Unconditional Security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel

Kiyoshi Tamaki *

*Perimeter Institute for Theoretical Physics

Collaboration with

Masato Koashi (Osaka Univ, Creat, Sorst),
Norbert Lütkenhaus (Univ. of Erlangen-Nürnberg, Max Plank Research Group), and
Nobuyuki Imoto (Sokendai, Creat, Sorst, NTT)
Summary of my talk

- B 92 QKD Protocol
- Outline of the proof
- Examples of the security
- Summary and Conclusion.


No Eve, noises and losses case (B92)

Alice

0 or encoder

1

|φ₀⟩ |φ₀⟩
|φ₁⟩ |φ₁⟩

Quantum Ch

Bob

Bob tells Alice whether the outcome is conclusive or not over the public ch.

Alice and Bob share identical bit values!

\[ M_{B92} = \{ F_0, F_1, F_? \} \]

\[
F_0 = |\bar{φ}_1\rangle\langle φ_1|/2 \\
F_1 = |\bar{φ}_0\rangle\langle φ_0|/2 \\
F_? = 1 - F_0 - F_1
\]

0,1: conclusive
The effects of noises or Eve

Noises, Eavesdropping → error, information leakage

For security

All noises are induced by Eve
Security proof of the B92 protocol

Is the B92 really unconditionally secure?

Is the B92 secure against Eve who has unlimited computational power and unlimited technology for state preparations, measurements and manipulations?

Assumptions on Alice and Bob

<table>
<thead>
<tr>
<th>Alice:</th>
<th>A single photon source.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob:</td>
<td>An ideal photon counter that discriminates single photon one hand and multi-photon or single photon on the other hand.</td>
</tr>
</tbody>
</table>
Outline of the security proof of the B92

Protocol 1 (Secure)  Key words: Error correction, Bell state, Entanglement distillation protocol (EDP)

(Equivalent with respect to key distribution)

The B92
Entanglement Distillation Protocol (By CSS Code) (by Shor and Preskill 2000)

\[ \hat{\sigma}_a^s = \hat{\sigma}_a^{s_1} \otimes \hat{\sigma}_a^{s_2} \otimes \hat{\sigma}_a^{s_3} \otimes \cdots \otimes \hat{\sigma}_a^{s_n}, (a = x, z) \text{ and } \sigma_a^0 = 1 \]
\[ s = (s_1, s_2, \cdots, s_n), (s_i = 0, 1) \]

Alice \( \rightarrow \) \((e_{bit}, e_{phase})\) \( \rightarrow \) Bob

Syndrome measurement \( \{ \hat{\sigma}_{z_i}^{r_i} \} \) \( \leftarrow \) Relative bit error position \( \rightarrow \) \{\hat{\sigma}_{z_i}^{r_i}\} \) Syndrome measurement

Public ch \{\hat{\sigma}_{x_i}^{t_j}\} \( \leftarrow \) Relative phase error position \( \rightarrow \) \{\hat{\sigma}_{x_i}^{t_j}\} \)

Error correction

\[ r_i \in C_1, t_j \in C_2, C_2 \subset C_1 \]

Sharing \( n \left(1 - h(e_{bit}) - h(e_{phase})\right) \) pairs of a Bell state
\[ |\Phi\rangle_{AB} = (|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B) / \sqrt{2} \]
\[ = \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B \]

Broadcasting the filtering succeeded or not

\[ F_{\text{fil}} = \alpha|0_x\rangle_B\langle 0_x| + \beta|1_x\rangle_B\langle 1_x| \]

Bit and phase error estimation

Quantum error correction

\( \sigma_z \)
Error estimations on the Protocol 1

\[
\begin{align*}
\Pi_{\text{bit}} &= |0_z\rangle_A\langle 0_z| \otimes F_S |1_z\rangle_B\langle 1_z| F_S + |1_z\rangle_A\langle 1_z| \otimes F_S |0_z\rangle_B\langle 0_z| F_S \\
\Pi_{\text{phase}} &= |0_x\rangle_A\langle 0_x| \otimes F_S |1_x\rangle_B\langle 1_x| F_S + |1_x\rangle_A\langle 1_x| \otimes F_S |0_x\rangle_B\langle 0_x| F_S
\end{align*}
\]

\[\{\Pi_{\text{bit}}, \Pi_{\text{phase}}\} \neq 0\]

