CS/Ph120 Homework 7 Solutions

November 29, 2016

Problem 1: Establishing keys in the presence of a limited eavesdropper.

Solution: (Due to Eric Fries)

(a) Define Protocol J_1 as follows: Alice chooses a string $X = x_1, \ldots, x_n \in \{0,1\}^n$ uniformly at random, Alice sends each bit x_i to Bob over the channel where Eve has a probability q of learning each bit, Alice picks a random seed $r \in \{0,1\}^m$, Alice uses a 2-universal extractor $\text{Ext} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^\ell$ to compute $k = \text{Ext}(x, r)$, Alice sends r to Bob over the classically authenticated channel, and Bob computes $k = \text{Ext}(x, r)$.

Eve either learns x_i with probability q and can guess it exactly, or does not learn x_i with probability $1 - q$ and can guess it with probability $\frac{1}{2}$. Therefore,

$$P_{\text{guess}}(X|E) = \left[q + \frac{1-q}{2}\right]^n = \left(\frac{1+q}{2}\right)^n \Rightarrow H_{\min}(X|E) = -n \log\left(\frac{1+q}{2}\right) = n\left[1 - \log(1+q)\right].$$

Page 5 of "Security of Quantum Key Distribution" (Renner 2005) gives

$$\ell \leq H_{\min}(X|E) + 2\log\epsilon - 1 \Rightarrow D\left(\rho_{KRE}, \frac{\mathbb{I}}{2^\ell} \otimes \rho_{RE}\right) \leq \epsilon.$$

For $\epsilon = 10^{-5}$, Protocol J_1 is secure when $\ell \leq n\left[1 - \log(1+q)\right] - 10\log 10 - 1$. The upper bound on ℓ is tightest when q is maximized, so $\frac{1}{3} \leq q \leq \frac{1}{2} \Rightarrow \ell \leq n(2 - \log 3) - 10\log 10 - 1$. Therefore, if the definition of $\text{Ext}(x, r)$ satisfies the previous inequality, then Protocol J_1 is 10^{-5}-secure.

When the amount of 10^{-5}-secure key is maximized,

$$\ell = n(2 - \log 3) - 10\log 10 - 1 \Rightarrow \frac{n}{\ell} = \frac{1}{2 - \log 3}\left(1 + \frac{1 + 10\log 10}{\ell}\right).$$

In the limit of a long key, the channel where Eve has a probability q of learning each bit must be used $\frac{1}{2-\log 3} \approx 2.409$ times per bit of 10^{-5}-secure key.

(TA's comment: One also needs to add m, the length of the seed, in the number of uses of the channel. So the correct ratio is actually $\frac{n+m}{l}$, but anyways the seed length is small and doesn't affect the final number by much)

(b) Define Protocol J_2 as follows: Alice chooses a string $X = x_1, \ldots, x_n \in \{0,1\}^n$ uniformly at random, Alice sends each bit x_i to Bob over the channel where Eve learns every bit but can only remember a maximum of $p = 1024$ of them, Alice picks a random seed $r \in \{0,1\}^m$, Alice uses a 2-universal extractor $\text{Ext} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^\ell$ to compute $k = \text{Ext}(x, r)$, Alice sends r to Bob over the classically authenticated channel, and Bob computes $k = \text{Ext}(x, r)$.

$n \leq p \Rightarrow$ Eve can remember all of $X \Rightarrow P_{\text{guess}}(X|E) = 1 \Rightarrow H_{\min}(X|E) = 0$. $n \geq p \Rightarrow$ there are $n-p$ bits of X that Eve does not remember $\Rightarrow P_{\text{guess}}(X|E) = \left(\frac{1}{2}\right)^{n-p} = 2^{-(n-p)} \Rightarrow H_{\min}(X|E) = n-p$. Therefore, $H_{\min}(X|E) = \max\{0, n-p\}$. From here on forward, assume $n > p \Rightarrow H_{\min}(X|E) = n - p$.

Page 5 of "Security of Quantum Key Distribution" (Renner 2005) gives

$$\ell \leq H_{\min}(X|E) + 2\log\epsilon - 1 \Rightarrow D\left(\rho_{KRE}, \frac{\mathbb{I}}{2^\ell} \otimes \rho_{RE}\right) \leq \epsilon.$$

For $\epsilon = 10^{-10}$, Protocol J_2 is secure when $\ell \leq n - p - 20\log 10 - 1$. For $p = 1024$, Protocol J_2 is secure when $\ell \leq n - 1025 - 20\log 20$.

