Efficient TFHE Bootstrapping in the Multiparty Setting

Jeongeun Park [1] Sergi Rovira [2]

[1]imec-COSIC, KU-Leuven

[2]WiSeCom, Universitat Pompeu Fabra (UPF)

June 1, 2023

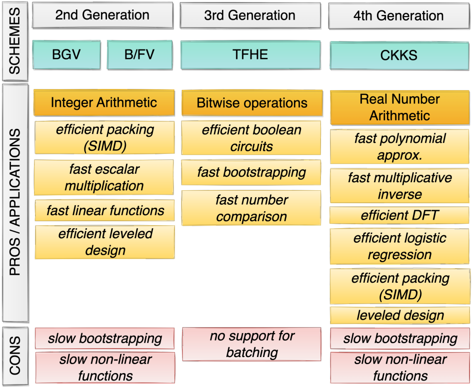
Motivation

- Handling multiple users securely and efficiently for privacy preserving protocol is important for real world applications.
- Two main approaches for multiple users: Multikey (MKHE) and Multiparty (MPHE)
- State of the art FHE schemes such as BGV, B/FV and CKKS are already efficiently extended to their MPHE version, but there is no concrete such extension of TFHE.

Scheme	**MKHE**	**MPHE**
BGV	[CZW17]	[Par21]
B/FV	[CDKS19, KLSW21]	[AJLA+12, MTPBH21, Par21, KLSW21]
TFHE	[CCS19, LP19]	This work, [LMK+23]
CKKS	[CDKS19]	[Par21]

Table: Main MKHE and MPHE extensions of the most well-known FHE schemes

Motivation

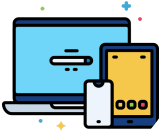


Thank you to Chiara Marcolla for providing the figure. Extracted from [MSM+23].

Contents

Contents

PC

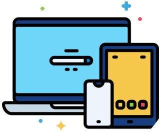


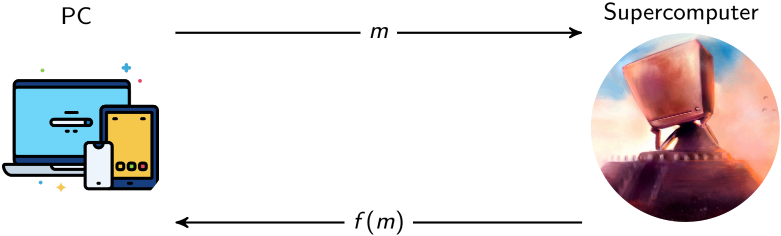
Supercomputer

PC

m

Supercomputer

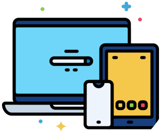



PC
m
Supercomputer
f(m)

PC

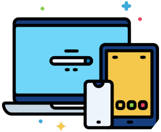
Supercomputer

(pk, sk)



PC

(pk, sk)



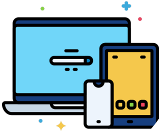
$Enc_{pk}(m)$ →

Supercomputer

Homomorphic Encryption: Delegation of computation

PC

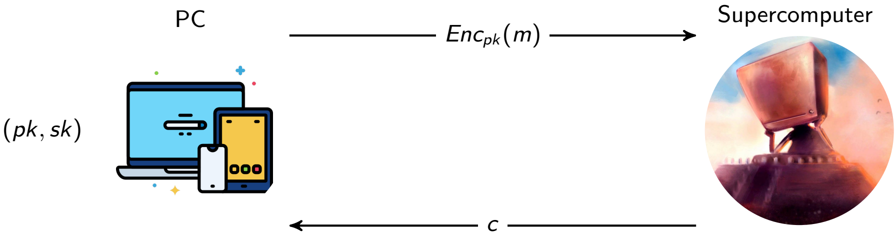
(pk, sk)



$\xrightarrow{Enc_{pk}(m)}$

Supercomputer

$\xleftarrow{c}$

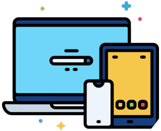


Properties:

Correctness: $Dec_{sk}(c) = f(m)$

PC

(pk, sk)



$\longrightarrow Enc_{pk}(m) \longrightarrow$

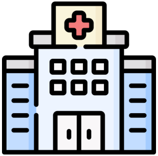
$\longleftarrow c \longleftarrow$

Supercomputer

Properties:

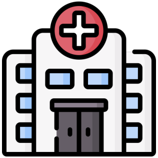
Correctness: $Dec_{sk}(c) = f(m)$
Compactness: The size of c is independent of f

Hospital A



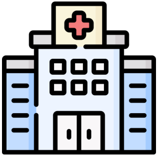
Supercomputer

Hospital B



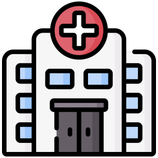
Hospital A

(pk, sk)

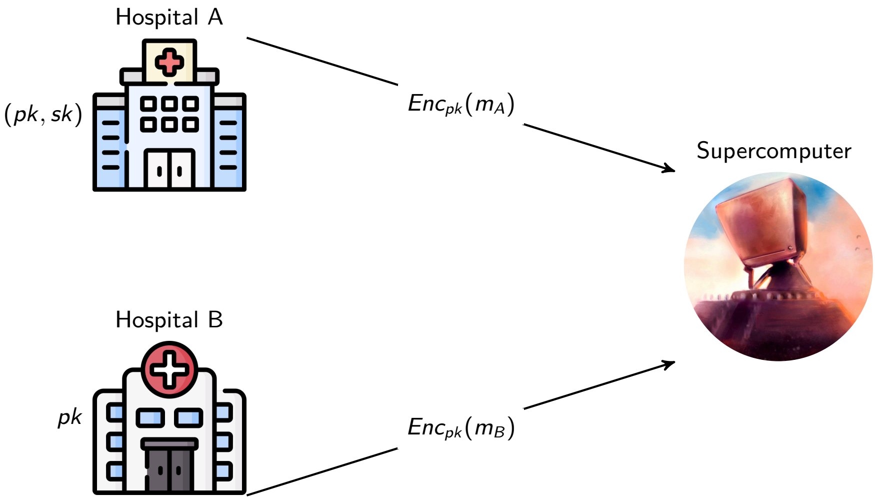


Hospital B

