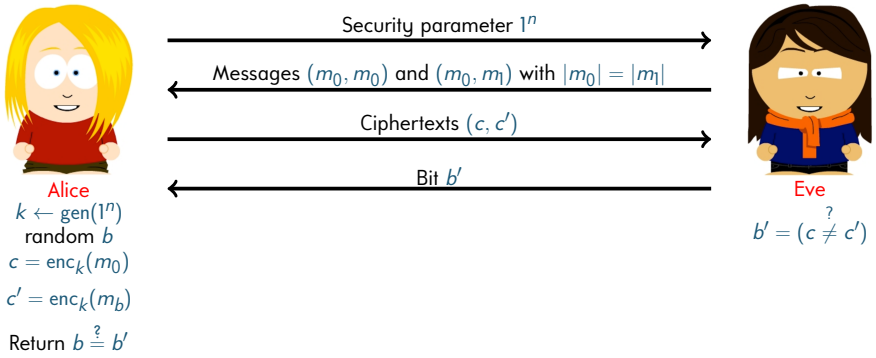
Cryptography

Lecture 6: Pseudorandom Functions

November 20, 2026

Multiple Encryptions



Notes

- Pair of equal messages yields valid (message, ciphertext) pair
- Weak form of chosen-plaintext attack (CPA)

Multiple Encryptions

§5.5 Definition (Deterministic scheme)

Private-key encryption scheme $(\text{gen}, \text{enc}, \text{dec})$ is deterministic if $\text{enc}(r, k, m) = \text{enc}(r', k, m)$ for all $r, r' \in R$, $k \in K$, and $m \in M$

Notes

- Deterministic scheme = encryption function $\text{enc}\colon K \times M \to C$
- Simplistic schemes are deterministic

§5.6 Principle (Probabilistic encryption)

Deterministic private-key encryption schemes are never multiple-encryption EAV-secure

Multiple Encryptions

Observation

- Multiple-encryption EAV-secure requires $\mathrm{P}\left[\mathrm{PrivK}^{\text{many}}_{\mathcal{E},\mathcal{A}}(n)\right] \simeq \frac{1}{2}$

$$\mathrm{P}\left[\mathrm{PrivK}^{\text{many}}_{\mathcal{E},\mathcal{A}}(n)\right] = \frac{1}{2}\Big(\mathrm{P}[b' = 0 \mid b = 0] + \mathrm{P}[b' = 1 \mid b = 1]\Big) \simeq \frac{1}{2}$$

- Hence

$$\begin{aligned} &\mathrm{P}[b' = 0 \mid b = 0] + \mathrm{P}[b' = 1 \mid b = 1] \\ &= \big(1 - \mathrm{P}[b' = 1 \mid b = 0]\big) + \mathrm{P}[b' = 1 \mid b = 1] \simeq 1 \end{aligned}$$

- Thus $\mathrm{P}[b' = 1 \mid b = 1] - \mathrm{P}[b' = 1 \mid b = 0] \simeq 0$
  so "success" probabilities of $\mathcal{A}$ for both $b = 0$ and $b = 1$ almost equal
- Obviously also true in opposite direction
  (almost equal success implies multiple-encryption EAV-secure)

Multiple Encryptions

§5.7 Definition (Adversarial acceptance probability)

Let $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ private-key encryption scheme and $\mathcal{A}$ PPT algorithm. For every security parameter $n \in \mathbb{N}$ and bit $b \in \{0,1\}$ $\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A},b}(n)$ is game $\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A}}(n)$ with changes

- Use given b (without $b \leftarrow U_1$)
- Without final step instead returning answer b' of $\mathcal{A}$

§5.8 Lemma

Private-key encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is multiple-encryption EAV-secure iff for all PPT algorithms $\mathcal{A}$

$$\mathsf{P}\left[\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A},0}(n)\right] \simeq \mathsf{P}\left[\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A},1}(n)\right]$$

Chosen-Plaintext-Attack Security

Notes

- Skip "known plaintext attack" security (stronger notions prevalent today)
- Multiple encryption → weak "chosen plaintext attack"

Oracles

- Answers queries immediately & truthfully (at no complexity cost)
- Encryption oracle provides access to enc_k for currently used key k (given message m returns ciphertext c with $\mathsf{P}[c \leftarrow \mathsf{enc}_k(m)] \neq 0$)
- Decryption oracle provides access to dec_k for currently used key k (given ciphertext c returns message $m = \mathsf{dec}_k(c)$)
- Do not predict used random bits (uses its own random bits)

Chosen-Plaintext-Attack Security

§5.9 Definition (CPA-secure)

