Semi-device-independent quantum money

Karol Horodecki\textsuperscript{1,2,4} and Maciej Stankiewicz\textsuperscript{3}

\textsuperscript{1} Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland
\textsuperscript{2} International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland
\textsuperscript{3} Institute of Mathematics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland
\textsuperscript{4} Author to whom any correspondence should be addressed.

E-mail: khorodec@inf.ug.edu.pl and maciej@stankiewicz.edu.pl

Abstract
The seminal idea of quantum money, not forgeable due to laws of Quantum Mechanics, proposed by Stephen Wiesner, has laid the foundations for the Quantum Information Theory in the early ’70s. Recently, several other schemes for quantum currencies have been proposed, all, however, relying on the assumption that the quantum source device, acts according to its specification. This makes several known quantum money protocols vulnerable to the so-called hardware Trojan horse attacks. We, therefore, study the following problem: to what extent quantum money schemes can be made independent from the inner working of source and verification-devices used by the honest parties (bank and mint) in creating and processing the quantum money? Drawing inspirations from the semi-device-independent quantum key distribution protocol, we introduce the first scheme of quantum money with this assumption partially relaxed, along with the proof of its unforgeability. Finally, we formulate and discuss a quantum analog of the Oresme–Copernicus–Gresham’s law of economy, that may hold in the future.

1. Introduction
Quantum Information Science originates from the seminal idea of the scheme of quantum money due to Stephen Wiesner [1]. According to his brilliant concept, the randomly polarized photons could, in principle, represent the banknote, while the Bank’s secret key represents the random choices of polarization. During verification, the Bank checks and accepts the banknote if the photons appear to be polarized as they have been designed and rejects otherwise. Although it is rather intuitive that due to quantum no-cloning [2–4] the banknote cannot be forged without disturbing it, this scheme, has been proven to be secure against counterfeiter only recently [5, 6]. Wiesner’s scheme bases firmly on the assumption that measurements of the verification are performed according to the specification. Dmitry Gavinsky [7] has designed a protocol powerful enough to drop this assumption. However, the security of the latter relies on the functioning of the device manufacturing banknotes (called here source), which is at the disposal of (otherwise trusted) mint.

1.1. A threat model—hardware Trojan horse attack on quantum money
We go a step further, considering not only the verification device but also the source device as potentially untrusted, implemented by some adversary. This approach involves three parties: mint, bank, and a counterfeiter. They also possess the banknote and several devices. The banknote is a classical-quantum state of physical memory, shared between Bank and counterfeiter’s wallet. A source-device (the device which produces a banknote) is at hand of the mint. Verification-device (a measurement device) and software that handles the usage of the devices is at the disposal of the counterfeiter whenever he wants to get a banknote to go through the verification process. The mint is honest, so it delivers the correct number of banknotes at a wish of the Bank according to the specification of the source device. Naturally, the Bank is also considered to be fully honest in all respects. Crucially, we consider the source-device and the verification-device as untrusted. It means that these
devices may not work according to official specifications and are manufactured by some adversary in order to produce malformed banknotes. The counterfeiter is untrusted, and we consider that he may be aware of the inner workings of the source and terminal devices. In that, for reducing the number of actors, he can be considered to be an adversary himself. We consider then Bob, who is in the bank, and Frederick, who is the counterfeiter. When describing the honest implementation of the scheme, we also consider Alice as the honest client. When we pass to the proof, with a little abuse of notation, we consider, however, that she might collaborate with Frederick.

1.2. Motivation—the hacker’s and cryptanalyst’s point of view
Before going into details, it is crucial to ask if the above scenario is indeed a one that can happen in real life, which would yield a direct motivation. At first thought, according to the traditional understanding, the whole mint is trusted, including all machines involved in the process of minting. However, the first thing to note is that the quantum money scheme is, in fact, a cybersecurity-based way of representing cash. We then observe the hidden assumption that mint’s devices are honest, need not be practical from the perspective of cybersecurity. Following this, we describe the motivation from both the hacker’s and the cryptanalyst’s point of view.

First, from the hacker’s perspective, considering the mint using the untrusted device is equivalent in cybersecurity language to finding the way to protect the mint (and so the Bank and honest clients) against a Trojan-Horse attack. Indeed, the source-device can be either (i) composed from parts designed with backdoors impossible to check by eye inspection or (ii) designed in a way open to security loopholes. Regarding (i), introducing backdoors in microchips on the physical level of their manufacturing has been recently demonstrated by an attack on random number generator [8]. Regarding (ii) exploiting the loopholes is the new area of successful experimental research aimed at hacking particular implementations of the quantum key distribution devices [9]. With these examples, mentioning the fact that the manufacturing process can be infected by classical viruses seems then unnecessary.

The problem of designing an unforgeable scheme of quantum money belongs to the class of problems from two-party cryptography (the trusted Bank can not trust clients who can be counterfeiters). Moreover, from the cryptoanalyst’s perspective, any security proof is based on a set of assumptions. Finding an answer to the question what is the minimal set of assumptions that assure the same functionality? is then a practical application of Ockham’s Razor principle commonly adopted in cryptography. Indeed, the quantum (or super quantum) device-independent information processing exemplifies it very well [10, 11]. The first protocol of quantum key distributions trusted all the inner working of the involved devices [12]. However, it turns out that one need not assume that these devices are produced according to specifications. They need not also be tested as being so since one can achieve the same goal (with a small price of lowering the key rate) without these assumptions. It has been demonstrated by the quantum device-independent security proofs [11]. The fewer assumptions a proof bases on, the more independent of the device the proof is. Any proof based on less number of assumptions about the inner working device than the fully device-dependent one is called now a semi-device-independent one [13].

We adopt this approach and terminology to study the problem: to what extent quantum money schemes can be made independent from the inner working of source and verification-devices used by the honest parties (Bank and mint) in creating and processing of the quantum money? As we will see, in the case of the problem presented above, the answer leading to narrowing the assumptions can be provided.

1.3. Results
The main result presented here is a novel money scheme, secure against a broad class of joined attacks of the source quantum device and testing device. It can be viewed as a modification of the testing procedure of the original Wiesner’s scheme both in measurement setup, as well as interpretation of the measurement results. We prove the security of the proposed scheme using strictly fewer assumptions than the original one.

To see this more precisely, let us briefly recall what Wiesner’s scheme takes for granted. These are (i) dimension of each subsystem of a banknote (register of qubits), (ii) tensor product structure of both the banknote’s state and the measurements for testing, (iii) state of each qubit of the banknote is from the set \{0, 1, +, –\}, and the measurements that are done on each of the qubits are projections in either classical \{0, 1\} or superposed basis \{+\}, \{–\}.

In our semi-device-independent approach, the assumptions (i)–(ii) are kept. However, we assume neither state of each qubit (each qubit of a banknote’s register can be prepared differently), nor the form of measurement (each qubit can be verified due to some unknown measurement strategy, including a POVM). These two relaxations express our lack of trust towards source-device and verification-device, respectively.

An honest implementation of the banknote’s state in our scheme is the same as in the original Wiesner’s scheme. However, because the source-device is untrusted, an arbitrary state of the form: 
shared between the Bank’s branch and Alice, that can pass certain test, is a valid banknote. (Here for simplicity a single Bank’s branch is shown and we omit the obvious serial number.) The $\rho_{y}^{(i)}$‘s are arbitrary states of qubits.

The idea of the verification in our scheme can be phrased in terms of a game. When Alice wants to get her banknote verified at some Bank’s branch, the branch sends a random bit-string of length $n$ to Alice. She should then give a correct answer (i.e. win the game) in as many as possible runs among all $n$. To this end, she can measure qubits of the banknote (via the tensor product of arbitrary measurements) subsequently and send corresponding answers. If the number of correct answers is high enough, the banknote is accepted as valid.

As a specific choice of a game, we base on the one used in [14], also known as a Random Access Code game [15]. Adapted to the case of our scenario, it is as follows. Alice is asked to guess correctly a randomly chosen bit ($y_0$ or $y_1$), out of the two that form the Bank’s part of the banknote (for each $i \in \{1, \ldots, n\}$). Alice correctly guesses the value of the bit chosen by the Bank’s branch as many times as possible. An important aspect of this game is that it encapsulates the so-called dimension witness [16, 17]. It is a test assuring a lower bound on the dimension of the physical system. Enough number of guesses implies, in particular, that the system held by Alice (i.e. quantum part of the banknote) was not classical (excluding thereby trivial vulnerability to forging). Other important consequences of this fact are discussed further.

Crucial to our scheme was to find the threshold number $\theta n$ of correct answers that imply acceptance. In that we base on a simple idea, that (roughly speaking) a finite-dimensional quantum system can not encode too many logically independent classical bits (call it a dimension constraint). A formal statement with the above meaning, used in [14], originates from [18] (see also [19]). In their case, a qubit can not hold both the value of two independent bits. The threshold $\theta$, we design then to satisfy an inequality:

$$\theta n \equiv \# \text{ of correct answers in the game}$$

$$> \frac{1}{2} \left\{ \# \text{ of all possible correct answers in the game played twice} \right\}. \quad (2)$$

The fact that given the above condition, the same banknote will not get accepted twice comes then from an observation that there are no two disjoint parts of anything containing each more than its half. In our case of the number of correct guesses. We can place a non-trivial bound on the threshold $\theta$, for the following reason. Trying to get accepted a banknote twice, Alice is visiting two different branches (the first one legally, and the second as a forgery called here Frederick). It implies playing the Random Access Code game twice. She would be then asked (with high probability) in half of the times for an answer that requires knowledge of two independent bits, which is, however, impossible due to the mentioned dimension constraint—each answer can be based on a single qubit only. It visualizes how our scheme differs from the original Wiesner’s one. We do not require the banknote to be the same as it was manufactured. Instead, the number of correct answers matters, as we do not assume prior knowledge about particular states of each of the qubits of the banknote.

On the one hand, the verification procedure almost coincides with the preamble (testing part of) the SDI QKD protocol of [14] so that one might think, that security of the money scheme should follow from the security of the SDI QKD. However, the relation between the SDI QKD of [14], and the proposed here money scheme is not that direct, due to the difference between the mentioned security scenarios. In the QKD scenario, Bob trusts Alice, and there is also a eavesdropper Eve. Contrary to this, the money scheme is a two-party cryptographic scenario: the Bank does not trust Alice (as she can come twice or collaborate with Frederick). To some extent action of Frederick can be viewed as the action of Eve, however only partially, as Alice can freely collaborate with Frederick, which is not the case in the QKD scenario, where she does not help Eve.

The relation between the SDI QKD and the SDI quantum money scheme is rather due to the fact that security proof for both schemes can be based on the same concepts: the dimension constraint and dimension witness. Regarding the idea of dimension witness contained in the Random Access Code game, it implies that the key can not be trivially copied on the way by Eve as the classical key could be, as well as it plays a role in that the banknote can not be trivially forged (as it is not classical). Regarding the dimension constraint, it implies both the proper balance between mutual information functions ($I(A:B) - I(A:E > 0)$ for the key generation and, as we show, a threshold shown in equation (2), which is the base for our money scheme. The latter two facts are otherwise unrelated as it is reflected by the fact that the threshold parameter in our scheme $\theta \approx 0.8475$ differs from the threshold that enables key generation that approximately equals 0.8415.

Straightforward as it is, we find instructive to demonstrate also three malicious source-devices which, along with proper verifying-device, can get a malformed banknote accepted. We show that both Wiesner’s and Gavinsky’s schemes are vulnerable to all three attacks. We focus on the third attack and prove the security of the presented scheme. Although the assumptions behind our scheme may still be considered as numerous and,
therefore, a strong set, they appear to be not too far from optimal. It is because, as it is easy to observe, the fully device-independent security proof of quantum money scheme cannot hold. We will discuss it in the latter part of the paper.

Finally, motivated by many proposed quantum currencies, we study a possible consequence of the coexistence of at least two legitimate quantum payment schemes. It is long known that whenever there are two types of money: those with high intrinsic value and those with lower intrinsic value, and both are valid (e.g. as currencies), then people tend to spend the latter ones while keeping the former. This fact was observed and formulated as a law of economy, known today as Gresham’s law, stated as follows: ‘Bad money drives out good’. We formulate the quantum analog of this statement, which says: ‘Bad quantum money drives out good quantum one’. It summarizes the consequences of the attack on the intrinsic value of money, which for historical reasons described further, we call Quantum Oresme–Copernicus–Gresham’s law. Whether such law will happen to hold is hard to predict as of now. We propose then, to initiate a discussion on the quantum intrinsic value of the quantum money schemes. It is because the intrinsic value of a quantum currency may be attributed in a much different way than the intrinsic value of a classical one.

The manuscript is organized as follows. In section 2, we review previous quantum money schemes both in private-key and public-key settings. In section 3, we show three different attacks on existing quantum money schemes and briefly discuss that a fully device-independent quantum money scheme cannot exist. In section 4, we present the main results of that work, stating a scheme for semi-device-independent quantum money. In section 5 we discuss a possible quantum analog of the Oresme–Copernicus–Gresham’s law. We conclude in section 6 by comparing our scheme to the existing ones (see 6.1), discussing the technological difficulties in possible implementation (see 6.2), and summarizing the paper with some interesting open problems (see 6.3). Additionally, in appendices A–C we present a rigorous security proof of the scheme, show that it is impossible to create fully device-independent quantum money scheme in appendix D, briefly describe honest implementation in appendix E, and discuss the amount of required memory in appendix F.

2. Previous works

An idea of quantum money proposed by Stephen Wiesner was, to our knowledge, the first application of the quantum effects to the information-theoretic, in fact, cryptographic task. In this section, we will discuss the previous research on this topic using division into private and public-key quantum money suggested by Aaronson [20, 21]. In the private-key quantum money schemes, only the mint itself can verify the banknote. It is worth to notice that in case of private-key quantum money schemes, the Bank and the mint can be treated together as one party. We can do this since the Bank can create money from the secret key needed for verification. On the other hand, in the public-key quantum money schemes, anyone can verify the banknote using publicly available verification procedure, but still, no one, except the mint, cannot copy or create a new banknote. We will conclude by giving (in figure 1) a comprehensive comparison of different classical and quantum money schemes together with their security assumptions.

2.1. Private-key quantum money

Around 1970 Stephen Wiesner suggested the first scheme of unforgeable quantum money. Unfortunately, his paper was rejected a few times and finally was published in 1983 [1]. Even though Wiesner claimed that the protocol is unconditionally secure, a full proof for the most generalized attacks was presented by Molina et al in 2013 [5].

Because the scheme requires the mint to maintain a massive database for all produced bills, Bennet et al [22] proposed a modification of the protocol, using a cryptographic pseudorandom function, to decrease the needed amount of the memory. The question if it is possible to reduce the database size without imposing any computational assumptions was analyzed by Aaronson [20]. Later he formally proved that the answer is negative and stated the so-called Tradeoff theorem for Quantum Money [23].