Problem 3: Generating a key using an anonymous message board.

Solution: (Due to Bolton Bailey)

(a) Consider the following protocol for Alice and Bob. Both Alice and Bob each uniformly randomly choose a bit. Then, Alice and Bob each broadcast their bits on the public channel. If their bits are the same, which happens with probability $\frac{1}{2}$, they consider the protocol failed. If the two bits are different, then both take the bits broadcast by Alice to be the secret key. From Eve's perspective it is impossible to tell which broadcast came from Alice and which from Bob, so she cannot tell which of the two different bits broadcast is the key, so the key is uniformly random from her perspective.

(b) Consider the following protocol, with $3n$ rounds. In each round, Alice and Bob generate a uniformly random bit and broadcast it. Then, (as in part a) each round where the bits matched is considered a failure and in each round where the bits were different, Alice and Bob both take Alice's broadcast bit from that round and append it to their key. By argument as (a), all the bits of this key should be independent of Eve and uniformly random. At the end, if Alice's and Bob's key length is greater than or equal to n, they take the first n bits of their key as their final key. If they have less than n bits, the protocol fails.

The number of bits generated by the $3n$ rounds is distributed accouring to a Bernoulli random variable with $3n$ trials an success probability $\frac{1}{2}$. To bound the chance of failure, we apply the Hoeffding inequality, which is mentioned in the lecutre notes as a variant of the Chernoff bound. The Hoeffding inequality states that the probability a Bernoulli random variable with n trials and probability p is less than or equal to $(p-\epsilon)n$ is bounded by

$$\Pr(B(n,p) \leq (p-\epsilon)n) \leq e^{-2\epsilon^2 n}$$

In this case, we have, with $\epsilon = \frac{1}{6}$

$$\Pr(\text{failure}) = \Pr(B(3n, \frac{1}{2}) < n) \leq \Pr(B(3n, \frac{1}{2}) \leq (\frac{1}{2} - \frac{1}{6})3n) \leq e^{-2(\frac{1}{6})^2 3n} = e^{-n/6}$$

And so the probability of failure is indeed exponentially small.

(c) The argument fails to apply here because in this case Alice and Bob have some information that Eve does not have. Namely, the identities of the people sending the messages. Because Alice and Bob can infer whether they or the other was one who sent a message, they can use this information to create a key. Eve can no longer simply carry out all the operations that Alice and Bob carry out because she doesn't have all the information.

Problem 4: Information reconciliation via linear codes.

Solution: (Due to Alex Meiburg)

(a) With 3 extra bits, there are 8 possible transmitted states that can be corrected to the same output state. One of them is the original text. The other 7 then, we hope, are 7 syndromes corresponding to single-bit flips: we see that indeed each single-bit flip will lead to a different syndrome, so we can correct single-bit errors in the plaintext always. Since this saturates the set of transmitted sets, we can only correct single-bit flip errors, so we have a probability of success of

$$(1-p)^7 + 7p(1-p)^6 = \boxed{1 - 21p^2 + 70p^3 - 105p^4 + 84p^5 - 35p^6 + 6p^7}$$

(b) Transmitting the 7-bit message with no reconcilliation has success rate of

$$(1-p)^7 = \boxed{1 - 7p + 21p^2 - 35p^3 + 35p^4 - 21p^5 + 7p^6 - p^7}$$

Transmitting the 3-bit scheme with the 2 parity-check bits has a success rate of

$$(1-p)^3 + 3p(1-p)^2 = \boxed{1 - 3p^2 + 2p^3}$$

To leading order in p, the 3-bit scheme is the most reliable (but also transmits less data than the 7-bit scheme), followed by the 7-bit with reconciliation, followed by the 7-bit without reconcilliation. Plotting these functions, we can check that this ordering holds for all $p \in (0, 1/2)$. So for these p, the highest success rate scheme is the 3-bit scheme. If we weight by information transmission rate (for instance, with $p = 0.05$, the 7-bit code transmits 7 bits with 10 with success probability 0.995 for information density of 0.669, while the 3-bit code has information density of only 0.596), then the 7-bit code is optimal for $p < 0.1083$, and the 3-bit code is optimal otherwise.

Problem 5: Cloning attacks.

Solution: (Due to Bolton Bailey)

(a) First, consider the case where $p = 0$, that is, Eve uses cloning map T_1 with certainty. Recall that the map T_1 takes

$$T_1 : \rho \mapsto \rho \otimes \frac{1}{2}\mathbb{I}$$

Since Eve forwards the first qubit to Bob, Bob receives ρ in this case. Then, if Bob correctly guesses θ_1, Bob is certain to get the correct measurement outcome.

