CSE 107 Final Exam June 6, 2022

Answer the questions in the spaces provided on the question sheets. You may use the back side of the paper as scratch. Write legibly. If we can't read your writing or your answer is not within the specified answer space, you will not receive credit. As the papers get scanned before grading, we strongly advise you to use a pen rather than a pencil.

Some questions ask you to write computer programs. It is expected that you write in pseudocode, and use terms like 0^n and standard mathematical notation, rather than worry about the details of a Python/PlayCrypt implementation.

You may use a single, double-sided, letter-size page of handwritten notes for reference.

You may **not** use your computer, tablet, phone, or smartwatch during the exam.

The last pages contain definitions of many of the security concepts we discussed in lecture for you to use during the exam. Please do not turn these pages in.

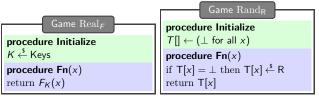
There are 8 questions, for a total of 90 points. The last question is optional.

Name:		
PID:		
1 ID.		

Question:	1	2	3	4	5	6	7	8	Total
Points:	20	14	12	14	10	14	6	0	90
Score:									

Games defining prf advantage of an adversary against F

Let $F: \text{Keys} \times D \to R$ be a family of functions.



Definition of **Adv**^{prf}

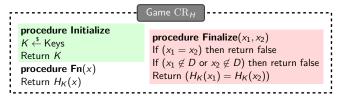
The (prf) advantage of A is $\mathbf{Adv}_F^{\mathrm{prf}}(A) = \mathsf{Pr}\left[\mathrm{Real}_F^A \Rightarrow 1\right] - \mathsf{Pr}\left[\mathrm{Rand}_R^A \Rightarrow 1\right]$

Security: F is a (secure) PRF if $\mathbf{Adv}_F^{\mathrm{prf}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

UCSD CSE107: Intro to Modern Cryptography

Collision-resistance of a function family

The formalism considers a family $H: \text{Keys} \times D \to R$ of functions, meaning for each $K \in \text{Keys}$ we have a function $H_K: D \to R$ defined by $H_K(x) = H(K, x)$.



Let

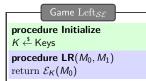
$$\mathsf{Adv}^{\mathrm{cr}}_{H}(A) = \mathsf{Pr}\left[\mathrm{CR}^{A}_{H} \Rightarrow \mathsf{true}\right].$$

UCSD CSE107: Intro to Modern Cryptography

2/12

Games for ind-cpa-advantage of an adversary A

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme



Game Right_{\mathcal{SE}}

procedure Initialize $\mathcal{K} \stackrel{5}{\leftarrow} \text{Keys}$ procedure LR(M_0, M_1)

return $\mathcal{E}_{\mathcal{K}}(M_1)$

Definition of Advind-cpa

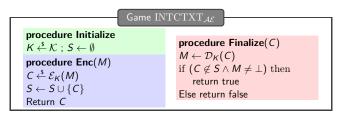
The (ind-cpa) advantage of A is $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(A) = \mathsf{Pr}\left[\mathrm{Right}^{\mathcal{A}}_{\mathcal{SE}} \Rightarrow 1\right] - \mathsf{Pr}\left[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} \Rightarrow 1\right]$

Security: \mathcal{SE} is IND-CPA-secure if $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

UCSD CSE107: Intro to Modern Cryptography

Ciphertext integrity

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme.



Definition: int-ctxt advantage

The int-ctxt advantage of an adversary A is

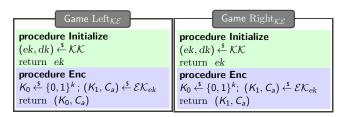
$$\mathsf{Adv}^{\mathrm{int-ctxt}}_{\mathcal{A}\mathcal{E}}(A) = \mathsf{Pr}[\mathsf{INTCTXT}^A_{\mathcal{A}\mathcal{E}} \Rightarrow \mathsf{true}]$$

UCSD CSE107: Intro to Modern Cryptography

4/12

KEM IND-CPA security games

Let KE = (KK, EK, DK) be a KEM with key length k.

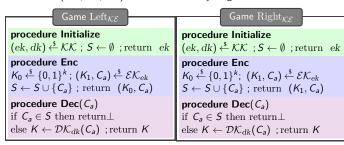


Definition (ind-cpa advantage Advind-cpa for KEMs)

The (ind-cpa) advantage of an adversary
$$A$$
 is
$$\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{KE}}(A) = \mathsf{Pr}\left[\mathrm{Right}^A_{\mathcal{KE}} \Rightarrow 1\right] - \mathsf{Pr}\left[\mathrm{Left}^A_{\mathcal{KE}} \Rightarrow 1\right]$$

KEM IND-CCA security games

Let KE = (KK, EK, DK) be a KEM with key length k.



