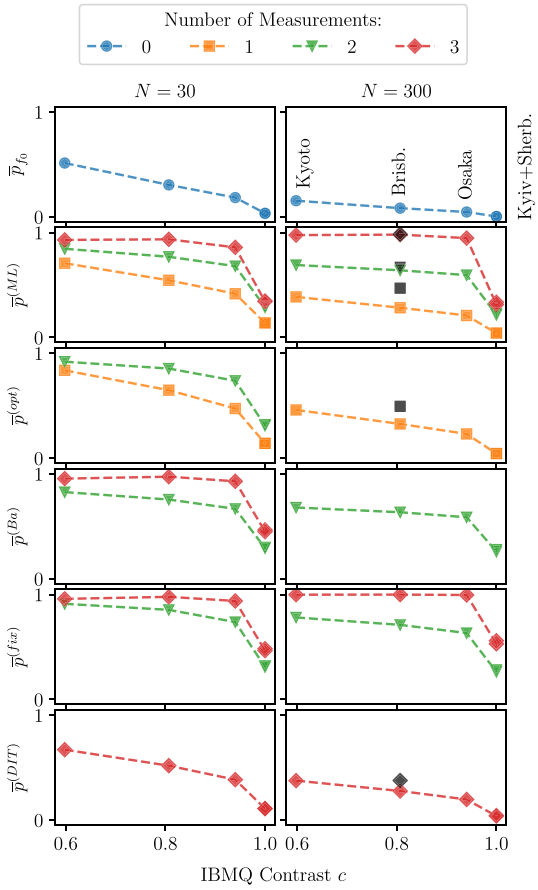

Figure 13. Acceptance probabilities from table 3 for the quantum token as implemented on the five different IBMQ platforms as a function of contrast as defined in equation (1). Black symbols denote experimental verification with the corresponding number of measurements (see legend). It is obvious that with better contrast more forged tokens are rejected by the bank. It can be clearly seen that three measurements are always advantageous when preparing a forged token. With better contrast this advantage is reduced.

see, that the acceptance probability for all cloning methods decreases, if one uses $N = 300$ instead of $N = 30$ qubits. Here, we observe a higher security level for an increase of qubits in the token for all methods. However, for a very high number of qubits the ensemble will behave classically and the quantum projection noise will vanish in the shot noise, so that the security will decrease again. In addition, the results in table 3 show that the optimization of the parameters in the two measurement case $\overline{p}_{f_2}^{(opt)}$ do not provide a significant improvement of the acceptance probability compared to the simple case $\overline{p}_{f_2}^{(fix)}$.

As one can clearly see in table 3 and also in figure 13, the ability to perform measurements on sub-ensembles of the quantum token provides significantly better acceptance probabilities for the forged tokens. The direct inversion method provides the worst results even using three measurements. The Ba method provides significantly better results than the ML method for three measurements. For two measurements, both methods show almost similar performance. For the one-, two- and three measurement case, the optimal scenario introduced in this work always outperforms the other methods presented. Nevertheless, as can be seen in table 3, the acceptance probability $\overline{p}_b$ of the token generated by the bank is always higher than for the forged tokens $\overline{p}_f$ for the different methods. We also summarized the experimental acceptance probabilities for the Brisbane IBMQ in the table. In the comparison it might be striking that the experimental acceptance probabilities for the single measurements deviate from our simulations for the same platform. This is caused by a different adjustment of the $n_T^{(e)}$ in order to achieve the same probability $\overline{p}_b > 0.9998$ for the bank accepting its own generated tokens. This was necessary because in the real experiments additional errors such as gate errors and decoherence effects needed to be taken into account which were not present in our simulations.

Observe that a small improvement of the quantum hardware, i.e. increase of contrast c, can induce a great improvement of the security, as can be seen by comparing Osaka with Kyiv and Sherbrooke. The security of our protocol thus will benefit from the evolution of the quantum hardware.

Table 4. Acceptance probability for forged coins on IBMQ Brisbane containing 1, 9, 100, 1024, 10 000 quantum tokens, each one with $N = 30$ qubits. Here, the acceptance probability of the bank coins with more than 1 token is always bigger than 0.999 99, where we take 100 digits of precision.