Although the above schemes are secure in a regime in which the mint destroys the verified banknote, it is dangerous when we allow to retrieve the bill after verification. So-called interactive attacks were independently proposed by Aaronson [21] and Lutomirski [24]. Even more sophisticated version of the interactive attack, based on the idea of Elitzur–Vaidman bomb tester, was later suggested by Nagaj et al [25].

The scenarios mentioned above require visiting the mint (or at least having a secure quantum channel), so Gavinsky suggested a version of quantum money with classical verification [7]. It is essential to notice that in Gavinsky’s scheme, the Bank does not need to trust the measurement device. Such types of schemes are commonly called measurement-device-independent. Another similar scheme was also presented by Georgiou and Kerenidis [26].
Additionally, Pastawski et al [6] and, more recently, Amiri and Arrazola [27] analyze the more realistic scenario in the presence of noise and errors. It is also worth to mention about fundamentally different approaches aimed at anonymity. Mosca and Stebila [28], (see also Tokunaga et al [29]) proposed quantum coins in such a way that all coins are identical. Their scheme uses a black-box model that makes thorough security analysis difficult.

Furthermore, Selby and Sikora [30] analyzed unforgeable money in the Generalized Probabilistic Theories. We should also point out experimental results in the quantum money field were presented by three groups of Bartkiewicz et al [31], Bozzio et al [32], and Guan et al [33] respectively. Although the theoretical schemes are secure, in the case of real-life, more practical implementation, new vectors of attack could appear. For example, Jiráková et al [34] show an attack on quantum money implementation.

Soon after the first version of this paper was published on arXiv preprints repository, Bozzio et al [13] presented the result with a similar title 'Semi-device-independent quantum money with coherent states'. Their result requires stronger security assumptions (trusted source device) but is more focused on realistic implementations.

Also, recent paper by Kumar [35] introduces novel quantum money protocol with very high tolerance to noise.

Finally, during the review process of our work Radian and Sattath proposed scheme called 'Semi-Quantum Money' [36]. The Authors of the latter article propose the scheme that achieves similar goals by allowing the mint only to perform classical operations. This approach is, however, based on computational assumptions, while in the present article, we focus on what can be achieved without such.

2.2. Public-key quantum money

The biggest drawback of all private-key quantum money schemes is that only the mint can verify the bill. In order to improve this, an idea of public-key quantum money was invented. In that approach, not only the mint but anyone, even untrusted party, could verify the quantum banknote without communication with the mint. General formulation of the public-key quantum money was presented by Aaronson [21], and later, its security was analyzed by Aaronson and Christiano [37].

Following these seminal results, many candidates for the private-key quantum money scheme was presented. The first such scheme, based on stabilizer states, was proposed by Aaronson [21], but it was later broken by Lutomirski et al [38]. There were also some attempts exploring an idea of local Hamiltonian problem.
that can also be broken using a single-copy tomography presented by Farhi et al [39]. Another idea, based on the
knot theory, was proposed by Farhi et al [40]. It remains unbroken, but there is no full security proof.

Until now, more papers concerning the public-key quantum money or an analysis of its security were
published that we should point out here [41–43].

In the most recent work, Zhandry [44] proved that if the injective one-way functions and an
indistinguishability obfuscator exist, then the scheme of the public-key quantum money exists. Furthermore, he
shows how to adapt the Aaronson and Christiano’s scheme [37] using these assumptions to get the secure
public-key quantum money.

We should also mention ongoing research on the decentralized quantum currencies. First Jogenfors [45]
proposed Quantum Bitcoin that connects ideas of quantum money and classical blockchain system like the one
used in Bitcoin. Later Ikeda [46] presented another approach called qBitcoin based on quantum teleportation
and a quantum chain instead of the classical blocks. Also, Sun et al [47] proposed a cryptocurrency called
qulogicoin, based on another version of the quantum blockchain. Recently Adrian Kent proposed a concept of
‘S-money’ [48], and Kane created a new money scheme based on modular forms [49]. Finally, Andrea
Coladangelo proposed a decentralized, blockchain-based, hybrid classical-quantum payment system [50],
strengthening the quantum lightning scheme.

3. Motivations

In this section, we first demonstrate simple attacks on some of the private-key quantum money schemes,
including Wiesner’s and Gavinsky’s ones, which are based on the cooperation of the untrusted quantum source
device and the counterfeiter. Next, we discuss why it is impossible to make a fully device-independent money
scheme in section 3.2.

3.1. Simple joined attacks: when the quantum source device and counterfeiter collaborate

We aim to demonstrate that both the original Wiesner’s scheme and that of Gavinsky are vulnerable to the
joined attack. Moreover, the attack is general enough to apply to other private-key quantum money schemes, as
it bases on dropping important security assumption: the privacy of the key. Before presenting the attacks we
recall how an honest source prepare the state:

$$
\sum_{(b,v) \in \{0,1\}^2} \frac{1}{4^k} |b, v \rangle \langle b, v | \rightarrow \text{honest}
$$

$$
\sum_{(b,v) \in \{0,1\}^2} \frac{1}{4^k} |b, v \rangle \langle b, v | = |W_{h, b,v} \rangle \langle W_{h, b,v} |
$$

where $\rho_k^W \in \{ |0,0 \rangle, |0,1 \rangle, |1,0 \rangle, |1,1 \rangle \}$, the bit-string $b$ tells the (random) choice of basis, while $v$ corresponds to
outcomes. In the original money, only the system $W$ contains banknote’s state.

Now we are ready to show here three attacks of different types. The first one enlarges the memory of the
banknote, the second one uses additional entanglement, and the third makes it a classical state. The first reduces
to simple imprinting of the secret key of the Bank directly in banknote’s state. It is at the expense of enlarging
dimension of its quantum memory:

$$
\sum_{(b,v) \in \{0,1\}^2} \frac{1}{4^k} |b, v \rangle \langle b, v | \rightarrow \text{attack}_b
$$

$$
\sum_{(b,v) \in \{0,1\}^2} \frac{1}{4^k} |b, v \rangle \langle b, v | = |W_{a, b,v} \rangle \langle W_{a, b,v} | \otimes |bH \rangle \langle bH |
$$

The mistrustfully prepared banknote has an additional ‘hidden’ register $H$ enabling the attack. This register
can be used to generate an unlimited number of identical banknotes via repetitive von Neumann measurement
of the system $W$ in the basis indicated by vector $|b \rangle \langle b |_H$. Allowing for such a strong attack, one can imagine that in
principle, the whole string $|b \rangle, \langle b |$ could also be imprinted in money’s memory at the price of doubling it.
However, imprinting $|b \rangle \langle b |$ is enough. The operation of copying such a ‘banknote’ can pass unnoticed from the
point of view of the honest Client. From this trivial example, we have then learned that when the dimension of
the banknote is unbounded, its security against forgery is compromised.

The second attack does not require extra memory in the banknote’s state but makes use of an additional
entanglement between adversary and the untrusted source device. Instead of preparing one from the four honest
states $\{ |0,0 \rangle, |0,1 \rangle, |1,0 \rangle, |1,1 \rangle \}$, the source performs locally one from the four Pauli unitaries on a half of a singlet and
sends it as a money state. Later the adversary performs global Bell measurement on the whole two-qubit system.
That procedure, based on superdense coding [51], allows him to obtain both parts of the secret key and prepare
an arbitrary number of valid banknotes.

In the third one, the untrusted quantum source device and the counterfeiter can attack jointly without
increasing the memory of the banknote and without any additional entanglement, by using only classical states
(diagonal in a single basis):
In each run, right before the measurement is physically done, the measurement device is given the type of basis \( b \) taking value 0 in case of \( \{ \uparrow, \downarrow \} \) and 1 for \( \{ \uparrow, \downarrow \} \). It can then safely output the value \( v \) of \( H_\uparrow \) as a good answer. The two bits that cannot be encoded in 1 qubit are split into measurement type \( v \) and 1 for \( \{ \uparrow, \downarrow \} \) and 1 for \( \{ \uparrow, \downarrow \} \).

\[
\sum_{(b,v) \in \{0,1\} \times \{0,1\}} \frac{1}{4} \left| b, v \right\rangle \left\langle b, v \right| \rightarrow \text{attack}, \quad \sum_{(b,v) \in \{0,1\} \times \{0,1\}} \frac{1}{4} \left| b, v \right\rangle \left\langle b \otimes \downarrow \right| \left\langle H_\uparrow \downarrow \right|.
\]

3.2. Impossibility of fully device-independent quantum money

In this section, we will show that it is impossible to create a fully device-independent money scheme. We will prove this in a scenario where the Bank has at least two branches that do not communicate during the verification phase. In the device-independent approach, both source and measurement devices are untrusted, and there are no restrictions on state dimension or additional entanglement, as opposed to the semi-device-independent approach that we will present in the next sections. On the other hand, we allow all Bank’s branches to have shared randomness that can be used both in the state preparation and verification phases. We also assume that the no-signaling condition is fulfilled, and post-processing is honest, which is the standard approach in most device-independent protocols.

**Observation 1 (No-go for device-independent quantum money).** It is impossible to create a fully device-independent money scheme with untrusted source and measurement devices that could be produced by an adversary.

Intuitively it is easy to see that we can break any money scheme using appropriate modification of the first attack from the previous section. Indeed, without communication between Bank’s branches, a malicious quantum source device can always prepare two copies of the banknote in such a way that both will pass verification in different branches. The only way a branch can verify the banknote is to check correlations with the client’s banknote. It is impossible to ensure that the verification will influence, or give knowledge about, correlations of another branch with a different malicious copy of the banknote. To justify these intuitions, we will provide more formal proof of the above theorem in appendix D.

Because of the impossibility result, we can ask how close one can go toward the device-independent approach. We partially answer this question by providing in the next section our main contribution, the semi-device-independent quantum money scheme. It requires weaker assumptions than any previous one. We prove its security against a broad class of essential attacks and conjecture that it is also secure in the general case.

4. Main result

In this section, we present the main result of our work. We first describe the scheme for semi-device-independent quantum money in section 4.1. Next, we compare our money scheme with the corresponding SDI QKD protocol of Pawłowski and Brunner, that we use as a base (see section 4.2). Finally, in section 4.3 we show the idea of the proof, details of which are presented in the appendices.
4.1. Semi-device-independent quantum money protocol

Motivated by the fact that joined attacks can compromise the security of some private-key quantum money schemes, we will show a partial solution to this problem. In this section, we present a scheme for semi-device-independent private-key quantum money. The concept of a semi-device-independent quantum key distribution was discovered by Pawłowski and Brunner [14]. In that scheme, the sender has to trust neither the quantum source nor the measuring device. Instead, there are two nontrivial assumptions about the states sent to the receiver. Firstly, the states have limited dimensions and, secondly, there is no entanglement between the states and the adversary. See figure 2.

Our scheme of money is similar to the SDI QKD scheme and has the assumption that each state that is sent from the sender to the receiver is a qubit (have dimension \(d = 2\)). In order to introduce both the concept and notation, it is instructive to recap the semi-device-independent quantum key generation protocol [14] briefly. The key is produced as follows. The sender sets up \(n\) pairs of random bits \((y_0^i, y_1^i)_{i=1}^n\). In each run of the experiment, \(i \in [n] = \{1, \ldots, n\}\), upon pressing the correct button sender’s device produces an untrusted state \(\rho_{y^i}^\prime\), which is assumed to be a qubit, and sends it to the receiver. The receiver’s device is fully untrusted. It measures the state in an arbitrary manner (perhaps knowing state’s preparation), yet upon a (random) input \(x^i\), it has to output a bit \(a^i\), which equals \(y^i\). In the classical case, the maximum success probability of guessing the bits of the sender is only \(3/4\), while in quantum case, it is \(P_q = \cos^2(\pi/4) \approx 0.8536\). If the guessing probability is larger than a certain value, the secure key can be established.

We are now ready to introduce our money scheme. In the SDI quantum money scheme, one branch of the Bank (mint) plays the role of the sender, while the client Alice is the receiver.

- **Money generation protocol.** In order to create the money, all \(k\) branches of the Bank have to possess common secret randomness (secret key) that is later stored in classical memories of the branches. Each portion of the bits \((y_0^i, y_1^i)_{i=1}^n\) of this key is associated to some serial number of a separate banknote \(SN\) in advance. (Note that the secret key can be obtained for example by measurement on the shared 2\(n\) GHZ states [52] or by encrypted classical communication.) To generate a quantum state of the banknote associated to the number \(SN\) one branch \(B_i\) (in practice the closest to Alice branch that can perform the function of the mint, i.e. posses quantum source devices) uses \((y_0^i, y_1^i)_{i=1}^n\) associated with this \(SN\) as a sequence of inputs to its untrusted quantum source devices \((S^i)_{i=1}^n\). The latter devices, in turn, generates \(n\) qubits \((\rho_{y^i}^\prime)\) that together form the quantum state of the banknote

\[
\bigotimes_{i=1}^n \rho_{y^i}^\prime.
\]  

The above state is sent to Alice’s wallet (dedicated quantum memory device). In the end, the banknote, i.e. the joined state of \(k\) branches of the Bank and Alice’s wallet takes the form:

\[
\sum_{(y^0, y^1)^k \in \{0,1\}^{2k}} |y_0^1\rangle|y_1^1\rangle \otimes \cdots \otimes |y_0^k\rangle|y_1^k\rangle \otimes \left(\bigotimes_{i=1}^n \rho_{y^i}^\prime\right).
\]  

- **Money verification protocol at the Bank.** In order to verify the money Alice comes to any branch of the Bank denote as \(B_i\). The branch \(B_i\) generates a question bit-string \((x^i)_{i=1}^n\), inputs the bits to the untrusted measurement devices \((M^i)_{i=1}^n\) and collects the output bit-string \((a^i)_{i=1}^n\). For a total data represented by a string of tuples: \(S_i = (y_0^i, y_1^i, x^i, d^i)_{i=1}^n\) the branch \(B_i\) accepts it if the following condition is satisfied:

\[
X_d(S_i) := |\{i \in [n]: a^i = y^i\}| \geq \theta n,
\]  

i.e. the number of correct guesses is above the threshold value \(\theta n\) and rejects otherwise.
Apart from the above scheme, the second main result (see theorem 1) is the proof that $q \approx 0.8475$ will assure the security of the money scheme within considered set of assumptions. More precisely, in real-life application, one should consider the value of threshold to be a bit larger, $q = (1/2 + \eta) + 2\eta$, where $M = (5 + \sqrt{5})/4$ and $\eta$ depends on $n$ (taking care of possible fluctuations of the number of guesses).

Figure 3. $B_1, \ldots, B_B$ represents arbitrary number of Bank’s branches that share common randomness $y = (y_1^n, y_B^n)$ stored in the classical memories. Branch $B_i$ inputs the string $y$ into untrusted source device $S$ and sends the generated $n$ quantum systems $\rho_y = \bigotimes_{i=1}^{n} \rho_{y_i}$ to Alice’s memory. When Alice wants to verify the money she visits some branch $B_i$. This branch generates random binary string $x = (x_i^n)$ of length $n$ and feeds as an input to untrusted measurement devices of the terminal $M = (M_i^n)^n$, which generates a string $a = (a_i^n)$. The branch then count in how many rounds game was won and accepts the banknote as valid or rejects it dependently on whether the condition from equation (8) was met.

