Analysis of BB84 and Six-State Protocols

Sumeet Khatri

Table of Contents

1 General considerations

The BB84 [BB84] and six-state [Bru98, BPG99] protocols are prepare-and-measure quantum key distribution (QKD) protocols in which Alice and Bob make use of states and measurements from mutually unbiased bases in order to distill a secret key. In this note, we provide details of the some of the steps used in the analysis of the BB84 and six-state protocols. The main goal is to show how the security of the key in both protocols can be determined by estimation of just one parameter Q, called the *quantum bit-error rate (QBER)*.

In both the BB84 and six-state protocols, Alice has two pieces of information, X_1 and X_2. X_1 is the random variable for Alice's basis choice, and X_2 is the binary random variable corresponding to the state taken from the chosen basis. The random variables X_1 and X_2 are independent. Similarly, Bob has two pieces of information, Y_1 and Y_2. Y_1 is the random variable for Bob's choice of measurement basis, and Y_2 is the random variable for the outcome of the measurement.

Let the alphabet $\mathcal{B}$ contain the possible basis choices. The random variables X_1 and Y_1 take values in $\mathcal{B}$. For the six-state protocol, $\mathcal{B}_{\text{six-state}} = \{0, 1, 2\}$, with "0" denoting the Z-basis, "1" the X-basis, and "2" the Y-basis. For the BB84 protocol, $\mathcal{B}_{\text{BB84}} = \{0, 1\}$. Then, let q_b^A and q_b^B be the probabilities that Alice and Bob, respectively, choose the basis $b \in \mathcal{B}$. In other words,

$$q_b^A \coloneqq \Pr[X_1 = b], \quad q_b^B \coloneqq \Pr[Y_1 = b]. \tag{1}$$

Let us make the following definitions:

$$\Pi_0^0 \coloneqq |0\rangle\langle 0| \equiv \rho_A^{0,0}, \quad \Pi_1^0 \coloneqq |1\rangle\langle 1| \equiv \rho_A^{0,1}, \tag{2}$$

$$\Pi_0^1 \coloneqq |+\rangle\langle +| \equiv \rho_A^{1,0}, \quad \Pi_1^1 \coloneqq |-\rangle\langle -| \equiv \rho_A^{1,1}, \tag{3}$$

$$\Pi_0^2 \coloneqq |+i\rangle\langle +i| \equiv \rho_A^{2,0}, \quad \Pi_1^2 \coloneqq |-i\rangle\langle -i| \equiv \rho_A^{2,1}. \tag{4}$$

Now, Alice chooses the basis $b_A \in \mathcal{B}$ with probability $q_{b_A}^A$, and with probability $\frac{1}{2}$ chooses one of the two states $\{\rho_A^{b_A,0}, \rho_A^{b_A,1}\}$ in the basis to send to Bob. These choices are independent, so we have

$$p_{X_1X_2}(b_A, x) \coloneqq \Pr[X_1 = b_A, X_2 = x] = q_{b_A}^A \cdot \frac{1}{2}. \tag{5}$$

The state $\rho_A^{b_A,x}$ is sent through a qubit-to-qubit quantum channel $\mathcal{N}_{A\to B}$ that is general *unknown* to Alice and Bob.

Once Bob receives the state, with probability $q_{b_B}^B$ he decides to measure in the basis b_B given by the POVM $\{\Pi_0^{b_B}, \Pi_1^{b_B}\}$. The corresponding conditional probability distribution is then

$$p_{Y_1Y_2|X_1X_2}(b_B, y|b_A, x) \coloneqq \Pr[Y_1 = b_B, Y_2 = y|X_1 = b_A, X_2 = x] = q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B}\mathcal{N}_{A\to B}(\rho_A^{b_A,x})]. \tag{6}$$

The complete joint probability distribution is then

$$\begin{aligned} p_{X_1X_2Y_1Y_2}(b_A, x, b_B, y) &\coloneqq \Pr[X_1 = b_A, X_2 = x, Y_1 = b_B, Y_2 = y] && (7)\\ &= p_{Y_1Y_2|X_1X_2}(b_B, y|b_A, x)p_{X_1X_2}(b_A, x) && (8)\\ &= \frac{1}{2}q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B}\mathcal{N}_{A\to B}(\rho_A^{b_A,x})]. && (9) \end{aligned}$$

