Problem Set 3

1. Consider the following security definition for pseudorandom generator.

> Let m and n be positive integers. Let $G : \{0,1\}^m \to \{0,1\}^n$ be a pseudorandom generator, and let A be an adversary against G. We define the following subroutines, experiment, and advantage function.
>
> | Subroutine `Initialize`(w) | Experiment $\mathbf{Exp}_G^{\text{prg-}w}(A)$ |
> |---|---|
> | If $w = 0$ | $y \xleftarrow{\$}$ `Initialize`(w) |
> | then $y \xleftarrow{\$} \{0,1\}^n$ | $d \xleftarrow{\$} A(y)$ |
> | else $s \xleftarrow{\$} \{0,1\}^m$; $y \leftarrow G(s)$ | Return d |
> | Return y | |
>
> We define the *prg* advantage* of an adversary A attacking G as
>
> $$\mathbf{Adv}_G^{\text{prg*}}(A) = \Pr\left[\mathbf{Exp}_G^{\text{prg-1}}(A) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}_G^{\text{prg-0}}(A) \Rightarrow 1\right] .$$

Recall the definition of $\mathbf{Adv}^{\text{prg}}$ defined in the textbook and studied in class. Prove that, for all G and A,

$$\mathbf{Adv}_G^{\text{prg*}}(A) = \mathbf{Adv}_G^{\text{prg}}(A) .$$

2. Let m and n be positive integers, and let $G_1 : \{0,1\}^m \to bits^n$ and $G_2 : \{0,1\}^m \to bits^n$ be pseudorandom generators. Define a pseudorandom generator $G : \{0,1\}^m \to \{0,1\}^{2n}$ as follows. For any $s \in \{0,1\}^m$,

$$G(s) \ = \ G_1(s) \| G_2(s) .$$

Suppose that G_1 and G_2 are secure under the PRG security notion. Is G necessarily a secure PRG? Prove your answer. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

3. Let m and n be positive integers, and let $G_1 : \{0,1\}^m \to bits^n$ and $G_2 : \{0,1\}^m \to bits^n$ be pseudorandom generators. Define a pseudorandom generator $G : \{0,1\}^{2m} \to \{0,1\}^{2n}$ as follows. For any $s_1, s_2 \in \{0,1\}^m$,

$$G(s_1 s_2) \ = \ G_1(s_1) \| G_2(s_2) .$$

Suppose that G_1 and G_2 are secure under the PRG security notion. Is G necessarily a secure PRG? Prove your answer. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

4. Let n be a positive integer. Recall that $[\mathsf{KG}]$ denotes the set of all possible keys output by the algorithm KG. Let $\mathsf{MA} = (\mathsf{KG}, \mathsf{Tag}, \mathsf{Vf})$ be a MAC scheme secure under the SUF-CMA security notion, and let $\{0,1\}^n$ be the message space for MA. We define $\mathsf{MA}' = (\mathsf{KG}, \mathsf{Tag}', \mathsf{Vf}')$ where, for all $M \in \{0,1\}^{2n}$, for all $K \in [\mathsf{KG}]$,

$$\mathsf{Tag}'_K(M) \; = \; \mathsf{Tag}_K(M[1]) \| \mathsf{Tag}_K(M[2])$$

where $M = M[1]M[2]$ and $|M[1]| = |M[2]|$.

(a) Write a deterministic and stateless algorithm Vf' that would ensure that MA' satisfies the correctness condition.

(b) Is MA' necessarily a secure MAC scheme? Prove your answer. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

5. Let n be a positive integer. Recall that $[\mathsf{KG}]$ denotes the set of all possible keys output by the algorithm KG. Let $\mathsf{MA} = (\mathsf{KG}, \mathsf{Tag}, \mathsf{Vf})$ be a MAC scheme secure under the SUF-CMA security notion, and let $\{0,1\}^n$ be the message space for MA. We define $\mathsf{MA}' = (\mathsf{KG}, \mathsf{Tag}', \mathsf{Vf}')$ where, for all $M \in \{0,1\}^n$, for all $K \in [\mathsf{KG}]$,

$$\mathsf{Tag}'_K(M) \; = \; \mathsf{Tag}_K(M) \| \mathsf{Tag}_K(M) \; .$$

(a) Write a deterministic and stateless algorithm Vf' that would ensure that MA' satisfies the correctness condition.

(b) Is MA' necessarily a secure MAC scheme? Prove your answer. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

6. Let n be a positive integer. Recall that $[\mathsf{KG}]$ denotes the set of all possible keys output by the algorithm KG. Let $\mathsf{MA}_1 = (\mathsf{KG}, \mathsf{Tag}_1, \mathsf{Vf}_1)$ and $\mathsf{MA}_2 = (\mathsf{KG}, \mathsf{Tag}_2, \mathsf{Vf}_2)$ be MAC schemes secure under the SUF-CMA security notion, and let $\{0,1\}^n$ be the message space for MA_1 and MA_2. We define $\mathsf{MA}_3 = (\mathsf{KG}, \mathsf{Tag}_3, \mathsf{Vf}_3)$ where, for all $M \in \{0,1\}^n$, for all $K \in [\mathsf{KG}]$,

$$\mathsf{Tag}_3(K, M) \; = \; \mathsf{Tag}_1(K, M) \| \mathsf{Tag}_2(K, M) \; .$$

(Note that the notation here is slightly different from the previous question to avoid potential confusion regarding the algorithm name and the subscript K.)

(a) Write a deterministic and stateless algorithm Vf_3 that would ensure that MA_3 satisfies the correctness condition.

(b) Is MA_3 necessarily a secure MAC scheme? Prove your answer. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.