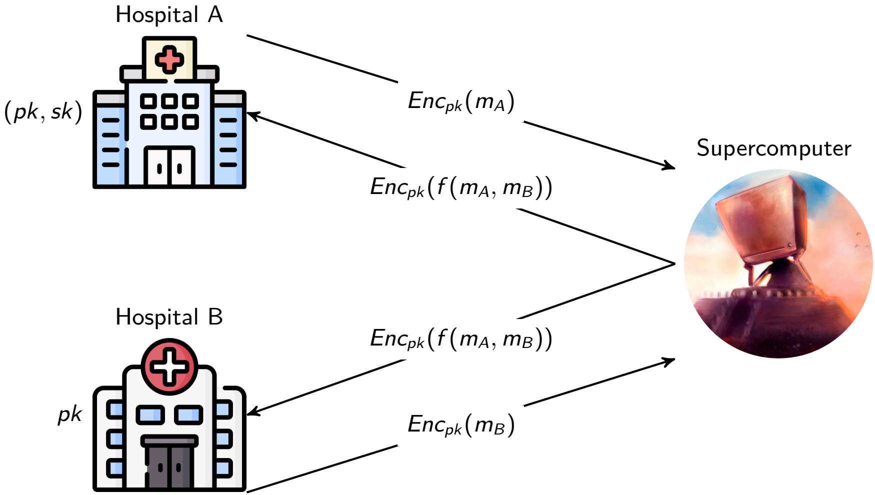
pk



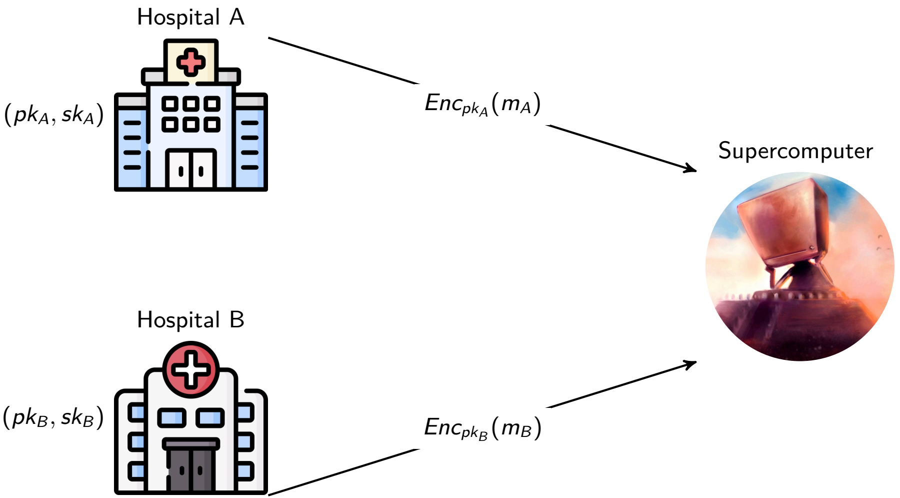
Supercomputer


Hospital A
(pk, sk)
$Enc_{pk}(m_A)$
Supercomputer
Hospital B
pk
$Enc_{pk}(m_B)$

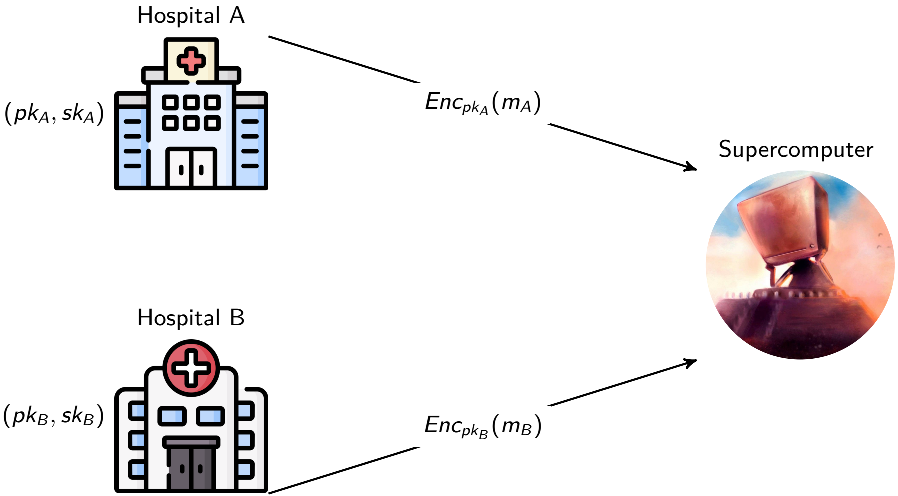
Multikey HE: Machine Learning based diagnosis



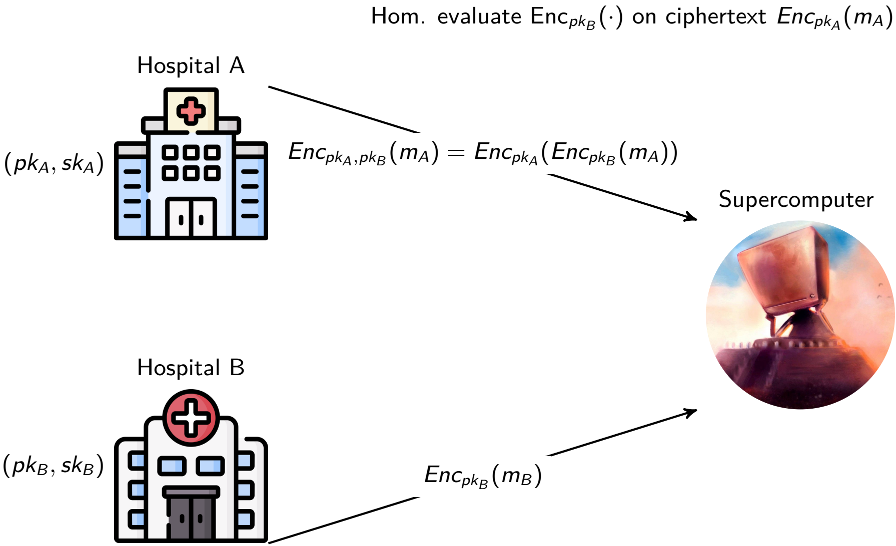
Multikey HE: Machine Learning based diagnosis