- Phase error rate and bit error rate is not independent
- Phase error rate is estimated by bit error rate (the Protocol 1 is secure)
Outline of the security proof of the B92

Protocol 1 (Secure)  Key words: Error correction, Bell state, Entanglement distillation protocol (EDP)

(Equivalent with respect to key distribution)

The B92
A brief explanation of the equivalence

Main Observation (by Shor and Preskill)

- Only the bit values are important
- No need for phase error correction

\[ \frac{1}{\sqrt{2}} (|0_z\rangle_A |0_z\rangle_B + |1_z\rangle_A |1_z\rangle_B) \quad \leftrightarrow \quad \frac{1}{\sqrt{2}} (|0_z\rangle_A |0_z\rangle_B - |1_z\rangle_A |1_z\rangle_B) \]

\[ \sigma_z \begin{cases} \hat{\sigma}^{r_i}_z \\ \hat{\sigma}^{t_i}_z \end{cases} \quad \leftrightarrow \quad \begin{cases} \hat{\sigma}^{r_i}_z \\ \hat{\sigma}^{t_i}_z \end{cases} \begin{cases} \sigma_z \\ \sigma_z \end{cases} \]

Commutate!

Alice and Bob are allowed to measure \( \sigma_z \) before \( \{\hat{\sigma}^{r_i}_z\} \).
Protocol 1 (Secure)

No need for phase error correction (Shor and Preskill)

\[ |\Phi\rangle_{AB} = (|0_z\rangle_A|\varphi_0\rangle_B + |1_z\rangle_A|\varphi_1\rangle_B) / \sqrt{2} \]

\[ = \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B \]

Equivalent!

Randomly chosen

Classical data processing
(error correction, privacy amplification)

Classical data processing
(error correction, privacy amplification)
Example of the security and estimation

$G$ : Optimal net growth rate of secret key per pulse

$\mathcal{P}$ : depolarizing rate

$L$ : the prob that Bob detects vacuum (Loss rate)

Channel: $\rho \rightarrow (1 - L) \left[ (1 - p)\rho + p/3 \sum_{a=x,y,z} \sigma_a \rho \sigma_a \right] + L |Vac\rangle\langle Vac|$

The vacuum state
Summary and conclusion

- We have estimated the unconditionally security of the B92 protocol with single photon source and ideal photon counter.

- We have shown the B92 protocol can be regarded as an EPP initiated by a filtering process.

- Thanks to the filtering, we can estimate the phase error rate.

Future study

- Relaxation of the assumptions.
- Security estimation of B92 with coherent state.


Derivation of the B92 measurement from that in the Protocol 1

\[ |\varphi_j\rangle \equiv \beta |0_x\rangle - (-1)^j \alpha |1_x\rangle, \ (j = 0, 1) \]

\[ |\overline{\varphi}_j\rangle \equiv \alpha |0_x\rangle + (-1)^j \beta |1_x\rangle, \ (j = 0, 1) \]

\[
\begin{align*}
F_{\text{fil}}|0_z\rangle_B \langle 0_z|F_{\text{fil}} &= |\overline{\varphi}_1\rangle \langle \overline{\varphi}_1|/2 = F_0 \\
F_{\text{fil}}|1_z\rangle_B \langle 1_z|F_{\text{fil}} &= |\overline{\varphi}_0\rangle \langle \overline{\varphi}_0|/2 = F_1 \\
1_{\text{single}} - F_0 - F_1 &= F? \\
1 - 1_{\text{single}} &= F_{\text{multi}}
\end{align*}
\] 

\( = \mathcal{M}_{\text{B92}} \)
The phase error rate estimation from the bit error rate

\[ \Pi_{\text{bit}} = |0_z\rangle_A \langle 0_z| \otimes F_S |1_z\rangle_B \langle 1_z| F_S + |1_z\rangle_A \langle 1_z| \otimes F_S |0_z\rangle_B \langle 0_z| F_S \]

\[ \Pi_{\text{phase}} = |0_x\rangle_A \langle 0_x| \otimes F_S |1_x\rangle_B \langle 1_x| F_S + |1_x\rangle_A \langle 1_x| \otimes F_S |0_x\rangle_B \langle 0_x| F_S \]

Given \( \langle \Pi_{\text{bit}} \rangle_{\text{obs}} \), how much is the upper bound of \( \langle \Pi_{\text{phase}} \rangle_{\text{obs}} \)?

