

Quantum Vault: Symmetric No-Cloning Protection for Token Issuer and User (Benchmarked on IBM Quantum)

Lucas Tsunaki

lucas.tsunaki@helmholtz-berlin.de

Helmholtz-Zentrum Berlin für Materialien und Energie

Boris Naydenov

Helmholtz-Zentrum Berlin für Materialien und Energie

Research Article

Keywords: Quantum Token, Quantum Communication, Quantum Money, Quantum Identity Authentication, IBM Quantum

Posted Date: October 16th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11244442/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

Quantum Vault: Symmetric No-Cloning Protection for Token Issuer and User (Benchmarked on IBM Quantum)

Lucas Tsunaki ^{1,*} and Boris Naydenov ^{1,2,†}

¹*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*

²*Department of Physics, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany*

(Dated: October 2, 2026)

Quantum tokens are underlying primitives for quantum money and network proposals, which leverage the no-cloning theorem to realize unforgeable authentication. A relevant but overlooked type of attack to such architectures is one in which a hacker steals the classical side information about the token states from the issuing agent (e.g., a bank), enabling the forgery of fake tokens without violating the no-cloning theorem. Our proposal addresses this threat by removing the classical side information about the token states, where instead a copy of the token is stored at the bank, i.e. a quantum vault. This copy can be accessed by anyone to perform authentication, consuming the token pair in the process. We benchmark the protocol and identify quality parameters within a hardware agnostic framework employing IBM Quantum processors, such that the protocol is applicable to arbitrary quantum platforms. By comparing the efficiency with which genuine tokens are produced and authenticated against a possible estimate-and-forge attack, we quantify the security of the protocol. We achieve probabilities lower than 10^{-4} for false-negative errors (Type 1) and 10^{-10} for successful attacks (Type 2) when considering quantum bills composed of 200 tokens, even in the worst performing processor and a conservative uncertainty estimate. The quantum vault not only protects both user and bank symmetrically with the same quantum principles, but provides a step towards public key authentication, since any untrusted party can have access granted by the bank to the tokens' authentication interface without being able to clone them. Besides this bank-mediated form of publicly accessible verifiability, our proposal achieves traceability and revocability, since the bank retains the vault copy of the tokens.

Keywords: Quantum Token, Quantum Communication, Quantum Money, Quantum Identity Authentication, IBM Quantum.

I. INTRODUCTION

Quantum communication infrastructure and technology are becoming central components for national sovereignty and geopolitics [1–5], with robust applications [6–8] achievable within current NISQ-era [9] hardware. The foundation for quantum communication lies in the no-cloning theorem, which states that arbitrary quantum states cannot be cloned in general [10–13]. While most applications rely on entanglement and photon exchange to communicate information, another paradigm within quantum communication is a physical object which holds a non-clonable quantum state that can be used for personal authentication, i.e. a quantum token. This concept was originally proposed by S. Wiesner in 1983 [14] and since then, overlapping applications have been introduced under different names: quantum money [14, 15], quantum ticket [16], quantum payment [17], quantum signature [18], quantum physical unclonable function [19], quantum identity authentication [20] or quantum token [21–24]. Meanwhile, the same terms often represent slightly distinct concepts across literature [19].

To be precise, we consider in this work a personal quantum token with classical state information as an

application consisting of three steps (Fig. 1):

1. **Token Issuing:** an issuing agent (e.g. a bank or mint) prepares an arbitrary quantum state $|\psi\rangle$ with Bloch sphere angles (θ, ϕ) known only to itself and classically stores this information about the prepared state.
2. **Token Storage:** the issuing agent remotely transmits or physically delivers the state $|\psi\rangle$ to the user, or claimant [25], who stores it until authentication is required.
3. **Token Authentication:** the user presents their token to the authentication agent referred to as verifier [25], which can be a vendor, the bank or another user. The verifier measures this state and compares with the initially prepared angles (θ, ϕ) and if the measured state is close up to some acceptance range to the prepared state, the token is accepted.

Here we use a terminology closer to quantum money applications, but in fact quantum tokens have broader applications for general authentication procedures. An important distinction from other quantum money proposals [26, 27] is that, here, we consider personal non-anonymous tokens, in analogy to classical credit cards compared to cash. This common quantum token definition presupposes secure classical communication channels between parties [27–30] to communicate (θ, ϕ) and/or

* tsunakilucas@gmail.com

† boris.naydenov@helmholtz-berlin.de

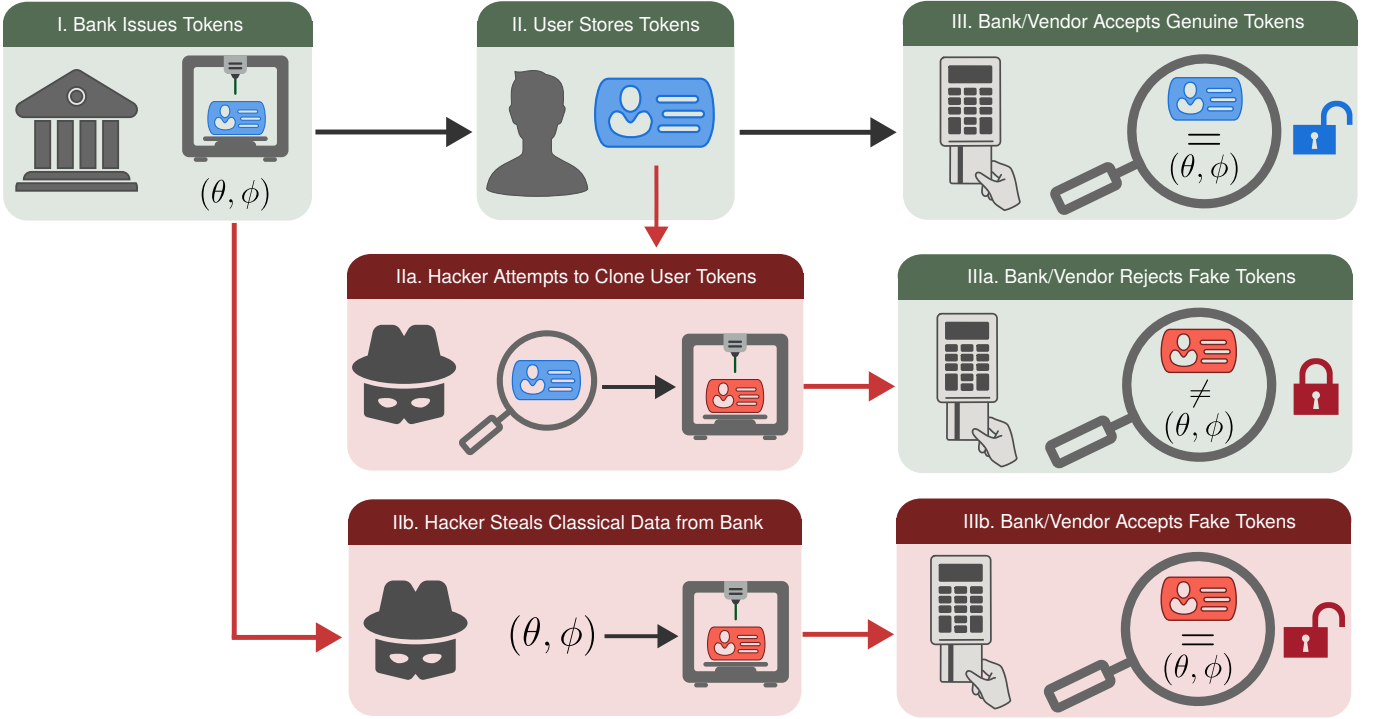


FIG. 1. Attack scenarios on previous quantum token proposals with classical side information. In general, a token protocol has three steps: **I.** a bank issues quantum tokens in states $|\psi\rangle$ with angles (θ, ϕ) ; **II.** the bank transmits the tokens to the user, who stores them until authentication; **III.** a vendor or bank authenticates the tokens by measuring their states and comparing them with the classically stored values of (θ, ϕ) . While the user's token is protected by the no-cloning theorem, an attacker could steal the values of (θ, ϕ) from the bank and create fake tokens without the bank realizing that it had been compromised.

classical storage in the bank [14, 16], which is precisely the vulnerability addressed in this work. This definition also carries a classical side information about the serial number of the token for user identification, which still remains in our proposal.

In simplified terms, a quantum token can thus be understood as an unclonable quantum memory equipped with a secure readout method. In a public-key architecture, any individual is able to verify these tokens using the readout method, but not clone them [27, 30, 31]. Conversely, in a private-key setting, only the bank or a trusted party such as a vendor is able to authenticate the token. As will be shown here, our proposal trivially works as a private-key architecture and can operate with public-accessible verifiability mediated by the bank, if there exists a quantum channel between the bank and the verifier.