Private-key encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is CPA-secure if for every PPT algorithm $\mathcal{A}$ with access to encryption oracle

$$\mathsf{P}\left[\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}}(n)\right] \simeq \frac{1}{2}$$

§5.10 Definition (Multiple-encryption CPA-secure)

Private-key encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is multiple-encryption CPA-secure if for every PPT algorithm $\mathcal{A}$ with access to encryption oracle

$$\mathsf{P}\left[\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A}}(n)\right] \simeq \frac{1}{2}$$

Chosen-Plaintext-Attack Security

§5.11 Theorem (CPA-secure implies multiple-encryption CPA-secure)

Any CPA-secure encryption scheme is also multiple-encryption CPA-secure

Notes

- Maybe in exercises
- Entirely similar to next proof

Chosen-Plaintext-Attack Security

We instead prove weaker statement

§5.12 Theorem (CPA-secure implies multiple-encryption EAV-secure)

Any CPA-secure encryption scheme is also multiple-encryption EAV-secure

Proof (1/4)

Let $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ be CPA-secure private-key encryption scheme.
Moreover, let $\mathcal{A}$ be arbitrary adversary for $\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A}}(n)$.
There exists polynomial p such that message lists returned by $\mathcal{A}$ have length $\leq p(n)$ for each n.
Wlog. assume that length of all message lists is exactly $p(n)$.
We show $\mathsf{P}\big[\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A},0}(n)\big] \simeq \mathsf{P}\big[\mathsf{PrivK}^{\mathsf{many}}_{\mathcal{E},\mathcal{A},1}(n)\big]$, which by Lemma §5.8 shows that $\mathcal{E}$ is multiple-encryption EAV-secure.

Chosen-Plaintext-Attack Security

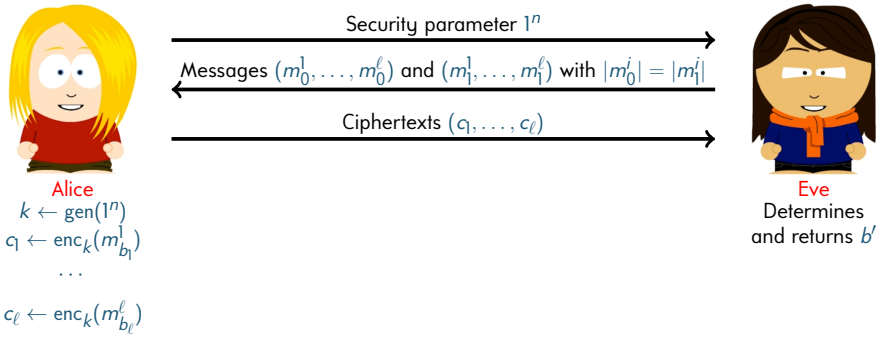
Proof (2/4)

We construct adversary $\mathcal{A}'$ with access to encryption oracle for game $\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}'}(n)$

1. Receive 1^n and generate $x \leftarrow \{1, \ldots, \ell\}$ with $\ell = p(n)$ uniformly
2. Call $\mathcal{A}(1^n)$ and receive message lists $(m^1_0, \ldots, m^\ell_0)$ and $(m^1_1, \ldots, m^\ell_1)$ with $|m^i_0| = |m^i_1|$ for all $1 \leq i \leq \ell$
3. Construct ciphertext list
   - $c_i \leftarrow \mathsf{enc}_k(m^i_0)$ for all $1 \leq i < x$ (using encryption oracle on m^i_0)
   - Output (m^x_0, m^x_1) and receive ciphertext c_x
   - $c_i \leftarrow \mathsf{enc}_k(m^i_1)$ for all $x < i \leq \ell$ (using encryption oracle on m^i_1)
4. Output result of call $\mathcal{A}(c_1, \ldots, c_\ell)$

Chosen-Plaintext-Attack Security

Game $\mathcal{G}(b_1 \cdots b_\ell)$



Chosen-Plaintext-Attack Security

Proof (3/4)

Consider game $\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}'}(n)$ with $\ell = p(n)$ and distinguish two cases

- Let $b = 0$. Then we essentially play $\mathcal{G}(0^x 1^{\ell-x})$ after sampling x

$$\mathsf{P}\big[\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}',0}(n)\big] = \sum_{x'=1}^{\ell} \mathsf{P}[x = x'] \cdot \mathsf{P}\big[\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}',0}(n) \mid x = x'\big] = \frac{1}{\ell} \sum_{x'=1}^{\ell} \mathsf{P}\big[\mathcal{G}(0^{x'} 1^{\ell-x'})\big]$$