IBMQ	M	n_{cT}	$\overline{p}_{Mf_0}$	$\overline{p}^{(opt)}_{Mf_1}$	$\overline{p}^{(opt)}_{Mf_2}$	$\overline{p}^{(fix)}_{Mf_3}$
	1	1	0.3045	0.6475	0.8537	0.9776
	9	8	$4.851{\cdot}10^{-4}$	0.1180	0.6123	0.9837
	16	15	$2.051{\cdot}10^{-7}$	$9.270{\cdot}10^{-3}$	0.2978	0.9511
	25	24	$7.143{\cdot}10^{-12}$	$2.790{\cdot}10^{-4}$	0.1013	0.8927
Brisbane	64	62	$9.496{\cdot}10^{-30}$	$5.260{\cdot}10^{-10}$	$2.857{\cdot}10^{-3}$	0.8269
	100	98	$5.951{\cdot}10^{-48}$	$2.025{\cdot}10^{-16}$	$2.208{\cdot}10^{-5}$	0.6113
	1024	1021	$3.323{\cdot}10^{-520}$	$1.483{\cdot}10^{-186}$	$4.143{\cdot}10^{-65}$	$2.058{\cdot}10^{-7}$
	10 000	9993	$4.794{\cdot}10^{-5138}$	$7.021{\cdot}10^{-1866}$	$9.746{\cdot}10^{-669}$	$2.771{\cdot}10^{-86}$

4. Quantum coin consisting of quantum tokens

As exemplified with the experimental results from Brisbane an increase in $n_T^{(e)}$ was necessary to keep $\overline{p}_b > 0.9998$ valid. This is carried through at the cost of making it easier for the forger to generate forged tokens. In order to achieve a predefined security of the protocol we assume that M quantum tokens prepared with individual angles are combined into a quantum coin. There are two conditions for the coin, which should be fulfilled:

1. The probability for the bank rejecting their own generated coins is less than a given limit $\varepsilon_{cb} > 0$.
2. The probability for the bank to accept forged coins is less than a given limit $\varepsilon_{cf} > 0$.

The usage of several quantum tokens within a coin allows the bank to generate coins that fulfill both conditions for any given limits $\varepsilon_{cb} > 0$ and $\varepsilon_{cf} > 0$, if the average acceptance probability of the bank generated tokens p_b is bigger than the acceptance probability of forged tokens p_f, which is fulfilled for all cases and attack scenarios, as can be seen in table 3.

The bank validates a coin, if at least n_{cT} tokens within the coin are accepted. The acceptance threshold n_{cT} is determined from the condition 1:

$$\sum_{n=n_{cT}}^{M} p_b^n \left(1-p_b\right)^{M-n} < \varepsilon_{cb}. \tag{26}$$

Here we use the fact that the probability for the bank accepting n quantum tokens within a coin is given by a binomial distribution with probability p_b. Furthermore, if the average forged token acceptance probability p_f is given, the bank demands to have an acceptance rate of forged coins being less than ε_{cf}:

$$\sum_{n=0}^{n_{cT}-1} p_f^n \left(1-p_f\right)^{M-n} < \varepsilon_{cf}. \tag{27}$$

In appendix C, we proof that for any $\varepsilon_{cb} > 0$ and $\varepsilon_{cf} > 0$ a number M of quantum tokens in the coin can be found such that conditions 1 and 2 are fulfilled. Practically, one can perform the following iterative procedure: One starts with a given M and derives the corresponding n_{cT} from equation (26). Then one checks if condition (27) is fulfilled. If not, one start the procedure again with $M + 1$.

Finally, we simulate a quantum coin composed of a variable number M of quantum tokens. For each number M, we calculate the acceptance threshold of the coin n_{cT} using equation (26) in such a way that the acceptance probability of the bank generated coins is always bigger than 0.999 99 or in other words, $\varepsilon_{cb} < 0.000\,01$. Then, we consider for zero, one, two and three measurements the optimal forged token scenario from table 3 and derive the average acceptance probability of the corresponding forged coin using equation (26). Note, we perform this calculations with 100 digits numerical precision. We present the obtained results for Brisbane in table 4 and visualize the values in figure 14. In table 5 of the appendix, we show the results for all IBMQ platforms. One can clearly see that for the coin any level of security can be obtained by just increasing the number of quantum tokens.