Quantum tokens can either be thought of as a portable object which the bank physically gives to the users (analogous to classical credit cards), forming a fundamental component for quantum money schemes [15, 32], or as a more abstract concept, where the token state is transmitted through flying qubits or teleported and stored locally by users, within quantum internet proposals [28, 33, 34] and other quantum network applications [35]. In any case, the implementation of such a device is still a long way from application-scale and commercial stages of development due to various practical constraints [36, 37].

Beyond the discussion around practical feasibility, a malicious attacker would not be able to efficiently clone a token held by the user [15, 29, 38, 39] (case IIa in Fig. 1). Within an estimate-and-forge model [19], this attacker can try to measure the user's token to gain some information about the state $|\psi\rangle$ and make a fake token with this information. However, as recently demonstrated within IBM Quantum platforms, the bank can distinguish genuine tokens from forged ones even in the presence of experimental errors [21, 22]. Another known type of attack [40, 41], but rarely covered by quantum token proposals [24], is a hacker that attacks the bank instead of the user. In most applications, the issuing agent is assumed to be an idealized entity which cannot be hacked [42]. But if an attacker is able to steal or intercept the classical information of the quantum token (θ, ϕ) (case IIb in Fig. 1), they would be able to create copies of the genuine token without violating the no-cloning theorem and the verifier would accept such tokens without even realizing the security breach (case IIIb in Fig. 1). Such a scenario might have been considered unrealistic until a few years ago, but recent events such as the XZ Utils backdoor in 2024 [43], the multi-billion-dollar North Korean crypto heists in 2025 [44] or the Axios attack in 2026 [45] have highlighted security vulnerabilities in the digital infrastructure and databases from financial institutions, as well as from other sectors. Therefore, a quantum verification

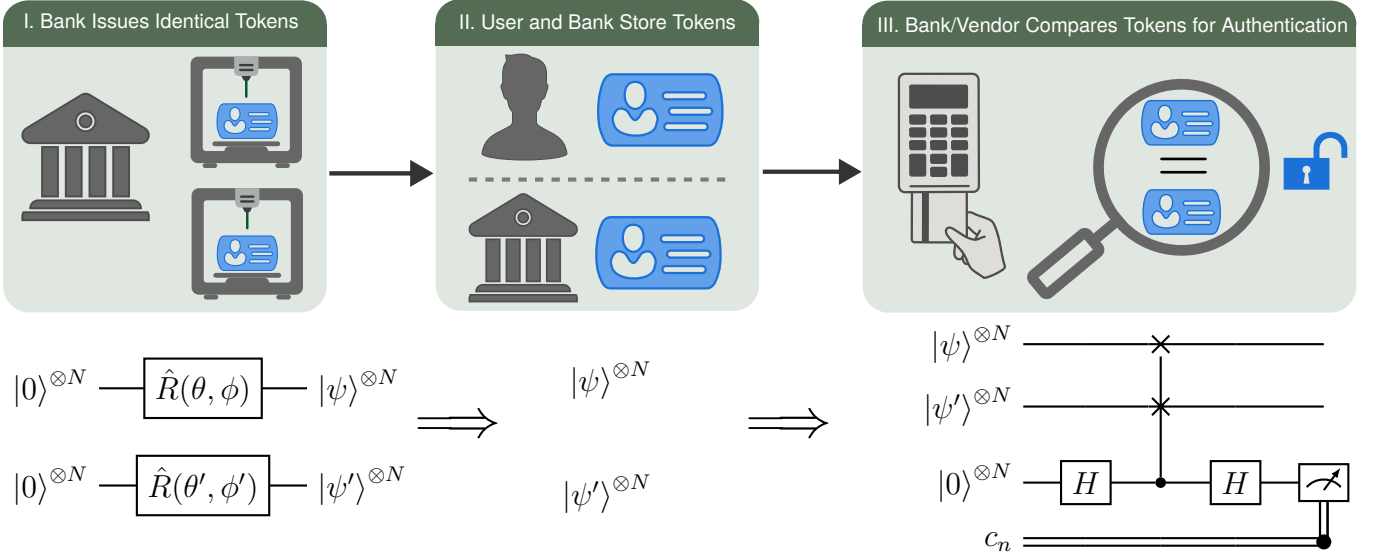


FIG. 2. Quantum vault protocol. Initially, the bank issues two tokens in identical Haar random states $|\psi\rangle^{\otimes N} = |\psi'\rangle^{\otimes N}$ and immediately discards any classical information about them. Each token is an ensemble of N non-entangled independent qubits. One token is stored in the bank's vault while the other is given to the user, such that both parties are no-cloning protected from attacks. For authentication, the bank or vendor performs SWAP tests between the N qubits of the tokens to verify if both tokens are in the same state or if one of them is fake.

scheme that also protects the bank is not simply a minor security improvement to previous proposals, but a crucial requirement for future quantum money and quantum internet architectures.

To answer this previously overlooked question on how to implement a protocol that protects both parties symmetrically with the same fundamental quantum principles, we introduce the concept of the quantum vault, as shown in Fig. 2 (the name quantum vault was already introduced in Ref. [46], but in a different context). Simply put, instead of preparing a quantum token and storing the information about the angles (θ, ϕ) classically as in prior proposals, the issuing agent now prepares two quantum tokens in the same state $|\psi\rangle^{\otimes N}$ and gives one of them to the user, while the other is stored, i.e. the quantum vault. We consider ensemble-based quantum tokens [21, 22] composed of N non-entangled independent qubits, in order to improve their readout efficiency. The authentication can then be performed by any party, trusted or not, by comparing the user's token with the one stored in the quantum vault. By eliminating the classical side information about (θ, ϕ) , we are not only able to achieve public-accessible verifiability mediated by the bank, but we also demonstrate unforgeability, traceability and revocability powers.

Before a scheme like this can be implemented in practical large-scale applications with arbitrary systems, the protocol needs to be benchmarked and thoroughly analyzed within a hardware agnostic framework. By doing so, key parameters can be identified and the security of the proposed scheme against attacks can be quantified. To realize that, we employ three IBM Quantum processors using Qiskit SDK [47], where the implementations

are open-source provided at a GitHub repository [48]. More details are given in Appendix A, while Table II provides a summary of all mathematical variables introduced in the text. We begin this work in Sec. II developing the quantum vault protocol and benchmarking it on the hardware. Following on that, Sec. III implements an estimate-and-forge attack, quantifying the security of the protocol. Finally, in Sec. IV, we discuss limitations and possible improvements for the protocol, outlining how the protocol could be implemented in practice.

II. QUANTUM VAULT PROTOCOL

In our proposal for the quantum vault scheme (Fig. 2), the bank starts by preparing two tokens in identical Haar random states $|\psi\rangle^{\otimes N} = |\psi'\rangle^{\otimes N}$ through a rotation applied to the $2N$ qubits as $|\psi\rangle^{\otimes N} = \hat{R}^{\otimes N}(\theta, \phi) |0\rangle^{\otimes N}$ and $|\psi'\rangle^{\otimes N} = \hat{R}^{\otimes N}(\theta', \phi') |0\rangle^{\otimes N}$, which does not violate the no-cloning theorem. The angles (θ, ϕ) are randomly drawn on the Bloch sphere, which could be done through a quantum random number generator [49], thus potentially reducing risks from side-channel attacks during token preparation [19, 42, 50]. During storage, both parties can use error correction and mitigation techniques [19, 51] to avoid decoherence of the states, such as dynamical decoupling from noises, as implemented in similar experiments with IBM Quantum [52].