Figure 4. The procedure of generation and verification of a single banknote in the SDI quantum money scheme. The $n$ untrusted source devices independently produce qubit states $\rho_{y_i}$ that form in total the banknote that is kept in Alice’s wallet and is exposed to the counterfeiting by her or Frederick (or even both). The verification of the banknote is done by $n$ independent (not necessarily identical) untrusted parts of a verification terminal, each checking if $a_i = y_i$ (i.e. if its output is equal to one of the two bits of Bank’s note at run $i$ chosen randomly as $x_i$). The banknote gets accepted if the number of correctly guessed bits exceeds $\theta n$ with

$$\theta = 2\eta(1/2 + \eta) + M(1/2 + \eta) + 2\eta,$$

where $M = (5 + \sqrt{5})/4$ and $\eta$ depends on $n$ (taking care of possible fluctuations of the number of guesses).

Apart from the above scheme, the second main result (see theorem 1) is the proof that $\theta \approx 0.8475$ will assure the security of the money scheme within considered set of assumptions. More precisely, in real-life application, one should consider the value of threshold to be a bit larger, $\theta = 0.8475 + 2.6950\eta$, depending on how small the probability of error, i.e. forgery one would like to tolerate. It is however proven (see theorem 1) to be exponentially small in the length of the banknote, scaling as $O(\exp(-2\eta^2(1/2 - \eta)n))$.

- **Money verification protocol at a distance.** Alice establishes an authenticated connection for classical communication with some (arbitrary) branch $B_i$ of the Bank. The $B_i$ gives her random inputs $(x_i^n)$, that she should use together with her quantum state from the memory of her wallet as inputs to the untrusted terminal (her own, or, e.g. the one operated by a seller in a shop). The classical output $(a_i^n)$ from the device (possibly modified by Alice to $(a_i^n)$) is then sent to $B_i$ that checks if the data $(y_0^n, y_1^n, x_i, a_i^n)$ are acceptable if inequality (8) holds, and rejects it otherwise.

For the sake of clarity, the whole process of the creation and the verification of the semi-device-independent quantum money is illustrated in figure 3 (for the general scheme with many branches) and figure 4 (for the creation and verification). Generation and verification protocols are also summarized in tables 1 and 2 respectively. We state below certain remarks on the variants of the above approach.
Table 1. Summary of semi-device-independent quantum money generation protocol.

| Money generation protocol |
|---------------------------|
| **Arguments:** |
| (B₁)'节目₁—honest Bank’s branches |
| Bₙ—the honest mint (Bank’s branch that creates the money) |
| (Sₙ)'节目ₙ—untrusted source devices (with single qubit outputs) |
| A—possibly dishonest client Alice that possesses quantum memory to store money (quantum wallet) |
| SN—serial number of the banknote |
| (yₙ)'节目ₙ₁ = (y₁ₙ, y₂ₙ) classical keys of the banknote shared by Bank’s branches |
| (wᵢ)'节目ᵢ —client’s part of the banknote |

| Protocol steps: |
| 1. Branches Bᵢ generate common classical key string consist of pair of bits (y') = (y₁', y₂'). |
| 2. Mint Bₙ inputs strings y' into untrusted source devices S'. |
| 3. Devices S' produce states |wᵢ' that are sent to the client A together with serial number SN. |
| 4. Client A stores states ⨂ᵢ |wᵢ' and SN in her quantum wallet. |

Table 2. Summary of semi-device-independent quantum money verification protocol.

| Money verification protocol |
|-----------------------------|
| **Arguments:** |
| (B₁)'节目₁—honest Bank’s branches |
| Bₙ—honest Bank’s branch that verifies the money |
| PP—Bₙ’s honest post-processing unit |
| (Mₙ)'节目ₙ₁—untrusted measurement devices |
| V—untrusted verification terminal |
| A—possibly dishonest client Alice that possesses quantum memory to store money (quantum wallet) |
| SN—serial number of the banknote |
| (yₙ)'节目ₙ₁ = (y₁ₙ, y₂ₙ) classical keys of the banknote shared by Bank’s branches |
| (xₙ)'节目ₙ₁—random questions send by verifying branch |
| (aᵢ)'节目ᵢ —classical output generated by measurement devices |
| ⊗ᵢ |wᵢ —client’s part of the banknote |

| Protocol steps: |
| 1. Client A inputs her quantum states ⨂ᵢ |wᵢ' and SN into terminal V. |
| 2. Bank’s branch Bₙ that have a classical connection with V sends questions (x')节目ₙ₁. |
| 3. Terminal T, using devices , measures states (Mₙ)'节目ₙ₁⨂ᵢ |wᵢ' according to questions (x')节目ₙ₁. |
| 4. The outputs of measurements (aᵢ)'节目ᵢ are sent to the branch Bₙ. |
| 5. The branch counts the number c of correct guesses, i.e. number of i such that yᵢ = a; using honest post-processing unit PP. |
| 6. The branch accepts the banknote if ε > θn and rejects otherwise. |

**Remark 1.** One might think that mint could check the quantum source device before its official use. However, one can never exclude the attack based on clock: the quantum device starts misbehaving after it has been (with high probability) tested and treated as honest from that on. Even more importantly, the attack that we show is split between two devices: the quantum source device and the verification device. Since the verification device can also be dishonest, i.e. the honesty of which can again depend on the clock, it is then rather not possible to detect the attack before the money is produced.

Despite this fact, our scheme circumvents a class of attacks of this type by testing each banknote against it during the standard validation procedure. Our scheme can be therefore seen as testing outputs of two not fully trusted devices by inspecting if these outputs possess welcome property.

**Remark 2 (The creation of the banknote without communication).** The branches can create money without communication. Using synchronized clocks, they can continuously generate new random inputs. When a client arrives, the serial number of her banknote would contain the time that uniquely indicates what remembered randomness verifying branch should use. Additionally, branches should agree among themselves on the allowed
4.2. Comparison of the SDI QKD and SDI quantum money scheme

We make now an explicit comparison of our protocol with that of the semi-device-independent QKD of Pawłowski and Brunner [14]. Although the honest implementation of two protocols and its assumptions are similar, the proof is fundamentally different. Furthermore, there are three more main differences.

- **Memory requirements**: A conceptual difference is that we defer the process of measurement and call the collection of states prepared by the source in SDI protocol the banknote. The process of the measurement is identified by us with the verification done later by the terminal. It is of particular convenience that the SDI protocol does not rely on the no-signaling principle, so the measurement of the banknotes can be done any time after they were prepared. In other words, our protocol needs quantum memory, whilst SDI QKD does not.

- **Limited number of runs**: A significant practical difference is that the SDI quantum money scheme corresponds to a limited SDI QKD protocol to the creation and the verification procedures without the privacy amplification and information reconciliation part. In particular, in our protocol, the number of runs of the corresponding SDI QKD experiment (i.e. the length of the banknote) is only long enough to enable estimation of the guessing probability which depends only on the possible systematic error in the experiment and the concentration property due to the law of large numbers. It is in contrast with the SDI QKD protocol, which involves as many runs (at least) as the number of key bits needed to be generated. Indeed, we do not aim at creating the secret key because—there is no phase of public reconciliation and privacy amplification. Preparing and verifying a long key is equivalent to creating and verifying a huge number of banknotes.

- **An intermediate acceptance threshold**: The third difference concerns the acceptance threshold. Acceptable range of the value of the probability of guessing \( P_{\text{guess}} \) of the string \( \{p_i\}_{i=1}^{n} \) in the SDI QKD protocol varies from the maximal \( R_2 \approx 0.8536 \), which implies the highest possible key rate in this scenario, to the minimal \( P_{\text{key}} \approx 0.8415 \), which implies zero key rate. Let us stress here, that any value between \( P_{\text{guess}} \) and \( P_{\text{key}} \) is acceptable, as leading to a non-zero key rate (yet, one aims at the highest). Instead, in the corresponding SDI quantum money scheme one needs the value of this parameter to be larger than \( P_{\text{money}} \approx \left( R_2 + P_{\text{key}} \right) / 2 \approx 0.84755 \). On the other hand, all money schemes with the acceptance threshold \( \theta \) in the range \( \left( P_{\text{money}} \right)^\prime, R_2 \) are protected against forgery given large enough number of qubits of the banknote \( n \).

4.3. Security proof of the SDI quantum money scheme

In this section, we provide the proof of the main result: the SDI quantum money scheme is protected against the qubit-by-qubit forgery. That is, against the case when the source device, the counterfeiter, and the verification terminal possibly created by the counterfeiter cooperate in a manner that each qubit is attacked (prepared, copied and tested) independently. Under some additional necessary assumptions, which we list below, we show that two cooperating clients, Alice and Frederick, cannot get the banknote accepted as valid in many branches have access to a private fully random number generator that they use to generate \( y' \)’s and \( x' \)’s.

**ASM1** Bank’s branches have access to a private fully random number generator that they use to generate \( y' \)’s and \( x' \)’s.

**ASM2** Branches of the Bank use honest classical post-processing units in the verification procedure.

**ASM3** The dimension of the state that is produced at the output of the source is bounded, and there is no other information leaking from the source to Alice or Frederick.

**ASM4** The state produced by the source is unentangled from the dishonest parties (Alice and Frederick).

**ASM5** The source devices create the states in an independent way, which also implies that each of the sources has access only to its input (not the inputs of the other sources).

**ASM6** The measurement devices are independent, each measure only its subsystem, and the outputs of Alice and Frederick in each run are independent of the inputs and the outputs from other runs.

generation time to make sure not to generate two bills from the same randomness. A similar idea can also be implemented in some previous money schemes, for example, Wiesner’s one.
It is crucial to notice that our assumptions are strictly weaker than the one used in Wiesner’s scheme. Furthermore, all existing quantum money schemes assume that the money state dimension is limited.

In particular case of the presented SDI quantum money scheme, in ASM3 we specify that each of the independent parts of the sources (as specified in ASM5) has output bounded by \( d = 2 \), i.e. the source works by producing independently \( n \) qubits (however not necessarily in the same way). What we will prove, our assumptions imply security against the third attack presented above.

Now we are ready to formally state main result of our work. Let us define (see appendix C)

\[
\beta_\eta = P_Q \left( \frac{1}{2} + \eta \right) + \frac{M}{2} \left( \frac{1}{2} + \eta \right) + \eta
\]

\[
= \frac{9 + 2\sqrt{2} + \sqrt{3}}{16} + \frac{17 + 2\sqrt{2} + \sqrt{3}}{8} \eta
\]

\[
\approx 0.8475 + 2.6950\eta
\]

for some small \( \eta \) chosen in such a way that \( \beta_\eta \leq P_Q \).

**Theorem 1 (Security of semi-device-independent Quantum Money).** Let acceptance threshold \( \theta \) be larger than \( \beta_\eta \). Then, under Assumptions ASM1—ASM6, where \( k \) denotes the number of Bank’s branches the probability of a successful forgery \( P(F_\theta) \) is exponentially small in number of banknote’s qubits \( n \) and is bounded by

\[
P(F_\theta) \leq 10k^2 e^{-2\sqrt{2}(1-\theta)n}.
\]

**Remark 3 (On the possible weakening of the assumptions).** It seems plausible that the assumption ASM6 could be omitted but, it would complicate the proof. The question of if we can omit the assumption ASM5 is a hard open problem, related to the formulation of the SDI QKD scheme and Random Access Codes [53, 54] in general. On the other hand, all other assumptions are necessary to prove the security of our scheme since rejecting any of them leads to a successful attack.

Let us briefly describe the idea of the proof of the security of the scheme. It is a consequence of two facts: (i) the monogamy inherent to the SDI key generation protocol and (ii) the fact that each Bank’s branch queries independently from the other branches during the verification procedure. It will hold for the case when the Bank verifies the banknote via untrusted terminal, i.e. Alice (or Frederick) come to the Bank to get the banknote accepted. We can reduce the case with the communication to the latter, under the assumption that the strategy to lie about the outputs of the devices (which is then at a choice of the dishonest parties) is individual, independent for each of the runs of the protocol (see appendix A). As we discuss in section 6, this a bit unrealistic assumption that can be in principle dropped given the protocol of SDI QKD is proven to be secure against the general, so-called forward signaling attacks.

4.3.1. The case of an attack on a single qubit

Like in Wiesner’s scheme, for a banknote to be accepted, its owner has to guess the bits of the Bank correctly. It is instructive to focus on the attack on a single qubit of the banknote to see that two dishonest persons, Alice and Frederick, cannot both pass the verification of our banknote. Suppose Alice and Frederick are trying to ‘split’ its use to maximize the probability of guessing \( P_{\text{guess}} \) in two experiments of some two branches of the Bank. Their joined attack can be described as a conditional probability distribution (a box): \( P(a_0, a_0 | x_A, x_F, y_0, y_0, y_1) \), where \( y_0 \) and \( y_1 \) are the secret keys of the Bank which Alice and Frederick are trying to guess, \( x_A \) and \( x_F \) are the random inputs, generated by the Bank, send to the verification device.

For simplicity of description, we will assume that Alice and Frederick come to the Bank, while the Bank sets the input to the devices (we will argue later how to relax this assumption partially). The joined attack aims at generating two bits \( a_A \) (by Alice), and \( a_F \) (by Frederick), such that the probability of guessing the \( x_A \)th bit of \( y_0 = (y_0, y_1) \) and \( x_F \)th bit of \( y_0 \) by Frederick are both maximal. The guessing probability for Alice and Frederick respectively read:

\[
P_{\text{guess}}^A = \frac{1}{8} \sum_{y_0, y_1, x_A} P(a_0 = y_0 | y_0, y_1, x_A),
\]

\[
P_{\text{guess}}^F = \frac{1}{8} \sum_{y_0, y_1, x_F} P(a_0 = y_0 | y_0, y_1, x_F).
\]

Let us observe first that in the case \( x_A = x_F \), they can both achieve the maximal possible probability of guessing \( P_Q = \cos^2(\pi/8) \approx 0.8536 \) [14]. Indeed, Alice can come first to one branch and behave honestly having the guessing probability \( P_{\text{guess}}^A = P_Q \), while Frederick can *copy her answer*, reaching the same probability of guessing.
However, when $x_A = x_B = x_A \oplus 1$, the dishonest parties need to guess opposite bits: $y_0$ (Alice) and $y_1$ (Frederick) or vice versa (with half probability). However, it is proven in [14] that

$$p_{\text{guess}}^A(y_0) + p_{\text{guess}}^B(y_1) \leq \frac{5 + \sqrt{5}}{4} = M. \tag{13}$$

Hence, even if Alice and Frederick were fully collaborating, the sum of the probabilities of guessing of the two bits is bounded.