The full classical-classical state corresponding to the probability distribution in (16) can then be written as

$$\rho_{X_1X_2Y_1Y_2} = \sum_{b_A,b_B\in\mathcal{B}} \sum_{x,y=0}^{1} \frac{1}{2}q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B}\mathcal{N}_{A\to B}(\rho_A^{b_A,x})]|b_A, b_B\rangle\langle b_A, b_B|_{X_1Y_1} \otimes |x, y\rangle\langle x, y|_{X_2Y_2}. \tag{10}$$

Remark 1. *Let us now show how the prepare-and-measure protocol as described so far is equivalent to an entanglement-based protocol. First, let*

$$\rho_{AB}^{\mathcal{N}} \coloneqq (\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(|\Phi^+\rangle\langle\Phi^+|_{AA'}) \tag{11}$$

be the Choi state of the channel $\mathcal{N}_{A\to B}^{\vec{Q}}$. Then, observe that

$$\begin{aligned} &q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\rho_{AB}^{\vec{Q}}(\Pi_x^{b_A} \otimes \Pi_y^{b_B})]\\ &\quad= q_{b_A}^A q_{b_B}^B \operatorname{Tr}\left[(\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(|\Phi^+\rangle\langle\Phi^+|_{AA'})(\Pi_x^{b_A} \otimes \Pi_y^{b_B})\right] && (12)\\ &\quad= q_{b_A}^A q_{b_B}^B \langle\Phi^+|(\Pi_x^{b_A} \otimes \mathcal{N}_{B\to A}^\dagger(\Pi_y^{b_B}))|\Phi^+\rangle && (13)\\ &\quad= \frac{1}{2}q_{b_A}^A q_{b_B}^B \operatorname{Tr}[(\Pi_x^{b_A})^\intercal \mathcal{N}_{B\to A}^\dagger(\Pi_y^{b_B})] && (14) \end{aligned}$$

$$= \frac{1}{2} q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B} \mathcal{N}_{A\to B}((\Pi_x^{b_A})^\mathsf{T})] \tag{15}$$

for all $b_A, b_B \in \mathcal{B}$ and all $x, y \in \{0,1\}$, where we have made use of the transpose trick to obtain the third equality. Using the equivalence $\Pi_x^{b_A} \equiv \rho_A^{b_A,x}$, we thus obtain

$$p_{X_1X_2Y_1Y_2}(b_A, x, b_B, y) = q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\rho_{AB}^{\mathcal{N}}((\Pi_x^{b_A})^\mathsf{T} \otimes \Pi_y^{b_B})], \tag{16}$$

for all $b_A, b_B \in \mathcal{B}$ and all $x, y \in \{0,1\}$.

The equality in (16) means that we can view the prepare-and-measure protocol in terms of an entanglement-based protocol in which Alice prepares two qubits in a maximally-entangled state and sends one of the qubits to Bob. Alice then chooses a basis $b_A \in \mathcal{B}$ and measures her qubit with the POVM $\{(\Pi_0^{b_A})^\mathsf{T}, (\Pi_1^{b_A})^\mathsf{T}\}$. Similarly, Bob chooses a basis $b_B \in \mathcal{B}$ and measures his qubit with the POVM $\{\Pi_0^{b_B}, \Pi_1^{b_B}\}$. Note that

$$(|0\rangle\langle 0|)^\mathsf{T} = |0\rangle\langle 0|, \quad (|1\rangle\langle 1|)^\mathsf{T} = |1\rangle\langle 1|, \quad (|\pm\rangle\langle\pm|)^\mathsf{T} = |\pm\rangle\langle\pm|. \tag{17}$$

However, we have

$$(|\pm i\rangle\langle\pm i|)^\mathsf{T} = |\mp i\rangle\langle\mp i|, \tag{18}$$

which means that for the entanglement-based protocol, in the ideal case, Alice and Bob's data are anti-correlated in the Y-basis.

Now, we define for each $b \in \mathcal{B}$ a *quantum bit-error rate (QBER)* Q_b as the probability that Alice and Bob's measurement outcomes disagree, given that they both used the same basis, i.e.,

