Homomorphic Encryption

Lecture 18
And some applications
Homomorphic Encryption
Homomorphic Encryption

**Group Homomorphism:** Two groups \( G \) and \( G' \) are homomorphic if there exists a function (homomorphism) \( f: G \rightarrow G' \) such that for all \( x, y \in G \), \( f(x) +_{G'} f(y) = f(x +_G y) \)
Homomorphic Encryption

- **Group Homomorphism**: Two groups $G$ and $G'$ are homomorphic if there exists a function (homomorphism) $f: G \rightarrow G'$ such that for all $x, y \in G$, $f(x) +_{G'} f(y) = f(x +_G y)$

- Homomorphic Encryption: A CPA secure (public-key) encryption s.t. $\text{Dec}(C) +_M \text{Dec}(D) = \text{Dec}(C +_C D)$ for ciphertexts $C, D$
**Homomorphic Encryption**

- **Group Homomorphism**: Two groups $G$ and $G'$ are homomorphic if there exists a function (homomorphism) $f: G \rightarrow G'$ such that for all $x, y \in G$, $f(x) +_{G'} f(y) = f(x +_G y)$.

- Homomorphic Encryption: A CPA secure (public-key) encryption s.t. $\text{Dec}(C) +_M \text{Dec}(D) = \text{Dec}(C +_C D)$ for ciphertexts $C, D$.

  - i.e. $\text{Enc}(x) +_C \text{Enc}(y)$ is like $\text{Enc}(x +_M y)$.
Homomorphic Encryption

**Group Homomorphism:** Two groups $G$ and $G'$ are homomorphic if there exists a function (homomorphism) $f: G \rightarrow G'$ such that for all $x, y \in G$, $f(x) +_{G'} f(y) = f(x +_G y)$

**Homomorphic Encryption:** A CPA secure (public-key) encryption s.t. $\text{Dec}(C) +_M \text{Dec}(D) = \text{Dec}(C +_C D)$ for ciphertexts $C, D$

- i.e. $\text{Enc}(x) +_C \text{Enc}(y)$ is like $\text{Enc}(x +_M y)$

- Interesting when $+_C$ doesn’t require the decryption key
Homomorphic Encryption

- **Group Homomorphism**: Two groups $G$ and $G'$ are homomorphic if there exists a function (homomorphism) $f: G \rightarrow G'$ such that for all $x, y \in G$, $f(x) +_{G'} f(y) = f(x +_G y)$

- Homomorphic Encryption: A CPA secure (public-key) encryption such that $\text{Dec}(C) +_M \text{Dec}(D) = \text{Dec}(C +_C D)$ for ciphertexts $C, D$
  
  - i.e. $\text{Enc}(x) +_C \text{Enc}(y)$ is like $\text{Enc}(x +_M y)$

- Interesting when $+_C$ doesn’t require the decryption key

- e.g. El Gamal: $(g^{x_1}, m_1 Y^{x_1}) \ast (g^{x_2}, m_2 Y^{x_2}) = (g^{x_3}, m_1 m_2 Y^{x_3})$
Homomorphic Encryption

**Group Homomorphism**: Two groups $G$ and $G'$ are homomorphic if there exists a function (homomorphism) $f: G \rightarrow G'$ such that for all $x, y \in G$, $f(x) +_{G'} f(y) = f(x +_G y)$

Homomorphic Encryption: A CPA secure (public-key) encryption s.t. $\text{Dec}(C) +_M \text{Dec}(D) = \text{Dec} (C +_C D)$ for ciphertexts $C, D$

- i.e. $\text{Enc}(x) +_C \text{Enc}(y)$ is like $\text{Enc}(x +_M y)$

- Interesting when $+_C$ doesn’t require the decryption key

- e.g. El Gamal: $(g^{x_1}, m_1 Y^{x_1}) \ast (g^{x_2}, m_2 Y^{x_2}) = (g^{x_3}, m_1 m_2 Y^{x_3})$

- Not covered today: Fully Homomorphic Encryption, which supports ring homomorphism (addition and multiplication of messages)
Rerandomization
Rerandomization

Often (but not always) another property is required of a homomorphic encryption scheme
Rerandomization

Often (but not always) another property is required of a homomorphic encryption scheme

- Unlinkability
Rerandomization

- Often (but not always) another property is required of a homomorphic encryption scheme

- Unlinkability

  - For any two ciphertexts $c_x = \text{Enc}(x)$ and $c_y = \text{Enc}(y)$, $\text{Add}(c_x, c_y)$ should be identically distributed as $\text{Enc}(x + M y)$. Add is a randomized operation
Rerandomization

Often (but not always) another property is required of a homomorphic encryption scheme

Unlinkability

For any two ciphertexts $c_x=\text{Enc}(x)$ and $c_y=\text{Enc}(y)$, $\text{Add}(c_x,c_y)$ should be identically distributed as $\text{Enc}(x + M y)$. $\text{Add}$ is a randomized operation.

Alternately, a ReRand operation s.t. for all valid ciphertexts $c_x$, ReRand($c_x$) is identically distributed as $\text{Enc}(x)$.
Rerandomization

Often (but not always) another property is required of a homomorphic encryption scheme.

Unlinkability

For any two ciphertexts \( c_x = \text{Enc}(x) \) and \( c_y = \text{Enc}(y) \), \( \text{Add}(c_x, c_y) \) should be identically distributed as \( \text{Enc}(x +_M y) \). \( \text{Add} \) is a randomized operation.

Alternately, a ReRand operation s.t. for all valid ciphertexts \( c_x \), \( \text{ReRand}(c_x) \) is identically distributed as \( \text{Enc}(x) \).

