

# COM-440, Introduction to Quantum Cryptography, Fall 2025

## Homework # 3 Solutions

---

### Problems:

#### 1. Information reconciliation via linear codes.

- (a) First note if  $X_A$  and  $X_B$  has only one error, then  $X_A - X_B = e_i$  for some standard vector basis  $e_i$  where  $i$ th bit is the erroneous bit. Hence  $H(X_A - X_B) = v_i$  where  $v_i$  is the  $i$ th column of  $H$ . But notice that all the columns of  $H$  are distinct, so given  $v_i$ , we can deduce precisely what  $i$ , the index of the erroneous bit, is (this is the error estimate map).
- (b) In the reconciliation scheme, Alice would send  $HX_A$  to Bob. Bob would then calculate  $HX_B$  and then subtract to find  $H(X_A - X_B)$ . Using this Bob would figure out which bit to flip through the error estimate map, and then recover Alice's string. However, this won't work if more than one error is present, as in all cases, Bob will only change one bit depending on the error estimate. The probability of Alice and Bob succeeding is consequently the probability that at most one error occurs, which is

$$(1-p)^7 + 7p(1-p)^6 = (1-p)^6(1-p+7p) = (1-p)^6(1+6p)$$

- (c) The probability that a 7-bit message is transferred perfectly without any reconciliation is just  $(1-p)^7$ , which is  $7p(1-p)^6$  smaller than if we could do a single error reconciliation as in the previous part. Using the 3-bit single error reconciliation scheme with the  $H$  given in this part, we successfully transmit the 3-bit message without error with probability

$$(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1-p+3p) = (1-p)^2(1+2p)$$

The leading term of all these probabilities is 1, but the linear term of the success probability of just transferring 7 bits without reconciliation,  $(1-p)^7 = 1 - 7p + \dots$ , is  $-7$ , while the linear term of the success probability of the 3-bit scheme,  $(1-p)^2(1+2p) = 1 + 0p - 3p^2 + \dots$ , is 0, and the linear term of the success probability of transferring 7 bits with reconciliation,  $(1-p)^6(1+6p) = 1 + 0p - 21p^2 + \dots$ , is also 0. However the  $p^2$  term is larger for the 3-bit scheme than the 7-bit scheme. Hence the leading order behavior in increasing order is the 7-bit transmission without reconciliation, then the 7-bit transmission with reconciliation, followed by the 3-bit transmission with reconciliation.

Plotting these polynomials on a graphing calculator, we see that this order is preserved in the region  $p \in (0, 1/2)$ . Hence in this region, if we were to think giving up 4 bits of communicating is worth it, the 3-bit scheme would be the best. Otherwise, the 7-bit scheme is the best.

## 2. Establishing keys in the presence of a limited eavesdropper.

- (a) Have Alice send an  $n$ -bit weak key  $X$  through these special classic channels to Bob. Then for each bit, Eve will obtain the bit with probability  $q$ , and will not with probability  $1 - q$  and just guess. Hence the probability Eve gets the correct bit is  $q + \frac{1-q}{2} = \frac{1+q}{2}$ , and the probability Eve guesses all of the message is  $P_{\text{guess}}(X|E) = \left(\frac{1+q}{2}\right)^n$ . Consequently

$$H_{\min}(X|E) = -\log \left( \left( \frac{1+q}{2} \right)^n \right) = n(1 - \log(1+q)) \geq (2 - \log 3)n$$

Now from our work done in class (Theorem 5.3.1 in notes), for  $\varepsilon = 10^{-5}$  and  $k = n(2 - \log 3)$  Alice and Bob can construct a  $(k, \varepsilon)$ -weak seeded 2-universal extractor  $\text{Ext}$  that takes  $X$  and a random string  $r \leftarrow \{0, 1\}^{2n}$ , and outputs an  $\varepsilon$ -secure key of size

$$m := n(2 - \log 3) + 2 \log \varepsilon = n(2 - \log 3) - 10 \log 10$$

Hence all Alice needs to do is create a length  $2n$  random string  $R$ , find  $\text{Ext}(X, R)$ , send  $R$  to Bob, and have Bob calculate  $\text{Ext}(X, R)$ .