$$Q_b := \Pr[X_2 \neq Y_2 | X_1 = Y_1 = b] \tag{19}$$
$$= \Pr[X_2 = 0, Y_2 = 1 | X_1 = Y_1 = b] + \Pr[X_2 = 1, Y_2 = 0 | X_1 = Y_1 = b] \tag{20}$$
$$= \frac{\Pr[X_2 = 0, Y_2 = 1, X_1 = b, Y_1 = b]}{\Pr[X_1 = b, Y_1 = b]} + \frac{\Pr[X_2 = 1, Y_2 = 0, X_1 = b, Y_1 = b]}{\Pr[X_1 = b, Y_1 = b]} \tag{21}$$
$$= \frac{1}{q_b^A q_b^B} \left(\frac{1}{2} q_b^A q_b^B \operatorname{Tr}[\Pi_1^b \mathcal{N}_{A\to B}(\rho_A^{b,0})] + \frac{1}{2} q_b^A q_b^B \operatorname{Tr}[\Pi_0^b \mathcal{N}_{A\to B}(\rho_A^{b,1})] \right) \tag{22}$$
$$= \frac{1}{2} \left(\operatorname{Tr}[\Pi_1^b \mathcal{N}_{A\to B}(\rho_A^{b,0})] + \operatorname{Tr}[\Pi_0^b \mathcal{N}_{A\to B}(\rho_A^{b,1})] \right). \tag{23}$$

In what follows, we let $Q_z \equiv Q_0$, $Q_x \equiv Q_1$, and $Q_y \equiv Q_2$.

1.1 Channel twirling

Since the channel $\mathcal{N}_{A\to B}$ is unknown to Alice and Bob, their task is to determine whether any eavesdropping has occurred by estimating the conditional probability distribution $p_{Y_1Y_1|X_1X_2}$, and using this estimate to decide whether their data is too noisy to proceed with further key distillation steps[1]. This esimation step is called *parameter estimation*.

[1] In QKD, we assume the worst-case scenario in which any deviation of the channel $\mathcal{N}_{A\to B}$ from an ideal one (i.e., the identity channel) is due to an eavesdropper.

In order to simplify the parameter estimation step, it is common to add an additional *channel twirling* step to the protocol, which essentially reduces the number of parameters that need to be estimated. In channel twirling, Alice picks at random one of the unitaries from the set $\{\mathbb{1}, X, Y, Z\}$ and applies it to her qubit before sending it through the channel to Bob. Alice also communicates this choice to Bob through a public authenticated channel, so that after he receives Alice's state he applies the inverse of the same unitary to it before performing his measurement. If we let Z be the random variable for Alice's choice of unitary, then

$$p_{Y_1Y_2|X_1X_2Z}(b_B, y|b_A, x, z) \coloneqq \Pr[Y_1 = b_B, Y_2 = y|X_1 = b_A, X_2 = x, Z = z] \tag{24}$$

$$= q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B} U^{z\dagger} \mathcal{N}_{A\to B}(U^z \rho_A^{b_A,x} U^{z\dagger})U^z], \tag{25}$$

where $z \in \{0, 1, 2, 3\}$, $U^0 = \mathbb{1}$, $U^1 = X$, $U^2 = Y$, $U^3 = Z$. Then,

$$p_{X_1X_2Y_1Y_2Z}(b_A, x, b_B, y, z) \coloneqq \Pr[X_1 = b_A, X_2 = x, Y_1 = b_B, Y_2 = y, Z = z] \tag{26}$$

$$= p_{Y_1Y_2|X_1X_2Z}(b_B, y|b_A, x, z)p_{X_1X_2Z}(b_A, x, z) \tag{27}$$

$$= \frac{1}{2} \cdot \frac{1}{4} q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B} U^{z\dagger} \mathcal{N}_{A\to B}(U^z \rho_A^{b_A,x} U^{z\dagger})U^z], \tag{28}$$

and

$$\rho_{X_1X_2Y_1Y_2Z} \tag{29}$$

$$= \sum_{b_A,b_B\in\mathcal{B}} \sum_{x,y=0}^{1} \sum_{z=0}^{3} \frac{1}{8} q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B} U^{z\dagger} \mathcal{N}_{A\to B}(U^z \rho_A^{b_A,x} U^{z\dagger})U^z] |b_A, b_B\rangle\langle b_A, b_B|_{X_1Y_1} \otimes |x, y\rangle\langle x, y|_{X_2Y_2} \otimes |z\rangle\langle z|_Z. \tag{30}$$