Hom. evaluate $\mathrm{Enc}_{pk_B}(\cdot)$ on ciphertext $Enc_{pk_A}(m_A)$



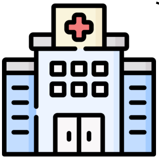
Multikey HE: Machine Learning based diagnosis



Hom. evaluate $\mathrm{Enc}_{pk_B}(\cdot)$ on ciphertext $Enc_{pk_A}(m_A)$

Hospital A

(pk_A, sk_A)

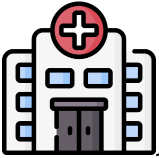


$Enc_{pk_A,pk_B}(m_A) = Enc_{pk_A}(Enc_{pk_B}(m_A))$

Supercomputer

Hospital B

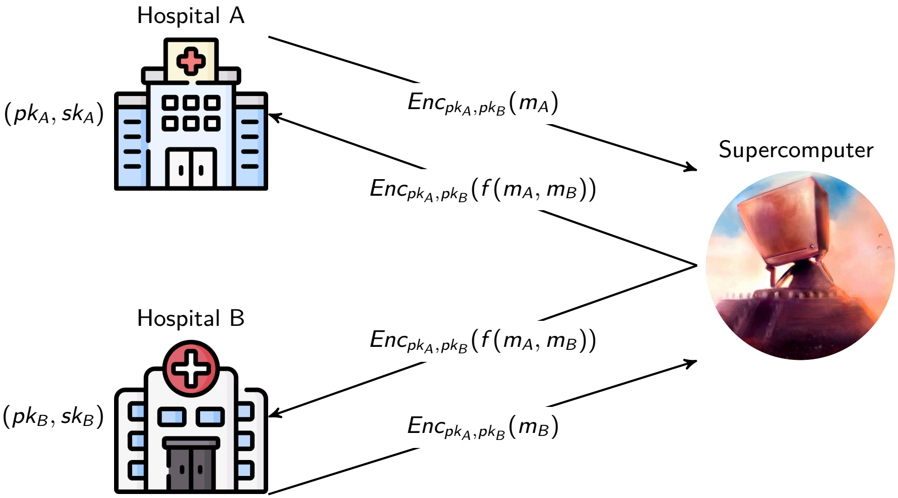
(pk_B, sk_B)



$Enc_{pk_A,pk_B}(m_B) = Enc_{pk_A}(Enc_{pk_B}(m_B))$

Multikey HE: Machine Learning based diagnosis

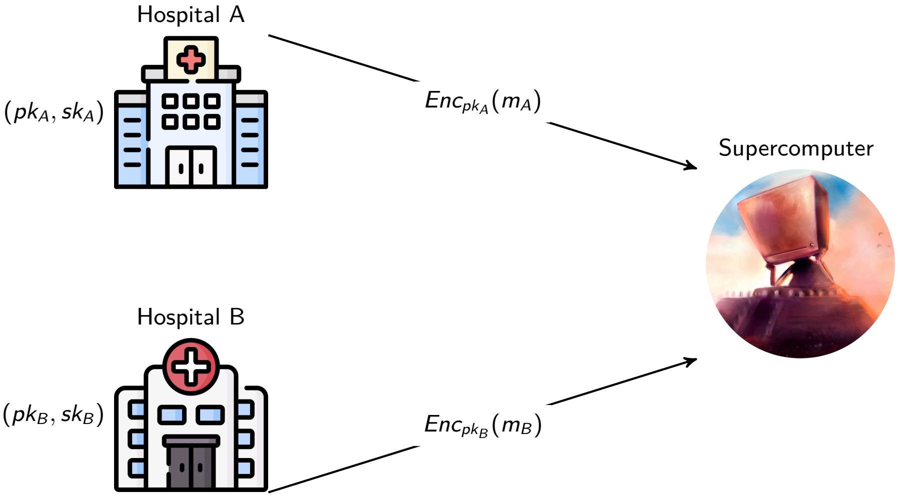
Hom. evaluate $\text{Enc}_{pk_B}(\cdot)$ on ciphertext $Enc_{pk_A}(m_A)$