- Let $b = 1$. Then we essentially play $\mathcal{G}(0^{x-1} 1^{\ell-x+1})$ after sampling x

$$\mathsf{P}\big[\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}',1}(n)\big] = \sum_{x'=1}^{\ell} \mathsf{P}[x = x'] \cdot \mathsf{P}\big[\mathsf{PrivK}^{\mathsf{one}}_{\mathcal{E},\mathcal{A}',1}(n) \mid x = x'\big] = \frac{1}{\ell} \sum_{x'=1}^{\ell} \mathsf{P}\big[\mathcal{G}(0^{x'-1} 1^{\ell-x'+1})\big] = \frac{1}{\ell} \sum_{x'=0}^{\ell-1} \mathsf{P}\big[\mathcal{G}(0^{x'} 1^{\ell-x'})\big]$$

Chosen-Plaintext-Attack Security

Proof (4/4)

Since $\mathcal{E}$ is CPA-secure we have

$$\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E},\mathcal{A}',0}(n)\big] \simeq \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E},\mathcal{A}',1}(n)\big]$$

into which we substitute our derived equalities

$$\frac{1}{p(n)}\sum_{x'=1}^{p(n)} \mathrm{P}\big[\mathcal{G}(0^{x'}1^{p(n)-x'})\big] \simeq \frac{1}{p(n)}\sum_{x'=0}^{p(n)-1} \mathrm{P}\big[\mathcal{G}(0^{x'}1^{p(n)-x'})\big]$$

multiply by $p(n)$ and subtract summands for $x' \in \{1,\dots,p(n)-1\}$

$$\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{many}}_{\mathcal{E},\mathcal{A},0}(n)\big] = \mathrm{P}\big[\mathcal{G}(0^{p(n)})\big] \simeq \mathrm{P}\big[\mathcal{G}(1^{p(n)})\big] = \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{many}}_{\mathcal{E},\mathcal{A},1}(n)\big]$$

Thus $\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{many}}_{\mathcal{E},\mathcal{A},0}(n)\big]$ and $\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{many}}_{\mathcal{E},\mathcal{A},1}(n)\big]$ are almost equal. □

Recall

Oracles

- Answers queries immediately & truthfully
- Encryption oracle provides access to enc_k for currently used key k
  (given message m returns ciphertext c with $\mathrm{P}[c \leftarrow \mathrm{enc}_k(m)] \neq 0$)
- Decryption oracle provides access to dec_k for currently used key k
  (given ciphertext c returns message $m = \mathrm{dec}_k(c)$)
- Do not predict used random bits (uses its own random bits)

Definition (§5.7 CPA-secure)

Private-key encryption scheme $\mathcal{E} = (\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ is CPA-secure if for every PPT algorithm $\mathcal{A}$ with access to encryption oracle

$$\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E},\mathcal{A}}(n)\big] \simeq \frac{1}{2}$$

Chosen-Plaintext-Attack Security

Notes

- Want to construct CPA-secure scheme
- Cannot be deterministic by Principle §5.6
- Use another primitive: pseudorandom functions
- Keyed variant $f\colon \bigcup_{n\in\mathbb{N}} \underbrace{\{0,1\}^n}_{\text{key}} \times \underbrace{\{0,1\}^n}_{\text{input}} \to \underbrace{\{0,1\}^n}_{\text{output}}$
- For every key $k \in \{0,1\}^n$ obtain function $f_k\colon \{0,1\}^n \to \{0,1\}^n$ given by $f_k(w) = f(k,w)$

Chosen-Plaintext-Attack Security

Intuition

- Represent function $g\colon \{0,1\}^n \to \{0,1\}^n$ by bit sequence of length $2^n n$

$$\underbrace{b_1\cdots b_n}_{=g(0^n)}\ \underbrace{b_{n+1}\cdots b_{2n}}_{=g(0^{n-1}1)}\ \underbrace{b_{2n+1}\cdots b_{3n}}_{=g(0^{n-2}10)}\cdots\ \underbrace{b_{(2^n-1)n+1}\cdots b_{2^n n}}_{=g(1^n)}$$

- So $2^{2^n n}$ functions of type $\{0,1\}^n \to \{0,1\}^n$
  Uniform distribution F_n on such functions

$$F_n\colon \{g \mid g\colon \{0,1\}^n \to \{0,1\}^n\} \to [0,1] \qquad F_n(g) = 2^{-2^n n}$$

- Using this description as input for distinguisher provides input of exponential length (in n)
- Instead provide access to function as oracle
  given algorithm D with oracle access to $\mathcal{O}$ we write D^g for instance, in which oracle is provided by g; i.e. $\mathcal{O} = g$