By forgetting the choice of the unitary (which means tracing out the classical register Z), we get

$$\rho_{X_1X_2Y_1Y_2} = \sum_{b_A,b_B\in\mathcal{B}} \sum_{x,y=0}^{1} \frac{1}{2} q_{b_A}^A q_{b_B}^B \operatorname{Tr}[\Pi_y^{b_B} \overline{\mathcal{N}}_{A\to B}(\rho_A^{b_A,x})] |b_A, b_B\rangle\langle b_A, b_B|_{X_1Y_1} \otimes |x, y\rangle\langle x, y|_{X_2Y_2}, \tag{31}$$

where

$$\overline{\mathcal{N}}_{A\to B}(\cdot) \coloneqq \frac{1}{4} \sum_{z=0}^{3} U^{z\dagger} \mathcal{N}_{A\to B}(U^z(\cdot)U^{z\dagger})U^z \tag{32}$$

is the *twirled* channel. It is straightforward to show (see, e.g., [DHCB05]) that the twirled channel is a Pauli channel. In particular,

$$\overline{\mathcal{N}}_{A\to B}(\rho_A) = \mathcal{N}_{A\to B}^{\vec{Q}}(\rho_A) \coloneqq \left(1 - \frac{1}{2}(Q_x + Q_y + Q_z)\right) \rho_A + \frac{1}{2}(Q_z - Q_x + Q_y) X\rho_A X + \frac{1}{2}(Q_x - Q_y + Q_z) Y\rho_A Y + \frac{1}{2}(Q_y - Q_z + Q_x) Z\rho_A Z. \tag{33}$$

1.2 Sifting

In both the BB84 and six-state protocols, there is a step called *sifting*, in which Alice and Bob discard the rounds in which they chose different bases. The resulting data is then used for parameter estimation, which is followed by key distillation. Let

$$\Pi^{\text{sift}}_{X_1Y_1} \coloneqq \sum_{b\in\mathcal{B}} |b,b\rangle\langle b,b|_{X_1Y_1} \tag{34}$$

be the projection onto the subspace corresponding to the same basis choice by Alice and Bob. Then, we define the state

$$\rho^{\text{sift}}_{X_1X_2Y_1Y_2} \coloneqq \frac{\Pi^{\text{sift}}_{X_1Y_1}\rho_{X_1Y_1X_2Y_2}\Pi^{\text{sift}}_{X_1Y_1}}{p_{\text{sift}}} \tag{35}$$

$$= \frac{1}{p_{\text{sift}}}\sum_{b\in\mathcal{B}}\sum_{x,y=0}^{1}\frac{1}{2}q_b^Aq_b^B\,\text{Tr}[\Pi_y^b\mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})]|b,b\rangle\langle b,b|_{X_1Y_1}\otimes|x,y\rangle\langle x,y|_{X_2Y_2}, \tag{36}$$

where

$$p_{\text{sift}} = \sum_{b\in\mathcal{B}} q_b^Aq_b^B \tag{37}$$

is the probability that Alice and Bob chose the same basis. The resulting probability distribution is

$$p^{\text{sift}}_{X_1X_2Y_1Y_2}(b,x,b,y) \coloneqq \frac{q_b^Aq_b^B}{2p_{\text{sift}}}\,\text{Tr}[\Pi_y^b\mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})], \tag{38}$$

and it is for this (conditional) probability distribution for which parameter estimation occurs and using which key distillation occurs in both the BB84 and six-state protocols.

The full classical-classical-quantum state of Alice, Bob, and the eavesdropper, can be written via an isometric extension $\mathcal{U}^{\mathcal{N}^{\vec{Q}}}_{A\to BE}$ of the channel $\mathcal{N}^{\vec{Q}}_{A\to B}$. Specifically,

$$\rho^{\text{sift}}_{X_1X_2Y_1Y_2E} = \frac{1}{p_{\text{sift}}}\sum_{b\in\mathcal{B}}\sum_{x,y=0}^{1} q_b^Aq_b^Bp_{X_2Y_2|X_1Y_1}(x,y|b,b)|b,b\rangle\langle b,b|_{X_1Y_1}\otimes|x,y\rangle\langle x,y|_{X_2Y_2}\otimes\rho_E^{b,x,y}, \tag{39}$$

where

$$p_{X_2Y_2|X_1Y_1}(x,y|b,b) = \frac{1}{2}\,\text{Tr}[\Pi_y^b\mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})], \tag{40}$$

$$\rho_E^{b,x,y} = \frac{1}{p_{X_2Y_2|X_1Y_1}(x,y|b,b)}\,\text{Tr}_B[\Pi_y^b\mathcal{U}^{\mathcal{N}^{\vec{Q}}}_{A\to BE}(\rho_A^{b,x})]. \tag{41}$$

1.3 Discarding basis information

Discarding, or “forgetting”, the basis information corresponds to tracing out the registers X_1 and Y_1 containing the basis information for Alice and Bob, respectively. We then have

$$\rho^{\text{sift}}_{X_2Y_2} \coloneqq \text{Tr}_{X_1Y_1}[\rho^{\text{sift}}_{X_1X_2Y_1Y_2}] = \frac{1}{p_{\text{sift}}}\sum_{x,y=0}^{1}\frac{1}{2}\left(\sum_{b\in\mathcal{B}}q_b^Aq_b^B\,\text{Tr}[\Pi_y^b\mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})]\right)|x,y\rangle\langle x,y|_{X_2Y_2}. \tag{42}$$