5. Discussion and outlook

We have presented an ensemble-based quantum token protocol with quantum coins consisting of individual quantum tokens, each one containing an ensemble of qubits prepared in the same state. We have shown

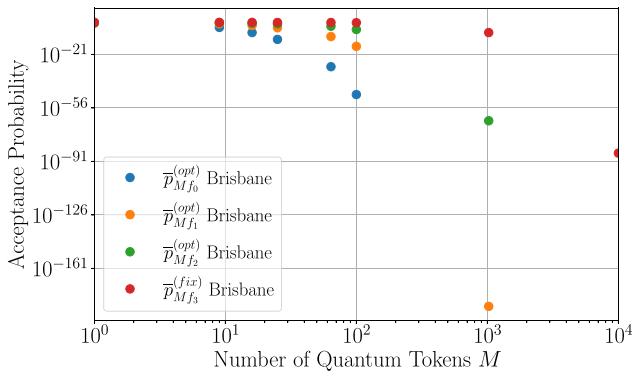

Figure 14. Acceptance probabilities from table 4 for Brisbane are shown for the different hack scenarios as a function of the number of quantum tokens M.

attack scenarios, which describe how to measure the state of the quantum tokens with quantum state tomography, Ba method and the ML method using one, two or three measurements. We have shown the optimal scheme to generate forged tokens with highest acceptance probability of the bank. Remarkably, these schemes provides significantly better results than the state-of the art quantum tomography methods. This is due to the fact that optimal state estimation has a different objective than trying to trick the bank into accepting a forged token when the attacker has knowledge about the setup parameters of the bank. Finally, we have shown that the coin becomes arbitrary safe if the number of quantum tokens within the coin is increased.

The presented protocol is hardware agnostic and can be applied to any qubit for which ensemble initialization, manipulation and readout is feasible. The ensemble-based quantum token protocol must be fortified against fake tokens. As an example, a forger might generate a dark token that always delivers zero photons. As the bank would normally rotate all states back into the dark state, such a dark token would be always accepted. As a countermeasure the bank should arbitrarily select tokens which are measured in the bright state, such that a forger cannot guess the dark and bright tokens.

Even though the IBMQ presented itself as an excellent platform for a hardware agnostic benchmark of the quantum coin protocol and testing of the attack scenarios, superconducting architectures have severe limitations regarding their applications for a quantum coin device. Foremost, superconducting qubits can hardly be made mobile, due to low temperature constrains. Optimal platforms for implementing the presented ensemble-based quantum token protocol have to further rely on long qubit storage times. Therefore, nuclear spin qubits are preferable as storage qubits. Hybrid quantum systems such as NV-color centers coupled to nuclear spin qubits or cold Alkali Atoms with long lived hyperfine splitted ground states would provide the ideal platform for an implementation of a real-world quantum token. The diamond platform can be used at room temperature and has reached T_2 lifetimes of 90 s with Floquet prethermalized nuclear spins [32]. It is additionally attractive due to the possibility of miniaturizing an entire diamond quantum coin on a single diamond substrate using nanofabrication techniques that allow to use diamond nano-pillars with integrated NV-centers [33] as a quantum token. This technique has the additional benefit that performing measurements of sub-ensembles of the quantum token may be unfeasible, thus greatly limiting the attacker's ability to generate forged tokens. Optimization of fabrication methods for quantum tokens based on color centers in diamond [34], as well as qubit control techniques for fast state transfer between solid state spins in these systems [35] could provide a robust room temperature platform for implementing ensemble-based quantum tokens.

Data availability statement

The data that support the findings of this study are openly available at the following URL/DOI: https://github.com/bauerhenne/diqtok-forge.

Acknowledgments

This work was supported by the German Federal Ministry of Education and Research (BMBF) within the initiative 'Grand Challenge of Quantumcommunication' under the Project '*DIamant-basiert QuantenTOKen*' (DIQTOK—nº 16KISQ034) and the German Science foundation (DFG, Grant 410866378). Computations were performed on the IT Servicecenter (ITS) University of Kassel and on the computing cluster FUCHS

University of Frankfurt. We thank Janis Nötzel from the TUM School of Computation, Information and Technology from Munich, Manika Bhardwaj and Moritz Göb for fruitful discussions.

Appendix A. Safety proof of ensemble-based quantum token protocol

We define the hypothesis H_0 and H_1 as follows:

H_0: Bank prepared the coin.
H_1: Forger prepared the coin.

We have the following errors $\varepsilon_{\mathrm{cb}}, \varepsilon_{\mathrm{cf}} \in [0,1]$ of first and second kind:

Error of first kind $\varepsilon_{\mathrm{cb}}$ Bank declines coin even thought it was prepared by the bank.

Error of second kind $\varepsilon_{\mathrm{cf}}$ Bank accepts coin even thought it was prepared by the forger.