Definition (ind-cca advantage **Adv**^{ind-cca} for KEMs)

The (ind-cca) advantage of an adversary A is

UCSD CSE107: Intro to Modern Cryptography

5/12

PKE IND-CPA security games

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme.

procedure Initialize $(ek, dk) \stackrel{5}{\sim} \mathcal{K}$ return ek procedure $\mathsf{LR}(M_0, M_1)$

procedure Initialize $(ek, dk) \stackrel{5}{\leftarrow} \mathcal{K}$ return ekprocedure LR (M_0, M_1) return $\mathcal{E}_{ek}(M_1)$

Definition (ind-cpa advantage **Adv**^{ind-cpa}, public-key version)

The (ind-cpa) advantage of an adversary A is

$$\textbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathcal{A}\mathcal{E}}(\textit{A}) = \mathsf{Pr}\left[\mathrm{Right}^{\textit{A}}_{\mathcal{A}\mathcal{E}} \Rightarrow 1\right] - \mathsf{Pr}\left[\mathrm{Left}^{\textit{A}}_{\mathcal{A}\mathcal{E}} \Rightarrow 1\right]$$

UCSD CSE107: Intro to Modern Cryptography

return $\mathcal{E}_{ek}(M_0)$

7/12

UF-CMA (MACs)

Let \mathcal{T} : Keys \times $D \to R$ be a message authentication code.

procedure Initialize $K \stackrel{\xi}{\sim} \text{Keys}; S \leftarrow \emptyset$ procedure Tag(M) $T \leftarrow \mathcal{T}_K(M); S \leftarrow S \cup \{M\}$ return T

procedure Finalize (M, T)If $M \in S$ then return false If $M \notin D$ then return false Return $(T = T_K(M))$

Definition: uf-cma advantage

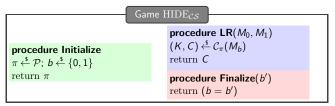
The uf-cma advantage of an adversary A is

$$\mathsf{Adv}^{\mathrm{uf\text{-}cma}}_{\mathcal{T}}(A) = \mathsf{Pr}\left[\mathrm{UFCMA}^{A}_{\mathcal{T}} \Rightarrow \mathsf{true}\right]$$

UCSD CSE107: Intro to Modern Cryptography

Hiding security

Let $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ be a commitment scheme.



Definition (hiding-advantage)

The hiding-advantage of an adversary \boldsymbol{A} is

$$\textbf{Adv}^{\mathrm{HIDE}}_{\mathcal{CS}}(\textit{A}) = 2 \cdot \mathsf{Pr}\left[\mathrm{HIDE}^{\textit{A}}_{\mathcal{CS}} \Rightarrow \mathsf{true}\right] - 1 \; .$$

Hiding security asks that an adversary having C but not K should not learn even partial information about the message M.

PKE IND-CCA security games

Let $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme.

procedure Initialize procedure Initialize $(ek, dk) \stackrel{s}{\leftarrow} \mathcal{K}; S \leftarrow \emptyset ; \text{return } ek$ $(ek, dk) \stackrel{\$}{\leftarrow} \mathcal{K}; S \leftarrow \emptyset ; \text{return } ek$ procedure $LR(M_0, M_1)$ procedure $LR(M_0, M_1)$ $C \stackrel{\$}{\leftarrow} \mathcal{E}_{ek}(M_0)$; $S \leftarrow S \cup \{C\}$ $C \stackrel{\$}{\leftarrow} \mathcal{E}_{ek}(M_1); S \leftarrow S \cup \{C\}$ return Creturn C procedure Dec(C)procedure Dec(C)if $C \in S$ then return \bot if $C \in S$ then return \bot else $M = \mathcal{D}_{dk}(C)$; return Melse $M = \mathcal{D}_{dk}(C)$; return M

Definition (ind-cca advantage Advind-cca)

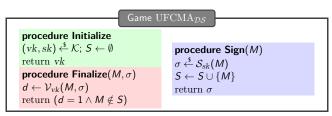
The ind-cca advantage of an adversary A is

$$\mathsf{Adv}^{\mathrm{ind}\text{-}\mathrm{cca}}_{\mathcal{A}\mathcal{E}}(\mathcal{A}) = \mathsf{Pr}\left[\mathrm{Right}^{\mathcal{A}}_{\mathcal{A}\mathcal{E}} \Rightarrow 1\right] - \mathsf{Pr}\left[\mathrm{Left}^{\mathcal{A}}_{\mathcal{A}\mathcal{E}} \Rightarrow 1\right]$$

UCSD CSE107: Intro to Modern Cryptograph

UF-CMA (digital signatures)

Let $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ be a signature scheme.



Definition: uf-cma advantage (digital signature version)

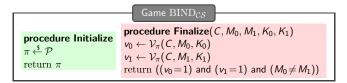
The uf-cma advantage of an adversary A is

$$\mathsf{Adv}^{\mathrm{uf\text{-}cma}}_{\mathcal{DS}}(A) = \mathsf{Pr}\left[\mathrm{UFCMA}^A_{\mathcal{DS}} \Rightarrow \mathsf{true}\right]$$

UCSD CSE107: Intro to Modern Cryptography

Binding security

Let CS = (P, C, V) be a commitment scheme.



Definition (binding-advantage)

The binding-advantage of an adversary \boldsymbol{A} is

$$\textbf{Adv}_{\mathcal{CS}}^{\operatorname{BIND}}(A) = \text{Pr}\left[\operatorname{BIND}_{\mathcal{CS}}^A \Rightarrow \text{true}\right] \;.$$

Binding security asks that an adversary be unable to create a commitment ${\it C}$ that it can open to two different messages.

11/12