Finally, during authentication, the user presents their token to the verifier for comparison with the one stored by bank in the vault. In a private-key setting, where the bank is both the issuing and verifier, this comparison is

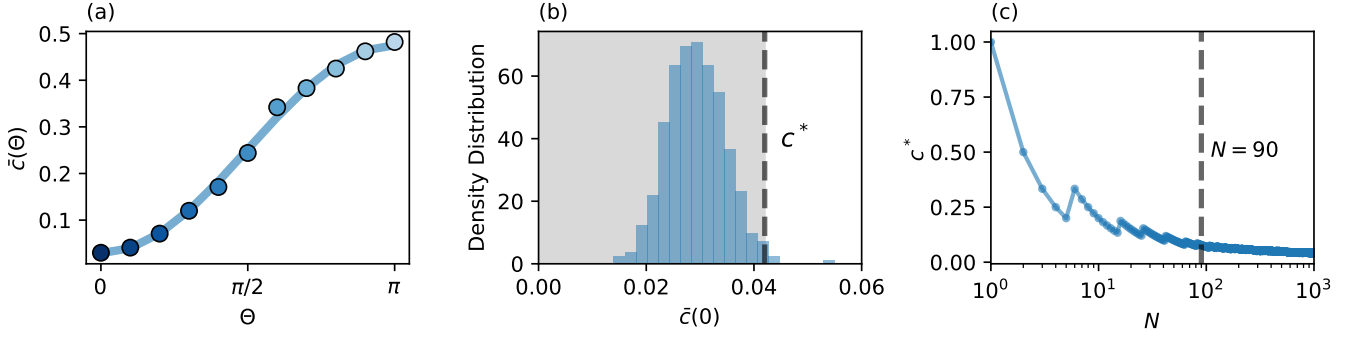


FIG. 3. Benchmark of quantum vault protocol in IBM Quantum Kingston. **(a)** SWAP test observable $\bar{c}(\Theta)$ for ensemble size $N = 1000$ (error bars are smaller than points). At $\Theta = 0$, $\bar{c}$ is close to 0, which then increases with Θ , enabling the verifier to authenticate if $|\psi\rangle^{\otimes N} = |\psi'\rangle^{\otimes N}$. The quality parameters Q_a and Q_o are obtained from the fit of the curve. **(b)** Distribution of $\bar{c}(0)$ from 400 angles $(\theta, \phi) = (\theta', \phi')$ uniformly distributed on the Bloch sphere with $N = 1000$. The acceptance threshold c^* is defined such that the probability that the bank accepts genuine tokens is $p_b[\bar{c} \leq c^*] = 0.99$, corresponding to the shaded area of the distribution below c^* . **(c)** Acceptance threshold c^* as a function of ensemble size. As N increases, the shot noise of the distribution decreases, leading to a more stringent acceptance criterion represented by the decrease in c^* . The ensemble size is taken as $N = 90$, such that c^* is not saturated and the discretization noise is already low.

direct, since the bank holds both the token stored in the vault and the one presented by the user. In the publicly accessible verification architecture on the other hand, the bank needs to allow anyone to verify the validity of the token, being a trusted vendor or even another untrusted user. For that to be realized, the verifier requests the bank to start an authentication procedure, where the bank can transfer the token stored in the vault to the verifier or allow the verifier to perform the authentication in the vault. This can be done through teleportation [53, 54] or flying qubits conversion [23, 24, 55], both of which require a quantum channel between the bank and the verifier based on existing quantum network technology [2–5]. Arguably, teleportation via heralded entanglement is a more viable alternative, since the tokens are safely stored in the vault until an entanglement is heralded, while flying qubits irretrievably lose many qubits. In connection to another wide-spread technology, a similar procedure takes place when a card payment is made by a user to a vendor, mediated by a centralized payment processor. The vendor reads the user’s card information and through a classical channel with the payment processor, verifies the veracity of their token. However, in our proposal for the quantum vault, the quantum channel does not necessarily need to be secure and the vendor does not have to be trusted, as argued in Sec. III.

The main technical question is then what is the most efficient way for the verifier to authenticate if both states are the same or if they have been cloned. S. Barnett et al. (2003) [56] theoretically demonstrated that it is impossible to identify if two single pure unknown states are identical with absolute certainty and established certain conditions for a measurement that compares two unknown quantum states to be optimal. This motivates the adoption of ensembles of independent qubits as tokens to improve the states comparison measurement. The use of ensembles as

quantum tokens can further facilitate the technological implementation of such technologies in certain physical systems [24, 36]. However, the no-cloning theorem is not trivially applicable in these cases, given that an ensemble is already a copy of individual qubits and an attacker can exploit that to perform quantum tomography of the $|\psi\rangle^{\otimes N}$ states, thus achieving a better estimate of $|\psi\rangle$. Refs. [21, 22] have nevertheless shown that ensemble-based quantum token protocols are still viable, even when the attacker has access to better quantum tomography capabilities.

One possible method which satisfies the optimal conditions for quantum state comparison [56] is the SWAP test [57–59], originally introduced for quantum fingerprinting applications, but which has also been proposed to be used for quantum token authentication [27, 35]. In the SWAP test, an auxiliary qubit is added to the system, as shown in Fig. 2. First, a Hadamard gate is applied to the auxiliary qubit, followed by a controlled SWAP between the token qubits and another Hadamard to the auxiliary. Lastly, the auxiliary qubit is measured in the standard basis $\{|0\rangle, |1\rangle\}$ and the measurement outcome is stored in the classical register c_n of the n -th test, with values 0 or 1. After the measurement, the system is collapsed into an eigenstate of the SWAP gate operator, which in practice means that the authentication consumes the tokens, as further discussed in Appendix B.

We define the SWAP test observable as the average of the classical register over the N qubits,

$$\bar{c} = \frac{1}{N} \sum_{n=1}^N c_n. \quad (1)$$

While c_n can only be 0 and 1, $\bar{c}$ has $N + 1$ possible discrete values between 0 and 1, converging to a continuous variable for large N . The value of $\bar{c}$ depends on the projection

various states $m = 1, \dots, M$. This proposed architecture is represented in Fig. 4, with a total of M independent tokens, each with N qubits. The quantum state of the whole quantum bill thus corresponds to

$$|\Psi\rangle = \bigotimes_{m=1}^M |\psi\rangle_m^{\otimes N}. \quad (5)$$

Given that the probability that a single token is accepted by the bank is p_b , the probability $\mathcal{P}_b$ that at least m^* token states out of a total M are accepted corresponds to a cumulative binomial distribution as

$$\mathcal{P}_b(m^*, M, p_b) = \sum_{m=m^*}^M \binom{M}{m} p_b^m (1 - p_b)^{M-m}. \quad (6)$$

Likewise, m^* acts as another threshold parameter for the minimum number of token states which need to be accepted in the bill. By adjusting the values of m^* and M , desired levels for $\mathcal{P}_b$ can be achieved as well. If the acceptance threshold m^* is lowered, the Type 1 error rate of rejecting genuine tokens can be decreased. But on the other hand, a lower threshold m^* leads to higher chances of Type 2 errors for accepting fake tokens, as further discussed in Sec. III. In this work, we choose m^* such that $\mathcal{P}_b \geq 1 - 10^{-4}$. In addition, increasing the total number of states in the bill M leads to a more stringent acceptance threshold m^* , again improving the overall security [21, 22, 60].

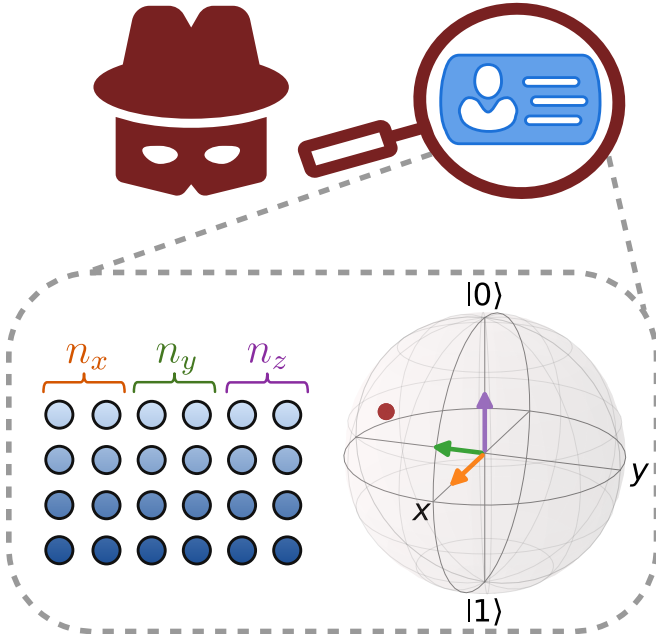


FIG. 5. Estimate-and-Forge attack method. The attacker subdivides the ensemble in the $|\psi\rangle^{\otimes N}$ state into three equal parts to perform SWAP test measurements along the x , y and z axes. With this information, they use maximum-likelihood estimation to reconstruct $|\psi\rangle$ and then forge fake tokens and attempt authentication with the bank.

Prior to the application of the quantum vault protocol, the bank thus needs to perform a calibration procedure as developed here to obtain the $\bar{c}(0)$ distribution and the acceptance threshold c^* . By doing so, the measurement of the variable $\bar{c}$ by the SWAP test can be used to verify if the two bills are in the same states $|\Psi\rangle$ and consequently authenticate the identity of the user. The only classical information involved in the protocol is therefore c^* and the serial number to identify the tokens, completely eliminating any information about the angles $(\theta, \phi)_m$. These classical parameters can even be made public for a public accessible authentication architecture. The values of Q_a and Q_o are not strictly necessary for the practical implementation of the method, but they can still be valid quality parameters for comparing different hardware.

