Quantum Cyber Security

Lecture 9: Other QKD and similar protocols

Mina Doosti

In this lecture…

We learn about:

- 6-State BB84 protocol
- Bennett ‘92 (B92) protocol
- BBM92 protocol (Entangled-based BB84)
- Wiesner's quantum money: A very simple quantum money protocol

The Six-State Protocol

- Proposed by: Bechmann-Pasquinucci and Gisin (1999)
- **Difference to BB84:** Uses states from three orthogonal bases $\{X, Y, Z\}$ (thus six-states) rather than two bases (four-states).

Alice

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

Bob

$S = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, \underbrace{|+y\rangle, |-\rangle_y}\}$

$|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$

1) Sends strings of states from S

↳ for each i → chooses a random pair (a_i, x_i)

where $x_i = \{0, 1, 2\}$ selects the basis

and a_i select the state/bit (ex: $|0\rangle$ or $|1\rangle$)

She stores strings of pair $(a_0, x_0), (a_1, x_1), \ldots, (a_n, x_n)$

2) for each $\underline{\underline{i}}$ chooses a random basis $y_i = \{0, 1, 2\}$ and $\underline{\underline{\text{measures}}}$ the qubit in that basis and obtain outcome b_i

Stores pairs

$(b_0, y_0), (b_1, y_1), \ldots, (b_n, y_n)$

The Six-State Protocol: public communication

Now (similar to BB84) Alice and Bob need to classically communicate:

- Alice/Bob publicly announce ONLY the bases x_i, y_i
  They keep the positions where $x_i = y_i$ → raw key k_r
- If there is no eavesdropping: $\forall i \ \in k_r(a,b),: \ a_i = b_i$ of the raw key
- Parameter Estimation Phase: They choose small fraction of the raw key randomly and announce a_i, b_i to estimate the QBER (Quantum-Bit Error Rate)
- Information Reconciliation (IR) and Privacy Amplification (PA) exactly as in BB84.

The Six-State Protocol: security and comparison to BB84

The ideas for the security proof of this protocol are same as BB84.

Key Rate: Let D be the (symmetric) quantum-bit error then the key rate is:

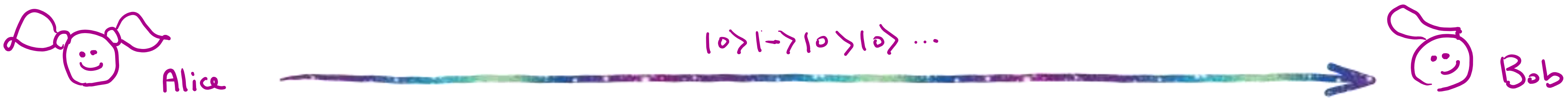
$$R_{6S} = \frac{1}{3}[1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1 - \frac{3D}{2}\right)\log_2(1 - \frac{3D}{2})]$$

Comparison to BB84:

- **Advantage:** Using 6 states makes it harder for the adversary to attack or guess correctly the basis, hence the protocol has higher loss tolerance.
- **Disadvantages:**
  - Fewer qubits in the raw key (only 1/3 cases $x_i = y_i$ – an overall factor 1/3 at the key rate)
  - Slightly harder to implement because it needs the preparation of one-of-six states

B92 Protocol

- Proposed by: Bennett (1992)
- **Difference to BB84:** Uses two non-orthogonal states only (instead of four).



$S = \{|0\rangle, |-\rangle\}$

1) Alice sends strings of qubits from S

↳ for each i : chooses a random bit $a_i = \{0, 1\}$

if $a_i = 0 \rightarrow |0\rangle_i$, if $a_i = 1 \rightarrow |-\rangle_i$

and she stores the pairs.

2) for each i chooses a random basis

$y_i = 0 \rightarrow \{|0\rangle, |1\rangle\}$ $y_i = 1 \rightarrow \{|+\rangle, |-\rangle\}$

and measures the qubit obtain b_i

stores the pairs $(b_0, y_0), \dots, (b_n, y_n)$

3) Bob "keeps" the position where he obtains results $\{|1\rangle, |+\rangle\}$

B92 Protocol

What's going on?

Alice $|0\rangle|-\rangle|0\rangle$ $\longrightarrow$ Bob

$y_0 = 1$	$y_1 = 1$	$y_2 = 0$
$\downarrow$	$\downarrow$	$\downarrow$
$b_0 = 0$	$b_1 = 1$	$b_2 = 0$
$\downarrow$	$\downarrow$	$\downarrow$
$\|+\rangle$	$\|-\rangle$	$\|0\rangle$
✓	✗	✗

The only way to get $|+\rangle$ is when Alice sends $|0\rangle$ $\leftarrow$
(similar for $|1\rangle \rightarrow |-\rangle$)

This is an example of Unambiguous State Discrimination (USD). Bob can unambiguously conclude what Alice state is.

