3 Quantum money

In this chapter we put our freshly acquired formalism of qubits and measurements to good use by exploring a rather ancient cryptographic task: money! While traditional coins and bills can always be copied, the idea for "uncloneable" quantum money was discovered in the first paper ever written on quantum information, by Stephen Wiesner in the 1970s. Wiesner's key observation was that the possibility to encode information in different bases, such as the standard basis and the Hadamard basis, provides a natural mechanism for copy-protection. In this chapter we explain Wiesner's idea and take the opportunity to deepen our understanding of quantum states and measurements.

So what is money? Generally, a bill has two components. First, there is a physical object, such as a piece of paper or metal. Second, there is some identifier associated with the physical object, such as a serial number. The serial number is created on the day that the bill is minted, and it is used to specify all kinds of information about the bill, such as its value, its provenance, the date on which it was minted, etc. This information is kept by the bank as a means to keep track of all valid money in circulation.

The main security guarantee that one wants of money is that it cannot be duplicated. This is what the "paper" part of the bill is meant for: if the bill only consisted of a serial number, this number could be easily copied and the amount of real currency associated to it spent twice. A piece of paper is technically a little harder to duplicate than a mere number... but not impossible!

Remember the *no-cloning principle* from Chapter 1. Informally, this principle states that there is no quantum operation that can perfectly copy an arbitrary qubit. In other words, qubits cannot be duplicated. You can see where this is going, right? Let us first explore a very simple (but flawed) idea for a quantum money scheme.

3.1 A (too) simple quantum money scheme

Let us give a preliminary definition of a quantum bill as a physical object that consists of two parts: first, a classical "serial number" $\$$ which uniquely identifies the state and a copy of which is stored by the bank, and second a quantum state $|\psi_\$\rangle$ that constitutes the "uncloneable" component of the bill. Think of the serial number as a string of bits that is publicly known and records general information about the bill, such as when it was created, how much money it is worth (such as its gold equivalent), etc. Generally we will take the serial number to be $\$ \in \{0,1\}^n$ for some integer n that is sufficiently large so that we never run out of serial numbers, such as $n = 1024$.

Let's see the simplest quantum money scheme you might think of. To create a quantum bill, first generate a serial number $\$ \in \{0,1\}^n$ uniformly at random. Then create an n-qubit quantum state such that the i-th qubit is initialized in the standard basis state equal to the i-th bit of $\$$. In other words, create the quantum state $|\psi_\$\rangle = |\$\rangle$. The quantum bill is the pair $(\$, |\psi_\$\rangle)$ of the serial number and the state associated to it. Since qubits (and a fortiori n qubits) cannot be cloned, the scheme is secure, right?

Of course not! This scheme has no secret information. Given a quantum bill $(\$, |\psi_\$\rangle)$ it is very easy to create an unlimited number of identical copies of it, simply by using the serial number to prepare the state $|\psi_\$\rangle$. This does not violate the no-cloning principle, because we are given a classical description of the state: it is the standard basis state associated with the n-bit string $\$$. Given this classical description, and a quantum computer, it is straightforward to create as many copies of $|\psi_\$\rangle$ as desired. In fact, even if we didn't have access to the classical serial number, the scheme would be entirely broken, as an attacker could first measure $|\psi_\$\rangle$ in the standard basis to obtain $\$$, and then re-create as many copies of it as desired.

In case you're not sure why the no-cloning principle does not apply, remember that the impossible task is to design a quantum machine that has the ability to clone *every* state. But there still can be machines that clone specific families of states, such as all standard basis states. An interesting money scheme will necessarily involve states that are more complicated than simple standard basis states!

3.2 Wiesner's quantum money

In Wiesner's money scheme, each serial number $\$$ is made of two strings $x_\$, \theta_\$ \in \{0,1\}^n$, where n is an integer that parametrizes the security of the scheme (for example, $n = 1024$). In the following, we drop the subscript $\$$ and simply write x, θ for $x_\$, \theta_\$$. It is important that the pair (x, θ) is kept secret: it is generated at random by the bank on the day when the quantum bill is minted, but it is never revealed, even to the honest holder of the bill.