III. SECURITY AGAINST ESTIMATE-AND-FORGE ATTACK

Having benchmarked the quantum vault protocol and characterized the efficiency in which tokens are issued and authenticated, we now implement a possible estimate-and-forge attack scenario. By comparing the efficiency which an attacker can forge fake tokens with the efficiency in which the bank can generate and authenticate genuine ones, we can quantify the security of the protocol. The quantum vault protocol requires that the hardware can execute a SWAP test circuit. A fair assumption is that an attacker could have access to the same authentication interface to realize SWAP tests. Moreover, in a publicly accessible authentication architecture, untrusted parties already need to interact with the vault's tokens through the SWAP test authentication interface anyway. We thus consider an attack model where the attacker attempts to gain information about the token states and then creates fake ones for authentication with the verifier (case IIa in Fig. 1). Both user and bank are symmetrically protected by the no-cloning theorem, but if the attacker attempts to hack the vault's tokens, then no authentication can be performed afterwards, since the vault's copy is destroyed in the process. We therefore consider the case where the attacker attempts to hack the user's token, even though this security analysis is valid for both token holders.

In order to gain information about the genuine token states $|\psi\rangle^{\otimes N}$ along the unit vector $\hat{n} = (n_x, n_y, n_z) = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$, the attacker can prepare known probing states and perform SWAP tests to estimate the angle Θ between them. By setting this probing state as $|+X\rangle$, the attacker measures $\bar{c}_x$ which can be used to estimate the n_x component of $|\psi\rangle$. Conversely, with $|+Y\rangle$ and $|0\rangle$, they obtain $\bar{c}_y$ and $\bar{c}_z$, which can be used to estimate the n_y and n_z components respectively. From the measured values of $\bar{c}_{x,y,z}$, Eq. 3 can be inverted as

$$n_{x,y,z} = \cos \Theta_{x,y,z} = 1 + \frac{4(Q_o - \bar{c}_{x,y,z})}{Q_a}, \quad (7)$$

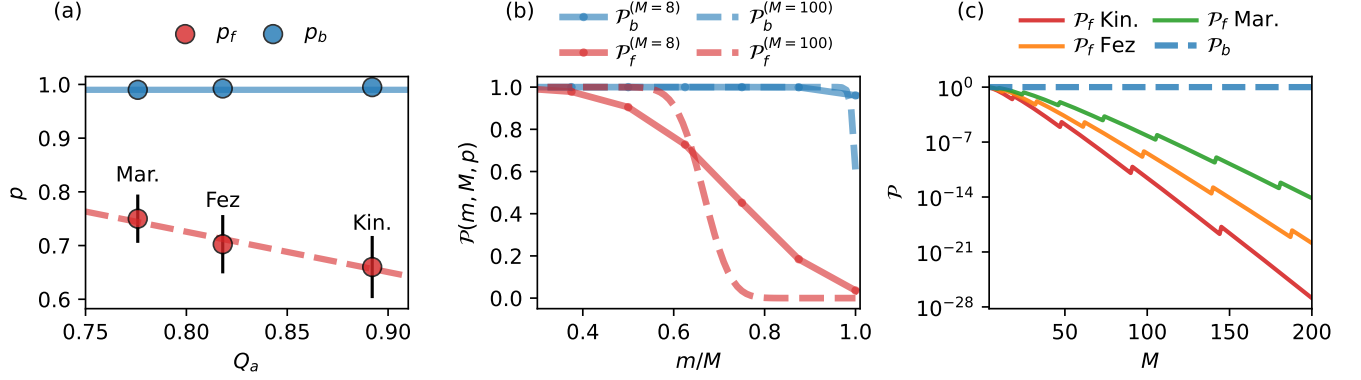


FIG. 6. Forgery Attack on Quantum Vault. **(a)** Acceptance probabilities p_b for single genuine tokens and forged ones p_f , with error bars obtained from bootstrapping [61]. p_f is constant within error bars, but agrees with a linear decrease with Q_a (red guide line), as observed in Refs. [21, 22]. **(b)** Probability to accept genuine and forged bills $\mathcal{P}(m^*, M, p)$ composed of $M = 8, 100$ tokens as a function of m^*/M in IBM Quantum Kingston. Both probabilities decrease as the acceptance threshold m^*/M increases, but faster with $\mathcal{P}_f$. With larger M , the cumulative binomial distribution approaches a rectangular function, improving security. **(c)** Probability of successful forgery $\mathcal{P}_f(M, p)$ for m^* fixed such that $\mathcal{P}_b \geq 1 - 10^{-4}$ in all three processors. $\mathcal{P}_f$ decays exponentially with M , reaching negligible values at large M , even in the worst performing hardware.

for $|1 + 4(Q_o - \bar{c}_{x,y,z})/Q_a| \leq 1$, so that $\Theta_{x,y,z}$ is real. To gain any useful information from the SWAP test, the attacker still needs to know Q_o and Q_a (Eq. 3). This provides an additional layer of security to the vault protocol, since now the attacker also needs to consume some of the tokens in the bill to obtain these values. In the following, we conservatively assume that the attacker has perfect knowledge of these quality parameters.

The attacker can subdivide the N qubits of the token into three equal parts of $N/3 = 30$ qubits and perform measurements along the three axes to gain more information about $|\psi\rangle$, as illustrated in Fig. 5. Now the question is how the attacker can optimally estimate $|\psi\rangle$ based on Eq. 7 and the measured values of $\bar{c}_{x,y,z}$. The most straightforward method is to perform a direct inversion tomography $\hat{n} = (n_x, n_y, n_z)/|n|$, but this was demonstrated to be less efficient compared to other estimation methods [22]. In this work, we employ an improved version of the maximum likelihood estimation (MLE) method as reported in Ref. [22], where the three values of $n_{x,y,z}$ constrained to $|\hat{n}| = 1$ are simultaneously optimized by numerically maximizing the joint binomial probability for the measurements, instead of analytically solving an overdetermined set of equations. More details on the mathematical implementation of the MLE are discussed in Appendix C.

After the probing of the genuine tokens, the attacker uses the estimated angles to prepare fake tokens and attempt authentication with the verifier, who accepts them if they are measured below the SWAP test acceptance threshold c^* . This attack scenario was implemented in the three processors considering 400 token states uniformly distributed over the Bloch sphere with optimal $N = 90$. The resulting acceptance probabilities for fake tokens $p_f[\bar{c} \leq c^*]$ as a function of the quality factors Q_a

are shown in Fig. 6 and in Tab. I, while the distributions of the SWAP test observable $\bar{c}$ from forged tokens are given in the GitHub repository [48]. The three processors present p_f probabilities below 0.8, while the probability for accepting genuine tokens is $p_b \geq 0.99$ by construction (Eq. 4). The p_f values are within the same range of uncertainty, obtained by the bootstrap method [61]. Despite that, as shown by the guide line obtained with a linear fit, these values agree with the trend observed in Refs. [21, 22], where better quality parameters lead to increased security of the tokens.

The probabilities for accepting single genuine p_b and fake ones p_f are relatively close. However, as discussed in Sec. II, the quantum bill security stems from the multiple tokens which it contains. The probability then of a Type 2 error where a fake bill with M tokens is accepted $\mathcal{P}_f$ follows a cumulative binomial distribution, as in Eq. 6, but substituting p_f for the bank value p_b . Fig. 6 (b) shows these probabilities of acceptance from the bank $\mathcal{P}_b$ and forger $\mathcal{P}_f$ as a function of the ratio m^*/M , for $M = 8$ and $M = 100$ in IBM Quantum Kingston. As the ratio m^*/M increases, the probabilities of acceptance $\mathcal{P}$ decrease, resulting from the sum of binomial distributions. However, the decrease in $\mathcal{P}_f$ starts at lower m^*/M values than $\mathcal{P}_b$, given that $p_f < p_b$. For the larger M , Eq. 6 approaches a rectangular function, making the protocol safer, since the acceptance threshold m^* can be chosen such that $\mathcal{P}_b$ is still large but $\mathcal{P}_f$ is already decayed.

