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: ______________________________

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: Keys $\times$ D $\rightarrow$ R be a family of functions.

Game Real_F

procedure Initialize
$K \xleftarrow{\$}$ Keys

procedure Fn(x)
return $F_K(x)$

Game Rand_R

procedure Initialize
$T[] \leftarrow (\perp$ for all $x)$

procedure Fn(x)
if $T[x] = \perp$ then $T[x] \xleftarrow{\$}$ R
return $T[x]$

Definition of $\mathbf{Adv}^{\mathrm{prf}}$

The (prf) advantage of A is

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

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

Collision-resistance of a function family

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

Game CR_H

procedure Initialize
$K \xleftarrow{\$}$ Keys
Return K

procedure Fn(x)
Return $H_K(x)$

procedure Finalize(x_1, x_2)
If $(x_1 = x_2)$ then return false
If $(x_1 \notin D$ or $x_2 \notin D)$ then return false
Return $(H_K(x_1) = H_K(x_2))$

Let

$$\mathbf{Adv}_H^{\mathrm{cr}}(A) = \Pr\left[\mathrm{CR}_H^A \Rightarrow \text{true}\right].$$

Games for ind-cpa-advantage of an adversary A

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

Game $\mathrm{Left}_{\mathcal{SE}}$

procedure Initialize
$K \xleftarrow{\$}$ Keys

procedure LR(M_0, M_1)
return $\mathcal{E}_K(M_0)$

Game $\mathrm{Right}_{\mathcal{SE}}$

procedure Initialize
$K \xleftarrow{\$}$ Keys

procedure LR(M_0, M_1)
return $\mathcal{E}_K(M_1)$

Definition of $\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}$

The (ind-cpa) advantage of A is

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

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

Ciphertext integrity

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

Game $\mathrm{INTCTXT}_{\mathcal{AE}}$

procedure Initialize
$K \xleftarrow{\$} \mathcal{K}$; $S \leftarrow \emptyset$

procedure Enc(M)
$C \xleftarrow{\$} \mathcal{E}_K(M)$
$S \leftarrow S \cup \{C\}$
Return C

procedure Finalize(C)
$M \leftarrow \mathcal{D}_K(C)$
if $(C \notin S \wedge M \neq \perp)$ then
return true
Else return false

Definition: int-ctxt advantage

The int-ctxt advantage of an adversary A is

$$\mathbf{Adv}_{\mathcal{AE}}^{\mathrm{int\text{-}ctxt}}(A) = \Pr[\mathrm{INTCTXT}_{\mathcal{AE}}^A \Rightarrow \text{true}]$$

KEM IND-CPA security games

Let $\mathcal{KE} = (\mathcal{KK}, \mathcal{EK}, \mathcal{DK})$ be a KEM with key length k.

Game $\mathrm{Left}_{\mathcal{KE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{KK}$
return ek

procedure Enc
$K_0 \xleftarrow{\$} \{0,1\}^k$; $(K_1, C_a) \xleftarrow{\$} \mathcal{EK}_{ek}$
return (K_0, C_a)

Game $\mathrm{Right}_{\mathcal{KE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{KK}$
return ek

procedure Enc
$K_0 \xleftarrow{\$} \{0,1\}^k$; $(K_1, C_a) \xleftarrow{\$} \mathcal{EK}_{ek}$
return (K_1, C_a)

Definition (ind-cpa advantage $\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}$ for KEMs)

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

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

KEM IND-CCA security games

Let $\mathcal{KE} = (\mathcal{KK}, \mathcal{EK}, \mathcal{DK})$ be a KEM with key length k.

Game $\mathrm{Left}_{\mathcal{KE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{KK}$; $S \leftarrow \emptyset$; return ek

procedure Enc
$K_0 \xleftarrow{\$} \{0,1\}^k$; $(K_1, C_a) \xleftarrow{\$} \mathcal{EK}_{ek}$
$S \leftarrow S \cup \{C_a\}$; return (K_0, C_a)

procedure Dec(C_a)
if $C_a \in S$ then return $\perp$
else $K \leftarrow \mathcal{DK}_{dk}(C_a)$; return K

Game $\mathrm{Right}_{\mathcal{KE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{KK}$; $S \leftarrow \emptyset$; return ek

procedure Enc
$K_0 \xleftarrow{\$} \{0,1\}^k$; $(K_1, C_a) \xleftarrow{\$} \mathcal{EK}_{ek}$
$S \leftarrow S \cup \{C_a\}$; return (K_1, C_a)

procedure Dec(C_a)
if $C_a \in S$ then return $\perp$
else $K \leftarrow \mathcal{DK}_{dk}(C_a)$; return K