B92 Protocol: public communication

Now (similar to BB84) Alice and Bob need to classically communicate:

- Bob announces the (i)'s he received $|1\rangle_i, |+\rangle_i$ (NOT the result)
  They keep only these positions for the raw key.
- If there is no eavesdropping: $\forall i \ \in k_r(a,b),: \ a_i = b_i$ of the raw key
- Parameter Estimation Phase: They choose small fraction of the raw key randomly and announce a_i, b_i to estimate the QBER (Quantum-Bit Error Rate)
- Information Reconciliation (IR) and Privacy Amplification (PA) exactly as in BB84.

B92 Protocol: security and comparison to BB84

Intuition for security: Eve could mimic Bob (perform USD), but the positions she gets unambiguous outcome would differ from Bob's Post-selecting on positions that Bob got unambiguous outcome gives advantage to Bob.
The formal security proof, however, is more complicated and relies on another protocol called Entanglement distillation.

Key Rate: The expression is complicated, but much lower than BB84 (e.g. for depolarising channels it gives $\sim 3.34\%$ compared to $\sim 16.5\%$)

Comparison to BB84:

- **Advantage:** Simpler implementation (it's the simplest QKD) especially using optical implementation (CV)
- **Disadvantages:**
  - Less secure → lower noise tollerence
  - Lower rate

BBM92 Protocol

- Proposed by: Bennett, Brassard, Mermin (1992)
- **Difference to BB84:** Uses entanglement.
  Alice and Bob share maximally entangled states (EPR pairs) and perform measurements. It is also known as entanglement-based BB84.

Alice

1) share n copies of $|EPR\rangle = |\phi^+\rangle_i = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$

Bob

2) Measures her qubit in a random basis

$x_i = 0 \rightarrow \{|0\rangle, |1\rangle\}$ $\quad x_i = 1 \rightarrow \{|+\rangle, |-\rangle\}$

She obtains result $a_i \begin{cases} 0 & |0\rangle \text{ or } |+\rangle \\ 1 & |1\rangle \text{ or } |-\rangle \end{cases}$

Stores the pairs: $(a_0, x_0), \ldots, (a_n, x_n)$

3) Measures his qubit in a random basis

$y_i = 0 \rightarrow \{|0\rangle, |1\rangle\}$ $\quad y_i = 1 \rightarrow \{|+\rangle, |-\rangle\}$

He obtains result $b_i = \begin{cases} 0 & |0\rangle, |+\rangle \\ 1 & |1\rangle \text{ or } |-\rangle \end{cases}$

Stores the pairs $(b_0, y_0), \ldots, (b_n, y_n)$

BBM92: public communication

Now (similar to BB84) Alice and Bob need to classically communicate:

- Alice/Bob publicly announce ONLY the bases x_i, y_i
  They keep the positions where $x_i = y_i$ → raw key k_r
- If there is no eavesdropping i.e., they really shared the state $|\Phi^+\rangle$ then: $\forall i \ \in k_r(a,b),:\ a_i = b_i$ of the raw key
- Parameter Estimation Phase: They choose small fraction of the raw key randomly and announce a_i, b_i to estimate the QBER (Quantum-Bit Error Rate).
- They abort if QBER higher than a threshold.
- Information Reconciliation (IR) (the classical post-processing part) and Privacy Amplification (PA) same as in BB84.

BBM92 Protocol: security and comparison to BB84

Intuition for security: From QBER can bound the distance of the real initial state to the ideal shared entangled state which quantifies the information eavesdropper can get.
Also, one can look at the entropy of the shared state for that.
The interesting fact is that from adversary’s view, the protocol is indistinguishable from BB84! (This version is used to provide modern security proofs of BB84)