Then, we can let \( \text{Add}(c_x, c_y) = \text{ReRand}(c_x +_c c_y) \) where \( +_c \) may be deterministic.
Rerandomization

Often (but not always) another property is required of a homomorphic encryption scheme.

Unlinkability

For any two ciphertexts $c_x = \text{Enc}(x)$ and $c_y = \text{Enc}(y)$, $\text{Add}(c_x, c_y)$ should be identically distributed as $\text{Enc}(x + M y)$. $\text{Add}$ is a randomized operation.

Alternately, a $\text{ReRand}$ operation s.t. for all valid ciphertexts $c_x$, $\text{ReRand}(c_x)$ is identically distributed as $\text{Enc}(x)$.

Then, we can let $\text{Add}(c_x, c_y) = \text{ReRand}(c_x + c c_y)$ where $+ c$ may be deterministic.

Rerandomization useful even without homomorphism.
Unlinkable Homomorphic Encryption
Unlinkable Homomorphic Encryption

Considers only passive corruption
Unlinkable Homomorphic Encryption

Considers only passive corruption
Unlinkable Homomorphic Encryption

Considers only passive corruption
Unlinkable Homomorphic Encryption

Consider only passive corruption
Unlinkable Homomorphic Encryption

Considers only passive corruption
Unlinkable Homomorphic Encryption

REAL

A (PK) \rightarrow B (PK)
E(m_1), E(m_2), ...

Add(c_1, c_2)

B (PK) \rightarrow (SK)

A
(PK)

Recv

H

h_1, h_2, ...

IDEAL

h_1, h_2, ...

A

m_1, m_2, ...

\text{add}(h_1, h_2)

A
Considers only passive corruption
Unlinkable Homomorphic Encryption

Considers only passive corruption
Unlinkable Homomorphic Encryption

IDEAL

A

B

\(m_1, m_2, \ldots\)

\(h_1, h_2, \ldots\)

add(h_1, h_2)

m_1 + m_2

Recv

REAL

A

B (PK)

E(m_1), E(m_2), \ldots

(\text{SK})

Add(c_1, c_2)

\(c_1, c_2\)

Considers only passive corruption

Functionality gives “handles” to messages posted; accepts requests for posting fresh messages, or derived messages
Unlinkable Homomorphic Encryption

Considers only passive corruption

Functionality gives “handles” to messages posted; accepts requests for posting fresh messages, or derived messages

Unlinkability: Above, receiver gets only the message $m_1+m_2$ in IDEAL; is not told if it is a fresh message or derived from other messages
An OT Protocol
(for passive corruption)
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme
Using an (unlinkable) rerandomizable encryption scheme

An OT Protocol (for passive corruption)

$c_b = E(1), c_{1-b} = E(0)$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme
An OT Protocol (for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and $E(0), E(1)$ in suitable order

c
b
= $E(1)$,
$c_{1-b}$ = $E(0)$

$PK, c_0, c_1$

$x_0, x_1$

$b$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK,SK). Sends PK and E(0), E(1) in suitable order

\[ \begin{align*}
    c &= E(1), \\
    c_{1-b} &= E(0)
\end{align*} \]

\[ \begin{align*}
    z_0 &= x_0 \ast c_0 \\
    z_1 &= x_1 \ast c_1
\end{align*} \]
Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK,SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” $c_i$ with $x_i$:
$1*c:=\text{ReRand}(c)$, $0*c:=E(0)$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” $c_i$ with $x_i$:

$1 \ast c := \text{ReRand}(c)$,
$0 \ast c := E(0)$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” c_i with x_i: 
1*c := ReRand(c), 0*c := E(0)
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” $c_i$ with $x_i$:
$1*c := \text{ReRand}(c)$, $0*c := E(0)$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” $c_i$ with $x_i$:
$1*c := \text{ReRand}(c), \ 0*c := E(0)$

Simulation for passive-corrupt receiver: set $z_b = E(x_b)$ and $z_{1-b} = E(0)$
An OT Protocol
(for passive corruption)

Using an (unlinkable) rerandomizable encryption scheme

Receiver picks (PK, SK). Sends PK and E(0), E(1) in suitable order

Sender “multiplies” $c_i$ with $x_i$:
1*$c$:=ReRand($c$), 0*$c$:=E(0)

Simulation for passive-corrupt receiver: set $z_b = E(x_b)$ and $z_{1-b} = E(0)$

Simulation for passive-corrupt sender: Extract $x_0, x_1$ from input; set $c_0, c_1$ to be say E(1)
Private Information Retrieval
Private Information Retrieval

Setting: A server holds a large vector of values ("database"). Client wants to retrieve the value at a particular index i.
Private Information Retrieval

Setting: A server holds a large vector of values ("database"). Client wants to retrieve the value at a particular index i.

Client wants privacy against an honest-but-curious server.
Private Information Retrieval

- Setting: A server holds a large vector of values ("database").
- Client wants to retrieve the value at a particular index $i$.
- Client wants privacy against an honest-but-curious server.
- Server has no security requirements.
Private Information Retrieval

- Setting: A server holds a large vector of values ("database").
  - Client wants to retrieve the value at a particular index $i$.
  - Client wants privacy against an honest-but-curious server.
  - Server has no security requirements.

