P-Set 2 Handin

Alex Miller

October 16, 2021

1

- Consider some $n \in Z, n > 2$ and $OPT'_n : K'xM' \leftarrow C$
- Consider two distinct messages $m_0, m_1 \in M'$, and a cipher text $c = m_0$
- Say we want to calculate the probabilities $Pr[OPT'_n(k, m_0) = c]$ and $Pr[OPT'_n(k, m_1) = c]$, where k is a uniform random variable on K
- There is (at least) one $k_1 \in K$ such that $k_1 \oplus m_1 = c$, since $m_1 \neq c$, meaning $k_1 \oplus m_1 = c$ for some non-zero string in K. Therefore $Pr[OPT'_n(k, m_1) = c] \geq \frac{1}{|K|}$
- However, $k_0 \notin K$ such that $k_0 \oplus m_0 = c$. This follows because $m_0 = c_0$, so $\{0\}^n \oplus m_o = c$, but $\{0\}^n \notin K$. Therefore $Pr[OPT'_n(k, m_0) = c] = 0$
- Therefore $Pr[OPT'_n(k, m_0) = c] \neq Pr[OPT'_n(k, m_1) = c]$, where k is a uniform random variable on K
- OTP'_n is not perfectly secret
- **QED**

2

1. Consider some r. r is a bit string of length $2n$. It contains n '0's and n '1's
   (a) r is generated by concatenating a bit string m of length n to its complement $\neg m$.
   (b) Let the number of '0's in m be z, and the number of '1's be o.
   (c) $o = n - z$
   (d) Let the number of '0's in r be z_r, and the number of '1's be o_r.
   (e) $o_r = z + o = z + n - z = n$
   (f) Therefore $z_r = o_r = n$

2. Consider some c generated from r by some $\pi in K$. c also contains n '0's and n '1's since its generated by a permutation on the bits in r by π.

3. Therefore $\forall m \in M, \exists \pi \in K, s.t. E(\pi, m) = c$. In other words any pair of plain text messages $m_0, m_1 \in M$ can be encoded into one of the same set of cipher texts; $\{E(\pi, m_0) : \pi \in K\} = \{E(\pi, m_1) : \pi \in K\}$

4. Moreover $\forall m_0, m_1 \in M, \forall c \in C, Pr[E(\pi, m_0) = c] = Pr[E(\pi, m_1) = c]$, where π is a uniform random variable over K

   (a) Consider any pair of plain text messages m_0, m_1 and their corresponding intermediate values, $r_0 = m_0 || \neg m_0$ and $r_1 = m_1 || \neg m_1$.

   (b) *Case 1*: consider a cipher text c s.t. $c \in \{E(\pi, m_0) : \pi \in K\} = \{E(\pi, m_1) : \pi \in K\}$. In other words, let c be bit string of length $2n$ with n '0's and n '1's.

   (c) Let $K_0 \subseteq K s.t. \forall \pi_0 \in K_0, E(\pi_0, m_0) = c$. K_0 describes all the distinct $\pi \in K$ that permute r_0 to c

   (d) Let $K_1 \subseteq K s.t. \forall \pi_1 \in K_1, E(\pi_1, m_1) = c$. K_1 describes all the distinct $\pi \in K$ that permute to r_1 to c

   (e) Given that π is a uniform random variable over K, $Pr[E(\pi, m_0) = c] = \frac{|K_0|}{|K|}$ and $Pr[E(\pi, m_1) = c] = \frac{|K_1|}{|K|}$

   (f) $|K_0| = |K_1|$

      i. For either r_0 and r_1, we can count $|K_0|$ and $|K_1|$ the same way.

      ii. Imagine that we separate r_0 and r_1 into buckets of '0' and '1' bits. For each r-string, the '0' and '1' buckets each start with n objectified bits.

      iii. Consider the $2n$ bits of c in order. Say that the first bit of c is '0'; we would have n ways of populating it from r_0's '0'-bucket, and n ways of populating it from r_1's '0'-bucket.