Key Rate: same as BB84

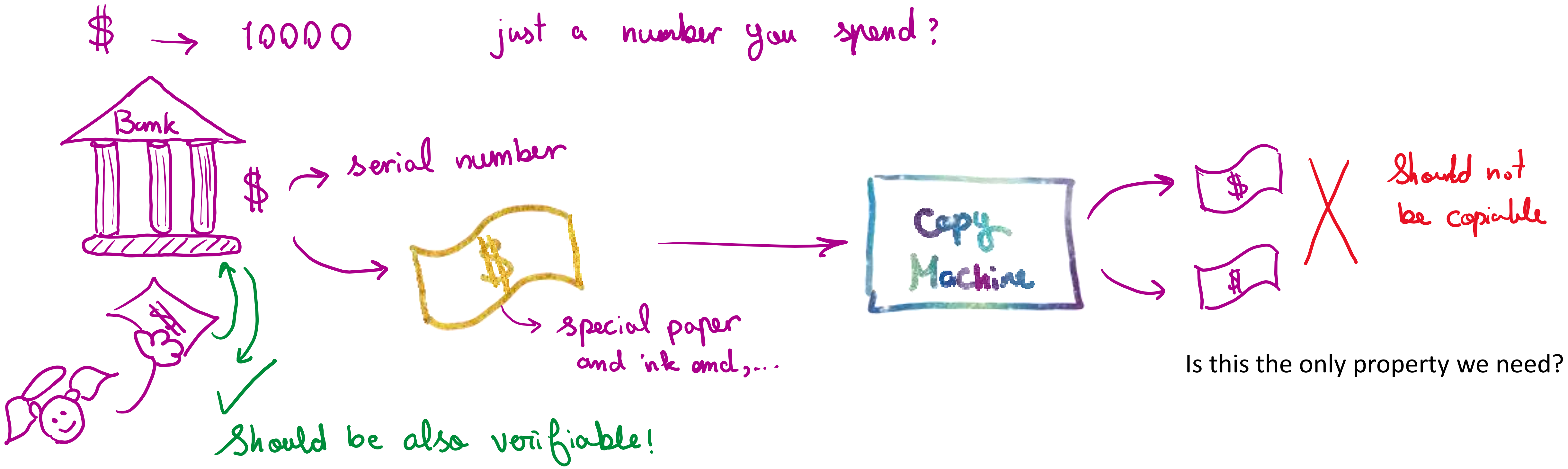
Comparison to BB84:

- **Advantage:**
  - Helps to clarify the security proof
  - It allows for a third (untrusted) party to prepare the states, and both parties can do with only measuring devices.
  - On some specific implementation is more robust.

- **Disadvantages:**
  - In general, the implementation is harder. It is harder to prepare the entangled states and share them, than prepare-and-send single qubits.

Quantum Money (idea)

First… What is money?



Is this the only property we need?

In general, any quantum money scheme needs to have unclonability (also called anti-counterfeiting or unforgeability) and verifiability.

What if we use unclonable states instead of special papers to get unclonable money?

Wiesner's Quantum Money

- Proposed by: Stephen Wiesner in 1969 (but published in 1983)

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.

Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

Wiesner realized that the quantum No-Cloning of quantum states can be used to make a notion of "money" with quantum properties. So Wiesner proposed using qubits to make money that would be physically impossible to duplicate (counterfeit).

But to have a money scheme, we don't only need unclonability but we also verifiability!

How did Wiesner solve this problem?

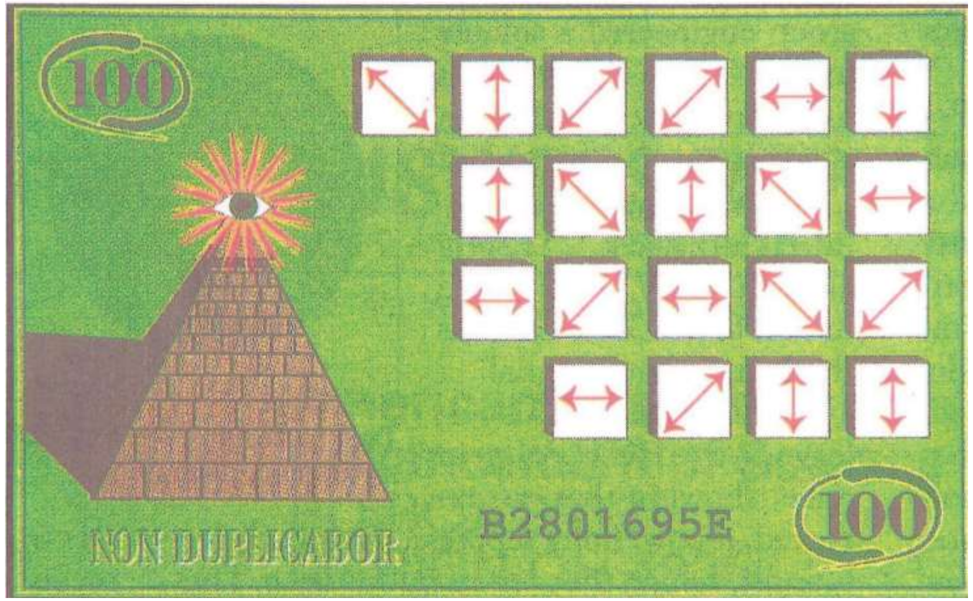
Wiesner's Quantum Money Protocol

- Each serial number $\$$ is made of two strings $x_\$, \theta_\$ \ \in \{0,1\}^n$
- For each pair, a quantum state $|\psi_{x_i,\theta_i}\rangle$ is created which is one of the following states. (should remind you of BB84!)

$$|\psi_{00}\rangle = |0\rangle \quad |\psi_{01}\rangle = |1\rangle \quad |\psi_{10}\rangle = |+\rangle \quad |\psi_{11}\rangle = |-\rangle$$

- The total state is then:

$$|\Psi_S\rangle = \ |\psi_{x_1,\theta_1}\rangle \otimes |\psi_{x_2,\theta_2}\rangle \otimes \cdots \otimes |\psi_{x_n,\theta_n}\rangle$$



How to verify?