- Trivial solution: Server sends the entire vector to the client.
Private Information Retrieval

- Setting: A server holds a large vector of values ("database"). Client wants to retrieve the value at a particular index i
  - Client wants privacy against an honest-but-curious server
  - Server has no security requirements

- Trivial solution: Server sends the entire vector to the client

- PIR: to do it with significantly less communication
Private Information Retrieval

Setting: A server holds a large vector of values ("database"). Client wants to retrieve the value at a particular index \( i \)
- Client wants privacy against an honest-but-curious server
- Server has no security requirements

Trivial solution: Server sends the entire vector to the client

PIR: to do it with significantly less communication

Variant (we don’t look at): multiple-server PIR, with non-colluding servers
Private Information Retrieval

Setting: A server holds a large vector of values ("database"). Client wants to retrieve the value at a particular index $i$

- Client wants privacy against an honest-but-curious server
- Server has no security requirements

Trivial solution: Server sends the entire vector to the client

PIR: to do it with significantly less communication

- Variant (we don’t look at): multiple-server PIR, with non-colluding servers

Tool: Homomorphic encryption over the message space
Private Information Retrieval

- Setting: A server holds a large vector of values ("database").
- Client wants to retrieve the value at a particular index \(i\)
- Client wants privacy against an honest-but-curious server
- Server has no security requirements

Trivial solution: Server sends the entire vector to the client

PIR: to do it with significantly less communication

- Variant (we don’t look at): multiple-server PIR, with non-colluding servers

Tool: Homomorphic encryption over the message space

- When message space is \(\mathbb{Z}_n\): additively homomorphic encryption
Paillier’s Scheme
Paillier’s Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes
Paillier's Scheme

- Uses $\mathbb{Z}_{n^2}^* = \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within $2x$ of each other
  
To ensure $\gcd(n,\phi(n))=1$
Paillier’s Scheme

- Uses $\mathbb{Z}_{n^2}^* = \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other.
  - Isomorphism: $\psi(a,b) = g^{ab^n} \pmod{n^2}$ where $g=(1+n)$

To ensure $\gcd(n,\phi(n))=1$.
Pailler's Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
- Isomorphism: $\psi(a,b) = g^{abn} \pmod{n^2}$ where $g=(1+n)$
- Enc($m$) = $\psi(m,r)$ for $m$ in $\mathbb{Z}_n$ and a random $r$ in $\mathbb{Z}_n^*$
Paillier's Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n= pq$, $p,q$ primes within 2x of each other
- Isomorphism: $\psi(a,b) = g^{ab} \pmod{n^2}$ where $g = (1+n)$
- $\text{Enc}(m) = \psi(m,r)$ for $m$ in $\mathbb{Z}_n$ and a random $r$ in $\mathbb{Z}_n^*$
- $\psi$ can be efficiently inverted if $p,q$ known

To ensure $\gcd(n,\phi(n)) = 1$ within 2x of each other.
Paillier’s Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
- Isomorphism: $\psi(a,b) = g^{abn} \pmod{n^2}$ where $g=(1+n)$
- $\psi$ can be efficiently inverted if $p,q$ known
- (Additive) Homomorphism: $\text{Enc}(m) \cdot \text{Enc}(m')$ is $\text{Enc}(m+m')$
Paillier's Scheme

- Uses $\mathbb{Z}_{n^2}^* = \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
- Isomorphism: $\psi(a,b) = g^{abn} \pmod{n^2}$ where $g=(1+n)$
- $\psi$ can be efficiently inverted if $p,q$ known
- (Additive) Homomorphism: $\text{Enc}(m) \cdot \text{Enc}(m')$ is $\text{Enc}(m+m')$
  - $\psi(m,r) \cdot \psi(m',r') = \psi(m+m',r.r')$
Paillier's Scheme

- Uses $\mathbb{Z}^{n^2}_* \cong \mathbb{Z}_n \times \mathbb{Z}^*_n$, $n=pq$, $p,q$ primes within $2x$ of each other
  - Isomorphism: $\psi(a,b) = g^{abn} \pmod{n^2}$ where $g=(1+n)$
- $\text{Enc}(m) = \psi(m,r)$ for $m$ in $\mathbb{Z}_n$ and a random $r$ in $\mathbb{Z}_n^*$
- $\psi$ can be efficiently inverted if $p,q$ known
- (Additive) Homomorphism: $\text{Enc}(m) \cdot \text{Enc}(m')$ is $\text{Enc}(m+m')$
  - $\psi(m,r) \cdot \psi(m',r') = \psi(m+m',r \cdot r')$ in $\mathbb{Z}_n$
Paillier’s Scheme

- Uses $\mathbb{Z}_{n^2}^* \simeq \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other. To ensure $\gcd(n,\phi(n))=1$
  - Isomorphism: $\psi(a,b) = g^{ab} \pmod{n^2}$ where $g=(1+n)$

- $\text{Enc}(m) = \psi(m,r)$ for $m$ in $\mathbb{Z}_n$ and a random $r$ in $\mathbb{Z}_n^*$

- $\psi$ can be efficiently inverted if $p,q$ known

- (Additive) Homomorphism: $\text{Enc}(m).\text{Enc}(m')$ is $\text{Enc}(m+m')$
  - $\psi(m,r).\psi(m',r') = \psi(m+m',r.r')$ in $\mathbb{Z}_{n^2}^*$
Paillier’s Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  
  - Isomorphism: $\psi(a,b) = g^{abn} \pmod{n^2}$ where $g=(1+n)$

- Enc(m) = $\psi(m,r)$ for m in $\mathbb{Z}_n$ and a random r in $\mathbb{Z}_n^*$

- $\psi$ can be efficiently inverted if p,q known

- (Additive) Homomorphism: Enc(m).Enc(m’) is Enc(m+m’)

- IND-CPA secure under “Decisional Composite Residuosity” assumption: Given n=pq (but not p,q), $\psi(0,\text{rand})$ looks random (i.e. like $\psi(\text{rand},\text{rand})$)
Paillier's Scheme