To further characterize this effect, Fig. 6 (c) shows the values of $\mathcal{P}_f$ in all three IBM Quantum processors, with m^* fixed such that the probability to accept genuine bills is $\mathcal{P}_b \geq 1 - 10^{-4}$. Likewise, the probability for successful forgery $\mathcal{P}_f$ decays in an exponential regime with M . As in Fig. 3 (c), the decay is not monotonic due to the discretization noise of the variables. Tab. I

IBM Processor	Q_a	Q_o	$c^*(N = 90)$	p_f	1σ of $\mathcal{P}_f(M = 200)$
Kingston	0.892 (0.018)	0.029 (0.004)	0.078 (0.005)	0.66 (0.06)	$10^{-33} - 10^{-21}$
Fez	0.818 (0.018)	0.041 (0.004)	0.100 (0.007)	0.70 (0.05)	$10^{-25} - 10^{-15}$
Marrakesh	0.776 (0.020)	0.084 (0.005)	0.145 (0.009)	0.75 (0.04)	$10^{-18} - 10^{-10}$

TABLE I. Quality Parameters from IBM Quantum Processors, as defined in Tab. II. Uncertainties in Q_a and Q_o are obtained from the standard deviation of the fitted parameters, while in c^* and p_f they are obtained from bootstrap method [61]. 1σ confidence intervals of $\mathcal{P}_f(M = 200)$ are calculated from the propagated error of p_f and m^* and with the acceptance threshold m^* set such that $\mathcal{P}_b \geq 1 - 10^{-4}$. Kingston presents better quality parameters and an improved resulting safety, while Marrakesh is the worst performing hardware.

provides the 1σ confidence interval for $\mathcal{P}_f$ at $M = 200$ with propagated errors from the p_f values and m^* , leading to a wide range for $\mathcal{P}_f$. Nevertheless, values of $\mathcal{P}_f < 10^{-10}$ are observed in the worst performing hardware, assuming the pessimistic upper bound of the uncertainty. Another important observation is the contrast in the security of the different hardware, where small improvements in the quality parameters can yield significant gains in security. This shows a potential improvement to the protocol with the ongoing quantum hardware evolution [24, 36, 37, 62]. But still, compared to the results reported in Ref. [21] for an ensemble-based quantum token protocol with classical state information, these security metrics show that the elimination of the classical state information demands an increase in M to compensate for the loss of efficiency in the authentication method.

IV. DISCUSSION & OUTLOOK

Quantum tokens envision to accomplish fundamentally unclonable authentication schemes, with broad applications to quantum money and network applications. However, an overlooked vulnerability is an attack on the classical side-information regarding the quantum states of these tokens. In this work, we answer this question with a conceptual shift from current quantum token proposals by symmetrically protecting both sides (issuing agent and user) with quantum no-cloning. In the quantum vault proposal, the classical information (θ, ϕ) about the user's token is eliminated by instead preparing a pair of tokens with N qubits in the same state $|\psi\rangle^{\otimes N}$, one given to the user and the other kept at the bank's vault. The authentication is then performed through a SWAP test between the qubits in the tokens from the vault and the user.

We benchmark the whole protocol in a hardware-agnostic framework employing three IBM Quantum processors, with minimal assumptions about the hardware. Besides paving the way towards applications with different platforms, the intra-chip results from the processors provide an upper bound on the performance of concrete instantiations of the method in quantum networks, where additional errors are present, such as photon losses during token transfer or memory decoherence during storage. Based on the definition of the $\bar{c}$ observable obtained from the SWAP tests, we are able to identify quality param-

eters (Tab. I) for the hardware and to establish a criterion for acceptance. We further consider a viable estimate-and-forge attack to either one of the two tokens, where the attacker performs SWAP tests to gain information about the tokens and then use this information to create fake ones. Considering single tokens, an attacker has a high probability of success, demonstrating the efficiency of the attack method. However, in quantum bills composed of $M = 200$ tokens (Eq. 5), we obtain probabilities of successful attacks $\mathcal{P}_f < 10^{-10}$ even in the worst performing processor and upper 1σ uncertainty, while the probability for genuine tokens to be accepted is $\mathcal{P}_b \geq 1 - 10^{-4}$. By comparing the security metrics with previously reported results for an ensemble-based quantum token protocol with classical state information in IBM Quantum processors [21], we observe that the elimination of the classical state information lowers the authentication efficiency of genuine tokens, thus requiring more tokens per bill.

In practical terms, the results indicate that trusted or untrusted parties can have access to the authentication interface of tokens in the vault, without being able to impersonate the users and compromise security. In this sense, the keys can be 'semi-public', but still a centralized institution such as a bank needs to store and make them accessible. These results further support previous proposals for using SWAP tests in quantum token verification [27, 35]. The quantum vault scheme as presented here is intrinsically non-anonymous, since the bank needs to know who is the owner of the token in order to perform the comparison. This confers the governance properties of traceability and revocability [26, 63, 64], meaning that responsible authorities can trace a bill and revoke its use at any time, since the bank holds the vault copy. Another practical consideration for the protocol is that the authentication consumes the quantum tokens (Appendix B), which implies that the user should receive several units of them at once by the bank [27], or have them replenished through a quantum channel. With ongoing hardware evolution [24, 36, 37, 62], a further improvement of the method can be obtained with optimized ensemble states comparison, as proposed by M. Fanizza et al. (2020) [65].

The main technological limitation for the commercial application of such scheme lies in the short lived quantum memories presently available. Even though coherence times of several hours have been observed in nuclear spins in noble gases [66, 67] that can even be made mobile,

these quantum systems still lack a reliable interface with flying qubits. Other trapped atomic and molecular platforms [68, 69] can have a viable interface with flying qubits, long coherence, high fidelity gates, but can hardly be made mobile due to the required ultra-high vacuum or low temperatures. The same limitations apply to superconducting qubits, which provide an efficient platform for validating this protocol, but require mK temperatures for operation. Finally, a class of quantum systems that has great potential as quantum token platforms is the color center defects in solids [54, 70, 71]. With ongoing evolution of their fabrication techniques [23, 24, 36, 37], these systems exhibit naturally long coherence times at room temperature and pressure, with strong optical interface [23]. Another interesting feature of these systems is the ensemble inseparability guaranteed by diffraction limited optical initialization and readout [54, 72], which limits the attacker to perform SWAP tests along a single axis, but would also require a reformulation of the whole SWAP test authentication not based on Bernoulli trials. Alternative approaches that circumvent the necessity for long lived quantum memories are the S-money proposals, which instead support their security on relativistic principles [73, 74].

Even though the estimate-and-forge attack model considered here covers a wide range of possible forms of attack, it does not configure a full security proof. For instance, better cloning efficiency can be obtained if the attacker is not restricted to performing SWAP tests, but instead can also perform usual projective measurements. In this case, the attacker could obtain further information about the token state $|\psi\rangle$ from the collapsed state of the SWAP test (Appendix B). A restriction to perform only SWAP tests could be enforced in some hardware architectures by a fabrication which limits arbitrary gate operations in the token qubits and enable measurements only on the auxiliary qubit. An alternative type of attack are substitution attacks [38], where the attacker simply swaps the genuine tokens, without violating the no-cloning theorem. This attack form can also be avoided with hardware constraints on arbitrary SWAP gates to the token qubits. In addition, exact characteristics of each physical platform can be exploited by side-channel attacks [21, 42, 50] or better Bayesian estimation methods with different budget allocation of the ensemble could potentially be used by the attacker [22]. As argued by A. Behera and O. Sattath (2024) [27], many theoretically proposed constructions for public quantum money were later broken, while current ones are also susceptible to being broken [64, 75]. This motivates further theoretical examination of the quantum vault proposal and highlights the hardware-agnostic approach developed here of employing cloud-based quantum processors as a viable and practical means for testing quantum money and communication methods.

Appendix A: IBM Quantum Implementation

The quantum vault was implemented using Qiskit SDK version 2.3.0 [47] and Qiskit IBMQ Runtime version 0.45.1, as open-source provided at the author's GitHub repository [48]. The three processors used in this work are from the Heron r2 family with similar architecture [62], having the same native operations and 156 qubit count. Given that their parameters exhibited fluctuations in time which affect these results, all measurements were carried out within a few hours on 10 September 2026, with the calibrations reports provided by IBM Quantum also given in the repository [48]. The high-level representations of the quantum circuits were transpiled to the native gates of the hardware without optimization or gate approximation, in order to keep the circuit as close as possible from the model. The gates are translated by synthesis to the densest layout qubits, with longest coherence, shortest gate times and errors. In Kingston, qubits 10 and 11 were used for the vault with 12 as the auxiliary. In Fez, 109 and 110 are the vault, 111 is the auxiliary. Lastly, in Marrakesh, 135 and 139 are the vault, 155 is the auxiliary. All circuits were run in the sampler mode.