To verify a bill, you bring it back to the bank.

The bank verifies the bill by looking at the serial number, and then measuring each qubit in the bill in the basis in which it was supposed to be prepared.

A bit more formal: The verifier takes a pair $(|\Psi_S\rangle, \$)$ and outputs accept or reject.

Quantum Money Security

So… is Wiesner's quantum money secure?

Does simply no-cloning theorem ensure the security?

Trivial attack: Let's say the adversary tries to guess the serial number by measuring the state. What's the probability of success?

$$P_{guess} = \frac{1}{2} \longrightarrow P_{succ} = \left(\frac{1}{2}\right)^n$$

Is there any better attacks?

Let's consider the following Measure-and-prepare attack: Adversary measures in standard basis, if they get outcome 0, they return state 0, and if they get outcome 1 they return state 1.

Let's write the general succ. prob.

$$P_{succ} = \frac{1}{4}\left(\langle 00|\underbrace{\rho_0}_{\text{2-qubit density matrix}}|00\rangle + \langle 11|\rho_1|11\rangle + \langle ++|\rho_+|++\rangle + \langle --|\rho_-|--\rangle\right)$$

$$\begin{cases} 0 \rightarrow \rho = |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ 1 \rightarrow \rho = |1\rangle\langle 1| \otimes |1\rangle\langle 1| \end{cases} \longrightarrow P^{PM}_{scc} = \frac{1}{4}\left(1 + 1 + \frac{1}{4} + \frac{1}{4}\right) = \frac{5}{8}$$

$$P^n_{succ} = \left(\frac{5}{8}\right)^n$$

Quantum Money Security

Cloning (or almost cloning) attack: What if the adversary tries to clone the state as good as they can (although not perfectly). In general, this is not forbidden by no-cloning theorem.

$$\left.\begin{array}{l}|0\rangle\\|1\rangle\\|+\rangle\\|-\rangle\end{array}\right\} \xrightarrow{|?\rangle} \boxed{\text{Almost Cloner}} \rightarrow |\phi\rangle \approx |0\rangle, |1\rangle, |+\rangle, |-\rangle$$

$$|?\rangle, |adv\rangle \rightarrow \boxed{U} \rightarrow |\Psi\rangle \rightarrow \rho \rightarrow \langle 00|\rho|00\rangle = 2/3$$

Let's say this is possible with prob 2/3

$$P^{clone}_{succ} = \frac{1}{4}\left(\frac{2}{3}+\frac{2}{3}+\frac{2}{3}+\frac{2}{3}\right) = \frac{2}{3} \rightarrow \text{overall} \quad \left(\frac{2}{3}\right)^n$$

There is an even better attack that achieves probability 3/4 so overall $\left(\frac{3}{4}\right)^n$ (that's the best you can do.)

Drawbacks:

- The scheme requires private verification i.e. only bank can verify the bills (not any merchant).

Side note: Having a fully secure public quantum money scheme is still one of the main open questions in quantum cryptography!

- This type of quantum money has an important practical problem: We need to ensure that the qubits in a bill don't lose their state (coherence).

Resources

1. Petros Wallden's QCS lecture from last year

2. Introduction to Quantum Cryptography by *Thomas Vidick and Stephanie Wehner*: chapter 3

3. Scott Aaronson's QC lecture, lecture 7

Extra materials:

The original Wiesner's paper on quantum money and conjugate coding:
http://users.cms.caltech.edu/~vidick/teaching/120_qcrypto/wiesner.pdf

A Wiki-style library of quantum protocol with many tools and resources:
https://wiki.veriqloud.fr/index.php?title=Protocol_Library

Proof of B92:
Tamaki, Kiyoshi, Masato Koashi, and Nobuyuki Imoto. "Unconditionally secure key distribution based on two nonorthogonal states." Physical review letters 90, no. 16 (2003): 167904.

A complete proof of QKD, both BB84 and entangled version, with their security relation to each other:
Tomamichel, Marco, and Anthony Leverrier. "A largely self-contained and complete security proof for quantum key distribution." Quantum 1 (2017): 14.