- Uses $\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - To ensure $\gcd(n,\phi(n))=1$
- Isomorphism: $\psi(a,b) = g^{ab^n} \pmod{n^2}$ where $g=(1+n)$
- $\text{Enc}(m) = \psi(m,r)$ for $m$ in $\mathbb{Z}_n$ and a random $r$ in $\mathbb{Z}_n^*$
- $\psi$ can be efficiently inverted if $p,q$ known
- (Additive) Homomorphism: $\text{Enc}(m).\text{Enc}(m')$ is $\text{Enc}(m+m')$
  - $\psi(m,r).\psi(m',r') = \psi(m+m',r.r')$
- IND-CPA secure under "Decisional Composite Residuosity" assumption: Given $n=pq$ (but not $p,q$), $\psi(0,\text{rand})$ looks random (i.e. like $\psi(\text{rand},\text{rand})$)
- Unlinkability: $\text{ReR}(c) = c.\text{Enc}(0)$
Private Information Retrieval
Private Information Retrieval

- Using additive homomorphic encryption (need not be unlinkable)
Private Information Retrieval

Using additive homomorphic encryption (need not be unlinkable)

Client sends some encrypted representation of the index (need CPA security here)
Private Information Retrieval

- Using additive homomorphic encryption (need not be unlinkable)

- Client sends some encrypted representation of the index (need CPA security here)

- Server operates on the entire database using this encryption (homomorphically), so that the message in the resulting encrypted data has the relevant answer (and maybe more). It sends this (short) encrypted data to client, who decrypts to get answer (depends on correctness here)
Private Information Retrieval

- Using additive homomorphic encryption (need not be unlinkable)

- Client sends some encrypted representation of the index (need CPA security here)

- Server operates on the entire database using this encryption (homomorphically), so that the message in the resulting encrypted data has the relevant answer (and maybe more). It sends this (short) encrypted data to client, who decrypts to get answer (depends on correctness here)

- In the following: database values are integers in \([0,m)\); homom. enc. over a group with an element 1 s.t. \(\text{ord}(1) \geq m\). For integer \(x\) and ciphertext \(c\), define \(x \ast c\) using “repeated doubling”: \(0 \ast c = E(0); 1 \ast c = c; (a+b) \ast c = \text{Add}(a \ast c, b \ast c)\).
Private Information Retrieval

Using additive homomorphic encryption (need not be unlinkable)

Client sends some encrypted representation of the index (need CPA security here)

Server operates on the entire database using this encryption (homomorphically), so that the message in the resulting encrypted data has the relevant answer (and maybe more). It sends this (short) encrypted data to client, who decrypts to get answer (depends on correctness here)

In the following: database values are integers in [0,m); homom. enc. over a group with an element 1 s.t. \( \text{ord}(1) \geq m \).

For integer \( x \) and ciphertext \( c \), define \( x \cdot c \) using “repeated doubling”: \( 0 \cdot c = E(0); 1 \cdot c = c; (a+b) \cdot c = \text{Add}( a \cdot c, b \cdot c ) \).
Private Information Retrieval

\[ \begin{array}{c}
X_1 \\
X_2 \\
\vdots \\
X_i \\
\vdots \\
X_N \\
\end{array} \]
Private Information Retrieval

\[ 0 \quad 0 \quad \vdots \quad 0 \quad \vdots \quad 1 \quad \vdots \quad \vdots \quad 0 \]

\[ X_1 \quad X_2 \quad \vdots \quad X_i \quad \vdots \quad \vdots \quad X_N \]
Private Information Retrieval

\[ \begin{align*}
X_1 & \quad 0 \\
X_2 & \quad 0 \\
\vdots & \quad \vdots \\
X_i & \quad 1 \\
\vdots & \quad \vdots \\
X_N & \quad 0
\end{align*} \]
Private Information Retrieval

\[ \begin{align*}
X_1 & \quad 0 \\
X_2 & \quad 0 \\
X_i & \quad 0 \\
\vdots & \quad \vdots \\
X_N & \quad 0
\end{align*} \]
Private Information Retrieval

\[
\begin{align*}
0 & \quad \cdot \quad 0 \\
0 & \quad \cdot \quad 0 \\
\vdots & \quad \cdot \quad \vdots \\
0 & \quad \cdot \quad 0 \\
1 & \quad \cdot \quad 1 \\
\vdots & \quad \cdot \quad \vdots \\
0 & \quad \cdot \quad 0 \\
\end{align*}
\]

\[
\begin{align*}
X_1 & \quad \cdot \quad 0 \\
X_2 & \quad \cdot \quad 0 \\
\vdots & \quad \cdot \quad \vdots \\
X_i & \quad \cdot \quad X_i \\
\vdots & \quad \cdot \quad \vdots \\
X_N & \quad \cdot \quad 0 \\
\end{align*}
\]

\[
\begin{align*}
0 & \quad \cdot \quad 0 \\
0 & \quad \cdot \quad 0 \\
\vdots & \quad \cdot \quad \vdots \\
0 & \quad \cdot \quad 0 \\
\end{align*}
\]

\[
\begin{align*}
* & \quad \cdot \quad + \\
\end{align*}
\]

\[
\begin{align*}
\downarrow & \quad \cdot \quad \downarrow \\
X_i & \quad \cdot \quad X_i \\
\end{align*}
\]

\[
\begin{align*}
X_i & \quad \cdot \quad X_i \\
\end{align*}
\]
Private Information Retrieval

\[ X_1 \quad X_2 \quad \vdots \quad X_i \quad X_{N} \]

\[ \begin{array}{c}
X_1 \\
X_2 \\
\vdots \\
X_i \\
X_N \\
\end{array} \times \begin{array}{c}
0 \\
0 \\
\vdots \\
0 \\
0 \\
\end{array} = \begin{array}{c}
0 \\
0 \\
\vdots \\
0 \\
0 \\
\end{array} \]

