CS4236 Assignment 2 feedback, discussion, marking schedule

October 19, 2022

1 Questions with feedback, discussion, marking schedule

1. Let $G(s) \stackrel{\text{def}}{=} s \oplus \text{rand}()$, where rand() is a function which returns a truly random bitstring the same size as s, and as usual, $\oplus$ is XOR. Prove or disprove that $G(s)$ is a PRG (a pseudorandom generator). (2 marks)

Feedback: Y*our answer had to be correct, and had to have a proof.*

(a) $G(s)$ is not a PRG .

(b) *One clear reason is that the output of the generator is the same size as the input, so the function does not extend the length. A PRG must be longer than the input (rule 1).*

Discussion: $G(s)$ is not a PRG. *Definition 3.14 states that a PRG must have two properties - expansion ($\ell(n) > n$) and pseudorandomness. Clearly the size of the function is the same as the input seed so the function does not have the first property, and so cannot be a PRG.*

Marking schedule: *One mark for each part.*

(a) *$G(s)$ is not a PRG.* (1 mark)

(b) *Does not length extend as in Definition 3.14, expansion rule.* (1 mark)

2. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Prove or disprove that the function $G'(s) \stackrel{\text{def}}{=} G(s')$ is also a PRG, where s' is the least significant $n-1$ bits of s. (3 marks)

Feedback: Y*our proof had to take a particular stance (i.e. clearly state yes or no), and then provide a strong justification. In my view I think the function* $G'(s) \stackrel{\text{def}}{=} G(s')$ is a PRG.

Discussion: *The function* $G'(s) \stackrel{\text{def}}{=} G(s')$ is a PRG. *Assuming* $n \geq 2$, *then it still has expansion, no matter what view you take of the signature. For the second part we can try either a suppose-not proof, or a direct proof.*

A direct proof might identify that the input is any of the values $\{0,1\}^{n-1}$. *Since the least significant* $n-1$ *bits of* s *are normally distributed if* s *is normally distributed, then the function* $G : \{0,1\}^{n-1} \to \{0,1\}^{2n}$ *is a PRG.* ∎

A suppose not proof might start by assuming that $G'(s) \stackrel{\text{def}}{=} G(s')$ *is not a PRG. If this is the case then this means that a distinguisher can identify the function* $G()$ *when applied to the subset* s' *of* $s \in S$. *If this is the case, then the function* $G : \{0,1\}^n \to \{0,1\}^{2n}$ *is not a PRG. Finally we have that* $G'(s)$ is a PRG. ∎

Marking schedule: *The proof should*

(a) show clear understanding of the question. (1 mark)

(b) give a clear justification or proof. (2 mark)

(c) a half mark is given for those who said NO, using the $2n-2$ no-expansion argument when $n=2$, which was corrected in class. ($\frac{1}{2}$ mark)

3. A length preserving function is where the key, the index and the result are all the same size. For example the function $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. If $n = 4$, how many different such functions are there? (2 marks)

Feedback: *This was discussed at the beginning of one of the classes. During that, I explained that in my view, the question clearly asked for how many different functions are there of the type given, and that it did not discuss $F_k(x)$ as used in PRFs. Your explanation had to*

- ***(a)*** *have the correct answer.*
- ***(b)*** *explain why.*

Discussion: *The slides for Topic4 showed a function $F^* : \{0,1\}^n \rightarrow \{0,1\}^n$, with one representation of such a function as an array of 2^n values, each of n bits. This array has $n \times 2^n$ bits, and represents/defines just one function with this particular signature. The number of such $n \times 2^n$ bit values (and hence the number of such functions) is $2^{n \times 2^n}$.*
In the question's case though, we have a function like $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. There are two inputs to the function, and we could rewrite this function as $F : \{0,1\}^{2 \times n} \rightarrow \{0,1\}^n$, concatenating the two inputs. This example then is an array of $2^{2 \times n}$ values, each of n bits. This array has $n \times 2^{2 \times n}$ bits, and represents/defines just one function with this particular signature. The number of such $n \times 2^{2 \times n}$ bit values (and hence the number of such functions) is $2^{n \times 2^{2 \times n}}$. For our example, it is $2^{4 \times 2^{2 \times 4}} = 2^{1024} = 17976931348623159077293051907890....$

Marking schedule: *The answer should...*

- ***(a)*** *...have the answer $2^{4 \times 2^{2 \times 4}} = 2^{1024} = 1797....$* (1 mark)
- ***(b)*** *...have some explanation, even if it is just "from the lecture notes".* (1 mark)

4. In the third lecture session, we saw Construction 3.17 which was EAV-Secure (Theorem 3.18, described in class, is the proof). Prove the opposite - i.e. if G is not a PRG, then 3.17 cannot be EAV-secure. (4 marks)

Feedback: *I expected a detailed proof or an argument. There may be multiple ways of doing this - perhaps directly, perhaps by suppose not...*

Discussion: *(Direct construction) To prove if G is not a PRG, then 3.17 cannot be EAV secure, we could use a direct construction of an adversary which can win the EAV game against 3.17. If G is not a PRG, then we have a PPT distinguisher D with*

$$|\Pr[D(G(s)) = 1] - Pr[D(r) = 1]| = \epsilon(n) \qquad (\geq \frac{1}{p(n)})$$

We construct an (EAV) adversary which simulates this distinguisher:

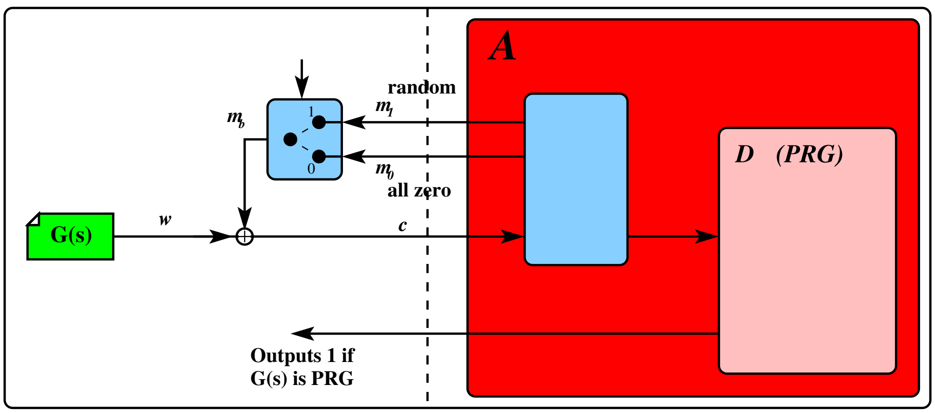

Figure 1: Adversary with simulated PRG distinguisher

In the above, we are directly constructing an adversary to play the EAV game. The adversary simulates the (PRG) distinguisher. Our PPT adversary uses two messages: $m_1 \in \{0,1\}^n$ (i.e. a random bit string), and $m_0 = 0^n$. The adversary passes on the ciphertext c, which is either $G(s)$ or random, because if the challenger chooses 0^n then $G(s)$ passes straight through unchanged as $c = G(s) \oplus 0 = G(s)$. Otherwise c will be random. If the challenger chooses m_0, the distinguisher is able to correctly identify $G(s)$ with probability $\epsilon(n)$, and as a result will win the EAV game with probability $\Pr[D(G(s)) = 1] = \frac{\epsilon(n)}{2}$. As such this constructed adversary can win the game with probability greater than negl, and it is not EAV secure. This finishes the proof. ■

Marking schedule: *The answer should*

- ***(a)*** *Give a reasonable proof strategy or outline.* (1 mark)
- ***(b)*** *Clearly explain the steps in the proof, or train of argument (perhaps) as above.* (3 marks)

5. Construct a PRG G from a (length preserving) PRF F, and show it is a PRG. (4 marks)

Feedback: *Your answer cannot just be replacing a PRG by a PRF. A length-preserving PRF would not have the expansion property. I was expecting a (formal) construction, and a proof why it is a PRG.*

Discussion: *Perhaps one simple construction would be to concatenate two calls to the same PRF:*

$$G(s) \stackrel{\mathsf{def}}{=} F_s(0) \mathbin{+\!\!+} F_s(1)$$

To prove that it is a PRG, we note that the length is longer: $\ell(n) = 2 \times n$, so the function has extension. To prove the other part of the definition, that if F is a PRF, then G is a PRG *we could use suppose not, starting with the assumption that G is not a PRG. This means that a distinguisher can distinguish G, and from Definition 3.14 we have a PPT distinguisher D with*

$$|\Pr[D(G(s)) = 1] - Pr[D(r) = 1]| = \epsilon(n) \qquad (\geq \frac{1}{p(n)})$$

(where $r \in \{0,1\}^{2\times n}, s \in \{0,1\}^n$). As for the proof given in class, we construct a distinguisher for a PRF, which simulates this distinguisher for the PRG:

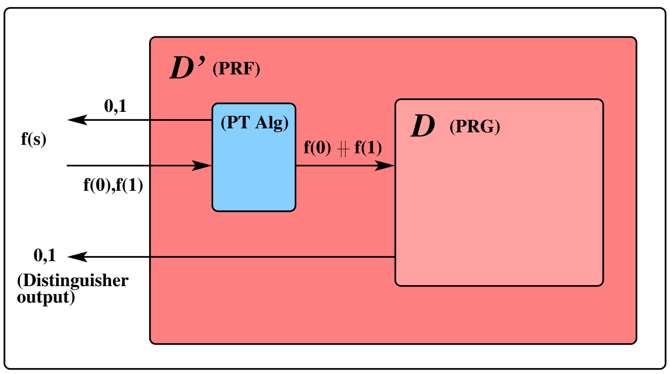

Figure 2: PRF distinguisher with simulated PRG distinguisher

In the above, we simulate a distinguisher which can distinguish the PRG $f(0) \mathbin{+\!\!+} f(1)$, derived from the external PRF oracle (with the PPT algorithm querying the external oracle and concatenating the answers). The output of this outer PRF distinguisher D' is exactly the output of the inner PRG distinguisher D and distinguishes with the same probability:

$$\left|\Pr\left[D'^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[D'^{f(\cdot)}(1^n) = 1\right]\right| = \varepsilon(n)$$

As such it distinguishes the PRF. We have that if G is not a PRG then F is not a PRF, and of course this means that if F is a PRF, then G is a PRG. *This finishes the proof.* ■

Marking schedule: *The answer should*

- ***(a)*** *Give a reasonable PRG, $\frac{1}{2}$ a mark off if you do not mention expansion.* (1 mark)
- ***(b)*** *Clearly explain the steps in the proof, or train of argument (perhaps) as above.* (3 marks)