We have M quantum tokens in the coin. If H_0 is valid, then each token is represented by the random variable $X_j \in \{0,1\}$, which is 1, if the token is accepted by the bank, which has the probability p_{b}, and 0 otherwise. If H_1 is valid, then each token is represented by the random variable $Y_j \in \{0,1\}$, which is 1, if the token is accepted by the bank, which has the probability p_{f}, and 0 otherwise. We define

$$\langle X\rangle := \frac{1}{M}\sum_{j=1}^{M} X_j,$$
$$\langle Y\rangle := \frac{1}{M}\sum_{j=1}^{M} Y_j.$$

The set of quantum tokens have to fulfill the following two conditions:

$$\langle X\rangle \geqslant \frac{n_{\mathrm{cT}}}{M},$$
$$\langle Y\rangle < \frac{n_{\mathrm{cT}}}{M}.$$

The number n_{cT}, which corresponds to the accept criteria, is well chosen, if the following two conditions hold:

$$p\left(\langle X\rangle < \frac{n_{\mathrm{cT}}}{M}\right) \leqslant \varepsilon_{\mathrm{cb}},$$
$$p\left(\langle Y\rangle \geqslant \frac{n_{\mathrm{cT}}}{M}\right) \leqslant \varepsilon_{\mathrm{cf}} \iff p\left(\langle Y\rangle < \frac{n_{\mathrm{cT}}}{M}\right) \geqslant 1-\varepsilon_{\mathrm{cf}}.$$

The random variables X_j, Y_j obey a Bernoulli distribution with mean $p_{\mathrm{b}}, p_{\mathrm{f}}$ and standard deviation $\sqrt{p_{\mathrm{b}}(1-p_{\mathrm{b}})}$, $\sqrt{p_{\mathrm{f}}(1-p_{\mathrm{f}})}$, respectively. The central limit theorem [30] yields that

$$\lim_{M\to\infty} p\left(\sqrt{M}\frac{\langle X\rangle - p_{\mathrm{b}}}{\sqrt{p_{\mathrm{b}}(1-p_{\mathrm{b}})}} \leqslant z\right) = \Phi(z),$$
$$\lim_{M\to\infty} p\left(\sqrt{M}\frac{\langle Y\rangle - p_{\mathrm{f}}}{\sqrt{p_{\mathrm{f}}(1-p_{\mathrm{f}})}} \leqslant z\right) = \Phi(z),$$

where the $\Phi(z)$ is the cumulative distribution function of the normal distribution and hence given as

$$\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{x^2}{2}}\,\mathrm{d}x = \frac{1}{2}\left(1+\mathrm{erf}\left(\frac{z}{\sqrt{2}}\right)\right).$$

We conclude that for each $\varepsilon > 0$ there exists a $n_{\mathrm{b}} \in \mathbb{N}$ so that for all $M \geqslant n_{\mathrm{b}}$:

$$p\left(\sqrt{M}\frac{\langle X\rangle - p_\mathrm{b}}{\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}} \leqslant z\right) \in \left(\Phi\left(z\right)-\varepsilon, \Phi\left(z\right)+\varepsilon\right),$$
$$p\left(\sqrt{M}\frac{\langle Y\rangle - p_\mathrm{f}}{\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}} \leqslant z\right) \in \left(\Phi\left(z\right)-\varepsilon, \Phi\left(z\right)+\varepsilon\right).$$

Using the error bounds $\varepsilon_\mathrm{cb}, \varepsilon_\mathrm{cf}$ for the errors of first and second kind, we obtain finally

$$\begin{aligned}\varepsilon_\mathrm{cb} \geqslant & \Phi\left(z_X\right)+\varepsilon \geqslant p\left(\sqrt{M}\frac{\langle X\rangle - p_\mathrm{b}}{\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}} < \underbrace{\sqrt{M}\frac{\frac{n_\mathrm{cT}}{M} - p_\mathrm{b}}{\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}}}_{=:z_X}\right) \\ = & p\left(\langle X\rangle < \frac{n_\mathrm{cT}}{M}\right)\end{aligned}$$

and

$$\begin{aligned}1-\varepsilon_\mathrm{cf} \leqslant & \Phi\left(z_Y\right)-\varepsilon \leqslant p\left(\sqrt{M}\frac{\langle Y\rangle - p_\mathrm{f}}{\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}} < \underbrace{\sqrt{M}\frac{\frac{n_\mathrm{cT}}{M} - p_\mathrm{f}}{\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}}}_{=:z_Y}\right) \\ = & p\left(\langle Y\rangle < \frac{n_\mathrm{cT}}{M}\right).\end{aligned}$$