Main problems with the MKHE approach

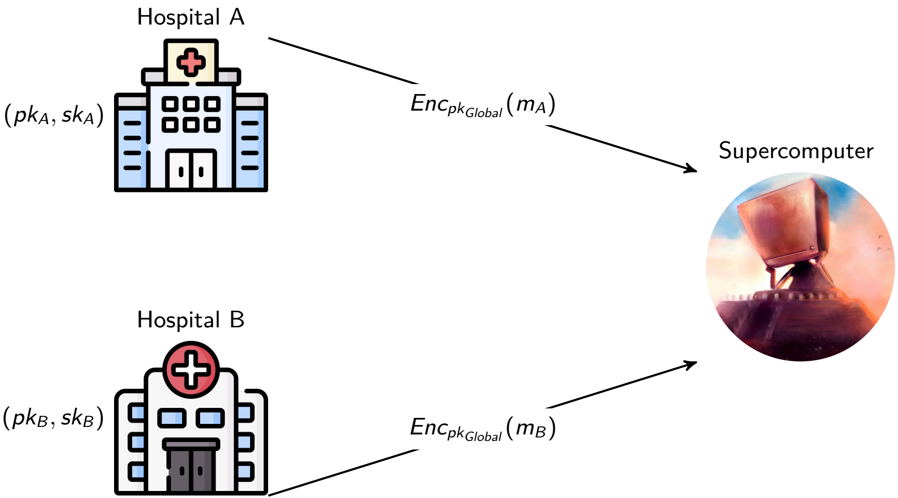
- **Problem 1**: Most constructions require an expensive ciphertext expansion mechanism.
- **Problem 2**: The size of the expanded ciphertexts grows linearly or quadratically on the number of parties.

Multiparty HE to the rescue



Multiparty HE to the rescue

$$pk_{Global} = pk_A + pk_B$$



Multikey vs Multiparty HE

- MKHE
  - Pros
    - Parties can join the protocol at any time
    - Faster key generation than MPHE
  - Cons
    - Requires ciphertext expansion
    - The size of ciphertexts grows with the number of parties involved
- MPHE
  - Pros
    - Similar performance to single-key HE schemes
    - No ciphertext expansion
  - Cons
    - Fix set of users during setup phase
    - No other parties can join the protocol afterwards

Contents

- The core operation of TFHE bootstrapping is *blind rotation*.
  - By *rotation*, we mean:

$$P(X) = a_0 + a_1 X + \cdots + a_{\mu-1} X^{\mu-1} + a_\mu X^\mu + \cdots + a_{N-1} X^{N-1} \in \mathcal{R}_q$$

$$P(X) \cdot X^{-\mu} = a_\mu + a_{\mu+1} X + \cdots + a_{N-1} X^{N-\mu-1} - a_0 X^{N-\mu} - \cdots - a_{\mu-1} X^{N-1} \in \mathcal{R}_q$$

  - By *blind*, we mean that we convert a $\mathrm{LWE}_s(\mu) = (a_1, \ldots, a_n, b)$ into a RLWE encryption of $X^{-\mu} \cdot v$, where v is a test polynomial and

$$-\mu \approx -b + \sum_{j=1}^{n} s_j a_j, \text{ with } s = (s_1, \ldots, s_n) \in \{0,1\}^n$$

  - In the binary case, we require n bootstrapping keys, computed as $bsk[j] \leftarrow RGSW(s_j)$.

Algorithm 1 Blind rotation in the binary case

1: $\mathrm{acc} \leftarrow (0, \ldots, 0, X^{-b} \cdot v)$
2: **for** $j = 1$ to n **do**
3: $\quad \mathrm{acc} \leftarrow \mathrm{acc} + \mathrm{bsk}[j] \boxdot ((X^{a_j} - 1) \cdot \mathrm{acc})$
4: **end for**
5: **return** acc

- Assume that we have a secret key space $\mathcal{S} = \{0, \ldots, k\}$.
- We can write

$$X^{s_j a_j} = \sum_{i=0}^{k} \mathbb{1}\{i = s_j\} X^{i \cdot a_j} = \sum_{i=1}^{k} \mathbb{1}\{i = s_j\}(X^{i \cdot a_j} - 1)$$

- Therefore, we can compute acc by setting $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$ and iterating

$$acc \leftarrow acc + \left(\sum_{i=1}^{k} (X^{i \cdot a_j} - 1) bsk[k(j-1)+i] \right) \boxdot acc$$