2 BB84 protocol

For the BB84 protocol, we have $\mathcal{B} = \mathcal{B}_{\text{BB84}} = \{0,1\}$, corresponding to the X and Z bases. We typically take $q_b^A = \frac{1}{2} = q_b^B$ for all $b \in \mathcal{B}$, so that $p_{\text{sift}} = \frac{1}{2}$. The state in (36) is

$$\rho_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}} \coloneqq \frac{1}{p_{\text{sift}}} \sum_{b=0}^{1} \sum_{x,y=0}^{1} \frac{1}{2} q_b^A q_b^B \operatorname{Tr}[\Pi_y^b \mathcal{N}_{A\to B}^{\vec{Q}}(\rho_A^{b,x})] |b,b\rangle\langle b,b|_{X_1Y_1} \otimes |x,y\rangle\langle x,y|_{X_2Y_2}, \tag{43}$$

and

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(b,x,b,y) = \frac{q_b^A q_b^B}{2p_{\text{sift}}} \operatorname{Tr}[\Pi_y^b \mathcal{N}_{A\to B}^{\vec{Q}}(\rho_A^{b,x})], \quad b \in \{0,1\}, \quad x,y \in \{0,1\}. \tag{44}$$

We then have

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(1,0,1,0) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+\rangle\langle+|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|+\rangle\langle+|_A)\right] = \frac{1}{4}(1-Q_x), \tag{45}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(1,0,1,1) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-\rangle\langle-|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|+\rangle\langle+|_A)\right] = \frac{1}{4}Q_x, \tag{46}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(1,1,1,0) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+\rangle\langle+|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|-\rangle\langle-|_A)\right] = \frac{1}{4}Q_x, \tag{47}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(1,1,1,1) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-\rangle\langle-|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|-\rangle\langle-|_A)\right] = \frac{1}{4}(1-Q_x), \tag{48}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(0,0,0,0) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|0\rangle\langle0|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|0\rangle\langle0|_A)\right] = \frac{1}{4}(1-Q_z), \tag{49}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(0,0,0,1) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|1\rangle\langle1|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|0\rangle\langle0|_A)\right] = \frac{1}{4}Q_z, \tag{50}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(0,1,0,0) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|0\rangle\langle0|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|1\rangle\langle1|_A)\right] = \frac{1}{4}Q_z, \tag{51}$$

$$p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(0,1,0,1) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|1\rangle\langle1|_B \mathcal{N}_{A\to B}^{\vec{Q}}(|1\rangle\langle1|_A)\right] = \frac{1}{4}(1-Q_z) \tag{52}$$

The mutual information of the full distribution $p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}$ is

$$I(X_1X_2;Y_1Y_2)_{\rho^{\text{BB84}|\text{sift}}} = \frac{1}{2}(4 - h_2(Q_x) - h_2(Q_z)). \tag{53}$$

If we discard the basis information, then

$$\rho_{X_2Y_2}^{\text{BB84}|\text{sift}} = \frac{1}{p_{\text{sift}}} \sum_{x,y=0}^{1} \frac{1}{2} \left(\sum_{b=0}^{1} q_b^A q_b^B \operatorname{Tr}[\Pi_y^b \mathcal{N}_{A\to B}^{\vec{Q}}(\rho_A^{b,x})] \right) |x,y\rangle\langle x,y|_{X_2Y_2}, \tag{54}$$

so that the probability distribution is

$$p_{X_2Y_2}^{\text{BB84}|\text{sift}}(0,0) = p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(0,0,0,0) + p_{X_1X_2Y_1Y_2}^{\text{BB84}|\text{sift}}(1,0,1,0) = \frac{1}{4}(1-Q_x) + \frac{1}{4}(1-Q_z)$$

$$= \frac{1}{2}(1-Q), \tag{55}$$

$$p^{\text{BB84}|\text{sift}}_{X_2Y_2}(0,1) = p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(0,0,0,1) + p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(1,0,1,1) = \frac{1}{4}Q_x + \frac{1}{4}Q_z = \frac{1}{2}Q, \tag{56}$$