Overall, we use the channel to first send the  $n$ -bit message  $X$ , and then the  $2n$ -bit random seed  $R$ . Hence the number of channel uses per bit of  $\varepsilon$ -secure key is

$$\frac{3n}{m} = \frac{3n}{n(2 - \log 3) - 10 \log 10} = \frac{3}{2 - \log 3 - 10 \log 10/n}$$

If we assume that Eve is the most powerful with  $q = 1/2$  and if we make  $n$  to be quite large for practical security purposes, we will have

$$\frac{3n}{m} \rightarrow \frac{3}{2 - \log 3} \approx 7.23$$

channel uses per bit of  $10^{-5}$ -strong key.

- (b) Let Alice send an  $n$ -bit weak key  $X$  through the classical channel to Bob ( $n \gg b$ ). We can then see that Eve can intercept any  $b$  of them, and hence  $P_{\text{guess}}(X|E) = 2^{b-n}$ , and so

$$k := H_{\min}(X|E) = -\log P_{\text{guess}}(X|E) = n - b$$

Now again from class or Theorem 5.3.1, for  $\varepsilon = 10^{-10}$ , Alice and Bob can construct a  $(k, \varepsilon)$ -weak seeded 2-universal extractor  $\text{Ext}$  that takes  $X$  and a random string  $r \leftarrow \{0, 1\}_u^{2n}$  and outputs an  $\varepsilon$ -secure key of size

$$m = k + 2 \log \varepsilon = n - b - 20 \log 10 = n - 2014 - 20 \log 10$$

Hence we can have Alice generate  $R \leftarrow \{0, 1\}^{2n}$ , calculate  $\text{Ext}(X, R)$ , send  $R$  to Bob, and then have Bob also calculate  $\text{Ext}(X, R)$ . As a result, both Alice and Bob will have  $\varepsilon$ -secure keys.

### 3. Min-entropy from the matching outcomes bound

- (a) Recall that  $X$  is a single bit, the output of Alice's measurement. Therefore its min-entropy is upper-bounded by 1. Since Eve is totally uncorrelated and Alice's local density matrix is  $\frac{1}{2}\mathbb{I}$ ,  $X$  is a uniform random bit with respect to Eve's point of view. That is,  $H_{\min}(X | E\Theta) = 1$ .
- (b) We want to compute the probability that Alice and Bob obtain the same outcome. Suppose  $\Theta = 0$ , so that Alice and Bob both measure in the standard basis. The expected value of the product of their measurement outcomes is  $\langle \Psi_{ABE} | Z \otimes Z \otimes I | \Psi_{ABE} \rangle$ . If they make the same measurement, then the product of their measurements is +1. If they make different measurements, this product is -1. Therefore the expectation is equal to  $p_{\text{same}|\Theta=0} - p_{\text{different}|\Theta=0}$ . These two probabilities sum to 1, so we conclude that

$$p_{\text{same}|\Theta=0} = \frac{1}{2} + \frac{1}{2} \langle \Psi_{ABE} | Z \otimes Z \otimes I | \Psi_{ABE} \rangle.$$

Similarly,

$$p_{\text{same}|\Theta=1} = \frac{1}{2} + \frac{1}{2} \langle \Psi_{ABE} | X \otimes X \otimes I | \Psi_{ABE} \rangle.$$

Finally,

$$p_{\text{same}} = \frac{1}{2}p_{\text{same}|\Theta=0} + \frac{1}{2}p_{\text{same}|\Theta=1} = \frac{1}{2} + \frac{1}{4} \langle \Psi_{ABE} | X \otimes X \otimes I | \Psi_{ABE} \rangle + \frac{1}{4} \langle \Psi_{ABE} | Z \otimes Z \otimes I | \Psi_{ABE} \rangle.$$

Therefore,  $a = b = 1/4$ ,  $c = 1/2$ .

- (c) Applying the standard basis expansion suggested in the problem, along with the identity  $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ , we can rewrite  $\langle \Psi_{ABE} | X_A \otimes X_B \otimes I_E | \Psi_{ABE} \rangle$  as

$$(\langle 0|_A \otimes \langle u_0|_{BE} + \langle 1|_A \otimes \langle u_1|_{BE}) [(|0\rangle\langle 1| + |1\rangle\langle 0|)_A \otimes X_B \otimes I_E] (|0\rangle_A \otimes |u_0\rangle_{BE} + |1\rangle_A \otimes |u_1\rangle_{BE}).$$

