Quantum Cyber Security
Lecture 9: Quantum Key Distribution III

Petros Wallden

University of Edinburgh

25th February 2025

This Lecture: Other QKD protocols

1. The Six-State BB84
2. Bennett '92 (B92)
3. BBM92 (entanglement-based version of BB84)
4. Quantum Money (Wiesner)

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).

The protocol:

Alice

- Sends string of qubits from: $\{|h\rangle, |v\rangle, |+\rangle, |-\rangle, |+_y\rangle, |-_y\rangle\}$

  Note: $|\pm_y\rangle := \frac{1}{\sqrt{2}}(\pm|h\rangle + i\,|v\rangle)$

- For each (i) chooses randomly a pair $(a^{(i)}, x^{(i)})$
- $x^{(i)} \in \{0, 1, 2\}$ selects the basis (brown, blue or red)
- $a^{(i)}$ selects state (first or second in corresponding basis)
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

The Six-State Protocol

The protocol:

Alice

- Sends string of qubits from: $\{|h\rangle, |v\rangle, |+\rangle, |-\rangle, |+_y\rangle, |-_y\rangle\}$

  Note: $|\pm_y\rangle := \frac{1}{\sqrt{2}}(\pm|h\rangle + i|v\rangle)$
- For each (i) chooses randomly a pair $(a^{(i)}, x^{(i)})$
- $x^{(i)} \in \{0, 1, 2\}$ selects the basis (brown, blue or red)
- $a^{(i)}$ selects state (first or second in corresponding basis)
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

Bob

- For each (i) chooses rand basis $y^{(i)} \in \{0, 1, 2\}$ and measures
- Obtains result $b^{(i)}$: $(b^{(1)}, y^{(1)}), (b^{(2)}, y^{(2)}), \cdots, (b^{(n)}, y^{(n)})$

Subsequent Public Communication

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ ONLY
  They keep the positions where $x^{(i)} = y^{(i)}$ **raw key**

Subsequent Public Communication

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ ONLY
  They keep the positions where $x^{(i)} = y^{(i)}$ **raw key**
- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ of the raw key

Subsequent Public Communication

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ ONLY
  They keep the positions where $x^{(i)} = y^{(i)}$ **raw key**
- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ 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

Subsequent Public Communication

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ ONLY
  They keep the positions where $x^{(i)} = y^{(i)}$ **raw key**
- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ 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

- Intuition for security: Same as BB84
- Key Rate: Let D be the (symmetric) quantum-bit error then

$$R_{\mathrm{SSP}} = \frac{1}{3}\left(1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1 - \frac{3D}{2}\right)\log_2\left(1 - \frac{3D}{2}\right)\right)$$

The Six-State Protocol

- Intuition for security: Same as BB84
- Key Rate: Let D be the (symmetric) quantum-bit error then

$$R_{\mathrm{SSP}} = \frac{1}{3}\left(1 + \frac{3D}{2}\log_2\frac{D}{2} + \left(1 - \frac{3D}{2}\right)\log_2\left(1 - \frac{3D}{2}\right)\right)$$

- Comparison with BB84:
  - **Positive:** Adversary less likely to guess correctly the basis (higher loss tolerance)
  - **Negative:** Fewer qubits in the raw key (only $1/3$ cases $x^{(i)} = y^{(i)}$ – an overall factor $\frac{1}{3}$ at the key rate)
  - **Negative:** Slightly harder to prepare one-of-six states

The B92 Protocol

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

The B92 Protocol

The protocol:

Alice

- Sends string of qubits from: $\{|h\rangle, |-\rangle\}$
- For each (i) chooses randomly a bit $a^{(i)}$, where $a^{(i)} = 0 \rightarrow |h\rangle_i$ and $a^{(i)} = 1 \rightarrow |-\rangle_i$, and stores it

The B92 Protocol

The protocol:

Alice

- Sends string of qubits from: $\{|h\rangle, |-\rangle\}$
- For each (i) chooses randomly a bit $a^{(i)}$, where $a^{(i)} = 0 \rightarrow |h\rangle_i$ and $a^{(i)} = 1 \rightarrow |-\rangle_i$, and stores it

Bob

- For each (i) chooses rand basis:

  $y^{(i)} = 0 \ \rightarrow \{|h\rangle, |v\rangle\}$; $y^{(i)} = 1 \ \rightarrow \{|+\rangle, |-\rangle\}$ and measures
- Obtains result $b^{(i)}$: $(b^{(1)}, y^{(1)}), (b^{(2)}, y^{(2)}), \cdots, (b^{(n)}, y^{(n)})$
- "Keeps" positions he obtained results $|v\rangle_i, |+\rangle_i$. Note that $b_i = 1$ for $|v\rangle_i$ and $b_i = 0$ for $|+\rangle_i$
- Example of **Unambiguous State Discrimination** (USD)