$$p^{\text{BB84}|\text{sift}}_{X_2Y_2}(1,0) = p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(0,1,0,0) + p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(1,1,1,0) = \frac{1}{4}Q_x + \frac{1}{4}Q_z = \frac{1}{2}Q, \tag{57}$$

$$p^{\text{BB84}|\text{sift}}_{X_2Y_2}(1,1) = p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(0,1,0,1) + p^{\text{BB84}|\text{sift}}_{X_1X_2Y_1Y_2}(1,1,1,1) = \frac{1}{4}(1-Q_x) + \frac{1}{4}(1-Q_z)$$

$$= \frac{1}{2}(1-Q), \tag{58}$$

where we have defined the average QBER

$$Q \coloneqq \frac{1}{2}(Q_x + Q_z). \tag{59}$$

In other words, when we discard the basis information, Alice and Bob's classical data can be characterized using just one parameter.

Note that the the state $\rho^{\text{BB84}|\text{sift}}_{X_2Y_2}$ can be simplified in the case that $q^A_b = \frac{1}{2} = q^B_b$. First, note that

$$\Pi^b_y \equiv \rho^{b,y}_A = H^b|y\rangle\langle y|H^b \quad \forall\, b \in \{0,1\}, \quad \forall\, y \in \{0,1\}, \tag{60}$$

where H is the Hadamard operator, defined as

$$H \coloneqq |+\rangle\langle 0| + |-\rangle\langle 1|. \tag{61}$$

Then,

$$\sum_{b=0}^{1} q^A_b q^B_b \operatorname{Tr}[\Pi^b_y \mathcal{N}^{\vec{Q}}_{A\to B}(\rho^{b,x}_A)] = \frac{1}{4}\sum_{b=0}^{1} \operatorname{Tr}[H^b|y\rangle\langle y|H^b \mathcal{N}^{\vec{Q}}_{A\to B}(H^b|x\rangle\langle x|H^b)] \tag{62}$$

$$= \frac{1}{4}\sum_{b=0}^{1} \operatorname{Tr}[|y\rangle\langle y|H^b \mathcal{N}^{\vec{Q}}_{A\to B}(H^b|x\rangle\langle x|H^b)H^b] \tag{63}$$

$$= \frac{1}{2}\operatorname{Tr}\left[|y\rangle\langle y|\left(\frac{1}{2}\sum_{b=0}^{1} H^b \mathcal{N}^{\vec{Q}}_{A\to B}(H^b|x\rangle\langle x|H^b)H^b\right)\right] \tag{64}$$

$$= \frac{1}{2}\operatorname{Tr}\left[|y\rangle\langle y|\mathcal{N}^{\text{BB84},Q}_{A\to B}(|x\rangle\langle x|)\right], \tag{65}$$

where

$$\mathcal{N}^{\text{BB84},Q}_{A\to B}(\rho_A) \coloneqq (1-2Q+s)\rho_A + (Q-s)Z\rho_A Z + (Q-s)X\rho_A X + sY\rho_A Y \tag{66}$$

is known as the BB84 channel in [SS08], $Q = \frac{1}{2}(Q_x + Q_z)$, and $s = Q - \frac{Q_y}{2}$. So we can write $\rho^{\text{BB84}|\text{sift}}_{X_2Y_2}$ as

$$\rho^{\text{BB84}|\text{sift}}_{X_2Y_2} = \frac{1}{2}\sum_{x,y=0}^{1} \operatorname{Tr}\left[|y\rangle\langle y|\mathcal{N}^{\text{BB84},Q}_{A\to B}(|x\rangle\langle x|)\right]|x,y\rangle\langle x,y|. \tag{67}$$

Note that $s \in [0,Q]$ is an open parameter, which arises because there is no Y-basis measurement in the BB84 protocol, so that the QBER Q_y cannot be estimated by Alice and Bob. When calculating the key rate, therefore, we must take the worst-case value for s.

3 Six-state protocol

For the six-state protocol, we have $\mathcal{B} = \mathcal{B}_{\text{six-state}} = \{0, 1, 2\}$, corresponding to the X, Y, and Z bases. We typically take $q_b^A = \frac{1}{3} = q_b^B$ for all $b \in \mathcal{B}$, so that $p_{\text{sift}} = \frac{1}{3}$. The state in (36) is

$$\rho^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2} = \frac{1}{p_{\text{sift}}} \sum_{b=0}^{2} \sum_{x,y=0}^{1} \frac{1}{2} q_b^A q_b^B \operatorname{Tr}[\Pi_y^b \mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})] |b, b\rangle\langle b, b|_{X_1Y_1} \otimes |x, y\rangle\langle x, y|_{X_2Y_2}, \tag{68}$$

and

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(b, x, b, y) = \frac{q_b^A q_b^B}{2p_{\text{sift}}} \operatorname{Tr}[\Pi_y^b \mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})], \quad b \in \{0, 1, 2\}, \quad x, y \in \{0, 1\}. \tag{69}$$

