

CSE208: Advanced Cryptography (FHE)

Daniele Micciancio

UCSD

Fall 2026



Section 1

Defining FHE

Public Key Encryption

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

$\text{PKE}(\text{Gen}, \text{Enc}, \text{Dec})$
 $\text{Gen}: () \rightarrow (\text{pk}, \text{sk})$
 $\text{Enc}: (\text{pk}, m) \rightarrow c$
 $\text{Dec}: (\text{sk}, c) \rightarrow m$

- All algorithms are given an implicit security parameter k as input, and may be randomized
- **Gen**: Key Generation algorithm. Given a security parameter, produces a pair of matching secret and public keys
- **Enc**: Encryption algorithm, given the public key and a message, outputs a ciphertext
- **Dec**: Decryption algorithm, given the secret key and a ciphertext, recovers the message

Correctness of PKE

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

For every $(sk, pk) \leftarrow \text{Gen}()$ and $m \leftarrow [M]$, $r \leftarrow [R]$:

$$\text{Dec}(sk, \text{Enc}(pk, m; r)) = m$$

Notes:

- $[M]$: message space, may be just $\{0, 1\}$, or $\{0, 1\}^n$
- $[C]$: ciphertext space, usually $\{0, 1\}^m$ for $m > n + k$
- $r \leftarrow [R]$: randomness
- $A(x; r)$ means run algorithm A on input x and randomness r
- Fixed size message space
 - assume $[M], [C]$ are finite sets
- Variable length messages:
 - break long message into blocks of size n
 - encrypt each block independently

Chosen Plaintext Attack (IND-CPA) security

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Indistinguishability under Chosen Plaintext Attack
- Experiment:

```
GameINDCPA( $b : \{0, 1\}$ )  
  ( $sk, pk$ )  $\leftarrow$  Gen()  
  A( $pk$ )  $\rightarrow$  ( $m_0, m_1$ )  
   $b' \leftarrow$  A(Enc( $pk, m_b$ ))  
  return  $b' : \{0, 1\}$ 
```

Chosen Plaintext Attack (IND-CPA) security

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Indistinguishability under Chosen Plaintext Attack
- Experiment:

```
GameINDCPA( $b : \{0, 1\}$ )  
  ( $sk, pk$ )  $\leftarrow$  Gen()  
   $A(pk) \rightarrow (m_0, m_1)$   
   $b' \leftarrow A(Enc(pk, m_b))$   
  return  $b' : \{0, 1\}$ 
```

$$Adv(A) = |\Pr(\text{Game}(0)=1) - \Pr(\text{Game}(1)=1)|$$

Definition

(Gen, Enc, Dec) is **IND-CPA** secure if any efficient A has advantage $Adv(A) \approx 0$

(t, ϵ) security: If $\text{Time}(A) < t$ then $Adv(A) < \epsilon$

Pseudorandomness under CPA (RND-CPA)

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Similar to IND-CPA, but different experiment:

```
GameRNDCPA( $b : \{0, 1\}$ )  
  ( $sk, pk$ )  $\leftarrow$  Gen()  
   $A(pk) \rightarrow m$   
   $c_0 \leftarrow [C]$   
   $c_1 \leftarrow Enc(pk, m_b)$   
   $b' \leftarrow A(c_b)$   
  return  $b' : \{0, 1\}$ 
```

Pseudorandomness under CPA (RND-CPA)

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Similar to IND-CPA, but different experiment:

```
GameRNDCPA( $b : \{0, 1\}$ )  
  ( $sk, pk$ )  $\leftarrow$  Gen()  
   $A(pk) \rightarrow m$   
   $c_0 \leftarrow [C]$   
   $c_1 \leftarrow Enc(pk, m_b)$   
   $b' \leftarrow A(c_b)$   
  return  $b' : \{0, 1\}$ 
```

- How does IND-CPA security compare to RND-CPA?
 - If a scheme is RND-CPA, then it is also IND-CPA secure
 - A scheme can be IND-CPA, but not RND-CPA secure
 - Let's prove these statements on the blackboard

Significance of CPA security

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Adversary can choose messages m_0, m_1
 - No assumption about input distribution
 - Adversary may have partial information about messages
 - Adversary may influence the choice of messages
- Ciphertext $c = \text{Enc}(\text{pk}, m_b)$ is computed honestly
 - Adversary cannot tamper with ciphertexts
- Adversary models a passive attacker
- Equivalent to many other seemingly stronger definitions
 - Adversary sees encryption of many message pairs $(m_0[i], m_1[i])$ for $i=1,2,\dots$
 - Multiuser: Encryptions under many independent keys $(\text{pk}[i], \text{sk}[i]) \leftarrow \text{Gen}$
- Define formally, and give reductions similarly to RND-CPA

Homomorphic Encryption: first attempt

- Assume $f: M \rightarrow M$, later will extend to multi-input functions
- Intuition: “Encryption commutes with function application”

$$f(\text{Enc}(\text{pk}, m)) = \text{Enc}(\text{pk}, f(m))$$

- How to apply f to a ciphertext

$$\text{Eval}(\text{pk}, f, \text{Enc}(\text{pk}, m)) = \text{Enc}(\text{pk}, f(m))$$

- Recall, Enc is randomized!
 - Eval and Enc are unlikely to produce the same ciphertext
 - should Eval and Enc produce identical distribution?
 - should ciphertexts produced by Eval be independent?