Evaluating inner products simplifies this to

$$\langle u_0|_{BE} X_B \otimes I_E |u_1\rangle_{BE} + \langle u_1|_{BE} X_B \otimes I_E |u_0\rangle_{BE}.$$

Since the two terms in the above sum are complex conjugates of each other, their sum is equal to twice their real part. That is,

$$\langle \Psi_{ABE} | X_A \otimes X_B \otimes I_E | \Psi_{ABE} \rangle = 2\Re \langle u_0|_{BE} X_B \otimes I_E |u_1\rangle_{BE} = 2\Re \langle u_1|_{BE} X_B \otimes I_E |u_0\rangle_{BE}.$$

Thus  $a' = 2$ ,  $b' = 0$ .

- (d) First, observe that by part (b),

$$2p - 1 = \frac{1}{2} \langle \Psi_{ABE} | X \otimes X \otimes I | \Psi_{ABE} \rangle + \frac{1}{2} \langle \Psi_{ABE} | Z \otimes Z \otimes I | \Psi_{ABE} \rangle.$$

By part (c),

$$2p - 1 = \Re \langle u_0 | X_B \otimes I_E | u_1 \rangle + \Re \langle u_0 | Z_B \otimes I_E | u_1 \rangle.$$

By Ulmann's theorem,

$$| \langle u_0 | X_B \otimes I_E | u_1 \rangle | \leq F(\sigma_E^{X,0}, \sigma_E^{X,1}) \text{ and } | \langle u_0 | Z_B \otimes I_E | u_1 \rangle | \leq F(\sigma_E^{Z,+}, \sigma_E^{Z,-})$$

Finally, notice that for any complex  $z$ ,  $\Re z \leq |z|$ . Chaining and adding inequalities gives the desired inequality with  $\alpha = \beta = 1$ .

$$|2p - 1| \leq F(\sigma_E^{X,0}, \sigma_E^{X,1}) + F(\sigma_E^{Z,+}, \sigma_E^{Z,-}).$$

So  $\alpha = 1, \beta = 1$ .

(e) Recall that from part (d) we have

$$2p - 1 \leq F(\sigma_E^{X,0}, \sigma_E^{X,1}) + F(\sigma_E^{Z,+}, \sigma_E^{Z,-}) \quad (1)$$

Now,  $D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2} \Rightarrow F(\rho, \sigma) \leq \sqrt{1 - D(\rho, \sigma)^2}$ . Hence, we have

$$2p - 1 \leq \sqrt{1 - D(\sigma_E^{X,0}, \sigma_E^{X,1})^2} + \sqrt{1 - D(\sigma_E^{Z,+}, \sigma_E^{Z,-})^2} \quad (2)$$

Now, from the discussion at the start of the problem, we have the following lower bound on  $H_{\min}(X|E)$ .

$$H_{\min}(X|E) \geq -\log \left( \frac{1}{2} \left( \frac{1}{2} + \frac{1}{2} D(\sigma_E^{X,0}, \sigma_E^{X,1}) + \frac{1}{2} \left( \frac{1}{2} + \frac{1}{2} D(\sigma_E^{Z,+}, \sigma_E^{Z,-}) \right) \right) \right) \quad (3)$$

Simplifying the right-hand side results in

$$H_{\min}(X|E) \geq 1 - \log \left( 1 + \frac{D(\sigma_E^{X,0}, \sigma_E^{X,1}) + D(\sigma_E^{Z,+}, \sigma_E^{Z,-})}{2} \right) \quad (4)$$

We want to find the maximum value of  $D(\sigma_E^{X,0}, \sigma_E^{X,1}) + D(\sigma_E^{Z,+}, \sigma_E^{Z,-})$  subject to  $2p - 1 \leq \sqrt{1 - D(\sigma_E^{X,0}, \sigma_E^{X,1})^2} + \sqrt{1 - D(\sigma_E^{Z,+}, \sigma_E^{Z,-})^2}$ . We look at this as an optimization problem. The maximum value of  $x + y$  subject to the constraint  $\sqrt{1 - x^2} + \sqrt{1 - y^2} \geq \alpha$  is achieved when  $\sqrt{1 - x^2} = \sqrt{1 - y^2} = \alpha/2$ . Hence, we get the desired bound

$$H_{\min}(X|E) \geq 1 - \log \left( 1 + \sqrt{p(1-p) + \frac{3}{4}} \right). \quad (5)$$