Appendix B: Quantum State Evolution Under SWAP Test

The system composed of the two token qubits plus the auxiliary is submitted to the SWAP test in the initial state $|\psi\rangle|\psi'\rangle|0\rangle$. First, with the application of the Hadamard gate to the auxiliary qubit, the system evolves to

$$(\mathbb{1} \otimes \mathbb{1} \otimes H) |\psi\rangle |\psi'\rangle |0\rangle = \frac{1}{\sqrt{2}} |\psi\rangle |\psi'\rangle (|0\rangle + |1\rangle).$$

In succession, the controlled SWAP gate is applied as

$$\begin{aligned} \text{CSWAP} \frac{1}{\sqrt{2}} |\psi\rangle |\psi'\rangle (|0\rangle + |1\rangle) \\ = \frac{1}{\sqrt{2}} (|\psi\rangle |\psi'\rangle |0\rangle + |\psi'\rangle |\psi\rangle |1\rangle). \end{aligned}$$

The second Hadamard to the auxiliary qubit yields the state

$$\frac{1}{2} \left[(|\psi\rangle |\psi'\rangle + |\psi'\rangle |\psi\rangle) |0\rangle + (|\psi\rangle |\psi'\rangle - |\psi'\rangle |\psi\rangle) |1\rangle \right]. \quad (\text{B1})$$

Finally, the measurement of the auxiliary qubit collapses the system into one of these two eigenstates of the SWAP gate, with probabilities of measuring the classical register c_n into 0 or 1 given by

$$P(c_n = 0) = \frac{1 + |\langle\psi|\psi'\rangle|^2}{2}, \quad P(c_n = 1) = \frac{1 - |\langle\psi|\psi'\rangle|^2}{2}.$$

Where we thus have $\bar{c} \rightarrow P(c_n = 1)$ for large N , as in Eq. 1.

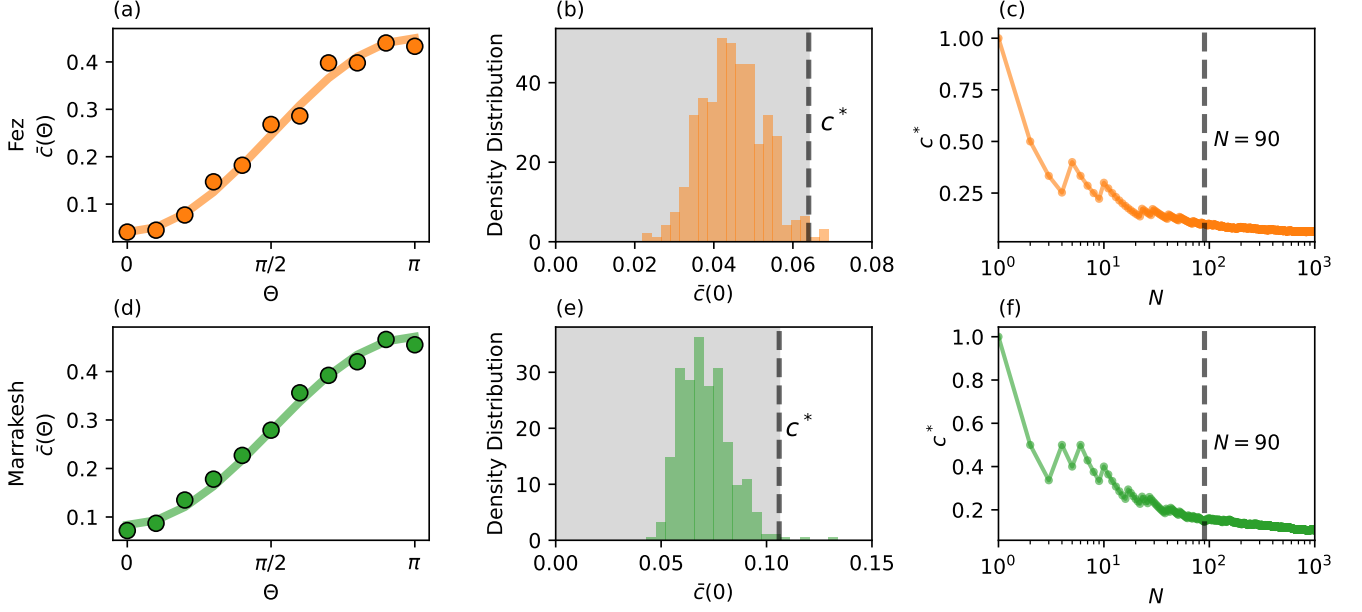


FIG. 7. Quantum Vault Benchmark in IBM Quantum Fez and Marrakesh. (a, d) SWAP test observable $\bar{c}$ as a function of separation angle Θ . (b, e) $\bar{c}(0)$ distributions for 400 Bloch sphere points. (c, f) Acceptance threshold c^* of the SWAP test as a function of the ensemble size N .

It is important to note that the SWAP test does not necessarily erase the information about the states $|\psi\rangle$ and $|\psi'\rangle$. For $c_n = 0$, the token qubits are projected onto the symmetric state $|\psi\rangle|\psi'\rangle + |\psi'\rangle|\psi\rangle$ up to a normalization factor, which still depends on both states and is entangled unless $|\psi\rangle = |\psi'\rangle$, while for $c_n = 1$ they are projected onto a singlet state, independently of the states. Either the bank or an ingenious attacker could thus, at least in principle, obtain further information about the states overlap $|\langle\psi|\psi'\rangle|^2$, since the quantum Fisher information [76] of the post-measurement state with respect to Θ is non-zero for $c_n = 0$. Extracting this information nonetheless is not trivial, requiring further operations on the residual token qubits, such as projective measurements or additional SWAP tests against probe states. A special case occurs when the two states are identical $|\psi\rangle = |\psi'\rangle$. In this scenario, the final state from Eq. B1 corresponds to the initial state $|\psi\rangle|\psi\rangle|0\rangle$, implying that the authentication does not actually consume the token. This suggests the possibility of non-consumable tokens, nevertheless the bank would not be able to distinguish if the quantum system is in the state $|\psi\rangle|\psi\rangle|0\rangle$ or $(|\psi\rangle|\psi'\rangle + |\psi'\rangle|\psi\rangle)|0\rangle$, which limits the practical usefulness of this feature. Overall then, it can be assumed from a practical perspective that the SWAP test consumes the tokens, even though the states $|\psi\rangle$ and $|\psi'\rangle$ can survive the authentication depending on the c_n outcome and the states. An adaptation of the SWAP test which collapses the tokens' states does exist [77], thus limiting the information that an ingenious attacker could obtain from the measured state from Eq. B1.

Appendix C: Maximum Likelihood Estimation

As discussed in Sec. III, the attacker probes the N genuine tokens in the state $|\psi\rangle^{\otimes N}$ along the vector $\hat{n} = (n_x, n_y, n_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ by subdividing them in three parts and performing measurements along the three axes, thus obtaining $\bar{c}_{x,y,z}$. Following Eq. 3, the model's probability to measure $c_n = 1$ on axis i as a function of the trial parameters (θ, ϕ) is

$$P_i(\theta, \phi) = Q_o + \frac{Q_a}{4} [1 - n_i].$$

Since the individual c_n measurements are Bernoulli trials of binary outcomes and each repetition is independent, the likelihood $\mathcal{L}(\theta, \phi | \bar{c}_{x,y,z})$ for measuring $\bar{c}_{x,y,z}$ is given by the product of the three binomial probabilities

$$\mathcal{L}(\theta, \phi | \bar{c}_{x,y,z}) = \prod_{i \in \{x,y,z\}} \binom{N/3}{N\bar{c}_i/3} P_i^{N\bar{c}_i/3} (1 - P_i)^{N(1-\bar{c}_i)/3}.$$

This is the function the attacker wants to maximize in order to estimate the state $|\psi\rangle$. However, maximizing $\mathcal{L}(\theta, \phi | \bar{c}_{x,y,z})$ corresponds to minimizing

$$-\log \mathcal{L}(\theta, \phi | \bar{c}_{x,y,z}) = - \sum_{i \in \{x,y,z\}} \frac{N}{3} [\bar{c}_i \log(P_i) + (1 - \bar{c}_i) \log(1 - P_i)] + \text{const},$$

given that log is a monotonic function. We can further drop the $N/3$ factor and the constant term, since