Homomorphic Encryption: second attempt

$$\text{Dec}(\text{sk}, \text{Eval}(\text{pk}, f, \text{Enc}(\text{pk}, m))) = f(m)$$

This “homomorphic correctness” definition captures the workflow of a typical application

- 1 trusted party generates a pair of keys $(\text{pk}, \text{sk}) \leftarrow \text{Gen}()$
- 2 data owner encrypts data m under pk , and stores ciphertext on public server
- 3 server carries out computation of program f on encrypted data
- 4 final result is decrypted using sk

This is the standard definition of correctness for homomorphic encryption.

Multi-input functions

- Many inputs are encrypted independently

$$c_1 \leftarrow \text{Enc}(\text{pk}, m_1)$$

...

$$c_k \leftarrow \text{Enc}(\text{pk}, m_k)$$

Multi-input functions

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Many inputs are encrypted independently

$$c_1 \leftarrow \text{Enc}(\text{pk}, m_1)$$

...

$$c_k \leftarrow \text{Enc}(\text{pk}, m_k)$$

- k -ary function $f: (m_1, \dots, m_k) \rightarrow m$

$$\begin{aligned} \text{Dec}(\text{sk}, \text{Eval}(\text{pk}, f, c_1, \dots, c_k)) \\ = f(m_1, \dots, m_k) \end{aligned}$$

- Different parties provide encrypted data to perform a joint computation
- Only owner of secret key sk can decrypt the result
- For added security, sk may be distributed using secret sharing scheme: this is called “Threshold FHE”, and there is much to say about it

Correctness and Function Composition

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Let $x, y, z \in M$ be messages and $f, g : M \rightarrow M$ two functions such that $y = f(x)$ and $z = g(y) = (g \circ f)(x)$
- Assume $(\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$ can evaluate f and g correctly:

$$\text{Dec}(\text{sk}, \text{Eval}(\text{pk}, f, \text{Enc}(\text{pk}, x))) = f(x)$$

$$\text{Dec}(\text{sk}, \text{Eval}(\text{pk}, g, \text{Enc}(\text{pk}, y))) = g(y)$$

Correctness and Function Composition

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- Let $x, y, z \in M$ be messages and $f, g : M \rightarrow M$ two functions such that $y = f(x)$ and $z = g(y) = (g \circ f)(x)$
- Assume $(\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$ can evaluate f and g correctly:

$$\text{Dec}(\text{sk}, \text{Eval}(\text{pk}, f, \text{Enc}(\text{pk}, x))) = f(x)$$

$$\text{Dec}(\text{sk}, \text{Eval}(\text{pk}, g, \text{Enc}(\text{pk}, y))) = g(y)$$

Question

Does it follow that

$$\text{ctX} \leftarrow \text{Enc}(\text{pk}, x)$$

$$\text{ctY} \leftarrow \text{Eval}(\text{pk}, f, \text{ctX})$$

$$\text{ctZ} \leftarrow \text{Eval}(\text{pk}, g, \text{ctY})$$

$$\text{Dec}(\text{sk}, \text{ctZ}) \stackrel{?}{=} z$$

Security of Homomorphic Encryption

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

```
INDCPAgame( $b : \{0, 1\}$ )  
  ( $sk, pk$ )  $\leftarrow$  Gen()  
  A( $pk$ )  $\rightarrow$  ( $m_0, m_1$ )  
  return A(Enc( $pk, m_b$ )):  $\{0, 1\}$ 
```

Remark

The IND-CPA security definition depends only on Gen and Enc, but not on Dec (or Eval)

Question

Can the IND-CPA security definition be applied as it is to FHE schemes (Gen, Enc, Dec, Eval)?

A trivial FHE scheme

Consider the following FHE scheme:

- Let $(\text{Gen}, \text{Enc}, \text{Dec})$ be IND-CPA secure
- Define $\text{TrivialFHE} = (\text{Gen}, \text{Enc}', \text{Dec}', \text{Eval})$

$\text{Enc}'(\text{pk}, m) = (\text{Enc}(\text{pk}, m), [])$

$\text{Dec}'(\text{sk}, (\text{ct}, [])) = \text{Dec}(\text{sk}, \text{ct})$

$\text{Dec}'(\text{sk}, (\text{ct}, [f; fs])) = f(\text{Dec}'(\text{sk}, (\text{ct}, fs)))$

$\text{Eval}(\text{pk}, f, (\text{ct}, [fs])) = (\text{ct}, [f; fs])$

Question

- *Is TrivialFHE a correct FHE scheme?*
- *Is TrivialFHE a secure FHE scheme?*
- *What makes the above scheme “trivial”?*

Compactness

CSE208:
Advanced
Cryptography
(FHE)

Daniele
Micciancio

Defining FHE

- The TrivialFHE scheme is both correct and secure
- The problem with TrivialFHE is that it is not efficient:
 - Computation is performed by **Dec**, not **Eval**!

Definition

A FHE scheme is **compact** if the size of ciphertext $ct = \text{Eval}(pk, f, \text{Enc}(pk, m))$ is independent of $\text{Size}(f)$

- Weaker forms of compactness:
 - Ciphertext size may grow logarithmic with $\text{Size}(f)$
 - Ciphertext size may depend on $\text{Depth}(f)$