For $x_i, \theta_i \in \{0,1\}$ we introduce the notation $|x_i\rangle_{\theta_i} = H_i^\theta |x_i\rangle$.[1] Then the money state associated with $\$$ is the n-qubit state $|\psi_\$\rangle$ whose i-th qubit is in state $|x_i\rangle_{\theta_i}$:

$$|\psi_\$\rangle \;=\; |x_1\rangle_{\theta_1} \otimes \cdots \otimes |x_n\rangle_{\theta_n} \;.$$

Quiz 3.2.1. *Suppose that $n = 2$, and consider a serial number $\$$ such that $x_\$ = 01$ and $\theta_\$ = 10$. Then the associated quantum money state is*

a) $|\psi_\$\rangle = |0\rangle\,|1\rangle$
b) $|\psi_\$\rangle = |0\rangle\,|+\rangle$
c) $|\psi_\$\rangle = |+\rangle \otimes |1\rangle$

[1] The four possible states are thus $|0\rangle, |1\rangle$ (for $\theta = 0$) and $|+\rangle, |-\rangle$ (for $\theta = 1$). These states are often referred to as "BB'84" states — we will see why in Chapter 8.

Now that we've described a scheme, can you break it? That is, can you forge multiple copies of a quantum bill, given a single copy as input? If not, then why?

Based on the intuition that quantum information cannot in general be cloned, intuitively we shouldn't be able to copy quantum bills. However, as we saw the no-cloning theorem requires care in its application: in particular, "classical" states of the form $|000\rangle, |001\rangle$, etc. certainly can be copied! So does the no-cloning theorem apply in our setting, or not? To answer this we need to go back to the proof of the theorem, given in Section 1.6.3. If you examine the proof closely you will notice that the theorem already applies in case the only states considered are $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. This seems to rule out a perfect cloning machine for our quantum bills. However, let's be careful! If you measure each qubit of $|\psi_\$\rangle$ in either the standard or the Hadamard basis, without knowing which is the correct basis, you expect to get the right answer for approximately half the qubits. So, you "learn" half the state in this way. What if you could learn more? What if you could recover 99% of the qubits? Or all the qubits, 99% of the time? This is not obviously ruled out by the "qualitative" no-cloning theorem which we have seen. If this were the case, would we still want to consider the scheme to be secure, even though perfect cloning is impossible?

To answer this question we have to go through one of the most important exercises in cryptography: introducing a security definition! Until now we have been arguing about security at a very intuitive level; to make progress we need to establish firm foundations to support our investigation.

3.2.1 Definition of quantum money

To specify a quantum money scheme we need to answer the following questions: How (and by whom) is a quantum bill generated? And what is the procedure for determining the validity of a (candidate) bill? More formally, we define a quantum money scheme to consist of two procedures, each meant to answer one of these two questions:

- A *state generation procedure* $\mathrm{GEN}(1^n)$: This is the procedure applied by the bank to mint money. It takes as input an integer n specified in unary called the "security parameter" (intuitively, the larger n is, the more secure is the scheme).[2] The procedure returns a triple $(\$, |\psi_\$\rangle, k_\$)$ of a classical serial number $\$$, a quantum state $|\psi_\$\rangle$, and a classical "private key" $k_\$$ that specifies secret information about the bill that is to be kept by the bank.
- A *bill verification procedure* $\mathrm{VER}(\$, |\psi\rangle, k)$: This is the procedure executed by the bank to verify a quantum state. It takes as input a pair $(\$, |\psi\rangle)$ of a serial number and a quantum state, as well as a key k, and returns either "accept" or "reject".

Note that the state generation procedure GEN does not explicitly specify a denomination for the quantum bills. The simplest implementation of the scheme will associate an identical value to each money state, such as 1€. It is also possible to associate different values to

[2] The reason that n is specified as a string of 1's of length n, as opposed to using its binary representation, is a convention motivated by the standard requirement that GEN runs in time bounded by a polynomial in the length of its input, and here we want to allow GEN to run in time polynomial in n, not just polynomial in $\log n$. Since we do not focus on algorithmic efficiency, you can ignore this requirement.