Variable	Physical Meaning
θ	polar angle on the Bloch sphere
ϕ	azimuthal angle on the Bloch sphere
$\hat{R}(\theta, \phi)$	rotation operator with angles (θ, ϕ)
$ \psi\rangle$	token state with angles (θ, ϕ)
Θ	angle between two states with unit vectors $\hat{n}$ and $\hat{n}'$: $\Theta = \arccos(\hat{n} \cdot \hat{n}')$
c_n	n -th classical register for the SWAP test
N	number of qubits in the token
$\bar{c}$	SWAP test observable given by the average $\sum_{n=1}^N c_n/N$
c^*	acceptance threshold of the SWAP test
Q_a	amplitude quality factor
Q_o	offset quality factor
p_b	probability that a genuine token is accepted
p_f	probability that fake token is accepted
M	total number of tokens in quantum bill
m^*	acceptance threshold for the minimum number of accepted tokens in a bill
$ \Psi\rangle$	quantum bill state with M tokens each with N qubits $\bigotimes_{m=1}^M \psi\rangle_m^{\otimes N}$
$\mathcal{P}_b$	probability that a genuine quantum bill is accepted
$\mathcal{P}_f$	probability that a fake quantum bill is accepted
$\mathcal{L}(\theta, \phi \bar{c}_{x,y,z})$	likelihood for an attacker to measure $\bar{c}_{x,y,z}$ over the three axes

TABLE II. Glossary of variables.

they do not affect the minimization. Finally, using the Nelder-Mead method [78], the optimal solution of (θ, ϕ) is numerically found, with the direct inversion tomography as initial guess. The Python implementation of the method can also be found at the GitHub repository [48]. Likewise, this method represents an improvement from the MLE reported in Ref. [22], by fully exploiting the information gained from the N measurements without equation over-determination.

DATA & CODE AVAILABILITY

All data used in this work and the code for implementing the quantum vault protocol and analyzing the results are open source under GPL3 license, provided at the author's GitHub repository [48].

AUTHOR CONTRIBUTIONS

L.T. conceptualized this work, developed the theory, implemented the protocols with IBM Quantum and analyzed the data. B.N. acquired funding and supervised the work. Both authors contributed to the writing and revision of the text.

COMPETING INTERESTS

The authors declare that they have no competing interests.

ACKNOWLEDGMENTS

I (L.T.) am extremely grateful to the anonymous scientist who attended my poster presentation at the KIT Graduate School of Quantum Matter (KSQM) in 2023 and through a constructive discussion, gave me the seed for the idea that motivated this work. This work was supported by the *Bundesministerium für Forschung, Technologie und Raumfahrt* (BMFTR) under the project *Diamant-basierte Quantenmaterialien* (DIAQUAM - n° 13N16956) and by the Helmholtz Quantum Use Challenge project QT-Batt. We acknowledge the use of IBM Quantum services for this work. The views expressed are those of the authors and do not reflect the official policy or position of IBM or the IBM Quantum team.

- [1] A. Ferrazzini, Quantum, diplomacy, and geopolitics (2026), [arXiv:2512.06052](https://arxiv.org/abs/2512.06052) [physics.soc-ph].
- [2] QuantumCTek Co., Ltd., China's national quantum communication backbone network, <https://www.quantum-info.com/English/> (2017), accessed: January 20, 2026.
- [3] Quantum Corridor Inc., Quantum corridor: Gateway to the quantum future, <https://www.quantumcorridor.com> (2025), accessed: January 20, 2026.
- [4] QuNET Initiative, QuNET - quantum networks, <https://qunet-initiative.de/en/homepage/> (2025), accessed: January 19, 2026.
- [5] Deutsche Telekom Technik GmbH and Partners, DemoQuandT, <https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt> (2025), accessed: January 19, 2026.
- [6] N. Gisin and R. Thew, Quantum communication, *Nature Photonics* **1**, 165 (2007).
- [7] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, Satellite-based entanglement distribution over 1200 kilometers, *Science* **356**, 1140 (2017).
- [8] ID Quantique, ID Quantique – Quantum-Safe Security Solutions, <https://www.idquantique.com/> (2026), accessed: March 17, 2026.
- [9] J. Eisert and J. Preskill, Mind the gaps: The fraught road to quantum advantage (2025), [arXiv:2510.19928](https://arxiv.org/abs/2510.19928) [quant-ph].
- [10] J. L. Park, The concept of transition in quantum mechanics, *Foundations of Physics* **1**, 23 (1970).
- [11] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, 802 (1982).
- [12] D. Dieks, Communication by EPR devices, *Physics Letters A* **92**, 271 (1982).
- [13] K. Yamaguchi and A. Kempf, Encrypted qubits can be cloned, *Physical Review Letters* **136**, 010801 (2026).
- [14] S. Wiesner, Conjugate coding, *ACM Sigact News* **15**, 78 (1983).
- [15] K. Bartkiewicz, A. Černoč, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, Experimental quantum forgery of quantum optical money, *npj Quantum Information* **3**, 7 (2017).
- [16] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, Unforgeable noise-tolerant quantum tokens, *PNAS* **109**, 16079 (2012).
- [17] P. Schiansky, J. Kalb, E. Sztatecsny, M.-C. Roehsner, T. Guggemos, A. Trenti, M. Bozzio, and P. Walther, Demonstration of quantum-digital payments, *Nature Communications* **14**, 3849 (2023).
- [18] D. Gottesman and I. Chuang, Quantum digital signatures, *arXiv preprint quant-ph/0105032* (2001).
- [19] P. Julià Farré, V. Galetsky, M. Belhassen, G. Pieplow, K. Nilesch, H. Boche, T. Schröder, J. Nötzel, and C. Deppe, Secure authentication via quantum physical unclonable functions: A review, *Advanced Quantum Technologies* **9**, e00648 (2026).
- [20] A. Dutta and A. Pathak, A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice?, *Quantum Information Processing* **21**, 369 (2022).
- [21] L. Tsunaki, B. Bauerhenne, M. Xibraku, M. E. Garcia, K. Singer, and B. Naydenov, Ensemble-based quantum token protocol benchmarked on IBM quantum processors, *Quantum Science and Technology* **10**, 10.1088/2058-9565/ae03e6 (2025).
- [22] B. Bauerhenne, L. Tsunaki, J. Thieme, B. Naydenov, and K. Singer, Security analysis of ensemble-based quantum token protocol under advanced attacks, *Quantum Science and Technology* **10**, 10.1088/2058-9565/ae03e7 (2025).
- [23] Y. Strocka, M. Belhassen, T. Schröder, and G. Pieplow, Secure quantum token processing with color centers in diamond (2025), [arXiv:2503.04985](https://arxiv.org/abs/2503.04985) [quant-ph].
- [24] N. P. Kukharchyk, H. Boche, C. Deppe, K. G. Fedorov, M. E. Garcia, I. Gerhardt, R. Gross, T. Halfmann, H. Huebl, D. Hunger, *et al.*, Practical quantum tokens: challenges and perspectives, *Quantum Science and Technology* **11**, 040501 (2026).
- [25] P. A. Grassi, M. E. Garcia, and J. L. Fenton, *NIST Special Publication 800-63-3: Digital Identity Guidelines*, Tech. Rep. (National Institute of Standards and Technology (NIST), 2017).
- [26] D. Gavinsky, D. Gilboa, S. Jain, D. Maslov, and J. R. McClean, Anonymous quantum tokens with classical verification, *arXiv preprint arXiv:2510.06212* (2025).
- [27] A. Behera and O. Sattath, Almost public quantum coins (2024), [arXiv:2002.12438v5](https://arxiv.org/abs/2002.12438v5) [quant-ph].
- [28] R. Radian and O. Sattath, Semi-quantum money, in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (2019) pp. 132–146.
- [29] K. Jiráková, K. Bartkiewicz, A. Černoč, and K. Lemr, Experimentally attacking quantum money schemes based on quantum retrieval games, *Scientific Reports* **9**, 16318 (2019).
- [30] P. Yuen, Noise-tolerant public-key quantum money from a classical oracle, *Quantum* **9**, 1691 (2025).
- [31] O. Shmueli, Public-key quantum money with a classical bank, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (2022) pp. 790–803.
- [32] D. Gavinsky, Quantum money with classical verification, in *2012 IEEE 27th Conference on Computational Complexity* (2012) pp. 42–52.
- [33] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
- [34] H. J. Kimble, The quantum internet, *Nature* **453**, 1023 (2008).
- [35] H. Chen, H. Jia, X. Wu, X. Wang, and M. Wang, Quantum token for network authentication, in *2021 IEEE International Conference on Web Services (ICWS)* (IEEE, 2021) pp. 688–692.
- [36] M. Mendoza Delgado, L. Tsunaki, S. Michaelson, J. Thieme, M. K. Kuntumalla, S. Trofimov, J. P. Reithmaier, K. Singer, A. Hoffman, B. Naydenov, *et al.*, Technological steps for realization of diamond-based quantum tokens, in *International Scientific Conference Management and Engineering* (Springer, 2024) pp. 29–45.
- [37] M. M. Delgado, L. Tsunaki, S. Michaelson, M. K. Kuntumalla, J. P. Reithmaier, A. Hoffman, B. Naydenov, and C. Popov, Impact of annealing and nanostructuring on properties of NV centers created by different techniques, *Diamond and Related Materials* **154**, 112126 (2025).