It follows

$$\begin{aligned}\Phi\left(z_X\right) \leqslant & \varepsilon_\mathrm{cb}-\varepsilon, \\ \Phi\left(z_Y\right) \geqslant & 1-\varepsilon_\mathrm{cf}+\varepsilon,\end{aligned}$$

which is equivalent to

$$\begin{aligned}\sqrt{M}\frac{\frac{n_\mathrm{cT}}{M} - p_\mathrm{b}}{\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}} \leqslant & \Phi^{-1}\left(\varepsilon_\mathrm{cb}-\varepsilon\right), \\ \sqrt{M}\frac{\frac{n_\mathrm{cT}}{M} - p_\mathrm{f}}{\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}} \geqslant & \Phi^{-1}\left(1-\varepsilon_\mathrm{cf}+\varepsilon\right),\end{aligned}$$

since $\Phi(z)$ is a monotonously increasing function. We obtain further

$$n_\mathrm{cT} \leqslant \Phi^{-1}\left(\varepsilon_\mathrm{cb}-\varepsilon\right)\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}\sqrt{M}+p_\mathrm{b}M, \tag{A1}$$
$$n_\mathrm{cT} \geqslant \underbrace{\Phi^{-1}\left(1-\varepsilon_\mathrm{cf}+\varepsilon\right)}_{=-\Phi^{-1}\left(\varepsilon_\mathrm{cf}-\varepsilon\right)}\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}\sqrt{M}+p_\mathrm{f}M. \tag{A2}$$

In summary, the above equations yield the interval for n_cT given by the boundaries above. Thus, n_cT is well chosen, if there exists a natural number within this interval. This is always the case, if the length of this interval is larger or equal to 1. Therefore, we obtain the following sufficient condition for n_cT to be well chosen:

$$1 \leqslant \Phi^{-1}\left(\varepsilon_\mathrm{cb}-\varepsilon\right)\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}\sqrt{M}+p_\mathrm{b}M++\Phi^{-1}\left(\varepsilon_\mathrm{cf}-\varepsilon\right)\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}\sqrt{M}-p_\mathrm{f}M.$$

This tranforms to

$$\underbrace{-\Phi^{-1}\left(\varepsilon_\mathrm{cb}-\varepsilon\right)\sqrt{p_\mathrm{b}\left(1-p_\mathrm{b}\right)}-\Phi^{-1}\left(\varepsilon_\mathrm{cf}-\varepsilon\right)\sqrt{p_\mathrm{f}\left(1-p_\mathrm{f}\right)}}_{=:d} \leqslant \underbrace{\left(p_\mathrm{b}-p_\mathrm{f}\right)}_{=:\Delta p}\sqrt{M}-\frac{1}{\sqrt{M}}.$$

The left hand side is bigger than zero due to $\varepsilon_\mathrm{cb}-\varepsilon, \varepsilon_\mathrm{cf}-\varepsilon \leqslant \frac{1}{2}$. If we have $p_\mathrm{b} > p_\mathrm{f}$, then the right hand side tends to ∞ with $M \to \infty$. This means, if M is large enough, there will always exist a well chosen n_b. We obtain further

$$
\begin{aligned}
& 0 \leqslant \Delta p \sqrt{M} - \frac{1}{\sqrt{M}} - d \\
\Leftrightarrow \quad & 0 \leqslant M - \frac{d}{\Delta p}\sqrt{M} - \frac{1}{\Delta p} + \underbrace{\frac{d^2}{4\Delta p^2} - \frac{d^2}{4\Delta p^2}}_{=0}
\end{aligned}
$$

and finally

$$
\begin{aligned}
\Leftrightarrow \quad & \frac{4\Delta p + d^2}{4\Delta p^2} \leqslant \left(\sqrt{M} - \frac{d}{2\Delta p}\right)^2 \\
\Leftrightarrow \quad & \frac{\sqrt{4\Delta p + d^2}}{2\Delta p} \leqslant \left|\sqrt{M} - \frac{d}{2\Delta p}\right|.
\end{aligned}
$$

If we have $\sqrt{M} - \frac{d}{2\Delta p} < 0$, then the following is fulfilled

$$
\sqrt{M} \leqslant \frac{d - \sqrt{4\Delta p + d^2}}{2\Delta p} < 0.
$$

This means that we have in this case no solution for M, since $\sqrt{M} \geqslant 0$. If we have in the other case $\sqrt{M} - \frac{d}{2\Delta p} \geqslant 0$, then it follows

$$
\sqrt{M} \geqslant \frac{d + \sqrt{4\Delta p + d^2}}{2\Delta p}.
$$

If the condition above is valid, then automatically $\sqrt{M} - \frac{d}{2\Delta p} \geqslant 0$ is fulfilled. Consequently, the only solution for M is given by

$$
M \geqslant \max\left\{\left(\frac{d + \sqrt{4\Delta p + d^2}}{2\Delta p}\right)^2, n_\mathrm{b}\right\}.
$$

After determining of M, one obtains n_cT from equations (A1) and (A2).