\[ X_i \quad \vdots \quad 0 \]

\[ X_i \times [+] = X_i \]
Private Information Retrieval

\[
\begin{align*}
&\quad \quad 0 \quad 0 \\
&\quad \quad \vdots \quad \vdots \\
&\quad 1 \quad X_1 \\
&\quad \vdots \quad \vdots \\
&\quad 0 \quad X_N \\
&\quad \vdots \\
&\quad 0 \quad 0
\end{align*}
\]

\[
\begin{align*}
&\quad \quad 0 \\
&\quad \vdots \\
&\quad 0 \\
&\quad X_i \\
&\quad \vdots \\
&\quad 0
\end{align*}
\]

\[
\begin{align*}
&\quad X_i \\
&\quad [+]
\end{align*}
\]

\[
\begin{align*}
&\quad X_i \\
&\quad Dec \\
&\quad X_i
\end{align*}
\]
Private Information Retrieval

Server communication is very short. But client communication is larger than the db!
Private Information Retrieval

<table>
<thead>
<tr>
<th></th>
<th>$X_{11}$</th>
<th>...</th>
<th>$X_{1N}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_{21}$</td>
<td>...</td>
<td>...</td>
<td>$X_{2N}$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$X_{i1}$</td>
<td>...</td>
<td>...</td>
<td>$X_{iN}$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$X_{N}$</td>
<td>...</td>
<td>...</td>
<td>$X_{NN}$</td>
</tr>
</tbody>
</table>
Private Information Retrieval

\[
\begin{array}{c|c|c}
X_{11} & \cdots & X_{1N} \\
X_{21} & \cdots & X_{2N} \\
\vdots & \ddots & \vdots \\
X_{i1} & \cdots & X_{ij} & \cdots & X_{iN} \\
\vdots & \ddots & \vdots \\
X_N & \cdots & X_{NN} \\
\end{array}
\]
Private Information Retrieval

\[
\begin{array}{cccc}
X_{11} & X_{i1} & X_{iN} & X_{1N} \\
X_{21} & X_{ij} & X_{iN} & X_{2N} \\
\vdots & \vdots & \vdots & \vdots \\
X_N & X_{NN} & X_{NN} & X_{NN} \\
\end{array}
\]
Private Information Retrieval

<table>
<thead>
<tr>
<th>$x_{11}$</th>
<th>$x_{1N}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_{21}$</td>
<td>$x_{2N}$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$x_{i1}$</td>
<td>$x_{ij}$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$x_{N}$</td>
<td>$x_{NN}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0</th>
<th>..</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>..</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>$x_{i1}$</td>
<td>$x_{ij}$</td>
<td>$x_{iN}$</td>
</tr>
<tr>
<td>..</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>0</td>
<td>..</td>
<td>0</td>
</tr>
</tbody>
</table>
Private Information Retrieval

\[
\begin{align*}
&x_{11} & & & x_{1N} \\
&x_{21} & & & x_{2N} \\
& & & & & \\
&x_{i1} & & x_{ij} & & x_{iN} \\
& & & & & \\
&x_N & & & & x_{NN}
\end{align*}
\]
Private Information Retrieval

Use PIR again!
Use PIR again!
Private Information Retrieval

Use PIR again!
Consider using **Private Information Retrieval (PIR)** to access your data. Let's consider the ciphertext as plaintext for the sub-PIR.

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR. Can chop ciphertexts into smaller blocks.

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks

Use PIR again!
Private Information Retrieval

Considering ciphertext as plaintext for the sub-PIR
Can chop ciphertexts into smaller blocks
Recurse? Exponential in recursion depth

Use PIR again!
Private Information Retrieval
Private Information Retrieval

Can dramatically improve efficiency if we have an efficient “recursive” homomorphic encryption scheme
Private Information Retrieval

- Can dramatically improve efficiency if we have an efficient “recursive” homomorphic encryption scheme
- Ciphertext in one level is plaintext in the next level
Private Information Retrieval

- Can dramatically improve efficiency if we have an efficient "recursive" homomorphic encryption scheme

- Ciphertext in one level is plaintext in the next level

- In Paillier, public-key (i.e., $n$) fixes the group for homomorphic operation (i.e., $\mathbb{Z}_n$)
Private Information Retrieval

- Can dramatically improve efficiency if we have an efficient “recursive” homomorphic encryption scheme

- Ciphertext in one level is plaintext in the next level

- In Paillier, public-key (i.e., $n$) fixes the group for homomorphic operation (i.e., $\mathbb{Z}_n$)

- Ciphertext size increases only “additively” from level to level
Private Information Retrieval

- Can dramatically improve efficiency if we have an efficient “recursive” homomorphic encryption scheme
- Ciphertext in one level is plaintext in the next level
  - In Paillier, public-key (i.e., n) fixes the group for homomorphic operation (i.e., $\mathbb{Z}_n$)
- Ciphertext size increases only “additively” from level to level
  - In Paillier, size of ciphertext about double that of the plaintext. (Note: can’t use “hybrid encryption” if homomorphic property is to be preserved.)
Private Information Retrieval

- Can dramatically improve efficiency if we have an efficient “recursive” homomorphic encryption scheme

- Ciphertext in one level is plaintext in the next level

- In Paillier, public-key (i.e., $n$) fixes the group for homomorphic operation (i.e., $\mathbb{Z}_n$)

- Ciphertext size increases only “additively” from level to level

- In Paillier, size of ciphertext about double that of the plaintext. (Note: can’t use “hybrid encryption” if homomorphic property is to be preserved.)