Second, consider the case where $p = 1$, that is, Eve uses cloning map T_2 with certainty. Since Eve forwards the first qubit to Bob, to get the probability that Bob correctly measures his bit, we trace out the second and third bits produced by the map T_2. Whether a 0 or 1 is sent, this leaves us with a probability of $\frac{5}{6}$ that Bob gets the right state.

$$q_B = \frac{5}{6}$$

In general the probability of Bob being correct is the sum of the probabilities that he is right in either case:

$$1(1-p) + \frac{5}{6}p = 1 - \frac{1}{6}p$$

(b) First, consider the case where $p = 0$, that is, Eve uses cloning map T_1 with certainty. Recall that the map T_1 takes

$$T_1 : \rho \mapsto \rho \otimes \frac{1}{2}\mathbb{I}$$

Since Eve keeps the second qubit, Eve keeps the maximally mixed state. Then, if Eve correctly guesses θ_1, she has a $\frac{1}{2}$ chance of getting the correct outcome.

Second, consider the case where $p = 1$, that is, Eve uses cloning map T_2 with certainty. Since Eve keeps the second bit, to get the probability that Eve correctly measures his bit, we trace out the first and third bits produced by the map T_2. Whether a 0 or 1 is sent, this leaves us with a probability of $\frac{5}{6}$ that Eve gets the right state.

$$q_E = \frac{5}{6}$$

In general the probability of Eve being correct is the sum of the probabilities that she is right in either case:

$$\frac{1}{2}(1-p) + \frac{5}{6}p = \frac{1}{2} + \frac{1}{3}p$$

(c) Bob and Eve's outcomes agree with each other and are correct only if both of the qubits produced by Eve's cloning are correct.

When $p = 0$, Bob is certain to be correct, and Eve is $\frac{1}{2}$ chance to be correct, so the probability of correctness is $\frac{1}{2}$.

When $p = 1$, both are correct only if, when we trace out the last bit of the T_2 output, the remaining two qubits are both correct. This happens with probability $\frac{2}{3}$.

In fact, the probabilities of both being correct in each of these cases are just the cloning success probabilities for these two maps.

Thus, in general, the probability that both are correct is

$$\frac{1}{2}(1-p) + \frac{2}{3}p = \frac{1}{2} + \frac{1}{6}p$$

Problem 6: BB84 against a cloning attack.

Solution: (Due to Alex Meiburg)

(a) From 5a, Bob has a success rate of $1-(1-q_B)p$ in each round, or $(1-q_B)p$ of getting an error in a round, so we expect

$$(1-q_B)pn$$

(b) There are n-choose-δn ways to have δn bits corrupted of n, which is by Stirling's formula is approximately

$$\frac{1}{\sqrt{2\pi n\delta(1-\delta)}} n^n (\delta n)^{-\delta n}(n-\delta n)^{-(1-\delta)n} \approx \frac{1}{\sqrt{n\delta}} n^{\delta n}$$

so that approximately $\delta n \log_2(n)$ bits are required for information reconciliation.
(c)

$$(1-q_B)pn = \delta n \implies \hat{p} = \frac{\delta}{1-q_B}$$

(d) In each of the rounds, Eve has a $\frac{1}{2}(1-p) + q_E p$ chance of guessing correctly, and the min entropy is the negative log of this, so

$$H_{\min}(A|E) = -\log\left(\frac{1}{2}(1-\hat{p}) + q_E\hat{p}\right) = \boxed{-\log\left(\frac{1}{2} + \left(q_E - \frac{1}{2}\right)\frac{\delta}{1-q_B}\right)}$$

(e) From class our affine extractor is a (K,ϵ)-strong extractor for $K \geq m - 2\log\epsilon$. Here we have K given by the $n - H_{\min}$ from (d), combined with the bits leaked out as (b) of $\delta n \log_2(n)$, and m is the bits we can extract. So an ϵ-secure system can be accomplished with

$$n - \left(-\log_2\left(\frac{1}{2} + \left(q_E - \frac{1}{2}\right)\frac{\delta}{1-q_B}\right) + \delta n\log_2(n) + 2\log_2(1/\epsilon)\right)$$

bits available of private key.
(f) We have $\delta \approx p(1-q_B)$, so

$$n - \left(-\log_2\left(\frac{1}{2} + \left(q_E - \frac{1}{2}\right)p\right) + \delta n\log_2(n) + 2\log_2(1/\epsilon)\right)$$

bits of private key available.