Appendix B. Coin acceptance probabilities for all IBMQ platforms

Table 5. Acceptance probabilities for forged coins for all IBMQ platforms containing 1, 9, 100, 1024, 10 000 quantum tokens, each one with $N = 30$ qubits. Here, the acceptance probability of the bank coins with more than 1 token is always bigger than 0.999 99, where we take 100 digits of precision.

IBMQ	M	n_{cT}	$\bar{p}_{Mf_0}$	$\bar{p}^{(opt)}_{Mf_1}$	$\bar{p}^{(opt)}_{Mf_2}$	$\bar{p}^{(fix)}_{Mf_3}$
Sherbrooke	1	1	0.032 26	0.1409	0.3196	0.4832
	9	9	$3.784\cdot10^{-14}$	$2.189\cdot10^{-8}$	$3.479\cdot10^{-5}$	0.001 436
	16	16	$1.376\cdot10^{-24}$	$2.413\cdot10^{-14}$	$1.185\cdot10^{-8}$	$8.831\cdot10^{-6}$
	25	25	$5.207\cdot10^{-38}$	$5.282\cdot10^{-22}$	$4.123\cdot10^{-13}$	$1.268\cdot10^{-8}$
	64	64	$3.585\cdot10^{-96}$	$3.391\cdot10^{-55}$	$1.972\cdot10^{-32}$	$6.083\cdot10^{-21}$
	100	100	$7.353\cdot10^{-150}$	$7.782\cdot10^{-86}$	$2.889\cdot10^{-50}$	$2.586\cdot10^{-32}$
	1024	1024	$7.453\cdot10^{-1528}$	$3.054\cdot10^{-872}$	$5.216\cdot10^{-508}$	$3.515\cdot10^{-324}$
	10 000	10 000	$4.402\cdot10^{-14914}$	$1.288\cdot10^{-8511}$	$1.169\cdot10^{-4954}$	$1.859\cdot10^{-3159}$
Kyiv	1	1	$3.370\cdot10^{-2}$	0.1408	0.3099	0.4651
	9	9	$5.606\cdot10^{-14}$	$2.175\cdot10^{-8}$	$2.636\cdot10^{-5}$	0.001 018
	16	16	$2.767\cdot10^{-24}$	$2.386\cdot10^{-14}$	$7.237\cdot10^{-9}$	$4.794\cdot10^{-6}$
	25	25	$1.551\cdot10^{-37}$	$5.189\cdot10^{-22}$	$1.908\cdot10^{-13}$	$4.883\cdot10^{-9}$
	64	64	$5.866\cdot10^{-95}$	$3.240\cdot10^{-55}$	$2.743\cdot10^{-33}$	$5.284\cdot10^{-22}$
	100	100	$5.794\cdot10^{-148}$	$7.249\cdot10^{-86}$	$1.325\cdot10^{-51}$	$5.683\cdot10^{-34}$
	1024	1024	$1.963\cdot10^{-484}$	$1.476\cdot10^{-872}$	$1.025\cdot10^{-521}$	$3.694\cdot10^{-341}$
	10 000	10 000	$1.991\cdot10^{-14724}$	$1.063\cdot10^{-8514}$	$1.643\cdot10^{-5088}$	$2.907\cdot10^{-3325}$
Osaka	1	1	0.1836	0.4726	0.7372	0.9384
	9	8	$9.724\cdot10^{-6}$	0.012 99	0.2706	0.8976
	16	15	$1.203\cdot10^{-10}$	$1.168\cdot10^{-4}$	$5.101\cdot10^{-2}$	0.7415
	25	23	$2.389\cdot10^{-15}$	$2.932\cdot10^{-6}$	$2.351\cdot10^{-2}$	0.8026
	64	62	$3.101\cdot10^{-43}$	$3.800\cdot10^{-18}$	$9.389\cdot10^{-7}$	0.2374
	100	98	$2.398\cdot10^{-69}$	$1.767\cdot10^{-29}$	$3.818\cdot10^{-11}$	0.050 07
	1024	1020	$2.861\cdot10^{-741}$	$3.405\cdot10^{-323}$	$1.900\cdot10^{-127}$	$4.773\cdot10^{-23}$
	10 000	9990	$4.420\cdot10^{-7322}$	$7.117\cdot10^{-3222}$	$6.504\cdot10^{-1296}$	$3.140\cdot10^{-255}$
Brisbane	1	1	0.3045	0.6475	0.8537	0.9776
	9	8	$4.851\cdot10^{-4}$	0.1180	0.6123	0.9837
	16	15	$2.051\cdot10^{-7}$	$9.270\cdot10^{-3}$	0.2978	0.9511
	25	24	$7.143\cdot10^{-12}$	$2.790\cdot10^{-4}$	0.1013	0.8927
	64	62	$9.496\cdot10^{-30}$	$5.260\cdot10^{-10}$	$2.857\cdot10^{-3}$	0.8269
	100	98	$5.951\cdot10^{-48}$	$2.025\cdot10^{-16}$	$2.208\cdot10^{-5}$	0.6113
	1024	1021	$3.323\cdot10^{-520}$	$1.483\cdot10^{-186}$	$4.143\cdot10^{-65}$	$2.058\cdot10^{-7}$
	10 000	9993	$4.794\cdot10^{-5138}$	$7.021\cdot10^{-1866}$	$9.746\cdot10^{-669}$	$2.771\cdot10^{-86}$
Kyoto	1	1	0.5128	0.8367	0.9192	0.9583
	9	8	0.023 42	0.5540	0.8391	0.9485
	16	15	$3.704\cdot10^{-4}$	0.2378	0.6251	0.8580
	25	24	$1.388\cdot10^{-6}$	$6.817\cdot10^{-2}$	0.3891	0.7198
	64	62	$5.143\cdot10^{-16}$	$1.000\cdot10^{-3}$	0.1011	0.4978
	100	98	$4.510\cdot10^{-26}$	$3.778\cdot10^{-6}$	0.010 53	0.2081
	1024	1020	$3.614\cdot10^{-287}$	$3.470\cdot10^{-72}$	$9.670\cdot10^{-32}$	$2.044\cdot10^{-14}$
	10 000	9991	$5.237\cdot10^{-2871}$	$5.651\cdot10^{-751}$	$1.095\cdot10^{-345}$	$1.623\cdot10^{-169}$