Since $x_A = x_B$ with the probability one half, averaging over the value of $x_A \oplus x_B$, we conclude that the average number of correctly guessed bits has an upper bound

$$\frac{1}{2} (2P_Q + M) = B. \tag{14}$$

In the next section, we will generalize this bound to the case banknotes that consists of many ($n$) qubits. Due to the independent nature of the attack, it will suffice to multiply the above bound by $n$ (up to fluctuations around the average). The corresponding bound enlarged by the maximal possible fluctuations reads then $n\beta$ with $\beta = 2P_Q (1/2 + \eta) + M (1/2 + \eta) + 2\eta$. We will then choose the threshold value $\theta$ to be larger than $\beta/2$. It will assure that the two dishonest parties cannot get the same banknote accepted in two Bank’s branches, as their total sum of the guesses would be larger than $2\beta/2 = \beta$, reaching the desired contradiction.

### 4.3.2. Extending the argument to the general case of the qubit-by-qubit attack

We would like to extend this reasoning to the case of the repeated experiment of $n$ runs ($n$ will be relatively small, as short as the length of a usual preamble of the QKD protocols). We assume here that the attack is ‘id’, i.e. by not necessarily equal however independently distributed random variables, according to the measure:

$$\mu \sim \otimes_{i=1}^n U(y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}')P(a_{i,0}', a_{i,1}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}'), \tag{15}$$

where $U(y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}')$ denotes the uniform distribution over its arguments. We then observe that, instead of providing $x_B$ to Alice and $x_B$ to Frederick, the two branches of the Bank could give $x_A$ to Alice and $x_B := x_A \oplus x_F$ to Frederick. This is because Alice and Frederick are collaborating, so they can compute value of $x_F$ from these data in case it is needed. We can, therefore, change the scenario to one in which the parties are given $(x_A, x_B)$, if the probability measure is changed accordingly to the following one:

$$\mu' \sim \otimes_{i=1}^n U(y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}')P(a_{i,0}', a_{i,1}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}'). \tag{16}$$

The measure $\mu'$ acts on $x_A$ and $x_B$ in the same way as $\mu$ would act on $x_A$ and $x_F$, so in some sense it is undoing the XOR operation. This modification of the scenario does not change the probability of successful forgery, i.e. the probability of an event in which both Alice will get accepted as supposed to have a valid banknote and so will Frederick. To see this, we first note that a set of events (denoted as $\mathcal{F}$) leading to a successful forgery reads:

$$\mathcal{F} := \{ (y_{i,0}', y_{i,1}', x_{i,0}', a_{i,0}', a_{i,1}', a_{i,0}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}') \}
\quad \text{with } \{|i| \leq [n]: a_{i,0}' = y_{i,0}' \} > \theta n, \quad \{|i| \leq [n]: a_{i,1}' = y_{i,1}' \} > \theta n \}. \tag{17}$$

We will also define a strategy $S$ by

$$S := (y_{i,0}', y_{i,1}', x_{i,0}', a_{i,0}', a_{i,1}', a_{i,0}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}')_{i=1}^n \tag{18}.$$

We then prove (see corollary 1) that

$$P(\mathcal{F}) = \sum_{S \in \mathcal{F}} P_{\mu}(S) \tag{19}$$

where $S' := (y_{i,0}', y_{i,1}', x_{i,0}', a_{i,0}', a_{i,1}', a_{i,0}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}')_{i=1}^n$ and

$$\mathcal{F}' := \{ (y_{i,0}', y_{i,1}', x_{i,0}', a_{i,0}', a_{i,1}', a_{i,0}'|y_{i,0}', y_{i,1}', x_{i,0}', x_{i,1}') \}
\quad \text{with } \{|i| \leq [n]: a_{i,0}' = y_{i,0}' \} > \theta n, \quad \{|i| \leq [n]: a_{i,1}' = y_{i,1}' \} > \theta n \}. \tag{20}$$

Because $x_B$ is created from fully random bits that are unknown for adversary during the creation of the money, we have

$$P(\mathcal{F}) = \sum_{x_B \in \{0,1\}^n} p(x_B) P(\mathcal{F}|x_B). \tag{21}$$
We can narrow considerations to the typical \( x_n \), i.e. those having number of symbol 0 and 1 approximately \( n/2 \) times. More formally the set of typical sequences is defined as

\[
\mathcal{T}_n := \left\{ x : \frac{|x_0|}{n} - \frac{1}{2} \leq \eta \right\},
\]

where \( |x_0| \) is the number of positions with symbol 0 in a bitstring \( x \). All sequences of the length \( n \) (given \( n \) is large enough) are with high probability typical (i.e. with a probability \( 1 - \epsilon(\eta) \) for \( \epsilon(\eta) = 2 \exp(-2\eta^2 n) \)). We have therefore

\[
P(\mathcal{F}) \leq \sum_{x, i \in \mathcal{T}_n} p(x, i) P(\mathcal{F} | x, i) + \epsilon(\eta).
\]

We then see that one can fix a typical \( x_n \), and prove that for any such \( x_n \), the probability of acceptance is low. We will assure it by setting an appropriate \( \theta \), so that with a high probability over the conditional measure \( \mu'' := \mu'(x_n) / p(x_n) \) the strings \( S' \) emerging from the attack will be rejected as having too small number of guessed bits of \( (y_{i0}^n, y_{i1}^n) \).

In more detail, we first note that for a fixed \( x_n \), on average, over \( n \) runs with respect to the measure \( \mu'' \), there are no more guessed inputs than \( n B \) with \( B \) given in equation (14). It remains to take into account the fact that the observed number of the guessed inputs need not be equal to its average. However, \( x_n \) is typical, hence the number of runs will be at least \( n/2 - \eta n \), so we can use the fact that the attack is performed in an independent manner. Due to Hoeffding’s inequality, we obtain that the observed number of guessed inputs is with a high probability bounded from above by:

\[
n \beta \equiv n \left[ 2P_\theta \left( \frac{1}{2} + \eta \right) + M \left( \frac{1}{2} + \eta \right) + 2\eta \right]
= n \left[ 2 \cos \left( \frac{\pi}{8} \right) + \frac{5 + \sqrt{5}}{4} \left( \frac{1}{2} + \eta \right) + 2\eta \right],
\]

where \( \eta \) takes care of the maximal possible fluctuations.

Before we explicitly control these fluctuations, we first define four random variables describing the guessing at the \( i \)th run of the verification procedure by Alice and Frederick as

\[
X_{\bar{i},A} := \begin{cases} \delta(a_{\bar{i}}, y_{\bar{i},A}^i) : \hat{x}_{\bar{i}}^A = x_{\bar{i}}^i \\ 0 : \hat{x}_{\bar{i}}^A = \bar{x}_{\bar{i}}^i \end{cases}
\]

(25)

\[
X_{\bar{i},F} := \begin{cases} \delta(a_{\bar{i}}, y_{\bar{i},F}^i) : \hat{x}_{\bar{i}}^F = x_{\bar{i}}^i \\ 0 : \hat{x}_{\bar{i}}^F = \bar{x}_{\bar{i}}^i \end{cases}
\]

(26)

\[
Y_{\bar{i},A} := \begin{cases} \delta(a_{\bar{i}}, y_{\bar{i},A}^{i+1}) : \hat{x}_{\bar{i}}^A = x_{\bar{i}}^i \\ 0 : \hat{x}_{\bar{i}}^A = \bar{x}_{\bar{i}}^i \end{cases}
\]

(27)

\[
Y_{\bar{i},F} := \begin{cases} \delta(a_{\bar{i}}, y_{\bar{i},F}^{i+1}) : \hat{x}_{\bar{i}}^F = x_{\bar{i}}^i \\ 0 : \hat{x}_{\bar{i}}^F = \bar{x}_{\bar{i}}^i \end{cases}
\]

(28)

Now we can get back to describing deviations from the average of the 4 random variables: \( \bar{X}_{x_n}^A, \bar{X}_{x_n}^F, \bar{Y}_{x_n}^A \) and \( \bar{Y}_{x_n}^F \), that are the sums over \( i \in \{ n \} \) for the variables described above. The values of \( \bar{X}_{x_n}^A, \bar{X}_{x_n}^F, \bar{Y}_{x_n}^A \) and \( \bar{Y}_{x_n}^F \) describe the number of correct guesses for \( i \) satisfying \( x_{i0}^A = x_{i0} \). Analogously, \( \bar{Y}_{x_n}^A, \bar{Y}_{x_n}^F \) describe the number of correct guesses for \( i \) such that \( x_{i1}^A = x_{i1} \). Details are given in lemma 2 and corollary 2 (see also appendix B for an explicit definition of random variables, their sum and expected values).

The last argument follows from a simple observation. Namely, if the total fraction of the correctly guessed positions by two persons is less than \( \beta \), the minimum of the fractions of the correct guesses by each of them separately is not greater than \( \beta/2 \). Setting the acceptance threshold \( \theta \) large enough that the minimum of the numbers of guesses is below \( \theta \), we assure that for each typical \( x_n \), the banknote is rejected with the high probability in at least one branch. In particular, for any \( \theta > \beta/2 \) this probability is at least \( 1 - 8 \exp(-\eta^2(n/2 - \eta)) \), where for every typical \( x_n \) the error \( 8 \exp(-\eta^2(n/2 - \eta)) \) upper bounds the probability of event that at least one of the 4 random variables \( \bar{X}_{x_n}^A, \bar{X}_{x_n}^F, \bar{Y}_{x_n}^A, \bar{Y}_{x_n}^F \) is far from its respective average.

Taking into account equations (23) and (19), we obtain finally

\[
P(\mathcal{F}) \leq 5e^{-\epsilon(\eta)},
\]

(29)

with \( \epsilon(\eta) := 2 \exp(-\eta^2(n/2 - \eta)) \).
5. Quantum Oresme–Copernicus–Gresham’s law

One of the famous laws of the economy is:

• **Bad money drives out good.**

This law states, colloquially speaking, that if certain money is cheaper to produce, then it will eventually subside the one that is more expensive to produce, where expensive is understood not in terms of face value but in terms of intrinsic value. Although it was named after Sir Gresham, it has been observed by others, even much earlier. The two most cited authors are Oresme [55] and Nicolaus Copernicus [56], so that the law is also referred to as Copernicus’, or the Oresme–Copernicus–Gresham’s law (OCG law). However, the first known appearance of a similar statement is in the comedy 'The Frogs', written by the Ancient Greek playwright Aristophanes around 405 BC [57]. For an overview of the law, see, e.g. [58].

From the perspective of the economy, the concept of money is a matter of a social agreement and properties of a given material/ procedure used to produce a coin or a banknote. So it might appear that there is no need to consider a quantum variant of Gresham’s law per se because one can apply the OCG law to the new method of mining—from quantum states. This is what happens to classical crypto-currencies. Instead, formulating quantum analog of the OCG law, we would like to stimulate a discussion on the intrinsic value of quantum currencies. This quantum intrinsic value is much different from one used in the case of classical money. For example, we can treat quantum money states as a source of randomness. Furthermore, we can also take into account how hard it is to implement different quantum money schemes. This is because one could choose a ‘cheaper’ way to produce money—from quantum states that are ‘cheaper’ to obtain whatever means ‘cheaper’ to quantum technology at a given moment of development. We, therefore, would like to introduce and discuss a version of Quantum Gresham’s law in the following way:

• **Bad quantum money drives out good quantum one.**

Deciding whether to keep a given quantum currency or not may be a complex process, depending on various mutually dependent parameters, the importance of which varies over a change of preferences of particular individuals or societies. It is therefore too early and hence too hard to foresee the behavior of the quantum currency flow between the schemes provided they happen to be realized experimentally. Nevertheless, we can exemplify a possible in real life situation, which may cause the quantum OCG law to hold. In that, we will restrict ourselves to show the interplay between the two different, yet both legible representations of quantum banknotes, of the same type of currency—the one which we introduce in this manuscript.

**Example 1.** For the presented SDI quantum money scheme, to be unforgeable in a qubit-by-qubit way, it is enough that the source of the banknote (if it can produce a large number of banknotes) manages to produce SDI key at a rate \( \theta > \beta/2 \). It is, however, not demanded that \( \theta \approx P_{\text{fl}} \), i.e. that the source would be able to produce money equivalent to the small number of runs of the SDI key generation experiment with the maximal possible rate \( P_{\text{fl}} \).

Suppose that some provider \( P_1 \) can produce the SDI quantum money which passes the acceptance threshold \( \theta = \beta/2 + \delta \) for some \( \delta > 0 \). Next, suppose that some other provider \( P_2 \) can produce a reliable SDI quantum money with the lower acceptance threshold \( \beta/2 + \delta \). As we have proved in theorem 1, banknotes of both providers are valid and cannot be forged under the same set of assumptions. However, the banknote of the provider \( P_1 \) can be attributed with a larger quantum commodity value defined as the SDI key rate of a source which produced the banknote. From the perspective of banknote’s holder, this key rate implies a nonzero rate of the min–entropy of banknote’s quantum state and hence the nonzero rate of the private randomness. An additional reason to keep the \( P_1 \) type money and spend more often \( P_2 \) type is that the first one could be more robust to noise. Indeed, even decrease by \( \delta \) of the observed fraction of the correct guesses will not invalidate the banknote.

We make then the following observation:

**Observation 2.** If the Quantum Oresme–Copernicus–Gresham’s law applies, the SDI quantum money with a lower acceptance threshold \( \theta \) will drive out the SDI quantum money with a higher \( \theta \). (We note here, that we have implicitly assumed that the hardware parameters of the realization by \( P_1 \) and \( P_2 \) are comparable. Otherwise, a realization of the banknote according to type \( P_1 \) receipt can be simply too expensive, e.g. in energy spent on keeping them in a quantum wallet).

The above example is minimal, as it concerns different ways of realization of the same money scheme (i.e. currency). It is however plausible that if the quantum version of the OCG law turns out to be accurate, the individuals will tend to keep the most secure, cheapest to produce and to store money of the highest commodity value (in the sense of its use for quantum information processing), and will spend the other currencies more often. Going a bit further, one can consider monies in a theory \( T \) (for such a general approach see [30]), and have
6. Discussion

6.1. A comparison of the money schemes

In table 3, we present the comparison of different protocols, including the original protocol of Stephen Wiesner [1] and that of Dimitry Gavinsky [7], and show which parties and devices have to be trusted by the Bank in order to maintain security.

6.2. How close we are to practice?

A fundamental obstacle in the realization of the presented one and many other money schemes is the fact that it relies on the existence of a reliable and long-time living quantum memory. It is hard to foresee when (if ever) such memories would be available. However, there are works in this direction. As an example of a recent substantial experimental progress in developing the quantum memory, we can invoke the paper by Wang et al [39], presenting a single-qubit quantum memory that exceeds coherence time of ten minutes. Furthermore, Harper and Flammia [60] demonstrated the first implementation of the error-correcting codes on a real quantum computer. It may indicate that the error-correcting codes can become useful in the near future quantum memories.

We want to emphasize here that the tasks of universal fault-tolerant quantum computing [61] and of a reliable quantum repeater [62] (for latest discovery see [63] and references therein) are both different from that of a fault-tolerant quantum storage (QS). The memory of the quantum computer need not be stable for a long time, because it is needed only for the time when the gates of the quantum algorithm are done, while the QS needs to be stable for a long time. However, operations on the QS are far from being universal [64], reduced to measurements in two bases (at least in the considered SDI quantum money scheme).