We then have

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(1, 0, 1, 0) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+\rangle\langle+|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|+\rangle\langle+|_A)\right] = \frac{1}{6}(1 - Q_x), \tag{70}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(1, 0, 1, 1) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-\rangle\langle-|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|+\rangle\langle+|_A)\right] = \frac{1}{6}Q_x, \tag{71}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(1, 1, 1, 0) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+\rangle\langle+|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|-\rangle\langle-|_A)\right] = \frac{1}{6}Q_x, \tag{72}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(1, 1, 1, 1) = \frac{q_1^A q_1^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-\rangle\langle-|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|-\rangle\langle-|_A)\right] = \frac{1}{6}(1 - Q_x), \tag{73}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(0, 0, 0, 0) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|0\rangle\langle0|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|0\rangle\langle0|_A)\right] = \frac{1}{6}(1 - Q_z), \tag{74}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(0, 0, 0, 1) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|1\rangle\langle1|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|0\rangle\langle0|_A)\right] = \frac{1}{6}Q_z, \tag{75}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(0, 1, 0, 0) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|0\rangle\langle0|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|1\rangle\langle1|_A)\right] = \frac{1}{6}Q_z, \tag{76}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(0, 1, 0, 1) = \frac{q_0^A q_0^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|1\rangle\langle1|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|1\rangle\langle1|_A)\right] = \frac{1}{6}(1 - Q_z), \tag{77}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(2, 0, 2, 0) = \frac{q_2^A q_2^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+i\rangle\langle+i|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|+i\rangle\langle+i|_A)\right] = \frac{1}{6}(1 - Q_y), \tag{78}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(2, 0, 2, 1) = \frac{q_2^A q_2^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-i\rangle\langle-i|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|+i\rangle\langle+i|_A)\right] = \frac{1}{6}Q_y, \tag{79}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(2, 1, 2, 0) = \frac{q_2^A q_2^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|+i\rangle\langle+i|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|-i\rangle\langle-i|_A)\right] = \frac{1}{6}Q_y, \tag{80}$$

$$p^{\text{6-state}|\text{sift}}_{X_1X_2Y_1Y_2}(2, 1, 2, 1) = \frac{q_2^A q_2^B}{2p_{\text{sift}}} \operatorname{Tr}\left[|-i\rangle\langle-i|_B \mathcal{N}^{\vec{Q}}_{A\to B}(|-i\rangle\langle-i|_A)\right] = \frac{1}{6}(1 - Q_y). \tag{81}$$

If we discard the basis information, then

$$\rho^{\text{6-state}|\text{sift}}_{X_2Y_2} = \frac{1}{p_{\text{sift}}} \sum_{x,y=0}^{1} \frac{1}{2} \left(\sum_{b=0}^{2} q_b^A q_b^B \operatorname{Tr}[\Pi_y^b \mathcal{N}^{\vec{Q}}_{A\to B}(\rho_A^{b,x})] \right) |x, y\rangle\langle x, y|_{X_2Y_2}, \tag{82}$$

so that the probability distribution is

$$\begin{aligned} p_{X_2Y_2}^{\text{6-state|sift}}(0,0) &= p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(0,0,0,0) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(1,0,1,0) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(2,0,2,0) \\ &= \frac{1}{6}(1-Q_x) + \frac{1}{6}(1-Q_z) + \frac{1}{6}(1-Q_y) = \frac{1}{2}(1-Q), \qquad (83) \\ p_{X_2Y_2}^{\text{6-state|sift}}(0,1) &= p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(0,0,0,1) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(1,0,1,1) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(2,0,2,1) \\ &= \frac{1}{6}Q_x + \frac{1}{6}Q_y + \frac{1}{6}Q_z = \frac{1}{2}Q, \qquad (84) \\ p_{X_2Y_2}^{\text{6-state|sift}}(1,0) &= p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(0,1,0,0) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(1,1,1,0) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(2,1,2,0) \\ &= \frac{1}{6}Q_x + \frac{1}{6}Q_y + \frac{1}{6}Q_z = \frac{1}{2}Q, \qquad (85) \\ p_{X_2Y_2}^{\text{6-state|sift}}(1,1) &= p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(0,1,0,1) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(1,1,1,1) + p_{X_1X_2Y_1Y_2}^{\text{6-state|sift}}(2,1,2,1) \\ &= \frac{1}{6}(1-Q_x) + \frac{1}{6}(1-Q_z) + \frac{1}{6}(1-Q_y) = \frac{1}{2}(1-Q), \qquad (86) \end{aligned}$$

where we have defined the average QBER

$$Q \coloneqq \frac{1}{3}(Q_x + Q_y + Q_z). \qquad (87)$$

In other words, when we discard the basis information, Alice and Bob's data can be characterized using just one parameter.