Definition (ind-cca advantage $\mathbf{Adv}^{\mathrm{ind\text{-}cca}}$ for KEMs)

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

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

PKE IND-CPA security games

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

Game $\text{Left}_{\mathcal{AE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{K}$
return ek

procedure LR(M_0, M_1)
return $\mathcal{E}_{ek}(M_0)$

Game $\text{Right}_{\mathcal{AE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{K}$
return ek

procedure LR(M_0, M_1)
return $\mathcal{E}_{ek}(M_1)$

Definition (ind-cpa advantage $\mathbf{Adv}^{\text{ind-cpa}}$, public-key version)

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

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A) = \Pr\left[\text{Right}^A_{\mathcal{AE}} \Rightarrow 1\right] - \Pr\left[\text{Left}^A_{\mathcal{AE}} \Rightarrow 1\right]$$

PKE IND-CCA security games

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

Game $\text{Left}_{\mathcal{AE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{K}$; $S \leftarrow \emptyset$; return ek

procedure LR(M_0, M_1)
$C \xleftarrow{\$} \mathcal{E}_{ek}(M_0)$; $S \leftarrow S \cup \{C\}$
return C

procedure Dec(C)
if $C \in S$ then return $\perp$
else $M = \mathcal{D}_{dk}(C)$; return M

Game $\text{Right}_{\mathcal{AE}}$

procedure Initialize
$(ek, dk) \xleftarrow{\$} \mathcal{K}$; $S \leftarrow \emptyset$; return ek

procedure LR(M_0, M_1)
$C \xleftarrow{\$} \mathcal{E}_{ek}(M_1)$; $S \leftarrow S \cup \{C\}$
return C

procedure Dec(C)
if $C \in S$ then return $\perp$
else $M = \mathcal{D}_{dk}(C)$; return M

Definition (ind-cca advantage $\mathbf{Adv}^{\text{ind-cca}}$)

The ind-cca advantage of an adversary A is

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

UF-CMA (MACs)

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

Game $\text{UFCMA}_{\mathcal{T}}$

procedure Initialize
$K \xleftarrow{\$}$ 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 $(T = \mathcal{T}_K(M))$

Definition: uf-cma advantage

The uf-cma advantage of an adversary A is

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

UF-CMA (digital signatures)

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

Game $\text{UFCMA}_{\mathcal{DS}}$

procedure Initialize
$(vk, sk) \xleftarrow{\$} \mathcal{K}$; $S \leftarrow \emptyset$
return vk

procedure Finalize(M, σ)
$d \leftarrow \mathcal{V}_{vk}(M, \sigma)$
return $(d = 1 \wedge M \notin S)$

procedure Sign(M)
$\sigma \xleftarrow{\$} \mathcal{S}_{sk}(M)$
$S \leftarrow S \cup \{M\}$
return σ

Definition: uf-cma advantage (digital signature version)

The uf-cma advantage of an adversary A is

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

Hiding security

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

Game $\text{HIDE}_{\mathcal{CS}}$

procedure Initialize
$\pi \xleftarrow{\$} \mathcal{P}$; $b \xleftarrow{\$} \{0, 1\}$
return π

procedure LR(M_0, M_1)
$(K, C) \xleftarrow{\$} \mathcal{C}_\pi(M_b)$
return C

procedure Finalize(b')
return $(b = b')$

Definition (hiding-advantage)

The hiding-advantage of an adversary A is

$$\mathbf{Adv}^{\text{HIDE}}_{\mathcal{CS}}(A) = 2 \cdot \Pr\left[\text{HIDE}^A_{\mathcal{CS}} \Rightarrow \text{true}\right] - 1\,.$$

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

Binding security

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

Game $\text{BIND}_{\mathcal{CS}}$

procedure Initialize
$\pi \xleftarrow{\$} \mathcal{P}$
return π

procedure Finalize(C, M_0, M_1, K_0, K_1)
$v_0 \leftarrow \mathcal{V}_\pi(C, M_0, K_0)$
$v_1 \leftarrow \mathcal{V}_\pi(C, M_1, K_1)$
return $((v_0 = 1)$ and $(v_1 = 1)$ and $(M_0 \neq M_1))$

Definition (binding-advantage)

The binding-advantage of an adversary A is

$$\mathbf{Adv}^{\text{BIND}}_{\mathcal{CS}}(A) = \Pr\left[\text{BIND}^A_{\mathcal{CS}} \Rightarrow \text{true}\right]\,.$$

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