Although there is no physical law that bounds from above the time of coherence of a qubit state, achieving a reliable QS appears to be an arduous task, because of quantum decoherence, which is usually happening very fast. This is the reason why the very first idea (of QS needed for money schemes) that appear in theory may become the last one (after quantum computer and quantum Internet) to be realized in practice. It may also happen because, in contrast to quantum computing or secure quantum communication, the money scheme requires to be widely implemented in order to be useful.

It is also worth to notice that, recently, the first experimental implementation of quantum money schemes were performed [31–33]. It indicates that real-life implementation of quantum money could potentially be achievable using near-future technologies.

6.3. Conclusions

In this article, we have presented an alternative testing method for the original Wiesner’s banknotes—a semi-device-independent quantum money scheme. To our knowledge, this is the first attempt to provide the quantum money scheme unforgeability of which would not entirely rely on trusting quantum source device and the inner workings of the verifying terminal at the same time.

Furthermore, we provide impossibility results for a fully device-independent quantum money scheme. It shows that our semi-device-independent approach is close to the strongest possible money scheme. To clarify, by the strongest, we mean here that we maximally reduce trust in the inner working of all quantum devices that are used in all stages of money production and verification.

---

**Table 3. Table of the Bank’s trust.**

| Protocol               | Classical scheme | Wiesner’s scheme [1] | Gavinsky’s scheme [7] | SDI[this work] | DI[this work] |
|------------------------|------------------|----------------------|----------------------|----------------|---------------|
| Source device          | Yes              | Yes                  | Yes                  | No             | No            |
| Alice’s measurement    | N/A              | Yes*                 | No                   | No             | No            |
| System dimension       | No               | No                   | No                   | Yes            | No            |
| Number of branches     | 1                | unlimited            | unlimited            | unlimited      | unlimited     |

* The measurement of Alice’s subsystem can be performed in Bank’s branch or inside the partially trusted terminal (for example, in a shop).
We have provided a protocol of quantum money, which has relaxed assumptions with respect to Wiesner’s protocol and is at the same time immune to a broader class of attacks.

Considered attacks and the aspect of classicality of the money have not been considered so far. The attacks are, in fact, hardware Trojan horse attacks that can exploit modification of both the production and verification process.

It is plausible that the proposed scheme inherits the security of the underlying, in our case, the original semi-device-independent quantum key distribution protocol. Given the full proof of security of the SDI QKD against a forward signaling adversary, as it is the case for the DI QKD [65] (see [66] for the latest breakthrough), it may follow that our suitably modified scheme is fully unforgeable. Sufficient modification concerns the communication in the verification procedure. The counterfeiter would need to give the answer(s) \((a^i, a^j)\) after getting inputs \((x^i, x^j)\), but before learning next inputs \((x^{i+1}, x^{j+1})\). In such a case, each possible history-dependent lie can be treated safely as a part of the attack of the device and hence would not affect the model. The rest of the proof would follow from similar arguments as above with proper use of the concentration of martingales. It is, therefore, important to verify if the SDI protocol is fully secure. An intermediate step would be to extend the security proof the presented SDI quantum money scheme to its variant given in [67] proves there to be secure against collective attacks.

One might think that we could have used the scheme of the device-dependent key secure against the quantum adversary [65] directly, avoiding thereby unnatural assumption that the terminal can change (lie about) output values only in an independent manner during verification procedure. It is indeed straightforward to extend the idea presented here for a single Bank’s branch with much weaker assumptions. However, it needs suitable modifications leading to a novel scheme, in order to be extended to the case with multiple Bank’s branches. This approach, therefore, results in a scheme fundamentally different from the original one and its follow-ups like the presented SDI quantum money scheme.

In general, SDI QKD and the SDI quantum money scheme are connected by the honest implementation and underlying game as well as by the common concepts that assure their security. However, they are also different, as we have discussed, in that, in particular, they have different thresholds for the number of correct guesses in the random access code game. It is because the conditions leading to security thresholds does not coincide, reflecting difference in security scenarios. It is important here to note that the moderate error threshold opens the possibility to some robustness to noise, which is important to study further (see in this context recent article [68]). It is also important to ask if other games than the random access code game, can lead to similar schemes via our concept of ‘winning in more than half of possible times’ as we exposed in equation (2). Considering other setups can lead possibly to weakening of the assumptions much in the same way as the assumptions of SDI QKD has been to some extent relaxed in [68] for private randomness certification.

Given a more promising for practical realization variant of this scheme exists, one should consider its robust version that can be realized in the laboratory, including all side effects that may potentially open it for the attacks of hackers. This aspect of the SDI QKD has been recently studied in [35, 67, 69–71].

Another important direction of development would be checking if the proposed scheme could be treated as an option for a user of the original Wiesner’s scheme or its other extensions like Gavinsky’s protocol. The resulting scheme would give higher protection against Trojan horse attacks, matching the best of two approaches. In the presented scheme, the banknotes (even in case of the honest client Alice) are inevitably lost during verification. It seems natural (like it is done by Gavinsky [7]) to extend our scheme to the case of the transactions, which we also defer to the future work.

Finally, in a bit speculative way, we have put forward a hypothesis called the Quantum Oresme–Copernicus–Gresham’s law: an analog of the classical law of the economy, also known as Gresham’s law. We have supported the possible validity of this hypothetical law based on different realizations of the SDI quantum money scheme, corresponding to the different values of the threshold leading to the acceptance of money. These speculations need further, more formal, exploration with examples based on more types of currencies, as well as an extension (what appears to be straightforward) to the case of resources within the paradigm of [72].

Acknowledgments

The work is supported by the grant Sonata Bis 5 no. 2015/18/E/ST2/00327 from the National Science Centre, Poland. KH acknowledges partial support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. 2018/MAB/5, co-financed by EU via Smart Growth Operational Programme).

The authors would like to thank Anubhav Chaturvedi, Ryszard Kostecki, Sergii Strelchuk, and Marek Winczewski for useful comments. MS thanks Or Sattath for the enlightening discussion about relating results presented as a poster at the 8th International Conference on Quantum Cryptography (QCrypt 2018) Shanghai, China, 27–31 August 2018.
Author Contributions: All authors researched, collated, and wrote this paper.
Competing interests: The authors declare that there are no competing interests.
Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Appendix A. Preliminary definitions

We will start by defining two crucial constants \( M \) and \( P_Q \), which come from [14],

\[
M = \frac{5 + \sqrt{3}}{4}, \quad P_Q = \cos^2\left(\frac{\pi}{8}\right).
\]  

(A1)

It is easy to see that \( P_Q > M/2 \).

Let us now define the notation used in the rest of the paper. By \( y \)’s we denote the inputs used by the Bank in order to create the money, \( x \)’s stand for the questions that the branches verifying Alice and Frederick ask them, \( \tilde{x} \) represents real value that Alice and Frederick input into the devices, and we use \( \alpha \)'s for Alice’s and Frederick’s outputs. Furthermore, \( i \) in an upper index denotes the \( i \)th run of the protocol that acts on the \( i \)th quantum subsystem. The general attack performed in a qubit-by-qubit manner (see Assumptions ASM5 and ASM6) can be described by a probability measure on the data used in the verification protocol. The Bank generates part of the data (inputs to the verification procedure). On the other hand, Alice and Frederick generates the outputs \( \alpha_A \) and \( \alpha_F \) according to their choice of the conditional distribution. The total joint distribution of the inputs and outputs reads

\[
\bigotimes_{i=1}^n P(y_0^i, y_{00}^i, y_{10}^i, x_{A}^i, x_{F}^i, \tilde{x}_{A}^i, \tilde{x}_{F}^i)P(\alpha_A^i, \alpha_F^i)P(y_0^i, y_{00}^i, y_{10}^i, x_{A}^i, x_{F}^i, \tilde{x}_{A}^i, \tilde{x}_{F}^i).
\]  

(A2)

In what follows we will simplify it due to certain assumptions. We know, from the definition of money generating protocol, that if Frederick wants to verify the same banknote as Alice, then \( y \)’s are the same for all branches, so we can omit variables for each branch and write just \( y_0^i \) and \( y_{10}^i \). Furthermore, if Bank’s branches input appropriate bits to the devices themselves, then we are sure that \( x_{A}^i = \tilde{x}_{A}^i \) and \( x_{F}^i = \tilde{x}_{F}^i \), obtaining

\[
\bigotimes_{i=1}^n P(y_0^i, y_{00}^i, x_{A}^i, x_{F}^i)P(\alpha_A^i, \alpha_F^i)P(y_0^i, y_{00}^i, x_{A}^i, x_{F}^i).
\]  

(A3)

Observation 3. Our scheme remains secure if we allow Alice and Frederick to set device inputs, under the assumption that they do independently in each run. Any run-independent cheating strategy where Alice or Frederick uses inputs \( x_{A}^i, \tilde{x}_{F}^i \) that are different from \( x_{A}^i, \tilde{x}_{F}^i \) provided by the Bank can be incorporated into the inner working of the untrusted devices so we can also omit it. Since we assume that \( y \)’s and \( x \)’s generated by Bank are fully random, what is possible due to Assumption ASM1, we can rewrite the above formula as

\[
\mu \sim \bigotimes_{i=1}^n U(y_0^i, y_{00}^i, x_{A}^i, x_{F}^i)P(\alpha_A^i, \alpha_F^i)P(y_0^i, y_{00}^i, x_{A}^i, x_{F}^i),
\]  

(A4)

where \( U \), here and in all measures defined later, stands for the uniform distribution over appropriate variables.

Now we can define the set describing successful forgery, meaning that both Alice and Frederick are accepted using the same banknote.

\[
\mathcal{F} \equiv \{(y_0^i, y_{00}^i, x_{A}^i, x_{F}^i, \alpha_F^i)_{i=1}^n \in \{0, 1\}^{6n} : |\{i \in [n] : a_F^i = y_{A}^i \}| > \theta n, |\{i \in [n] : a_F^i = \tilde{y}_{A}^i \}| > \theta n\}
\]  

(A5)

We also define sequences

\[
S_i \equiv (y_0^i, y_{00}^i, x_{A}^i, x_{F}^i, \alpha_F^i).
\]  

(A7)

Now we can make the observation that this is an easy consequence of the security proof of [14]. It is important to notice that we need here Assumptions ASM1, ASM2, ASM3, and ASM4 since there are also necessary in [14]. For clarity, we change notation by substituting \( B \) and \( E \) by \( A \) and \( F \), respectively.

Observation 4.

\[
P_{AF}(a_0) + P_{AF}(a_1) \leq M.
\]  

(A8)

Proof. From equation (12) of [14] and the comment that follows the equation we know that
\[ P_{AF}(a_0) + P_{AF}(a_1) + P_{AF}(a_0 \oplus a_1) \leq \frac{3}{2} \left( 1 + \frac{1}{\sqrt{3}} \right). \]  

Using equation (13) of [14], 
\[ P_{AF}(a_0) + P_{AF}(a_1) - 1 \leq P_{AF}(a_0 \oplus a_1), \]  
we obtain 
\[ P_{AF}(a_0) + P_{AF}(a_1) \leq \frac{1}{2} \left( \frac{3}{2} \left( 1 + \frac{1}{\sqrt{3}} \right) + 1 \right) = \frac{5 + \sqrt{3}}{4}. \]  
The right side is equal to \( M \), which completes the proof. \( \square \)

Appendix B. Main lemmas

We will use numerously the concentration property of a distribution of independently distributed \( n \) random variables on \([0, 1]\) due to Hoeffding, of the form 
\[ P(|\bar{X} - \mathbb{E}\bar{X}| \geq \eta) \leq 2e^{-2\eta^2/\sigma^2}, \]  
where \( \bar{X} = \frac{1}{n} \sum x_i \).

For a bitstring \( x \) of length \( n \) we will denote by \( |x|_0 \) the number of occurrences of symbol 0 in \( x \) (analogously \( |x|_1 \) will denote the number of 1s in \( x \)). Thus, 
\[ P\left( \left| \frac{|x|_0}{n} - \frac{1}{2} \right| \geq \eta \right) \leq 2e^{-2\eta^2/\sigma^2}, \]  
where \( \eta \geq 0 \). Due to the above concentration, probability mass function is concentrated on the so-called \( \eta \)-typical sequences, defined as the values of \( x \) satisfying \( \left| |x|_0/n - 1/2 \right| \leq \eta \). In other words, for a set 
\[ T_{\eta,n} = \left\{ x : \left| \frac{|x|_0}{n} - \frac{1}{2} \right| \leq \eta \right\}, \]  
there is, 
\[ P_{U(x)}(x \in T_{\eta,n}) \geq 1 - 2e^{-2\eta^2/\sigma^2} \]  
where the probability is taken from a uniform distribution \( U(x) \) of sequences \( x = (x^i)_{i=1}^n \) over \( \{0, 1\}^n \). In particular, for two sequences \( x_A \) and \( x_F \) drawn independently at random from \( \{0, 1\}^n \), 
\[ P(x_A \oplus x_F \in T_{\eta,n}) \geq 1 - 2e^{-2\eta^2/\sigma^2}, \]  
where by \( \oplus \) we mean the bit-wise XOR operation on the bits of \( x_A \) and \( x_F \). Indeed, for any fixed \( x_A \) the distribution of \( x_F \oplus x_A \) is uniform if such was that of \( x_A \). Then we can use the typicality argument and average over \( p(x_A) \).

At the expense of small error, one can deal only with such as \( S \) that have \( \eta \)-typical inputs \( x_A \) and \( x_F \). Such \( S \) will be called \( \eta \)-typical:
\[ S \equiv (y^0_0, y^1_0, x_A^0, a^1_0, x_F^0, a^0_0)_{i=1}^n \text{ is called } \eta \text{- typical if } x_A^i \oplus x_F^i \equiv (x_A^i \oplus x_F^i)_{i=1}^n \in T_{\eta,n}. \]  
The set of \( \eta \)-typical \( S \) will be denoted as \( T(\eta) \).

In what follows, we will show that the probability of acceptance of a banknote twice, i.e. \( P(\mathcal{F}) \), is equal to the probability accepting it twice in a different scenario (the XOR scenario). In the latter, Alice gets \( x_A \) while Frederick obtains \( x_F \). Even though it will not be the case in real life, this transformation of the scenario (and the corresponding probability measure) will simplify our considerations.