Note that the state $\rho_{X_2Y_2}^{\text{6-state|sift}}$ can be simplified in the case that $q_b^A = \frac{1}{3} = q_b^B$. First, define the operator

$$T \coloneqq |+\rangle\langle 0| - i|-\rangle\langle 1|. \qquad (88)$$

Then, observe that

$$\Pi_0^1 = |+\rangle\langle +| = T|0\rangle\langle 0|T^\dagger, \quad \Pi_1^1 = T|1\rangle\langle 1|T^\dagger, \qquad (89)$$

$$\Pi_0^2 = |+i\rangle\langle +i| = T^2|0\rangle\langle 0|T^{2\dagger}, \quad \Pi_1^2 = |-i\rangle\langle -i| = T^2|1\rangle\langle 1|T^{2\dagger}. \qquad (90)$$

In other words,

$$\Pi_y^b \equiv \rho_A^{b,y} = T^b|y\rangle\langle y|T^{b\dagger}, \quad \forall\ b \in \{0,1,2\}, \quad \forall\ y \in \{0,1\}. \qquad (91)$$

Therefore,

$$\begin{aligned} \sum_{b=0}^{2} q_b^A q_b^B \operatorname{Tr}[\Pi_y^b \mathcal{N}_{A\to B}^{\vec{Q}}(\rho_Q^{b,x})] &= \frac{1}{9}\sum_{b=0}^{2} \operatorname{Tr}[T^b|y\rangle\langle y|T^{b\dagger}\mathcal{N}_{A\to B}^{\vec{Q}}(T^b|x\rangle\langle x|T^{b\dagger})] \qquad (92) \\ &= \frac{1}{9}\sum_{b=0}^{2} \operatorname{Tr}[|y\rangle\langle y|T^{b\dagger}\mathcal{N}_{A\to B}^{\vec{Q}}(T^b|x\rangle\langle x|T^{b\dagger})T^b] \qquad (93) \\ &= \frac{1}{3}\operatorname{Tr}\left[|y\rangle\langle y|\left(\frac{1}{3}\sum_{b=0}^{2} T^{b\dagger}\mathcal{N}_{A\to B}^{\vec{Q}}(T^b|x\rangle\langle x|T^{b\dagger})T^b\right)\right] \qquad (94) \\ &= \frac{1}{3}\operatorname{Tr}\left[|y\rangle\langle y|\mathcal{N}_{A\to B}^{\text{6-state},Q}(|x\rangle\langle x|)\right], \qquad (95) \end{aligned}$$

where

$$\mathcal{N}^{\text{6-state},Q}_{A\to B}(\rho_A) \coloneqq \left(1 - \frac{3Q}{2}\right)\rho_A + \frac{Q}{2}X\rho_A X + \frac{Q}{2}Y\rho_A Y + \frac{Q}{2}Z\rho_A Z \tag{96}$$

is the depolarizing channel, with $Q = \frac{1}{3}(Q_x + Q_y + Q_z)$. So we have that

$$\rho^{\text{6-state}|\text{sift}}_{X_2Y_2} = \frac{1}{2}\sum_{x,y=0}^{1} \operatorname{Tr}\left[|y\rangle\langle y|\mathcal{N}^{\text{6-state},Q}_{A\to B}(|x\rangle\langle x|)\right]|x,y\rangle\langle x,y|. \tag{97}$$

References

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[BPG99] H. Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238–4248, June 1999.

[Bru98] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, October 1998. arXiv:quant-ph/9805019.

[DHCB05] W. Dür, M. Hein, J. I. Cirac, and H.-J. Briegel. Standard forms of noisy quantum operations via depolarization. *Physical Review A*, 72(5):052326, November 2005. arXiv:quant-ph/0507134.

[SS08] Graeme Smith and John A. Smolin. Additive extensions of a quantum channel. In *2008 IEEE Information Theory Workshop*, pages 368–372, May 2008. arXiv:0712.2471.