      iv. Moving down c, the next time we encounter a '0'-bit we would have $n-1$ remaining ways of populating it from r_0's '0'-bucket, and $n-1$ ways of populating it from r_1's '0'-bucket.

      v. Repeating this process for all n '0'-bits in c, we can see that there are $n!$ ways of permuting the '0's in r_0 to the '0's in c. The same is true for the '0's in r_1

      vi. We also have to account for '1'-bits in c. Applying the same reasoning we see that there are $n!$ ways of permuting the '1's in r_0 to the '1's in c. The same is true for the '1's in r_1

      vii. Putting it all together, the total number of ways to permute r_0 to c is $n!^2$, and the total number of ways to permute r_1 to c is also $n!^2$

      viii. These numbers describe $|K_0|$ and $|K_1$ respectively

      ix. $|K_0| = |K_1|$

(g) *Case 2*: Now consider a cipher text $c \in C$ s.t. $c \notin \{E(\pi, m_0) : \pi \in K\} = \{E(\pi, m_1) : \pi \in K\}$.

(h) In the first case, $Pr[E(\pi, m_0) = c] = Pr[E(\pi, m_1) = c] = \frac{|K_0|}{|K|} = \frac{|K_1|}{|K|}$. In other words, c can in fact be generated by E and any message $m \in M$ gets encrypted into c with some equal,non-zero probability.

(i) In the second case, c can't in fact be generated by E and any message $m \in M$ never gets encrypted to c. Therefore $Pr[E(\pi, m_0) = c] = Pr[E(\pi, m_1) = c] = 0$

(j) In either case, $Pr[E(\pi, m_0) = c] = Pr[E(\pi, m_1) = c]$, where π is a uniform random variable over K

5. E is therefore perfectly secret (Definition of Perfect Secrecy)

6. **QED**

3

I looked in the textbook
Consider a cipher $E : K$ X $M \leftarrow C$. Let the random variables k be uniformly distributed over K and m over M.
Let k and m be independent.
Let **c** define a random variable over C, $c := E(\mathbf{k}, \mathbf{m})$
First I will prove that if E is perfectly secure, then it has independent cipher texts. In other words, I will show that if E is perfectly secure, **c** is independent of **m**

1. We assume that E is perfectly secure and consider any fixed $m \in M$ and $c \in C$
2. We want to show that $Pr[\mathbf{c} = cAND\mathbf{m} = m] = Pr[\mathbf{c} = c]Pr[\mathbf{m} = m]$
3. $Pr[\mathbf{c} = cAND\mathbf{m} = m] = Pr[E(\mathbf{k}, \mathbf{m}) = cAND\mathbf{m} = m]$
4. $= Pr[E(\mathbf{k}, m) = cAND\mathbf{m} = m]$
5. $= Pr[E(\mathbf{k}, m) = c]Pr[\mathbf{m}]$ (by independence of **m** and **k**)
6. Therefore we need to show that $Pr[E(\mathbf{k}, m) = c] = Pr[\mathbf{c} = c]$. In other words, we can show that the probability of generating the cipher text c is independent of **m**
7. So starting from $c := E(\mathbf{k}, \mathbf{m})$, $Pr[\mathbf{c} = c] = Pr[E(\mathbf{k}, \mathbf{m}) = c]$
8. $= \Sigma_{m' \in M} Pr[E(\mathbf{k}, \mathbf{m}) = cAND\mathbf{=}m = m']$ (Law of total probability)
9. $= \Sigma_{m' \in M} Pr[E(\mathbf{k}, m') = cAND\mathbf{=}m = m']$
10. $= \Sigma_{m' \in M} Pr[E(\mathbf{k}, m') = c]Pr[\mathbf{=}m = m']$ (Independence of **k** and **k**)

11. $= \Sigma_{m' \in M} Pr[E(\mathbf{k}, m) = c] Pr[=m = m']$ (Def of Perfect Secrecy)
12. $= Pr[E(\mathbf{k}, m) = c] \Sigma_{m' \in M} Pr[=m = m']$
13. $= Pr[E(\mathbf{k}, m) = c]$(probabilities sum to 1)
14. **QED**

Next I will prove that if E has independent cipher texts, it is perfectly secret.