The XOR scenario is obtained from the original one by the following map on the events \( S \):
\[ S = (y^0_0, y^1_0, x_A^0, a^1_0, x_F^0, a^0_0)_{i=1}^n \rightarrow \mathcal{S}' = (y^0_0, y^1_0, x_A^0, a^1_0, x_F^0, a^0_0)_{i=1}^n. \]  
We will refer to the transformed event as the one having \( x_F^0 \) on the position where \( x_A^0 \) is in \( S \):
\[ S' = (y^0_0, y^1_0, x_A^0, a^1_0, x_F^0, a^0_0)_{i=1}^n. \]  
We define the set of all forged \( S' \) in a way analogous to the definition of the set \( \mathcal{F} \):
\[ \mathcal{F}' = \{ (y^0_i, y^1_i, x_A^i, a^1_i, x_F^i, a^0_i)_{i=1}^n \in \{0, 1\}^n : |\{|i \in [n] : a^1_i = y^1_i\}| > \theta n, |\{|i \in [n] : a^0_i = y^1_i \oplus x_A^i\}| > \theta n \}. \]
A new probability measure \( \mu' \) defined on the set of events \( S' \) is defined as

\[
\mu' \sim \bigotimes_{i=1}^{n} U \left( y_0^i, y_1^i, x_A^i, x_D^i \right) P \left( a_i, a_i' | y_0^i, y_1^i, x_A^i, x_D^i \right).
\] (B10)

**Observation 5.** The map \( \pi \):

1. is bijective and involutive;
2. satisfies \( S \in \mathcal{F} \iff S' \in \mathcal{F}' \); and
3. satisfies \( \mu'(S') = \mu(S) \).

**Proof.** The bijectivity follows directly from the fact that \((x_A, x_D)\) is bijectively mapped to \((x_A, x_D \oplus x_F)\). The first input is preserved, while the second one can be reconstructed uniquely by XORing inputs. It is also easy to see that \( \pi \) is an involution, since \((x_A, x_D \oplus x_F)\) is mapped back to \((x_A, x_D)\).

We show now Property 2. Let \( S \in \mathcal{F} \). This happens if and only if

\[
\left| \{ i \in [n] : a_i = y_{x_A^i}^i \} \right| > \theta n \quad \text{and} \quad \left| \{ i \in [n] : a_i' = y_{x_D^i}^i \} \right| > \theta n.
\] (B11)

The event \( S' \) equals \((y_0^i, y_1^i, x_A^i, a_i, x_D^i)_{i=1}^{n}\). By definition of \( \mathcal{F}' \), we have that \( S' \in \mathcal{F}' \) if and only if

\[
\left| \{ i \in [n] : a_i = y_{x_A^i}^i \} \right| > \theta n \quad \text{and} \quad \left| \{ i \in [n] : a_i' = y_{x_D^i}^i \} \right| > \theta n.
\] (B12)

Since the left conditions are identical, we only have to prove equality of the right conditions. By definition of a map \( \pi^{-1} \), we obtain

\[
\left| \{ i \in [n] : a_i' = y_{x_D^i}^i \} \right| = \left| \{ i \in [n] : a_i = y_{x_A^i}^i \} \right| = \left| \{ i \in [n] : a_i' = y_{x_D^i}^i \} \right|,
\] (B13)

which proves an appropriate equality and implies that \( S \in \mathcal{F} \iff S' \in \mathcal{F}' \).

Finally, we argue that the Property 3 also holds. Let us fix arbitrary \( S \). Hence, \( x_A^j = x_D^j \oplus x_F^j \) in definition of \( S' \), and

\[
\mu'(S') = \bigotimes_{i=1}^{n} U \left( y_0^i, y_1^i, x_A^i, x_D^i \right) P \left( a_i, a_i' | y_0^i, y_1^i, x_A^i, x_D^i \right)
\]

\[
= \bigotimes_{i=1}^{n} U \left( y_0^i, y_1^i, x_D^i, x_A^i \right) P \left( a_i, a_i' | y_0^i, y_1^i, x_A^i, x_D^i \right)
\]

\[
= \bigotimes_{i=1}^{n} U \left( y_0^i, y_1^i, x_D^i, x_A^i \right) P \left( a_i, a_i' | y_0^i, y_1^i, x_A^i, x_D^i \right) = \mu(S),
\] (B14)

where \( \pi^{-1} \) above denotes that equality follows from the properties of the inverse of map \( \pi \), which due to involution property is equal to \( \pi \).

Alice, as before, gets bit \( x_A^j \), but Frederick obtains XOR of bits \( x_A^j \) and \( x_F^j \). Despite this, ‘original’ box, due to ‘wirings’, receives \( x_A^j \) and \( x_F^j \). We have then an important corollary that we can focus now on the XOR scenario because the probability of forgery in the latter equals the probability of forgery in the former.

**Corollary 1.**

\[
P_{\mu}(\mathcal{F}) = P_{\mu'}(\mathcal{F}').
\] (B15)

One can focus on the typical sequences \( S \), i.e. those for which \( x_S \in \mathcal{T}(\eta) \), at the expense of exponentially small inaccuracy in estimating the probability of forgery due to measure \( \mu' \).

**Lemma 1.**

\[
P(\mathcal{F}) \leq P(\mathcal{F} \cap T(\eta)) + \epsilon(\eta),
\] (B16)

with \( \epsilon(\eta) = 2 \exp(-2 \eta^2 n) \).

**Proof.** With a little abuse of notation we will mean by \((y_0^i, y_1^i, a_D^i, x_D^i, a_F^i)\) the properly ordered sequence of tuples \((y_0^i, x_D^i, a_D^i, x_D^i, a_F^i)_{i=1}^{n}\), where \( y_0 = (y_0^i)_{i=1}^{n} \), and by analogy the same for other symbols.
We will show first a sequence of (in)equalities:

\[
P(\mathcal{F}) = \sum_{S' \in \mathcal{F}} P_{\mu'}(S')
= \sum_{S' \in \mathcal{F} \cup T(\eta)} P_{\mu'}(S')
+ \sum_{S' \in \mathcal{F} \cap T(\eta)} P_{\mu'}(S')
= \sum_{S', x_{\text{str}} \in S' \cap \mathcal{F}} u(x_{\text{str}}) u(y_{\text{str}}) P(ax_{\text{str}}, ay_{\text{str}} | ay_{\text{str}}, y_{\text{str}}, x_{\text{str}}) + x_{\text{str}} \oplus x_{\text{str}}
+ \sum_{S', x_{\text{str}} \in S' \cap \mathcal{F} \cap T(\eta)} u(x_{\text{str}}) u(y_{\text{str}}) P(ax_{\text{str}}, ay_{\text{str}} | ay_{\text{str}}, y_{\text{str}}, x_{\text{str}} \oplus x_{\text{str}})
\leq \sum_{S', x_{\text{str}} \in S' \cap \mathcal{F}} u(x_{\text{str}}) u(y_{\text{str}}) u(y_{\text{str}}) P(ax_{\text{str}}, ay_{\text{str}} | ay_{\text{str}}, y_{\text{str}}, x_{\text{str}} \oplus x_{\text{str}})
+ \sum_{S', x_{\text{str}} \in S' \cap \mathcal{F} \cap T(\eta)} u(x_{\text{str}}) u(y_{\text{str}}) u(y_{\text{str}}) P(ax_{\text{str}}, ay_{\text{str}} | ay_{\text{str}}, y_{\text{str}}, x_{\text{str}} \oplus x_{\text{str}})
\leq P(\mathcal{F} \cap T(\eta)) + \epsilon(\eta).
\]

We have used the fact that the distribution of \(x_{\text{str}}\) is the same (uniform) irrespectively of a particular attack. This is because the distributions of \(x_{\text{str}}\) and \(x_{\text{str}}\) with respect to the measure \(\mu\) are uniform and independent from the attack. It follows from the fact that there are being prior to the attack. Similarly, \(x_{\text{str}}\) has the distribution of \(x_{\text{str}} \oplus x_{\text{str}}\) according to the definition of a measure \(\mu\). In the last inequality, we have used the typicality argument from equation (B5).

Due to the random nature of variable \(x_{\text{str}}\),

\[
P(\mathcal{F} \cap T(\eta)) = \sum_{x_{\text{str}} \in T(\eta)} P(x_{\text{str}}) P(\mathcal{F} | x_{\text{str}}).
\]

The advantage of the measure \(\mu\) is that we can easily divide the set of each run \(i\) according to the values of the \(x_{\text{str}}\). Technical as it sounds, it will simplify the argument. In the runs where \(x_{\text{str}} = 0\), the best strategy achieves quantum value \(P_T\) for both Alice and Frederick. However, for \(x_{\text{str}} = 1\), they are in a position of Alice guessing the opposite bit to the one which Frederick is at the same time in this run \(i\) to guess. Hence, they are limited, as it is shown in the original paper by Pawlowski and Brunner [14].

From now on, we will fix \(x_{\text{str}} := (x_{\text{str}})_{i=1}^n - 1\) and prove a common bound on guessing for all of its typical values. We can then define new conditional measure \(\mu^n\) that depends on \(x_{\text{str}}\) as

\[
\mu^n := \mu_{x_{\text{str}}} = \delta(x_{\text{str}}, x_{\text{str}}) \otimes \delta (x_{\text{str}}) u(x_{\text{str}}) u(y_{\text{str}}) P(x_{\text{str}} | x_{\text{str}}) d_{x_{\text{str}}} x_{\text{str}} x_{\text{str}} \oplus x_{\text{str}}, y_{\text{str}}, y_{\text{str}}.
\]

We will now show that, on average, the forgeries Alice and Frederick have the total number of correctly guessed bits of \(y_{\text{str}}\) bit-strings bounded from above by particular value. Let us first define the set of indexes

\[
D(x_{\text{str}}) := \{i \in [n]: x_{\text{str}} = 0\},
\]

and its complement \(D(x_{\text{str}})\). It is important to notice that, for runs in the set \(D(x_{\text{str}})\), Alice and Frederick will be asked about the same Bank’s bit and in the case of \(D(x_{\text{str}})\) they will have to guess two different bits of the Bank.

Then we can consider four types of random variables defined on \(\Omega_1\), each depending on the value of the \(x_{\text{str}}\). It is important to notice that these variables describe the probabilities of guessing appropriate bits in \(i\)th run, by Alice and Frederick respectively and furthermore have a strong connection with the definition of \(\mathcal{F}\).

\[
X_{x_{\text{str}}} := \delta(a_{x_{\text{str}}}, y_{x_{\text{str}}}); \quad i \in D(x_{\text{str}})
\]

\[
Y_{x_{\text{str}}} := \delta(a_{x_{\text{str}}}, y_{x_{\text{str}}}); \quad i \in D(x_{\text{str}})
\]

\[
X_{x_{\text{str}}} := P_{i} \oplus X_{x_{\text{str}}}; \quad i \in D(x_{\text{str}})
\]

\[
Y_{x_{\text{str}}} := P_{i} \oplus Y_{x_{\text{str}}}; \quad i \in D(x_{\text{str}})
\]

where the sample space is defined as

\[
\Omega_{x_{\text{str}}} := \{S^i: x_{\text{str}}(S^i) = x_{\text{str}}\}
\]

while \(x_{\text{str}}(S^i)\) denotes taking a variable with a label \(x_{\text{str}}\) from the sequence \(S^i\). We will also define sums

\[
X_{x_{\text{str}}} := X_{x_{\text{str}}} + X_{x_{\text{str}}}, \quad Y_{x_{\text{str}}} := Y_{x_{\text{str}}} + Y_{x_{\text{str}}},
\]

and the random variables built from \(X_{x_{\text{str}}}\) and \(Y_{x_{\text{str}}}\) that is their sums:

\[
\hat{X}_{x_{\text{str}}} := \sum_{i \in [n]} X_{x_{\text{str}}}, \quad \hat{X}_{x_{\text{str}}} := \sum_{i \in [n]} X_{x_{\text{str}}}, \quad \hat{X}_{x_{\text{str}}} := \sum_{i \in [n]} X_{x_{\text{str}}},
\]

\[
\hat{Y}_{x_{\text{str}}} := \sum_{i \in [n]} Y_{x_{\text{str}}}, \quad \hat{Y}_{x_{\text{str}}} := \sum_{i \in [n]} Y_{x_{\text{str}}}, \quad \hat{Y}_{x_{\text{str}}} := \sum_{i \in [n]} Y_{x_{\text{str}}},
\]

and its complement \(D(x_{\text{str}})\). It is important to notice that these variables describe the probabilities of guessing appropriate bits in \(i\)th run, by Alice and Frederick respectively and furthermore have a strong connection with the definition of \(\mathcal{F}\).
From equation (B19) we know that the measure $\mu''$ is a product of measures
\[
\mu'' = u(x'_1)u(y'_1)u(y'_2)P^i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)
\] (B27)
what implies that $X^a, X^e, X_{x_i}, X_{y_i}, T^{e_i}, T_{y_i}$ are described by Poisson distribution.

The respective averages over the measure $\mu''$ read
\[
\mathbb{E}X_{x_i} = \sum_{j \in [n]} \sum_{(x'_i, y'_i) \in \{0,1\}^2} \frac{1}{8} \sum_{(a'_i, d'_i) \in \{0,1\}} P_i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)X^a(j),
\] (B28)
\[
\mathbb{E}Y_{x_i} = \sum_{j \in [n]} \sum_{(x'_i, y'_i) \in \{0,1\}^2} \frac{1}{8} \sum_{(a'_i, d'_i) \in \{0,1\}} P_i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)Y^a(j).
\] (B29)

Although the above averages are defined on the whole range $[n]$, they depend only on their respective subsets:
\[
\mathbb{E}X_{x_i} = \sum_{j \in D(x_i)} \sum_{(x'_i, y'_i) \in \{0,1\}^2} \frac{1}{8} \sum_{(a'_i, d'_i) \in \{0,1\}} P_i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)\delta(a'_i, y'_1) + \delta(a'_i, 0)
\] (B30)
\[
\mathbb{E}Y_{x_i} = \sum_{j \in D(x_i)} \sum_{(x'_i, y'_i) \in \{0,1\}^2} \frac{1}{8} \sum_{(a'_i, d'_i) \in \{0,1\}} P_i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)\delta(a'_i, y'_1)
\times [\delta(a'_i, y'_1) + \delta(a'_i, 0)]
\] (B31)

We will prove now that the above averages are bounded if the attack is made in a qubit-by-qubit manner, and adversaries are quantum (see Assumptions ASM3–ASM6).

**Lemma 2.**
\[
\mathbb{E}X_{x_i} + \mathbb{E}Y_{x_i} \leq 2P_D|D(x_i)| + M|D(x_i)|.
\] (B32)

**Proof.** We will separately prove that the first term of lhs is bounded by the first term of rhs, and later that the second term of lhs is bounded by the second term of rhs. The best quantum strategy for a single person (say, Alice) in a single run of experiment is upper bounded by $P_Q$, while the other party is asked to guess the same bit as Alice was asked, so can copy her answer. We have
\[
\mathbb{E}X_{x_i} = \sum_{j \in D(x_i)} \sum_{(x'_i, y'_i) \in \{0,1\}^2} \frac{1}{8} \sum_{(a'_i, d'_i) \in \{0,1\}} P_i(a'_i, a'_i|x'_i, x'_i \oplus x'_i, y'_1, y'_1)\delta(a'_i, y'_1) + \delta(a'_i, 0)
\] (B33)
Now, for each $i \in D$, there is:
\[
\mathbb{E}X^a_{x_i} = \frac{1}{2}(P_A(y_0|x_A = 0) + P_A(y_1|x_A = 1) \leq P_Q
\] (B34)
where we here used equation (7) of [14] (note the change of notation: our $x, y, a_A$ correspond to $y, a_i, b$ there, respectively). Analogously, for $i \in D$,
\[
\mathbb{E}X^e_{x_i} = \frac{1}{2}(P_T(y_0|x_F = 0) + P_T(y_1|x_F = 1) \leq P_Q
\] (B35)
Summing the above inequalities over $i \in D$ we obtain $\mathbb{E}X_{x_i} \leq 2P_D|D(x_i)|$. 