Appendix C. Glossary of main variables

Table 6. Glossary of the main variables in the text.

Variable	Physical quantity
θ	Polar angle on the Bloch sphere
ϕ	Azimuthal angle on the Bloch sphere
θ_b, ϕ_b	Angles with which the bank prepares and measures the token
θ_{f_j}, ϕ_{f_j}	Angles used by the attacker to measure the bank token in the jth measurement
θ_f, ϕ_f	Angles forged by the attacker
n_{f_j}	Number of photons measured in the jth measurement
N_j	Number of qubits used in the jth measurement
N	Total number of qubits in the quantum token
P_0	Probability to detect a photon if qubit is in state $\|0\rangle$
P_1	Probability to detect a photon if qubit is in state $\|1\rangle$
σ_N	Total uncertainty of photon counts
$\overline{n}$	Averaged normalized counts of photons
p_q	Probability that a qubit emits a photon
p_t	Probability that a quantum token emits a given number of photons
$\overline{p}_b$	Average probability of acceptance for bank token
$\overline{p}_{f_j}$	Average probability of acceptance for forged token generated from j-measurements
ε_b	Limit for the bank declining own token
ε_{cb}	Limit for bank declines own coins
ε_{cf}	Limit for bank accepting forged coins
n_T	Photon count threshold for accepting the quantum token
n_{cT}	Minimum number of accepted token for accepting coin
M	Number of quantum tokens in the coin
p_b	Self-acceptance probability of the bank tokens
p_f	Acceptance probability of forged tokens
$\mathcal{L}$	Likelihood function

ORCID iDs

Bernd Bauerhenne 0000-0002-3397-2290
Lucas Tsunaki 0009-0003-3534-6300
Jan Thieme 0009-0005-8849-1944
Boris Naydenov 0000-0002-5215-3880
Kilian Singer 0000-0001-9726-0367