- Does such a family of encryption schemes exist?
Damgård-Jurik Scheme
Damgård-Jurik Scheme

Uses $\mathbb{Z}_{n^{(s+1)}}^* = \mathbb{Z}_{n^s} \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
Damgård-Jurik Scheme

- Uses \( \mathbb{Z}_{n^{s+1}}^* \cong \mathbb{Z}_{n^s} \times \mathbb{Z}_n^* \), \( n=pq \), \( p,q \) primes within 2x of each other
- Isomorphism: \( \psi_s(a,b) = g^{abn^s} \) where \( g=(1+n) \)
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_n^{(s+1)*} \approx \mathbb{Z}_n^s \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
  - Enc($m$) = $\psi_s(m,r)$ for $m$ in $\mathbb{Z}_n^s$ and a random $r$ in $\mathbb{Z}_n^*$
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n^{s+1}}^* \cong \mathbb{Z}_{n^s} \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
- Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
- Enc($m$) = $\psi_s(m,r)$ for $m$ in $\mathbb{Z}_{n^s}$ and a random $r$ in $\mathbb{Z}_n^*$
- $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n^{(s+1)}}^* \approx \mathbb{Z}_{ns} \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{ab^n^s}$ where $g=(1+n)$
  - Enc(m) = $\psi_s(m,r)$ for m in $\mathbb{Z}_{ns}$ and a random r in $\mathbb{Z}_n^*$
  - $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
  - Homomorphism: Enc(m).Enc(m’) is Enc(m+m’)
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n(s+1)}^\ast \simeq \mathbb{Z}_{n^s} \times \mathbb{Z}_n^\ast$, $n=pq$, $p,q$ primes within 2x of each other
  
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
  
  - Enc$(m) = \psi_s(m,r)$ for $m$ in $\mathbb{Z}_{n^s}$ and a random $r$ in $\mathbb{Z}_n^\ast$

- $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)

- Homomorphism: $\text{Enc}(m) \cdot \text{Enc}(m')$ is $\text{Enc}(m+m')$
  
  - $\psi_s(m,r) \cdot \psi_s(m',r') = \psi_s(m+m',r\cdot r')$
Damgård-Jurik Scheme

- Uses $Z_{n(s+1)}^* \cong Z_n^s \times Z_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{a b^{n^s}}$ where $g=(1+n)$
  - Enc($m$) = $\psi_s(m,r)$ for $m$ in $Z_n^s$ and a random $r$ in $Z_n^*$
  - $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
  - Homomorphism: $\text{Enc}(m).\text{Enc}(m')$ is $\text{Enc}(m+m')$

  $$\psi_s(m,r).\psi_s(m',r') = \psi_s(m+m',r.r')$$
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n(s+1)}^* \cong \mathbb{Z}_{ns} \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
  - $Enc(m) = \psi_s(m,r)$ for $m$ in $\mathbb{Z}_{ns}$ and a random $r$ in $\mathbb{Z}_n^*$
  - $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
  - Homomorphism: $Enc(m).Enc(m')$ is $Enc(m+m')$

In $\mathbb{Z}_{n(s+1)}^*$, $\psi_s(m,r).\psi_s(m',r') = \psi_s(m+m',r.r')$ in $\mathbb{Z}_{ns}$
**Damgård-Jurik Scheme**

- Uses $\mathbb{Z}_{n(s+1)^*} \cong \mathbb{Z}_{ns} \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
  - Enc(m) = $\psi_s(m,r)$ for $m$ in $\mathbb{Z}_{ns}$ and a random $r$ in $\mathbb{Z}_n^*$
  - $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
  - Homomorphism: Enc(m).Enc(m') is Enc(m+m')
    - $\psi_s(m,r).\psi_s(m',r') = \psi_s(m+m',r.r')$

Recursive encryption: Output (ciphertext) of $\psi_s (\mathbb{Z}_{n(s+1)^*})$ is an input (plaintext) for $\psi_{s+1} (\mathbb{Z}_{n(s+1)})$ for the same public-key $n$.

Note: $s$ log $n$ bits encrypted to $(s+1)$log $n$ bits.
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n^{(s+1)}}^* \cong \mathbb{Z}_{ns} \times \mathbb{Z}_n^*$, $n = pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g = (1+n)$
  - Enc(m) = $\psi_s(m,r)$ for $m$ in $\mathbb{Z}_{ns}$ and a random $r$ in $\mathbb{Z}_n^*$
  - $\psi_s$ can still be efficiently inverted if $p,q$ known (but more involved)
  - Homomorphism: $\text{Enc}(m) \cdot \text{Enc}(m')$ is $\text{Enc}(m+m')$
  - $\psi_s(m,r) \cdot \psi_s(m',r') = \psi_s(m+m',rr')$
  - Recursive encryption: Output (ciphertext) of $\psi_s(\mathbb{Z}_{n^{(s+1)}}^*)$ is an input (plaintext) for $\psi_{s+1}(\mathbb{Z}_{n^{(s+1)}}^*)$ for the same public-key $n$.

Note: $s \log n$ bits encrypted to $(s+1)\log n$ bits.