The B92 Protocol

- Ideal case (no-noise, no eavesdropping) Bob obtains $|v\rangle_i$ **only** if Alice sent $|-\rangle_i$, so can unambiguously conclude that Alice chose $a^{(i)} = 1$ (and similarly for $a^{(i)} = 0$ happens when Bob obtained $|+\rangle_i$)

The B92 Protocol

- Ideal case (no-noise, no eavesdropping) Bob obtains $|v\rangle_i$ **only** if Alice sent $|-\rangle_i$, so can unambiguously conclude that Alice chose $a^{(i)} = 1$ (and similarly for $a^{(i)} = 0$ happens when Bob obtained $|+\rangle_i$)

Subsequent Public Communication

- Bob announces the (i)'s he got $|v\rangle_i, |+\rangle_i$ (NOT the result) They keep only these positions for the **raw key**

- Ideal case (no-noise, no eavesdropping) Bob obtains $|v\rangle_i$ **only** if Alice sent $|-\rangle_i$, so can unambiguously conclude that Alice chose $a^{(i)} = 1$ (and similarly for $a^{(i)} = 0$ happens when Bob obtained $|+\rangle_i$)

Subsequent Public Communication

- Bob announces the (i)'s he got $|v\rangle_i, |+\rangle_i$ (NOT the result) They keep only these positions for the **raw key**

- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ of the raw key

The B92 Protocol

- Ideal case (no-noise, no eavesdropping) Bob obtains $|v\rangle_i$ **only** if Alice sent $|-\rangle_i$, so can unambiguously conclude that Alice chose $a^{(i)} = 1$ (and similarly for $a^{(i)} = 0$ happens when Bob obtained $|+\rangle_i$)

Subsequent Public Communication

- Bob announces the (i)'s he got $|v\rangle_i, |+\rangle_i$ (NOT the result) They keep only these positions for the **raw key**
- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ 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

The B92 Protocol

- Ideal case (no-noise, no eavesdropping) Bob obtains $|v\rangle_i$ **only** if Alice sent $|-\rangle_i$, so can unambiguously conclude that Alice chose $a^{(i)} = 1$ (and similarly for $a^{(i)} = 0$ happens when Bob obtained $|+\rangle_i$)

Subsequent Public Communication

- Bob announces the (i)'s he got $|v\rangle_i, |+\rangle_i$ (NOT the result) They keep only these positions for the **raw key**
- If there is no eavesdropping $a^{(i)} = b^{(i)}\ \forall\ i$ 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 B92 Protocol

- 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**.

  Estimate the errors in each basis, and complicated proof to bound the from these the error rate exists

The B92 Protocol

- 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**.

  Estimate the errors in each basis, and complicated proof to bound the from these the error rate exists
- Key Rate: The expression is complicated, but much lower than BB84 (e.g. for depolarising channels it gives $\sim 3.34\%$ compared to $\sim 16.5\%$)

The B92 Protocol

- 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**.

  Estimate the errors in each basis, and complicated proof to bound the from these the error rate exists
- 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 with BB84:
  - **Negative:** Lower noise tolerance and rate
  - **Positive:** Simpler implementations (improved versions with better tolerance and also entanglement-based protocols, exits)

The BBM92 Protocol

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

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

Alice

- Measures in random basis $x^{(i)} = 0 \to \{|h\rangle, |v\rangle\}; x^{(i)} = 1 \to \{|+\rangle, |-\rangle\}$
- Obtains result $a^{(i)} = 0 \to \{|h\rangle \text{ or } |+\rangle\}$; $a^{(i)} = 1 \to \{|v\rangle \text{ or } |-\rangle\}$
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

The protocol:

Any trusted or untrusted party (even Eve)

- Distributes to Alice and Bob n copies of the state:

$$|\Phi^+\rangle^{(i)} = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$$

Alice

- Measures in random basis $x^{(i)} = 0 \to \{|h\rangle, |v\rangle\}; x^{(i)} = 1 \to \{|+\rangle, |-\rangle\}$
- Obtains result $a^{(i)} = 0 \to \{|h\rangle \text{ or } |+\rangle\}$; $a^{(i)} = 1 \to \{|v\rangle \text{ or } |-\rangle\}$
- Stores string of pairs: $(a^{(1)}, x^{(1)}), (a^{(2)}, x^{(2)}), \cdots, (a^{(n)}, x^{(n)})$

Bob

- Measures in random basis $y^{(i)} = 0 \to \{|h\rangle, |v\rangle\}; y^{(i)} = 1 \to \{|+\rangle, |-\rangle\}$
- Obtains result $b^{(i)} = 0 \to \{|h\rangle \text{ or } |+\rangle\}$; $b^{(i)} = 1 \to \{|v\rangle \text{ or } |-\rangle\}$
- Stores string of pairs: $(b^{(1)}, y^{(1)}), (b^{(2)}, y^{(2)}), \cdots, (b^{(n)}, y^{(n)})$

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where $x^{(i)} = y^{(i)}$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)} \; \forall \; i$ of the raw key

The BBM92 Protocol

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where $x^{(i)} = y^{(i)}$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)} \; \forall \; i$ of the raw key