References

[1] Wiesner S 1983 *ACM Sigact News* **15** 78
[2] Gavinsky D 2011 *2012 IEEE 27th Conf. on Computational Complexity* (available at: https://api.semanticscholar.org/CorpusID:11673644) p 42
[3] Molina A, Vidick T and Watrous J 2013 *Theory of Quantum Computation, Communication and Cryptography* ed K Iwama, Y Kawano and M Murao (Springer) pp 45–64
[4] Pastawski F, Yao N Y, Jiang L, Lukin M D and Cirac J I 2012 *Proc. Natl Acad. Sci.* **109** 16079
[5] Georgiou M and Kerenidis I 2015 *10th Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015)* (Leibniz Int. Proc. in Informatics (LIPIcs)) vol 44, ed S Beigi and R König (Schloss Dagstuhl – Leibniz-Zentrum für Informatik) pp 92–110
[6] Moulick S R and Panigrahi P K 2016 *Quantum Inf. Process.* **15** 2475
[7] Amiri R and Arrazola J M 2017 *Phys. Rev. A* **95** 062334
[8] Bozzio M, Diamanti E and Grosshans F 2019 *Phys. Rev. A* **99** 022336
[9] Kumar N 2019 *Cryptography* **3** 26
[10] Horodecki K and Stankiewicz M 2020 *New J. Phys.* **22** 023007
[11] Kent A, Lowndes D, Pitalúa-García D and Rarity J 2022 *npj Quantum Inf.* **8** 28
[12] Singer K, Popov C and Naydenov B 2022 *Verfahren zum Erstellen eines Quanten-Datentokens* Germany DE 10 2022 107 528 A1 2023.10.05
[13] Tsunaki L, Bauerhenne B, Xibraku M, Garcia M E, Singer K and Naydenov B 2024 *Quantum Sci. Technol.* **10** 045042
[14] Itano W M, Bergquist J C, Bollinger J J, Gilligan J M, Heinzen D J, Moore F L, Raizen M G and Wineland D J 1993 *Phys. Rev. A* **47** 3554
[15] Schmied R 2016 *J. Mod. Opt.* **63** 1744
[16] Paris M and Rehacek J 2016 *Quantum State Estimation* (Springer)
[17] Hannemann T, Reiss D, Balzer C, Neuhauser W, Toschek P E and Wunderlich C 2002 *Phys. Rev. A* **65** 050303
[18] Bauerhenne B 2024 Diqtok forge (available at: https://github.com/bauerhenne/diqtok-forge)
[19] Kandala A, Wei K X, Srinivasan S, Magesan E, Carnevale S, Keefe G, Klaus D, Dial O and McKay D 2021 *Phys. Rev. Lett.* **127** 130501

[20] Bravyi S, Cross A W, Gambetta J M, Maslov D, Rall P and Yoder T J 2024 *Nature* **627** 778
[21] Glick J R, Gujarati T P, Corcoles A D, Kim Y, Kandala A, Gambetta J M and Temme K 2024 *Nat. Phys.* **20** 479
[22] Javadi-Abhari A, Treinish M, Krsulich K, Wood C J, Lishman J, Gacon J, Martiel S, Nation P D, Bishop L S, Cross A W, Johnson B R and Gambetta J M 2024 arXiv:2405.08810 [quant-ph]
[23] Tsunaki L 2024 Quantum token (available at: https://github.com/lucas-tsunaki/quantum-token)
[24] Bagan E, Monras A and Muñoz Tapia R 2005 *Phys. Rev. A* **71** 062318
[25] Gerlach W and Stern O 1922 *Z. Phys.* **9** 353
[26] Rabi I I, Ramsey N and Schwinger J 1954 *Rev. Mod. Phys.* **26** 167
[27] Schwarz H R and Köckler N 2011 *Numerische Mathematik* 8th edn (Teubner)
[28] Gruber A, Dräbenstedt A, Tietz C, Fleury L, Wrachtrup J and von Borczyskowski C 1997 *Science* **276** 2012
[29] Jelezko F, Gaebel T, Popa I, Gruber A and Wrachtrup J 2004 *Phys. Rev. Lett.* **92** 076401
[30] Handl A and Kuhlenkasper T 2018 *EinfüHrung in die Statistik* (Springer)
[31] Jacob G, Groot-Berning K, Wolf S, Ulm S, Couturier L, Dawkins S T, Poschinger U G, Schmidt-Kaler F and Singer K 2016 *Phys. Rev. Lett.* **117** 043001
[32] Beatrez W *et al* 2021 *Phys. Rev. Lett.* **127** 170603
[33] Schmidt A, Bernardoff J, Singer K, Reithmaier J P and Popov C 2019 *Phys. Status Solidi a* **216** 1900233
[34] Delgado M M, Tsunaki L, Michaelson S, Kuntumalla M K, Reithmaier J P, Hoffman A, Naydenov B and Popov C 2025 *Diam. Relat. Mater.* **154** 112126
[35] Tsunaki L, Singh A, Volkova K, Trofimov S, Pregnolato T, Schröder T and Naydenov B 2024 arXiv:2407.09411 [quant-ph]