1. Assume that **c** and **m** are independent and each message in M occurs with nonzero probability.
2. Let $m \in M$, $c \in C$. It is enough to show from this that $Pr[\mathbf{c} = c] = Pr[E(\mathbf{k}, \mathbf{m}) = c]$ to demonstrate perfect secrecy.
3. $Pr[E(\mathbf{k}, m) = c] Pr[=m = m] = Pr[E(\mathbf{k}, m) = cAND{=}m = m]$ (**k,m** are independent, $Pr[=m] \neq 0$
4. $= Pr[E(\mathbf{k}, \mathbf{m}) = cAND{=}m = m]$
5. $= Pr[\mathbf{c} = cAND{=}m = m]$
6. $= Pr[\mathbf{c} = c] Pr[=m = m]$ (by independence of **c** and **m**)

A cipher $E : KxM \leftarrow C$ **is perfectly secret** $\Leftrightarrow \forall m_0, m_1 \in M, \forall c \in C, Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$

A cipher $E : KxM \leftarrow C$ **has independent cipher texts if for all random variables** $\Leftrightarrow \forall m_0, m_1 \in M, \forall c \in C, Pr[E(\pi, m_0) = c] = Pr[E(\pi, m_1) = c]$

4

4.1 a

1. Lets define a new cipher $E : K$ X K' X $M \leftarrow C$ with the following properties:
   (a) $K = \{0, 1\}$, $K' = \{0, 1\}^2$, $M = \{0, 1\}^n$, $C = \{0, 1\}^{n+1}$
   (b) Define some function $OP : K' \leftarrow \{0, 1\}^1$, and which maps two bit strings to one bit strings in a fixed but non-uniform grouping. For
   (c) Given an $k \in K$, $k' \in K'$, $m \in M$, we calculate $c \in C$ accordingly: $c = E(k, k', m) = k \oplus m || OP(k')$
2. E is perfectly secret:

(a) Say that k is a uniform random variable on K. Being a bit string, we can also say that parts of k are equivalently uniformly random on their sections. As such, we can say that the string $k_{n+1}||k_{n+2}$ is a uniform random variable on $\{0,1\}^2$.

(b) Consider any message pair $m_0, m_1 \in M$, and any $c \in C$.

(c) Let k and k' be uniform random variables on the sets K and K', respectively

(d) Consider the first n bits and last bit of our c. Call these c' and c'', respectively.

(e) $Pr[k \oplus m_0 = c'] = Pr[k \oplus m_1 = c']$ (The One Time Pad is Perfectly Secret)

(f) Moreover, since the derivation of c'' is independent of either m_0 or m_1 we can further say that $Pr[E(k,k',m_0) = c'||c'' = c] = Pr[E(k,k',m_1) = c'||c'' = c]$

(g) Therefore $\forall m_0, m_1 \in M, \forall c \in C, Pr[E(k,k',m_0) = c] = Pr[E(k,k',m_1) = c]$ where k and k' are uniform random variables on K and K' respectively

3. However, E does **not** have uniform cipher texts

   (a) Depending on how we choose to define OP, we can change the probabilities with which the values of c'' get encrypted by E. For example, if we make OP an OR operation on the bits in k', E encodes c'' to 1 with a bias of .75.

   (b) Therefore, For every random variable m on M, k on K, k' on K', the random variable $C = E(K,M)$ is not uniform on the $Img(E)$

4. **QED**

4.2 b

1. Assume E has uniform cipher texts and that it is not perfectly secret

2. Then, for any random variable m on M, $C = E(K,M)$ is uniform on $Img(E)$

3. However, if E wasn't perfectly secret, then C wouldn't be uniform over $Img(E)$, because given a uniform m, the messages M would map to cipher texts on C with non uniform distribution.

4. This is not the case, because we assume E has uniform cipher texts.

5. Therefore E must be perfectly secret.

6. If E has uniform cipher texts it is perfectly secret

7. **QED**