- [38] A. Molina, T. Vidick, and J. Watrous, Optimal counterfeiting attacks and generalizations for Wiesner’s quantum money, in *Conference on Quantum Computation, Communication, and Cryptography* (Springer, 2012) pp. 45–64.
- [39] D. Nagaj, O. Sattath, A. Brodutch, and D. Unruh, An adaptive attack on Wiesner’s quantum money, *Quantum Information & Computation* **16**, 1048 (2016), originally posted as arXiv:1404.1507.
- [40] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor, Breaking and making quantum money: toward a new quantum cryptographic protocol, arXiv preprint arXiv:0912.3825 (2009).
- [41] S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and A. Lutomirski, Quantum money, *Communications of the ACM* **55**, 84 (2012).
- [42] Federal Office for Information Security (BSI), C. Marquardt, U. Seyfarth, S. Bettendorf, M. Bohmann, A. Buchner, M. Curty, D. Elser, S. Eul, T. Gehring, N. Jain, T. Klocke, M. Reinecke, N. Sieber, R. Ursin, M. Wehling, and H. Weier, *Implementation Attacks against QKD Systems*, BSI Project Report 575 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023).
- [43] Wikipedia contributors, XZ Utils backdoor, https://en.wikipedia.org/wiki/XZ_Utils_backdoor (2024), wikipedia, The Free Encyclopedia. Accessed: March 31, 2026.
- [44] Chainalysis, 2025 crypto theft reaches \$3.4 billion, <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/> (2025), chainalysis 2026 Crypto Crime Report. Accessed: March 31, 2026.
- [45] S. Lyngaas, North Korean hackers bug software used by thousands of US companies in potential crypto heist attempt, CNN Politics (2026), accessed: April 7, 2026.
- [46] A. Broadbent, R. A. Kazmi, and C. Minwalla, A quantum vault scheme for digital currency, in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Vol. 1 (IEEE, 2024) pp. 239–249.
- [47] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, *Quantum computing with Qiskit* (2024), arXiv:2405.08810 [quant-ph].
- [48] L. Tsunaki *et al.*, Github repository: Quantum vault, https://github.com/lucas-tsunaki/quantum_vault (2026).
- [49] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Information* **2**, 1 (2016).
- [50] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent, and D. Pitalúa-García, Multiphoton and side-channel attacks in mistrustful quantum cryptography, *PRX Quantum* **2**, 030338 (2021).
- [51] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O’Brien, Quantum error mitigation, *Rev. Mod. Phys.* **95**, 045005 (2023).
- [52] L. Tsunaki, M. Dotan, K. Volkova, and B. Naydenov, Quantum gates via dynamical decoupling of a central qubit on IBMQ and ^{15}N -vacancy centers in diamond, *Phys. Rev. A* **113**, 042627 (2026).
- [53] X.-M. Hu, Y. Guo, B.-H. Liu, C.-F. Li, and G.-C. Guo, Progress in quantum teleportation, *Nature Reviews Physics* **5**, 339 (2023).
- [54] L. Tsunaki, A. Singh, S. Trofimov, and B. Naydenov, Digital twin simulations toolbox of the nitrogen-vacancy center in diamond, *Advanced Quantum Technologies* **9**, e00691 (2026).
- [55] W. Li, H. Sun, Y. Liu, T. Li, and R.-B. Wu, Flying-qubit control: Basics, progress, and outlook, *Advanced Devices & Instrumentation* **5**, 0059 (2024).
- [56] S. M. Barnett, A. Chefles, and I. Jex, Comparison of two unknown pure quantum states, *Physics Letters A* **307**, 189 (2003).
- [57] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, Stabilization of quantum computations by symmetrization, *SIAM Journal on Computing* **26**, 1541 (1997).
- [58] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, Quantum fingerprinting, *Physical Review Letters* **87**, 167902 (2001).
- [59] H. Nishimura, A survey: SWAP test and its applications to quantum complexity theory, in *Algorithmic Foundations for Social Advancement: Recent Progress on Theory and Practice* (Springer, 2025) pp. 243–261.
- [60] A. Çakan, V. Goyal, F. Kitagawa, R. Nishimaki, and T. Yamakawa, Multi-copy security in unclonable cryptography, in *Advances in Cryptology – CRYPTO 2026* (2026) to appear; also accepted at QCRYPT 2026. Originally posted as arXiv:2510.12626.
- [61] B. Efron and R. J. Tibshirani, *An Introduction to the Bootstrap*, Monographs on Statistics and Applied Probability No. 57 (Chapman and Hall/CRC, New York, 1993).
- [62] M. AbuGhanem, IBM quantum computers: evolution, performance, and future directions, *The Journal of Supercomputing* **81**, 687 (2025).
- [63] A. Çakan, V. Goyal, and T. Yamakawa, Anonymous public-key quantum money and quantum voting, in *Advances in Cryptology – CRYPTO 2026* (2026) to appear; also presented at QIP 2025 and QCRYPT 2025. Originally posted as arXiv:2411.04482.
- [64] S. Ben-David and O. Sattath, Quantum tokens for digital signatures, *Quantum* **7**, 901 (2023).
- [65] M. Fanizza, M. Rosati, M. Skotiniotis, J. Calsamiglia, and V. Giovannetti, Beyond the SWAP test: optimal estimation of quantum state overlap, *Physical Review Letters* **124**, 060503 (2020).
- [66] M. E. Limes, N. Dural, M. Romalis, E. Foley, T. Kornack, A. Nelson, and L. Grisham, Long spin-1/2 noble gas coherence times in mm-sized anodically bonded batch-fabricated ^3He - ^{129}Xe - ^{87}Rb cells, *Applied Physics Letters* **126** (2025).
- [67] F. Allmendinger, P. Blümler, M. Doll, O. Grasdjik, W. Heil, K. Jungmann, S. Karpuk, H.-J. Krause, A. Offenhäuser, M. Repetto, *et al.*, Precise measurement of magnetic field gradients from free spin precession signals of ^3He and ^{129}Xe magnetometers, *The European Physical Journal D* **71**, 98 (2017).
- [68] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, Trapped-ion quantum computing: Progress and challenges, *Applied Physics Reviews* **6** (2019).
- [69] P. Jessen, I. Deutsch, and R. Stock, Quantum information processing with trapped neutral atoms, *Quantum Information Processing* **3**, 91 (2004).
- [70] G. Thiering and A. Gali, Chapter one - color centers in diamond for quantum applications, in *Diamond for Quantum Applications Part 1*, Semiconductors and Semimetals, Vol. 103, edited by C. E. Nebel, I. Aharonovich, N. Mizuochi,

- and M. Hatano (Elsevier, 2020) pp. 1–36.
- [71] R. J. D. Tilley, Color centers, in *Encyclopedia of Color Science and Technology*, edited by R. Luo (Springer New York, New York, NY, 2014) pp. 1–9.
 - [72] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup, and C. von Borczyskowski, Scanning confocal optical microscopy and magnetic resonance on single defect centers, *Science* **276**, 1212 (1997).
 - [73] A. Kent, S-money: virtual tokens for a relativistic economy, *Proceedings of the Royal Society A* **475**, 20190170 (2019).
 - [74] A. Kent, D. Lownes, D. Pitalúa-García, and J. Rarity, Practical quantum tokens without quantum memories and experimental tests, *npj Quantum Information* **8**, 28 (2022).
 - [75] M. C. Pena, J.-C. Faugère, and L. Perret, Algebraic cryptanalysis of a quantum money scheme the noise-free case, in *IACR International Workshop on Public Key Cryptography* (Springer, 2015) pp. 194–213.
 - [76] S. L. Braunstein and C. M. Caves, Statistical distance and the geometry of quantum states, *Physical Review Letters* **72**, 3439 (1994).
 - [77] J. C. Garcia-Escartin and P. Chamorro-Posada, SWAP test and Hong-Ou-Mandel effect are equivalent, *Physical Review A* **87**, 052330 (2013).
 - [78] J. A. Nelder and R. Mead, A simplex method for function minimization, *The Computer Journal* **7**, 308 (1965).