Note: It is dangerous to put some assumptions on the state.
The bit error and the phase error have a correlation !!

\[ \Pi_{\text{bit}} = \frac{1}{2} |\Phi^-\rangle\langle \Phi^-| \oplus \frac{1}{2} |\Gamma^-\rangle\langle \Gamma^-| \]

Nonorthogonal

\[ \Pi_{\text{phase}} = 0 \oplus [\alpha^2 |01_x\rangle\langle 01_x| + \beta^2 |10_x\rangle\langle 10_x|] \]

\[ \Pi^B_{\text{phase}} \]

\[ (|\Phi^-\rangle \equiv \alpha|00_x\rangle - \beta|11_x\rangle) \]

\[ (|\Gamma^-\rangle \equiv \beta|01_x\rangle - \alpha|10_x\rangle) \]

: subspace \( H_L \) spanned by \{\ket{00_x}, \ket{11_x}\}

: subspace \( H_R \) spanned by \{\ket{01_x}, \ket{10_x}\}

\{ Qubit space \}

\[ \langle \Pi_{\text{bit}} \rangle_{obs} = p_{\text{Red}} \langle \Phi^- \rangle_{obs} + (1 - p_{\text{Red}}) \langle \Gamma^- \rangle_{obs} \]

\[ \langle \Pi_{\text{phase}} \rangle_{obs} = p_{\text{Red}} 0 + (1 - p_{\text{Red}}) \langle \Pi^B_{\text{phase}} \rangle_{obs} \]

Upper bound of \( \langle 01_x \rangle_{obs} \) for given \( \langle \Gamma^- \rangle_{obs} \) ?
Consider any $N$-qubit state that is symmetric under any permutation

For given $\langle \sigma_\alpha \rangle_{obs}$, how much is the upper bound of $\langle \sigma_\beta \rangle_{obs}$?

For the estimation, we are allowed to regard the state as having stemmed from Independently and Identically Distributed quantum source!
$S_p : \text{unitary operator corresponds to permutation of M qubit}$

$S_p \cong \bigoplus_\lambda 1 \otimes \tilde{\pi}_\lambda(p)$

M qubit state $\rho$ that is symmetric under any permutation

$\rho \cong \bigoplus_k (p_k/d_k^\vee) \rho_k \otimes 1$
M qubit space can be decomposed as \( \mathcal{H}^\otimes M \cong \bigoplus_\lambda U_\lambda \otimes V_\lambda \)

\( S_p \) : unitary operator corresponds to permutation of M qubit
\[ S_p \cong \bigoplus_\lambda 1 \otimes \tilde{\pi}_\lambda(p) \]

M qubit state \( \rho \) that is symmetric under any permutation
\[ \rho \equiv \bigoplus_k (p_k/d_k^2) \rho_k \otimes 1 \]
\[ j=0 \quad j=1 \quad \begin{array}{cccccccc}
\sigma_{\alpha} & \sigma_{\alpha} & \sigma_{\alpha} & \sigma_{\alpha} & \sigma_{\beta} & \sigma_{\beta} & \sigma_{\beta} & \sigma_{\beta}
\end{array} \]

\( n_{b,j} : \begin{array}{c}
b=\alpha \quad \{ |\alpha, 0\rangle, |\alpha, 1\rangle \} \\
b=B \quad \{ |\beta, 0\rangle, |\beta, 1\rangle \}
\end{array} \)
\( M_b \) : number of qubits measured in \( b \) basis

\[ |\chi\rangle \equiv \bigotimes_{b,j} |b, j\rangle^{\otimes n_{b,j}} \]

\[ p(\delta_0, \delta_1) = \langle \chi | \rho | \chi \rangle \prod_{b=0,1} \frac{M_b!}{n_{b,0}!n_{b,1}!} \leq \text{poly}(M) \exp[-M \min R] \]
The class of the eavesdropping

Individual Attack

Coherent Attack (General Attack)

\[ U_i, \quad U_c, \quad \text{and Eve's measurement is arbitrary.} \]
Quantum Key Distribution (QKD)

- A way to share a random bit string between sender (Alice) and receiver (Bob) whose info leaks arbitrary small to Eve.