Chosen-Plaintext-Attack Security

§6.1 Definition (Pseudorandom function)

Deterministic polynomial-time computable function

$$f\colon \bigcup_{n\in\mathbb{N}} \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$$

is pseudorandom function if for every PPT algorithm D with oracle access

$$\mathrm{E}\Big[\mathrm{P}\big(D^{f_k}(1^n)\big)\Big]_{k\leftarrow U_n} \simeq \mathrm{E}\Big[\mathrm{P}\big(D^{g}(1^n)\big)\Big]_{g\leftarrow F_n}$$

Notes

- Key k not supplied to D (Show distinction is easy with k)
- Show that universally $\left(\sum_{\substack{k\in U_n \\ f_k=f}} 2^{-2^n n}\right)_{f\leftarrow F_n} \not\equiv_{\mathrm{PPT}} F_n$ (Prove this)

  where function descriptions are directly supplied to distinguisher
  (Hint: function descriptions are long; construct universal distinguisher)

Chosen-Plaintext-Attack Security

Example (inspired by "two-time pad")

- Let $f(k,w) = k \oplus w$ for all $k, w \in \{0,1\}^n$
- Then $f_k(w)$ uniformly distributed for any w (for uniform choice of k)
- Construct distinguisher D with oracle $\mathcal{O}$
  1. $y = \mathcal{O}(0^n)$ and $y' = \mathcal{O}(1^n)$
  2. Return 1 if $y \oplus y' = 1^n$ and 0 otherwise
- If we run $g \leftarrow F_n$; $D^g(1^n)$, then we succeed with probability 2^{-n}
  (given $g(0^n)$ we must have $g(1^n) = \overline{g(0^n)}$)
- If we run $k \leftarrow U_n$; $D^{f_k}(1^n)$, then we always succeed
  (because $y = f_k(0^n) = 0^n \oplus k = k$ and $y' = f_k(1^n) = 1^n \oplus k = \overline{k}$
  thus $y \oplus y' = k \oplus \overline{k} = 1^n$)
- f no pseudorandom function

Chosen-Plaintext-Attack Security

§6.2 Theorem [Goldreich, Goldwasser, Micali 1986]

1. For every pseudorandom function f and $1 \le \ell \le 2^n - 1$

   $$G(s) = f_s(\mathrm{bin}_n(0))\ f_s(\mathrm{bin}_n(1))\ \cdots\ f_s(\mathrm{bin}_n(\ell)) \qquad \text{for all } s \in \{0,1\}^n$$

   is pseudorandom generator with expansion $(\ell+1)n$
2. For every pseudorandom generator G with expansion $p(n) = 2n$,
   let $G_0(s) = a_1 \cdots a_n$ and $G_1(s) = a_{n+1} \cdots a_{2n}$, where $G(s) = a_1 \cdots a_{2n}$.
   Then f given for every $k \in \{0,1\}^n$ and $b_1, \ldots, b_n \in \{0,1\}$ by

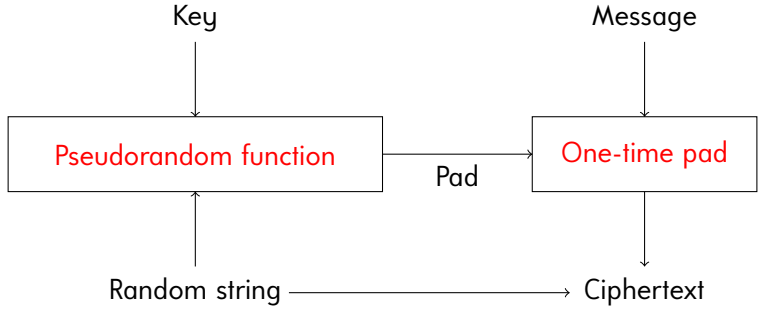
   $$f(k, b_1 \cdots b_n) = G_{b_n}\Big(\cdots G_{b_2}\big(G_{b_1}(k)\big)\cdots\Big)$$

   is pseudorandom function

Proof

Nice exercises □

Chosen-Plaintext-Attack Security



§6.3 Construction

Let f be pseudorandom function.
Define private-key encryption scheme $\mathcal{E}_f = (\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ with

- $\mathrm{P}^n_k(k) = 2^{-n}$ for all $k \in \{0,1\}^n$
- $\mathrm{enc}_k(m)$ is $r \leftarrow U_n$; return $\langle r, f_k(r) \oplus m \rangle$ for all $k, m \in \{0,1\}^n$
- $\mathrm{dec}_k(\langle r, w \rangle) = f_k(r) \oplus w$ for all $k, r, w \in \{0,1\}^n$

