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 ith bit is the erroneous bit. Hence $H(X_A - X_B) = v_i$ where v_i is the ith 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, $(1-p)^7 = 1-7p+\ldots$, is -7, while the linear term of the success probability of the 3-bit scheme, $(1-p)^2(1+2p) = 1+0p-3p^2+\ldots$, is 0, and the linear term of the success probability of transferring 7 bits with reconciliation, $(1-p)^6(1+6p) = 1+0p-21p^2+\ldots$, 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

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

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,ε)-weak seeded 2-universal extractor Ext that takes X and a random string $r \leftarrow \{0,1\}_u^{2n}$, and outputs an ε-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 ε-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

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

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,ε)-weak seeded 2-universal extractor Ext that takes X and a random string $r \leftarrow \{0,1\}_u^{2n}$ and outputs an ε-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 ε-secure keys.