- IND-CPA secure under “Decisional Composite Residuosity” assumption: Given $n = pq$ (but not $p,q$), $\psi_1(0,\text{rand})$ looks random (same as Paillier)
Damgård-Jurik Scheme

- Uses $\mathbb{Z}_{n(s+1)}^* \cong \mathbb{Z}_n^s \times \mathbb{Z}_n^*$, $n=pq$, $p,q$ primes within 2x of each other
  - Isomorphism: $\psi_s(a,b) = g^{abn^s}$ where $g=(1+n)$
- Enc(m) = $\psi_s(m,r)$ for $m$ in $\mathbb{Z}_n^s$ and a random $r$ in $\mathbb{Z}_n^*$
- $\psi_s$ can still be efficiently inverted if p,q known (but more involved)
- Homomorphism: Enc(m).Enc(m') is Enc(m+m')
- Recursive encryption: Output (ciphertext) of $\psi_s (\mathbb{Z}_{n(s+1)}^*)$ is an input (plaintext) for $\psi_{s+1} (\mathbb{Z}_{n(s+1)}^*)$ for the same public-key $n$.
  - in $\mathbb{Z}_{n(s+1)}^*$
- Note: $s \log n$ bits encrypted to $(s+1)\log n$ bits.
- IND-CPA secure under “Decisional Composite Residuosity” assumption: Given $n=pq$ (but not $p,q$), $\psi_1(0,\text{rand})$ looks random (same as Paillier)
- Unlinkability: ReRand(c) = $c.\text{Enc}(0)$ (using same $s$ in Enc as for $c$)
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol
Final PIR protocol

Diagram showing a protocol flow with operators and data blocks.
Final PIR protocol

\[ \begin{array}{c}
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\downarrow & \downarrow \\
0 & 1 \\
\end{array} \]
Final PIR protocol

Size of ciphertext at depth $d$ is $O(d \log m)$ where $m$ is the range of values in db
Final PIR protocol

Size of ciphertext at depth $d$ is $O(d \log m)$ where $m$ is the range of values in $db$

"Constant" in $O(.)$ contains security parameter
Final PIR protocol

- Size of ciphertext at depth \( d \) is \( O(d \log m) \) where \( m \) is the range of values in db.
- “Constant” in \( O(.) \) contains security parameter.
- Total communication from client = \( O(\log^2 N \log m) \), where \( N \) is the number of entries in the db.
Final PIR protocol

- Size of ciphertext at depth $d$ is $O(d \log m)$ where $m$ is the range of values in db
- "Constant" in $O(.)$ contains security parameter
- Total communication from client = $O(\log^2 N \log m)$, where $N$ is the number of entries in the db
- Total communication from server = $O(\log N \log m)$
Homomorphic Encryption for MPC
Homomorphic Encryption for MPC

- Recall GMW (passive-secure): each wire value was kept shared among the parties
Homomorphic Encryption for MPC

- Recall GMW (passive-secure): each wire value was kept shared among the parties
- Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared
Homomorphic Encryption for MPC

- Recall GMW (passive-secure): each wire value was kept shared among the parties
- Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared
- Will evaluate each wire using homomorphism (unlinkable)
Homomorphic Encryption for MPC

- Recall GMW (passive-secure): each wire value was kept shared among the parties
- Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared
  - Will evaluate each wire using homomorphism (unlinkable)

  Notation: $[x] + [y] = [x+y]$, and $a*[x] = [ax]$
Homomorphic Encryption for MPC

Recall GMW (passive-secure): each wire value was kept shared among the parties

Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared

Will evaluate each wire using homomorphism (unlinkable)

Notation: \([x] [+] [y] = [x+y]\), and \(a*[x] = [ax]\)

And decrypt the output wire value: threshold decryption
Homomorphic Encryption for MPC

Recall GMW (passive-secure): each wire value was kept shared among the parties.

Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared.

- Will evaluate each wire using homomorphism (unlinkable).
  - Notation: $[x][+][y] = [x+y]$, and $a*[x] = [ax]$.
- And decrypt the output wire value: threshold decryption.
  - Threshold decryption: KeyGen protocol so that PK is public and SK shared; Decryption protocol that lets the parties decrypt a ciphertext keeping their SK shares private.
Homomorphic Encryption for MPC

- Recall GMW (passive-secure): each wire value was kept shared among the parties
- Alternate approach: each wire value is kept encrypted, publicly, and the key is kept shared
  - Will evaluate each wire using homomorphism (unlinkable)
    - Notation: $[x] [+] [y] = [x+y]$, and $a*[x] = [ax]$
  - And decrypt the output wire value: threshold decryption
    - Threshold decryption: KeyGen protocol so that PK is public and SK shared; Decryption protocol that lets the parties decrypt a ciphertext keeping their SK shares private
    - (For active-security, also ZK proofs/proofs of knowledge)
Homomorphic Encryption for MPC
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK

- Each party encrypts its input and publishes
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes

For active-security, include ZK proofs of correctness/knowledge of plaintext, when publishing
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes
- At an addition gate, carry out homomorphic addition: $[z] = [x] + [y]$
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes
- At an addition gate, carry out homomorphic addition: \([z] = [x] + [y]\)
- At a multiplication gate, given \([x]\) and \([y]\), to compute \([xy]\):

For active-security, include ZK proofs of correctness/knowledge of plaintext, when publishing.
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes
- At an addition gate, carry out homomorphic addition: \( [z] = [x] + [y] \)
- At a multiplication gate, given \([x]\) and \([y]\), to compute \([xy]\):
  - Share \(x\): All parties except \(P_1\), choose their shares \(s_i\); to help \(P_1\) compute \(s_1\), they publish \([-s_i]\), \(P_1\) publishes \([r]\); they threshold decrypt \([t] = [r + x + \sum_{i=2}^{m} (-s_i)]\). \(P_1\) sets \(s_1 = t - r\)

