Unconditional Security of QKD

1. Cryptography
2. Quantum Key Distribution: BB84
3. EPR Protocol
4. CSS Code Protocol
5. Secure BB84

1 Cryptography

\[
\begin{array}{c}
\text{secret comm.} \\
\text{PKC} \\
\text{auth} \\
\text{DSS}
\end{array}
\]

In the Vernam Cipher (one-time pad), Alice and Bob share a secret key \( k \).

\[
\begin{array}{c}
A \\
\text{msg m} \\
\text{m+k} \\
m'
\end{array} \quad \begin{array}{c}
B \\
\text{m'+k=m}
\end{array}
\]

Eve has \( m + k \), but

\[
I(m + k, m) = H(m + k) - H(m + k/m)
\]

\[
= H(m + k) - H(k)
\]

\[
= 0
\]

The key \( k \) is called a “pad.” It is referred to as “one-time” because \( k \) can’t be reused.
**Distribution of $k \Rightarrow$ “security criterion”**

$$I(Eve, \text{key}) = 2^{-l}$$

where resources required $\sim \text{poly}(l)$.

## 2 Quantum Key Distribution: BB84

**Thm. Info gain $\Leftrightarrow$ disturbance.** In any attempt to distinguish non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$, information gain is only possible at the expense of disturbing the states.

**Proof.** WLOG assume

\[
\begin{align*}
|\psi\rangle|u\rangle &\rightarrow |\psi\rangle|v\rangle \\
|\phi\rangle|u\rangle &\rightarrow |\phi\rangle|u'\rangle \\
\langle \phi | \psi \rangle &\Rightarrow \langle \phi | \psi \rangle \langle v|v' \rangle \\
1 &= \langle v|v' \rangle \\
|v\rangle &= |v'\rangle
\end{align*}
\]

contradiction

**Problem:** collective attacks
3 EPR Protocol

Perfect EPR Pair ⇒ good key.

- A announces b
- B does
- Random checks (test Bell’s inequalities)
- Entanglement purification ⇒ m EPR pairs
- Measure, get key

Q: what is Eve’s mutual information with k? We want:

\[ I \sim e^{-l} \]

⇒ bound Eve’s errors

Does classical statistics apply? The most general model for Eve is:

\[ |00\rangle + |11\rangle \]

Eve can be treated as an error on the state \(|00\rangle + |11\rangle\):

| Error  |  \begin{align*} |00\rangle + |11\rangle &\to |00\rangle + |11\rangle \\ |00\rangle + |11\rangle &\to |00\rangle - |11\rangle \\ |00\rangle + |11\rangle &\to |01\rangle + |10\rangle \\ |00\rangle + |11\rangle &\to |01\rangle - |10\rangle \end{align*} |
Define:

\[
\Pi_{bf} = |\beta_{01}\rangle\langle \beta_{01}| + |\beta_{11}\rangle\langle \beta_{11}|
\]
\[
\Pi_{pf} = |\beta_{10}\rangle\langle \beta_{10}| + |\beta_{11}\rangle\langle \beta_{11}|
\]

Claim: we can use classical statistics because \([\Pi_{bf}, \Pi_{pf}] = 0\). Measure the following randomly on random pairs:

\[
\Pi_{bf}, \quad I - \Pi_{bf} \\
\Pi_{pf}, \quad I - \Pi_{pf}
\]

**Theorem: Random Sampling.** Consider \(2n\) bits with \(2\mu n\) ones. Measure \(n\) bits, obtaining \(kn\) ones. \(\text{Prob}(|k - \mu| > \epsilon) \sim e^{-O(n^2\epsilon)}\) as \(n \to \infty\) (Chernoff bound).

\(\Rightarrow\) How to purify?
Let \(\delta_n = n - nt\), where \(t\) is the estimated number of errors. Let \(E, D\) be an encoder pair for a \([n, \delta_n]\) QECC. Result: QECC garantees:

\[F(\rho, |\beta_{00}\rangle^{\otimes \delta n})^2 \geq 1 - 2^{-l}\]

Goal: Bound \(I(\text{Eve}, \text{key})\)

**Lemma:** High Fidelity \(\Rightarrow\) low entropy. If \(F(\rho, |\psi\rangle)^2 > 1 - 2^{-l}\), then \(S(\rho) < (n + l)2^{-l}\).

**Proof.** If \(\langle \psi|\rho|\psi\rangle > 1 - 2^{-l}\), then the maximum eigenvalue of \(\rho\) is greater than \(1 - 2^{-l}\).

\[
S(\rho) < S(\rho_{\text{max}}) = S\left(\begin{bmatrix}
1 - 2^{-l} & x \\
x & x \\
& & \ddots
\end{bmatrix}\right)
\]
where \( x = \frac{2^{-l}}{2^n - 1} \).

\[
S(\rho_{\text{max}}) = -(1 - 2^{-l}) \log(1 - 2^{-l}) \\
= -2^{-l} \log \frac{2^{-l}}{2^n - 1} \\
\sim (n + l) 2^{-l}
\]

Now Apply Holevo’s theorem.

\[
I(\text{Eve}, A\text{and}B) < S(\rho) < O(2^{-l})
\]

**Problems:**
1. need efficient codes (CSS works)
2. need quantum memory
3. need quantum computer

The last two are done away with by BB84.

## 4 CSS Code Protocol

**Step 1: EPR → Random Codes** The circuit is equivalent to:

\[
|\psi\rangle = DU_{xz}^\dagger s_{\text{Eve}}U_{xz} E |k\rangle
\]
Also equivalent to:

\[ |k\rangle \quad \xrightarrow{E} \quad |xz\rangle \quad \xrightarrow{U_{xz}} \quad |E\rangle \quad \xrightarrow{U_{xz}^+} \quad |D\rangle \]

**Step 2:** Let \( C_1, C_2 \) be classical \([n, k_1]\) and \([n, k_2]\) codes correcting up to \( t \) errors with \( C_2 \subset C_1 \). CSS\((C_1, C_2)\) is a \([[n, k_1, k_2]]\) quantum code with states:

\[ |\psi_k\rangle = \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w\rangle, \]

where \( v_k \) is a coset representative of \( C_2 \) in \( C_1 \).

Define: CSS\(_{xz}(C_1, C_2)\)

\[ |\psi_{kxz}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{v_k + w - z} \]

CSS code protocol:

- Alice announces \( x, z, p, b \)
Bob does:

- If error rate > tn, abort

## 5 Secure BB84

1. **Remove Quantum Computer** Bob doesn’t care about z errors.

\[
\rho = \frac{1}{2^n} \sum_z |\psi_{kxz}\rangle\langle\psi_{kxz}| \]

Alice need not reveal z!

\[
\rho = \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle\langle v_k + w + x| = |\text{random bit string}| \]

2. **Remove Quantum Memory** Double number of qubits and bob measures random b’, keep if b’ = b.

### Final Protocol

1. A and B discard if \(b_i \neq b'_i\)
2. compare check bits, obtain \(A : x, B : x + \epsilon\)
3. A announces \(x - v_k\)
4. B computes \(x + \epsilon - (x - v_k) = \epsilon + v_k\)
5. correction in \(C_1 \rightarrow v_k\)
6. Both compute coset index \(v_k \rightarrow k\)