22
More elaborative is relating the second terms of (B32). We begin analogously:

\[
\begin{align*}
\mathbb{E}^F_{x_o} &= \sum_{i \in \mathcal{D}(x_o)} \sum_{x' \in \mathcal{S}_i^{(x_o)}} \sum_{y' \in \mathcal{S}_i^{(x_o)}} P_i(a_i, a'_i|x, \hat{x}_i, +1, \hat{y}_i, \hat{y}'_i) \\
&\times \left[ \delta(a'_i, \hat{y}_i) + \delta(a'_i, \hat{y}'_i) \right] \\
&= \sum_{i \in \mathcal{D}(x_o)} \sum_{x' \in \mathcal{S}_i^{(x_o)}} \sum_{y' \in \mathcal{S}_i^{(x_o)}} P_i(a_i, a'_i|x, \hat{x}_i, +1, \hat{y}_i, \hat{y}'_i) \\
&\times \left[ \delta(a'_i, \hat{y}_i) + \delta(a'_i, \hat{y}'_i) \right] \\
&+ \sum_{i \in \mathcal{D}(x_o)} \sum_{x' \in \mathcal{S}_i^{(x_o)}} \sum_{y' \in \mathcal{S}_i^{(x_o)}} P_i(a_i, a'_i|x, \hat{x}_i, +1, \hat{y}_i, \hat{y}'_i) \cdot \delta(a'_i, \hat{y}_i) \\
&= \sum_{i \in \mathcal{D}(x_o)} EY^A_{i,x_o} + EY^F_{i,x_o},
\end{align*}
\]

(B36)

For each \( i \in \mathcal{D}(x_o) \),

\[
EY^A_{i,x_o} + EY^F_{i,x_o} = \frac{1}{2} \left[ P_A(y'_i|x'_i = 0) + P_F(y'_i|x'_i = 0) + P_A(y'_i|x'_i = 1) + P_F(y'_i|x'_i = 1) \right]
\]

\[
\leq \frac{1}{2} \left[ P_A(y'_i|x'_i = 0) + P_F(y'_i|x'_i = 0) + P_A(y'_i|x'_i = 1) + P_F(y'_i|x'_i = 1) \right]
\]

\[
= \frac{1}{2} \left[ P_A(y'_i|x'_i = 0) + P_A(y'_i|x'_i = 1) + \frac{1}{2} \left[ P_A(y'_i|x'_i = 0) + P_A(y'_i|x'_i = 1) \right] \right]
\]

\[
= P_A(y'_i) + P_A(y'_i) \leq M,
\]

(B37)

where in the pre-last inequality we have used the fact, that Alice and Frederick can collaborate. This can only increase the average probability of guessing. In the last inequality we have rephrased the results of [14] as in Observation 4. Summing up over \( i \in \mathcal{D}(x_o) \), we obtain

\[
\sum_{i \in \mathcal{D}(x_o)} EY^A_{i,x_o} + EY^F_{i,x_o} \leq M|\mathcal{D}(x_o)|,
\]

(B38)
as it was claimed.

We have shown above that the average number of guessed bits has an upper bound. We are going now to argue about the concentration properties of the random variables involved in the process.

We assume here that \( x_o \) is fixed, and results in the well defined sets \( \mathcal{D}(x_o) \) and \( \mathcal{D}(x_o) \). For brevity, we will sometimes omit \( x_o \) from the notation of \( D \). We will also define subsequences \( S_i \) and \( S_i' \) of particular realization of strategy \( S_i \).

\[
S_i = (S_i^{(x_o)})_{i \in \mathcal{D}(x_o)}, \quad S_i' = (S_i^{(x_o)})_{i \in \mathcal{D}(x_o)},
\]

(B39)

In the spirit of the above technical lemma, we will consider four random variables, each reporting the distance between the theoretical average value of a number of guessed inputs and the observed number of guessed inputs for the respective dishonest player on the respective set (\( D(x_o) \) or \( \mathcal{D}(x_o) \)).

\[
c_1 = \begin{cases} 1 : |\mathbb{E}^A_{x_o} - \hat{X}_{x_o}^{(A)}| \leq \eta |D(x_o)|, \\
0 : \text{else} \end{cases} \quad c_2 = \begin{cases} 1 : |\mathbb{E}^A_{x_o} - \hat{X}_{x_o}^{(A)}| \leq \eta |D(x_o)|, \\
0 : \text{else} \end{cases}
\]

\[
c_3 = \begin{cases} 1 : |\mathbb{E}^F_{x_o} - \hat{X}_{x_o}^{(F)}| \leq \eta |D(x_o)|, \\
0 : \text{else} \end{cases} \quad c_4 = \begin{cases} 1 : |\mathbb{E}^F_{x_o} - \hat{X}_{x_o}^{(F)}| \leq \eta |D(x_o)|, \\
0 : \text{else} \end{cases}
\]

(B40)

Due to the concentration property given in equation (B1) on the total measure \( \mu'' \), that is product of measures \( \mu'' \) (see equation (B27)), base on which the joined distribution of \( X_1, \ldots, X_k \) random variables defined above, we can bound the probability of 0’s as follows:

\[
p(c_1 = 0) \leq 2e^{-2\eta |D(x_o)|} = \epsilon_1(\eta), \quad p(c_2 = 0) \leq 2e^{-2\eta |D(x_o)|} = \epsilon_2(\eta),
\]

\[
p(c_3 = 0) \leq 2e^{-2\eta |D(x_o)|} = \epsilon_3(\eta), \quad p(c_4 = 0) \leq 2e^{-2\eta |D(x_o)|} = \epsilon_4(\eta),
\]

(B41)

where the probability of the above measures is taken over the measure \( \mu'' \).

Now, thanks to the union bound, we obtain:

**Corollary 2.** For any \( x_o \), there is

\[
P_{\mu''}(\{ |\mathbb{E}^A_{x_o} - \hat{X}_{x_o}^{(A)}| \leq \eta |D(x_o)| \} \land \{ |\mathbb{E}^F_{x_o} - \hat{X}_{x_o}^{(F)}| \leq \eta |D(x_o)| \} \\ \land \{ |\mathbb{E}^A_{x_o} - \hat{X}_{x_o}^{(A)}| \leq \eta |D(x_o)| \} \land \{ |\mathbb{E}^F_{x_o} - \hat{X}_{x_o}^{(F)}| \leq \eta |D(x_o)| \}) \geq 1 - \sum_{i} \epsilon_i(\eta),
\]

(B43)
The above rather technical results are summarized below in the upper bound on the total number of guesses. Namely, we will show that for a fixed $x_{\eta}$, and an attack defining the measure $\mu'' = \mu'_{|x_{\eta}}$, the random variable of the total number of guesses defined as a function of $S'(x_{\eta})$ sampled from $\mu''$ is bounded from above with high probability, as it is close to the sum of averages that are bounded. Indeed, let us define the random variable of the total number of guesses,

$$Z_{x_{\eta}} := \bar{X}_{x_{\eta}}^A + \bar{X}_{x_{\eta}}^F + \bar{Y}_{x_{\eta}}^A + \bar{Y}_{x_{\eta}}^F.$$  

We additionally define two other useful variables,

$$\bar{Z}_{x_{\eta}}^A := \bar{X}_{x_{\eta}}^A + \bar{Y}_{x_{\eta}}^A, \quad \bar{Z}_{x_{\eta}}^F := \bar{X}_{x_{\eta}}^F + \bar{Y}_{x_{\eta}}^F.$$  

**Lemma 3.** For any fixed $x_{\eta} \in T(\eta)$,

$$P_{\mu''}(Z_{x_{\eta}} > B) \leq \sum_{i=1}^{4} \epsilon_i(\eta),$$  

where

$$B = 2P_0\left(\frac{1}{2} + \eta\right)n + M\left(\frac{1}{2} + \eta\right)n + 2\eta n.$$  

**Proof.** From the corollary 2, omitting the modulus, we obtain a sequence of inequalities

$$1 - \sum_{i=1}^{4} \epsilon_i(\eta) \leq P_{\mu''}(|E\bar{X}_{x_{\eta}}^A - \bar{X}_{x_{\eta}}| \leq |E\bar{Y}_{x_{\eta}}^A - \bar{Y}_{x_{\eta}}| \leq \eta|D(x_{\eta})| \wedge |E\bar{X}_{x_{\eta}}^F - \bar{X}_{x_{\eta}}| \leq |E\bar{Y}_{x_{\eta}}^F - \bar{Y}_{x_{\eta}}| \leq \eta|D(x_{\eta})|)$$

$$\leq P_{\mu''}(E\bar{X}_{x_{\eta}}^A \leq \bar{X}_{x_{\eta}} + \eta|D(x_{\eta})| \wedge E\bar{Y}_{x_{\eta}}^A \leq \bar{Y}_{x_{\eta}} + \eta|D(x_{\eta})|)$$

$$\leq P_{\mu''}(E\bar{X}_{x_{\eta}}^A + \bar{Y}_{x_{\eta}}^A + \bar{X}_{x_{\eta}}^F + \bar{Y}_{x_{\eta}}^F \leq E\bar{X}_{x_{\eta}}^A + E\bar{Y}_{x_{\eta}}^A + E\bar{X}_{x_{\eta}}^F + E\bar{Y}_{x_{\eta}}^F + 2\eta n)$$

$$\leq P_{\mu''}(\bar{Z}_{x_{\eta}} \leq 2P_0|D(x_{\eta})| + M|D(x_{\eta})| + 2\eta n)$$

$$\leq P_{\mu''}(Z_{x_{\eta}} > B).$$  

In the second inequality we have used lemma 2. In the next one we have used definition of $\bar{Z}_{x_{\eta}}$, and then we have used the typicality of $x_{\eta}$, which implies upper bounds on the power of sets $D(x_{\eta})$ and $D(x_{\eta})$. This implies

$$P_{\mu''}(Z_{x_{\eta}} > B) \leq \sum_{i=1}^{4} \epsilon_i(\eta),$$  

as we have claimed.

Let us recall now definition of $\mathcal{F}'$ from equation (B9)

$$\mathcal{F}' := \{\{y'_i, x'_i, d'_i, x'_i, d'_i\}_{i=1}^{6n}: \{|i\in[n]: a'_i = y'_i| > \theta n, \} > \theta n\}.$$  

In what follows for clarity we will explicitly show dependence on $\theta$ using notation $\mathcal{F}'_{\theta}$.

**Observation 6.** Let the acceptance threshold be $\theta > B/2$. Then

$$P(\mathcal{F}'_{\theta} \cap T(\eta)) \leq \epsilon_2'(\eta) := \max_{x_{\eta} \in T(\eta)} \epsilon_2(\eta, x_{\eta}),$$  

where $\epsilon_2(\eta, x_{\eta}) = \sum_{i=1}^{4} \epsilon_i(\eta)$.

**Proof.** Let us fix $x_{\eta}$. Then there is

$$\mathcal{F}_{\theta|x_{\eta}} := \{S'(x_{\eta}) : Z_{x_{\eta}}^A \geq \theta \wedge Z_{x_{\eta}}^F \geq \theta\}$$

$$\subseteq \{S'(x_{\eta}) : Z_{x_{\eta}}^A + Z_{x_{\eta}}^F \geq 2\theta\}$$

$$= \{S'(x_{\eta}) : Z_{x_{\eta}} \geq B\}.$$  

The above fact is consequences of the sequence of implications, where the last follows from $2\theta > B$. We now invoke equation (B18) and note immediately a bound:
In the pre-last inequality we have used lemma 3 with \( \epsilon_2(\eta) = \sum_{\eta_{i=1}}^{4} \epsilon_{i}(\eta_{i}) = \epsilon_2(\eta). \)

**Appendix C. Proof of main theorem**

Finally, after presenting all necessary definitions and lemmas, we are ready to proof theorem 1. For convenience of the reader we will first restate the theorem. Let

\[
\beta_{\eta} = P_{0}\left(1 + \frac{1}{2} + \eta + \frac{M}{2} + \eta\right) + \eta
\]

\[
= \left(\cos^{2}\left(\frac{\pi}{8}\right) + \frac{5 + \sqrt{3}}{8}\right)\left(\frac{1}{2} + \eta\right) + \eta
\]

\[
= \frac{8 \cos^{2}\left(\frac{\pi}{8}\right) + 8 \cos^{2}\left(\frac{\pi}{8}\right) + 5 + \sqrt{3} + 8}{16} + \frac{17 + 2 \sqrt{2} + \sqrt{3}}{8} \eta
\]

\[
\approx 0.847 5 + 2.695 0 \eta,
\]

for some small \( \eta \) chosen in such a way that \( \beta_{\eta} \leq P_{0} \).

**Theorem 2 (Security of semi-device-independent Quantum Money).** Let acceptance threshold \( \theta \) be larger than \( \beta_{\eta} n \). Then, under Assumptions ASM1–ASM6, where \( k \) denotes the number of Bank’s branches the probability of a successful forgery \( P(\mathcal{F}_{\theta}) \) is exponentially small in number of banknote’s qubits \( n \) and is bounded by

\[
P(\mathcal{F}_{\theta}) \leq 10 k^{2} e^{-2\gamma\left(1 - \eta\right)n}.
\]

**Proof.** Using corollary 1, lemma 1, and Observation 6 we obtain the following bound on \( P(\mathcal{F}) \)

\[
\begin{align*}
P_{\eta}(\mathcal{F}) & \overset{\text{Eq. (B16)}}{=} P_{\eta}(\mathcal{F}') \\
& \overset{\text{Eq. (B15)}}{=} P_{\eta}(\mathcal{F}' \cap T(\eta)) + \epsilon(\eta) \\
& \overset{\text{Eq. (B51)}}{\leq} \max_{x_{i} \in T(\eta)} \epsilon_{2}(\eta, x_{i}) + \epsilon(\eta) \\
& \leq 5 \xi_{\eta} = 10 e^{-2\gamma\left(1 - \eta\right)n}.
\end{align*}
\]

Since there are many Bank’s branches, collaborating Alice and Frederick can use birthday attack in order to choose two branches that have the biggest common set \( D \). For \( k \) branches, we apply union bound obtaining another factor \( k^{2} \) what finalizes the proof.

**Appendix D. Proof of No-go for device-independent quantum money**

In this section, we will provide more formal proof of Observation 1.