For active-security, include ZK proofs of correctness/knowledge of plaintext, when publishing
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes
- At an addition gate, carry out homomorphic addition: \([z]=[x]+[y]\)
- At a multiplication gate, given \([x]\) and \([y]\), to compute \([xy]\):
  - Share \(x\): All parties except \(P_1\), choose their shares \(s_i\); to help \(P_1\) compute \(s_1\), they publish \([-s_i]\), \(P_1\) publishes \([r]\); they threshold decrypt \([t]= [r + x + \sum_{i=2:m} (-s_i)]\). \(P_1\) sets \(s_1 = t-r\)
  - Each party publishes \(s_i \cdot [y] = [s_i \cdot y]\); they compute \([\sum s_i \cdot y]=[xy]\)

For active-security, include ZK proofs of correctness/knowledge of plaintext, when publishing
Homomorphic Encryption for MPC

- Run KeyGen and obtain PK and private shares for SK
- Each party encrypts its input and publishes
- At an addition gate, carry out homomorphic addition: \([z]=[x][\oplus][y]\)
- At a multiplication gate, given \([x]\) and \([y]\), to compute \([xy]\):
  - Share \(x\): All parties except \(P_1\), choose their shares \(s_i\); to help \(P_1\) compute \(s_1\), they publish \([-s_i]\), \(P_1\) publishes \(r\); they threshold decrypt \([t]=[r+x+\sum_{i=2:m}(-s_i)]\). \(P_1\) sets \(s_1 = t-r\)
  - Each party publishes \(s_i[y] = [s_i y]\); they compute \([\sum s_i y]=[xy]\)
- Threshold decrypt the output

For active-security, include ZK proofs of correctness/knowledge of plaintext, when publishing
The plaintext domain
The plaintext domain

In some encryption schemes the plaintext domain is fixed as a system parameter.
The plaintext domain

- In some encryption schemes the plaintext domain is fixed as a system parameter
  
- e.g. El Gamal, when the DDH group is fixed
The plaintext domain

- In some encryption schemes the plaintext domain is fixed as a system parameter
  - e.g. El Gamal, when the DDH group is fixed

- But sometimes the plaintext domain is chosen as part of the public-key
The plaintext domain

- In some encryption schemes the plaintext domain is fixed as a system parameter
  - e.g. El Gamal, when the DDH group is fixed

- But sometimes the plaintext domain is chosen as part of the public-key
  - e.g. Paillier, when the modulus \( n = pq \) is chosen
The plaintext domain

- In some encryption schemes the plaintext domain is fixed as a system parameter
  - e.g. El Gamal, when the DDH group is fixed

- But sometimes the plaintext domain is chosen as part of the public-key
  - e.g. Paillier, when the modulus $n = pq$ is chosen

- For non-homomorphic encryption, not critical: can use a scheme with a larger domain into which the required domain can be embedded
The plaintext domain

- In some encryption schemes the plaintext domain is fixed as a system parameter
  - e.g. El Gamal, when the DDH group is fixed

- But sometimes the plaintext domain is chosen as part of the public-key
  - e.g. Paillier, when the modulus $n = pq$ is chosen

- For non-homomorphic encryption, not critical: can use a scheme with a larger domain into which the required domain can be embedded

- But not good for homomorphic encryption: say, an application needs to use addition modulo 10; can we use Paillier?
The plaintext domain
The plaintext domain

Say, an application needs to use addition modulo 10; can we use Paillier?
The plaintext domain

- Say, an application needs to use addition modulo 10; can we use Paillier?

- Suppose there is a bound on how many times the homomorphic operation will be carried out.
The plaintext domain

- Say, an application needs to use addition modulo 10; can we use Paillier?
  - Suppose there is a bound on how many times the homomorphic operation will be carried out.
  - Then, work with a suitably large modulus, so that no overflow occurs.
Say, an application needs to use addition modulo 10; can we use Paillier?

Suppose there is a bound on how many times the homomorphic operation will be carried out.

Then, work with a suitably large modulus, so that no overflow occurs.

But not unlinkable: 9+3 and 2 look different.
The plaintext domain

- Say, an application needs to use addition modulo 10; can we use Paillier?

- Suppose there is a bound on how many times the homomorphic operation will be carried out

- Then, work with a suitably large modulus, so that no overflow occurs

- But not unlinkable: 9+3 and 2 look different

- Also suppose OK to reveal how many operations were done
The plaintext domain

- Say, an application needs to use addition modulo 10; can we use Paillier?
- Suppose there is a bound on how many times the homomorphic operation will be carried out.
- Then, work with a suitably large modulus, so that no overflow occurs.
- But not unlinkable: 9+3 and 2 look different.
- Also suppose OK to reveal how many operations were done.
- Each time add a large random multiple of 10 (but not large enough to cause overflow): 9+3+10r and 2+10r are statistically close if r drawn from a large range.
Today
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
  - A simple (passive-secure) OT protocol using rerandomizable encryption
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
  - A simple (passive-secure) OT protocol using rerandomizable encryption
  - PIR (using Damgård-Jurik encryption scheme)
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
  - A simple (passive-secure) OT protocol using rerandomizable encryption
  - PIR (using Damgård-Jurik encryption scheme)
  - MPC
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
  - A simple (passive-secure) OT protocol using rerandomizable encryption
  - PIR (using Damgård-Jurik encryption scheme)
  - MPC
- Not covered: “Fully Homomorphic Encryption”, security against active corruption (ZK proofs, non-malleable homomorphic encryption)
Today

- Homomorphic Encryption: El Gamal, Paillier, Damgård-Jurik
- Applications of Homomorphic Encryption
  - A simple (passive-secure) OT protocol using rerandomizable encryption
  - PIR (using Damgård-Jurik encryption scheme)
  - MPC
- Not covered: “Fully Homomorphic Encryption”, security against active corruption (ZK proofs, non-malleable homomorphic encryption)
- Coming up: more applications – in voting