Chosen-Plaintext-Attack Security

§6.4 Theorem

Scheme $\mathcal{E}_f$ is CPA-secure for every pseudorandom function f

Proof (1/4)

Consider (inefficient) encryption scheme $\mathcal{E}' = (\mathrm{gen}', \mathrm{enc}', \mathrm{dec}')$ given by $\mathrm{P}_K^n(g) = 2^{-2^n n}$ for every $g\colon \{0,1\}^n \to \{0,1\}^n$, $\mathrm{enc}'_g(m)$ is $r \leftarrow U_n$; return $\langle r, g(r) \oplus m\rangle$, and $\mathrm{dec}_g(\langle r, w\rangle) = g(r) \oplus w$ (essentially $\mathcal{E}_f$ but using truely random function g instead of f_k for random k).
Let $\mathcal{A}$ be PPT adversary and p polynomial such that $p(n)$ is upper bound to number of (encryption) oracle queries of $\mathcal{A}$ for security parameter n.
We first prove

$$\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}_f,\mathcal{A}}(n)\big] \simeq \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)\big]$$

(winning chances of $\mathcal{A}$ are essentially the same against schemes $\mathcal{E}_f$ and $\mathcal{E}'$)

Chosen-Plaintext-Attack Security

Proof (2/4)

Construct PPT distinguisher D (against pseudorandomness of f) with oracle access to $\mathcal{O}$ and input 1^n:

1. Run $\mathcal{A}(1^n)$ and answer its encryption oracle queries as stated below
2. Receive messages $m_0, m_1 \in \{0,1\}^n$ with $|m_0| = |m_1|$
3. $b \leftarrow U_1$, $r \leftarrow U_n$, and let $y = \mathcal{O}(r)$
4. Run $\mathcal{A}(\langle r, y \oplus m_b\rangle)$ and again answer $\mathcal{A}$'s encryption oracle queries
5. Receive b' and return $b \stackrel{?}{=} b'$

Answer all encryption oracle queries $\mathrm{enc}(m)$ by $\mathcal{A}$ as follows:

$$r \leftarrow U_n\,;\, y = \mathcal{O}(r)\,;\, \text{return } \langle r, y \oplus m\rangle$$

Clearly D is PPT algorithm since $\mathcal{A}$ and $\mathcal{E}$ are efficient.

Chosen-Plaintext-Attack Security

Proof (3/4)

We observe that this distinguisher D succeeds exactly when

- $\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}_f,\mathcal{A}}(n)$ succeeds if oracle f_k with $k \leftarrow U_n$ is supplied
- $\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)$ succeeds if oracle g with $g \leftarrow F_n$ is supplied

Hence

$$\begin{aligned}\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}_f,\mathcal{A}}(n)\big] &= \mathrm{E}\Big[\mathrm{P}\big(D^{f_k}(1^n)\big)\Big]_{k\leftarrow U_n} \\ &\simeq \mathrm{E}\Big[\mathrm{P}\big(D^{g}(1^n)\big)\Big]_{g\leftarrow F_n} = \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)\big]\end{aligned}$$

so we achieved our first goal. Next we analyze $\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)$.

Chosen-Plaintext-Attack Security

Proof (4/4)

Let $g \leftarrow F_n$. Every time message m is encrypted (in game or by oracle) uniformly random $r \leftarrow U_n$ is chosen and $\langle r, g(r) \oplus m\rangle$ is returned.
Let $m_0 \neq m_1$ be selected messages and $\langle \hat{r}, g(\hat{r}) \oplus m_b\rangle$ be the challenge ciphertext. Now we distinguish two cases:

- $\overline{R(n)}$: $\hat{r}$ was never returned by oracle. Then $g(\hat{r})$ is completely unknown and $\mathcal{A}$ wins with probability $\frac{1}{2}$ as for one-time pad
- $R(n)$: $\hat{r}$ was returned as $\langle \hat{r}, s\rangle$ by encryption oracle query for some m. Then $g(\hat{r}) = s \oplus m$ is known to $\mathcal{A}$ and $\mathcal{A}$ can always win

$$\begin{aligned}\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)\big] &= \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n), R(n)\big] + \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n), \overline{R(n)}\big] \\ &\leq \mathrm{P}[R(n)] + \frac{1}{2} \leq \frac{1}{2} + \frac{p(n)}{2^n} \precsim \frac{1}{2}\end{aligned}$$

Hence $\mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}_f,\mathcal{A}}(n)\big] \simeq \mathrm{P}\big[\mathrm{PrivK}^{\mathrm{one}}_{\mathcal{E}',\mathcal{A}}(n)\big] \simeq \frac{1}{2}$ proving CPA-security □