**Proof.** We will follow the standard proof technique used in device-independent scenarios. Since all of the quantum devices are untrusted, the only way for Bank’s branches to verify the money is to use classical statistics of inputs and outputs from quantum black boxes. Without loss of generality, we can assume a four-partite scenario with two Bank’s branches \( B_{1}, B_{2} \), Alice A, and Frederick F that all share some nonlocal box. We will denote the device’s inputs as \( I \) and outputs as \( O \) with appropriate subscript denoting the party. The general scenario can be modeled by the probability distribution of the form

\[
D = P(O_{B_{1}}, O_{B_{2}}, O_{A}, O_{F}|I_{B_{1}}, I_{B_{2}}, I_{A}, I_{F}).
\]
In the verification phase, Alice tries to pass verification with branch $B_1$, while Frederick tries with branch $B_2$. Since Bank’s branches cannot communicate, they have access only to the part of outputs. Therefore, the only way is to check correlations from distribution
\[
D_1 = P(O_{B_1}, O_A | I_{B_1}, I_A, I_{B_2}, I_F)
\]
for the branch $B_1$ and
\[
D_2 = P(O_{B_2}, O_A | I_{B_2}, I_F, I_{B_1}, I_A)
\]
for the branch $B_2$. We assume here that Alice and Frederick can freely talk during the verification stage. In order to be secure, the money scheme has to disallow both Alice and Frederick to pass verification. Furthermore, the conditions for passing verification have to be the same for all branches. Since there must exist a honest quantum implementation (see appendix E) for Alice with distribution $H_1$, then Frederick could also pass verification using the same distribution $D_2 = H_2$. To obtain such a result, Adversary, controlling the source and measurement devices, can prepare joined devices with distribution $D \sim H_1 H_1$. Such preparation of state and measurement will always break any device-independent money scheme and cannot be detected by the Bank in any way without communication between the branches of the Bank.

**Appendix E. Honest implementation**

In this appendix we will present honest implementation based on Semi-Device-independent Quantum Key Distribution [14]. Let, for all runs $i$, the honest source prepare all states $\rho_{\psi^{i}_{\psi}}$ in the following way
\[
\rho_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho_{10} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},
\]
where $|1\rangle = (|\psi\rangle \pm |\psi\rangle)/\sqrt{2}$. Let us also choose an appropriate measurement $M_i$, depending on the branch’s question $x^i$,
\[
M_0 := \frac{\sigma_x + \sigma_z}{\sqrt{2}}, \quad M_1 := \frac{\sigma_x - \sigma_z}{\sqrt{2}},
\]
where $\sigma_x$ and $\sigma_z$ are Pauli matrices
\[
\sigma_x := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\]
It turns out, as shown in [14], that, using these states and measurements, the optimal guessing probability equals $P_Q = \cos^2(\pi/8)$.

**Remark 4 (Connection with Wiesner’s money scheme)**. In the honest implementation of our scheme, we use the same states as in the original Wiesner’s scheme. On the other hand, the measurement settings have to be different since, from [14], we know that Wiesner’s cannot be used in the semi-device-independent approach.

**Appendix F. Required number of qubits**

This appendix establishes the relation between the number of qubits and the upper bounds on the probability of forgery. Since from the equation (C) we know that $\beta_\eta \leq P_Q$, we can calculate that the maximal allowed value of $\eta$ equals
\[
\eta_{\text{max}} = \frac{-1 + 2\sqrt{2} - \sqrt{3}}{34 + 4\sqrt{2} + 2\sqrt{3}} \approx 0.0022.
\]
When we put that value into equation (10), for the trivial case of the single Bank without any additional branches, we obtain that
\[
P(\mathcal{F}) \leq 10e^{-2\eta_{\text{max}}^2 \left(1 - \eta_{\text{max}}\right)^n}.
\]
It is easy to calculate numerically that this bound becomes trivial when the number of qubits $n$ is smaller than 463018. Furthermore, when we demand that the probability of forgery is smaller than some security parameter and we want to assume a more realistic scenario the number of required qubits grows significantly.

Although one cannot expect that such a large number of qubits will be available in quantum memories soon, let us emphasize that the bounds used in the proof of theorem 1 are not tight, and there is some room for improvement. What is more important, we expect that using more complex random access codes, i.e. ones with more inputs and outputs, can lead to a significant decrease in the number of required qubits as it is discussed in section 6.
References

[1] Wiesner S 1983 Conjugate coding SIGACT News 15 78
[2] Park J I 1970 The concept of transition in quantum mechanics Found. Phys. 1 23
[3] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned Nature 299 802
[4] Diks D 1982 Communication by EPR devices Phys. Lett. A 92 271
[5] Molina A, Vidick T and Watrous J 2013 Optimal counterfeiting attacks and generalizations for wiesner’s quantum money Theory of Quantum Computation, Communication, and Cryptography K E Iwama et al (Berlin: Springer) pp 45–64
[6] Pastawski F, Yao N Y, Jiang L, Lukin M D and Cirac J I 2012 Unforgeable noise-tolerant quantum tokens Proc. Natl Acad. Sci. 109 16079
[7] Gavinsky D 2012 Quantum money with classical verification 2012 IEEE 27th Conf. on Computational Complexity (Piscataway, NJ) (Piscataway, NJ: IEEE) pp 42–52
[8] Becker G T, Regazzoni F, Paar C and Burleson W P 2013 Stealthy dopant-level hardware trojans Cryptographic Hardware and Embedded Systems—CHES 2013 (Berlin: Springer) pp 197–214
[9] Lydersen L, Wittmann W C C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination Nat. Photon. 4 686
[10] Barrett J, Hardy L and Kent A 2005 No signaling and quantum key distribution Phys. Rev. Lett. 95 010503
[11] Acín A, Gisin N and Masanes L 2006 From Bell’s theorem to secure quantum key distribution Phys. Rev. Lett. 97 120405
[12] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (New York, Bangalore, India) (IEEE Computer Society Press) pp 175–9
[13] Bozzo M, Diamanti E and Grosshans F 2019 Semi-device-independent quantum money with coherent states Phys. Rev. A 99 022336
[14] Pawłowski M and Brunner N 2011 Semi-device-independent security of one-way quantum key distribution Phys. Rev. A 84 010302
[15] Pawłowski M, Paterek T, Kaszlikowski D, Scarani V, Winter A and Zacikowski M 2009 Information causality as a physical principle Nature 461 1101
[16] Gallego R, Brunner N, Hadley C and Acín A 2010 Device-independent tests of classical and quantum dimensions Phys. Rev. Lett. 105 230501
[17] Brunner N, Navascués M and Vértesi T 2013 Dimension witnesses and quantum state discrimination Phys. Rev. Lett. 110 150501
[18] König R 2007 de Finetti theorems for quantum states PhD Thesis University of Cambridge
[19] Holevo A 1973 Bounds for the quantity of information transmitted by a quantum communication channel Problems Inf. Transm. 9 177
[20] Aaronson S 2016 The complexity of quantum states and transformations: from quantum money to black holes arXiv:1607.05256
[21] Brunner N, Navascués M and Vértesi T 2013 Dimension witnesses and quantum state discrimination Phys. Rev. Lett. 110 150501
[22] Acín A, Gisin N and Masanes L 2006 From Bell’s theorem to secure quantum key distribution Phys. Rev. Lett. 97 120405
[23] Bennett C H, Brassard G, Breidbart S and Wiesner S 1983 Quantum cryptography, or unforgeable subway tokens Found. Phys. Lett. 10 7
[24] Lutomirski M and Brunner N 2011 Semi-device-independent quantum money with coherent states Phys. Rev. A 99 022336
[25] Pawłowski M and Brunner N 2011 Semi-device-independent security of one-way quantum key distribution Phys. Rev. A 84 010302
[26] Pawłowski M, Paterek T, Kaszlikowski D, Scarani V, Winter A and Zacikowski M 2009 Information causality as a physical principle Nature 461 1101
[27] Amiri R and Arrazola J M 2017 Quantum money with nearly optimal error tolerance Phys. Rev. A 95 062334
[28] Mosca M and Stefka D 2010 Quantum coins Error-Correcting Codes, Finite Geometries and Cryptography, Contemporary Mathematics ed A A Bruen and D L Wehlau vol 523 (Providence, RI: American Mathematical Society) pp 35–47
[29] Tokunaga Y, Okamoto T and Imoto N 2003 Anonymous quantum cash ERATO Conf. on Quantum Information Science
[30] Selby J H and Sikora J 2018 How to make unforgeable money in generalised probabilistic theories Quantum 2 103
[31] Bartkiewicz K, vCernoch A, Chmizczak G, Lemer K, Miranowicz A and Nori F 2017 Experimental quantum forgery of quantum optical money npj Quantum Inf. 3 7
[32] Bozzo M, Orieuex A, Vidarte I T, Zaqine I, Kerenidis I and Diamanti E 2018 Experimental investigation of practical unforgeable quantum money npj Quantum Inf. 4 5
[33] Guan J-Y, Arrazola J M, Amiri R, Zhang W, Li H, You L, Wang Z, Zhang Q and Pan J-W 2018 Experimental preparation and verification of quantum money Phys. Rev. A 97 032338
[34] Jiráková K, Bartkiewicz K, vCernoch A and Lerner K 2019 Experimentally attacking quantum money schemes based on quantum retrieval games Sci. Rep. 9 16318
[35] Kumar N 2019 Practically feasible robust quantum money with classical verification Cryptography 3 26
[36] Radaï and Sattath 2019 Semi–quantum money Proc. 1st ACM Conf. on Advances in Financial Technologies—AFT ’19 (ACM) (https://doi.org/10.1145/3318041.3355462)
[37] Aaronson S and Christiano P 2012 Quantum money from hidden subspaces Proc. 44th Annual ACM Symp. on Theory of Computing, STOC’12 (New York, NY, USA) (ACM) pp 41–60
[38] Lutomirski A, Aaronson S, Farhi E, Gosset D, Kelner J A, Hassidim A and Shor P W 2010 Breaking and making quantum money: toward a new quantum cryptographic protocol Innovations in Computer Science—ICS 2010. Proc. (Tsinghua University, Beijing, China) pp 29–31
[39] Farhi E, Gosset D, Hassidim A, Lutomirski A, Nagaj D and Shor P 2010 Quantum state restoration and single–copy tomography for ground states of hamiltonians Phys. Rev. Lett. 105 190503
[40] Farhi E, Gosset D, Hassidim A, Lutomirski A and Shor P 2012 Quantum money from knots Proc. 3rd Innovations in Theoretical Computer Science Conf., ITCS ’12 (New York, NY, USA) (ACM) pp 276–89
[41] Lutomirski A 2011 Component mixers and a hardness result for counterfeiting quantum money arXiv:1107.0321
[42] Aaronson S, Farhi E, Gosset D, Hassidim A, Kelner J and Lutomirski A 2012 Quantum money *Commun. ACM* **55** 84
[43] Pena M C, Faugère J-C and Perret I 2015 Algebraic cryptanalysis of a quantum money scheme the noise-free case *Public-Key Cryptography—PKC 2015* ed J Katz (Berlin: Springer) pp 194–213
[44] Zhandry M 2019 Quantum lightning never strikes the same state twice *Advances in Cryptology—EUROCRYPT 2019* (Lecture Notes in Computer Science Vol 11478) ed Y Ishai and V Rijmen (Cham: Springer) pp 408–38
[45] Joge¡ors J 2019 Quantum bitcoin: an anonymous, distributed, and secure currency secured by the no-cloning theorem of quantum mechanics 2019 IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC) (Piscataway, NJ) IEEE (https://10.1109/ bloc.2019.8751473)
[46] Reda K 2018 qlightcoin: a peer-to-peer quantum cash system *Intelligent Computing. SAI 2018* (Advances in Intelligent Systems and Computing Vol 858) ed K Arai et al (Cham: Springer) (https://doi.org/10.1007/978-3-030-01174-1_58)
[47] Sun X, Wang Q, Kulicki P and Zhao X 2018 Quantum-enhanced logic-based blockchain: I. Quantum honest-success byzantine agreement and qulogicoin arXiv:1805.06768
[48] Kent A 2019 S-money: virtual tokens for a relativistic economy *Proc. R. Soc. A* **475** 20190170
[49] Kane D M 2018 Quantum money from modular forms arXiv:1809.05925
[50] Coladangelo A 2019 Smart contracts meet quantum cryptography arXiv:1902.05214
[51] Bennett C H and Wiensprer S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states *Phys. Rev. Lett.* **69** 2881
[52] Greenberger D M, Horne M A and Zeilinger A 1989 Going beyond Bell’s theorem *Bell’s Theorem, Quantum Theory and Conceptions of the Universe* (Dordrecht: Springer) pp 69–72
[53] Nayak A 1999 Optimal lower bounds for quantum automata and random access codes *Proc. 40th Annual Symp. on Foundations of Computer Science, FOCS ’99* (Washington, DC, USA) (IEEE Computer Society) p 369
[54] Wehner S, Christandl M and Doherty A C 2008 Lower bound on the dimension of a quantum system given measured data *Phys. Rev. A* **78** 062112
[55] Oresme N 1373 Tractatus de origine, natura, jure et de mutationibus monetarum
[56] Kopernik M 1526 Monetae cudendae ratio
[57] Oresme N 1373 Tractatus de origine, natura, jure et de mutationibus monetarum
[58] Sparavigna A C 2014 Some notes on the Gresham’s law of money circulation *Int. J. Sci.* **3** 80
[59] Wang Y, Um M, Zhang J, An S, Lyu M, Zhang J–N, Duan L, Yum D and Kim K 2017 Single-qubit quantum memory exceeding ten-minute coherence time *Nat. Photon.* **11** 646
[60] Harper R and Flammia R T 2019 Fault-tolerant logical gates in the IBM quantum experience *Phys. Rev. Lett.* **122** 080504
[61] Preskill J 2018 Quantum computing in the NISQ era and beyond *Quantum* **2** 79
[62] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 Quantum repeaters: the role of imperfect local operations in quantum communication *Phys. Rev. Lett.* **81** 5932
[63] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate–distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400
[64] Rausendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188
[65] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks *New J. Phys.* **11** 045021
[66] Arnon-Friedman R, Dupuis F, Fawzi O, Renner R and Vidick T 2018 Practical device-independent quantum cryptography via entropy accumulation *Nat. Commun.* **9** 439
[67] Wang Y, Bao W–S, Li H–W, Zhou C and Li Y 2014 Security of a practical semi-device-independent quantum key distribution protocol against collective attacks *Chin. Phys. B* **23** 080303
[68] Woodhead E and Pironio S 2015 Secrecy in prepare-and-measure Clauser–Horne–Shimony–Holt tests with a qubit bound *Phys. Rev. Lett.* **115** 110501
[69] Xu P, Bao W–S, Li H–W, Wang Y and Bao H–Z 2017 Proof of security of a semi-device-independent quantum key distribution protocol *Chin. Phys. Lett.* **34** 020302
[70] Zhou C, Xu P, Bao W–S, Wang Y, Zhang Y, Jiang M–S and Li H–W 2017 Finite-key bound for semi-device-independent quantum key distribution *Opt. Express* **25** 16971
[71] Chaturvedi A, Ray M, Veynar R and Pawłowski M 2018 On the security of semi-device-independent QKD protocols *Quantum Inf. Process.* **17** 131
[72] Sparaciari C, del Rio L, Scandolo C M, Faist P and Oppenheim J 2018 The first law of general quantum resource theories arXiv:1806.04937