Parameter Estimation

- They choose fraction of the raw key, announce $a^{(i)}, b^{(i)}$ and estimate the QBER

The BBM92 Protocol

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where $x^{(i)} = y^{(i)}$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)}\ \forall\ i$ of the raw key

Parameter Estimation

- They choose fraction of the raw key, announce $a^{(i)}, b^{(i)}$ and estimate the QBER
- Aborts if QBER higher than a threshold

The BBM92 Protocol

Raw Key

- Alice/Bob announce the bases $x^{(i)}, y^{(i)}$ and they keep positions where $x^{(i)} = y^{(i)}$ (raw key)
- If there was no eavesdropping (state shared was indeed the $|\Phi^+\rangle$) then $a^{(i)} = b^{(i)} \ \forall \ i$ of the raw key

Parameter Estimation

- They choose fraction of the raw key, announce $a^{(i)}, b^{(i)}$ and estimate the QBER
- Aborts if QBER higher than a threshold
- Classical post-processing of **Information Reconciliation** (IR) and **Privacy Amplification** (PA) follow as in regular BB84

- Intuition for security: From QBER can bound the distance of the real initial state to the ideal $|\Phi^{+}\rangle$, which quantifies the information eavesdropper can get.

  From adversary's view is indistinguishable from BB84! (This version is used to provide modern security proofs of BB84)

The BBM92 Protocol

- Intuition for security: From QBER can bound the distance of the real initial state to the ideal $|\Phi^+\rangle$, which quantifies the information eavesdropper can get.

  From adversary's view is indistinguishable from BB84! (This version is used to provide modern security proofs of BB84)

- Key Rate: Identical with the BB84

- Comparison with BB84:
  - **Negative:** It is harder to prepare the entangled states and share them, than prepare-and-send single qubits.
  - **Positive:** It makes security proof clearer.
  - **Positive:** It allows for a third (untrusted) party to prepare the states, and both parties can do with only measuring devices.

Money

- Each note has serial number
- Notes can be verified for authenticity
- Only the Bank can issue new notes
- Cannot "copy" convincingly notes

  Hard to guarantee!

Quantum Money: Idea

Money

- Each note has serial number
- Notes can be verified for authenticity
- Only the Bank can issue new notes
- Cannot "copy" convincingly notes

  Hard to guarantee!

Quantum Money

- Unknown quantum states cannot be copied **even in principle**
- Use quantum unclonability!
- Idea: notes that have quantum states on them

Quantum Money: Wiesner's protocol

First q-crypto paper (1969, publ. 1983) by Stephen Wiesner

- Notes have serial number $\$$ and a quantum state $|\Psi_\$\rangle$
- The quantum state consists of strings of BB84 states:

  $|\Psi_\$\rangle = \otimes_{i=1}^{n} |\psi_{x_i,a_i}\rangle$

  $|\psi_{00}\rangle = |h\rangle$; $|\psi_{01}\rangle = |v\rangle$; $|\psi_{10}\rangle = |+\rangle$; $|\psi_{11}\rangle = |-\rangle$
- The Bank stores in a database $\$$ and corresponding strings $(x_1, a_1, x_2, a_2, \cdots x_n, a_n)_\$$

First q-crypto paper (1969, publ. 1983) by Stephen Wiesner

- Notes have serial number \$ and a quantum state $|\Psi_\$\rangle$
- The quantum state consists of strings of BB84 states:

  $|\Psi_\$\rangle = \otimes_{i=1}^{n} |\psi_{x_i,a_i}\rangle$

  $|\psi_{00}\rangle = |h\rangle$; $|\psi_{01}\rangle = |v\rangle$; $|\psi_{10}\rangle = |+\rangle$; $|\psi_{11}\rangle = |-\rangle$
- The Bank stores in a database \$ and corresponding strings $(x_1, a_1, x_2, a_2, \cdots x_n, a_n)_\$$

To verify

- Bank checks \$, measures each qubit in $(x_1, x_2, \cdots, x_n)$ bases
- Original note gives $(a_1, \cdots, a_n)$ and remains unperturbed
- Tampered or fraudulent fails test (gives other outcomes)
- Adversaries cannot copy perfectly (will be detected)

Security

- To randomly guess n states without using the note: $\left(\frac{1}{4}\right)^n$
- Measure-and-prepare: Measure in $\{|0\rangle, |1\rangle\}$ basis. Prepare state and set comp. basis sting

  Probability to pass test (check!) $\left(\frac{3}{4}\right)^n$

Quantum Money: Security and Limitations

Security

- To randomly guess n states without using the note: $\left(\frac{1}{4}\right)^n$
- Measure-and-prepare: Measure in $\{|0\rangle, |1\rangle\}$ basis. Prepare state and set comp. basis sting

  Probability to pass test (check!) $\left(\frac{3}{4}\right)^n$

Limitations

- Hard to store, likely to have errors even in honest runs

  (robust versions explored)
- Only Bank can verify note

  (research for publicly-verifiable quantum money)