Blind rotation

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

Blind rotation

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

$$(j = 1, i = 1) \quad bsk[1] = \bar{1}$$

Blind rotation

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

$$(j = 1, i = 1) \quad bsk[1] = \bar{1}$$
$$(j = 1, i = 2) \quad bsk[2] = \bar{0}$$

Blind rotation

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

$$
\begin{aligned}
(j = 1, i = 1) \quad & bsk[1] = \bar{1} \\
(j = 1, i = 2) \quad & bsk[2] = \bar{0} \\
(j = 1, i = 3) \quad & bsk[3] = \bar{0}
\end{aligned}
$$

Blind rotation

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

$$
\begin{aligned}
(j = 1, i = 1) \quad & bsk[1] = \bar{1} \\
(j = 1, i = 2) \quad & bsk[2] = \bar{0} \\
(j = 1, i = 3) \quad & bsk[3] = \bar{0} \\
(j = 1, i = 4) \quad & bsk[4] = \bar{0}
\end{aligned}
$$

- Let us consider $\mathcal{S} = \{0, 1, 2, 3, 4\}$ the secret key $s = (1, 2, 3, 4)$.
- Recall that $bsk[k(j-1)+i] \leftarrow RGSW(\mathbb{1}\{i = s_j\})$
- Define $RGSW(m) := \bar{m}$, then:

$$
\begin{aligned}
(j=1, i=1) \quad & bsk[1] = \bar{1} & \qquad (j=2, i=1) \quad & bsk[5] = \bar{0} \\
(j=1, i=2) \quad & bsk[2] = \bar{0} & \qquad (j=2, i=2) \quad & bsk[6] = \bar{1} \\
(j=1, i=3) \quad & bsk[3] = \bar{0} & \qquad (j=2, i=3) \quad & bsk[7] = \bar{0} \\
(j=1, i=4) \quad & bsk[4] = \bar{0} & \qquad (j=2, i=4) \quad & bsk[8] = \bar{0}
\end{aligned}
$$

$$
\begin{aligned}
(j=3, i=1) \quad & bsk[9] = \bar{0} & \qquad (j=4, i=1) \quad & bsk[13] = \bar{0} \\
(j=3, i=2) \quad & bsk[10] = \bar{0} & \qquad (j=4, i=2) \quad & bsk[14] = \bar{0} \\
(j=3, i=3) \quad & bsk[11] = \bar{1} & \qquad (j=4, i=3) \quad & bsk[15] = \bar{0} \\
(j=3, i=4) \quad & bsk[12] = \bar{0} & \qquad (j=4, i=4) \quad & bsk[16] = \bar{1}
\end{aligned}
$$

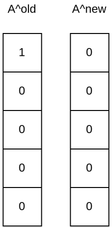
Blind rotation

- Consider a set of parties $\mathcal{P}_1, \ldots, \mathcal{P}_4$. Notation $RGSW(m) := \bar{m}$
- Each party i has a secret key $s_i \in \{0,1\}^n$.
- For example, assume that $s_{1,1} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$.
- In our MPHE scheme, the global LWE secret key s_G will have $s_{G,1} = 3$.
- In this example, we also have $\mathcal{S} = \{0,1,2,3,4\}$.
- Therefore, the global bootstrapping key bsk_G will start with

$$
\begin{aligned}
(j=1, i=1) \quad & bsk_G[1] = \bar{0} \\
(j=1, i=2) \quad & bsk_G[2] = \bar{0} \\
(j=1, i=3) \quad & bsk_G[3] = \bar{1} \\
(j=1, i=4) \quad & bsk_G[4] = \bar{0}
\end{aligned}
$$

- Problem: the server only has encryptions of the secret keys
- We need a way to go from $(\bar{s}_{1,1}, \bar{s}_{2,1}, \bar{s}_{3,1}, \bar{s}_{4,1})$ to $(\bar{0}, \bar{0}, \bar{1}, \bar{0})$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

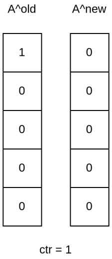
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



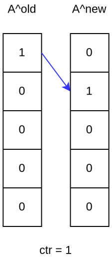
- For all $j = 0$ set

$$
\begin{aligned}
A^{new}[0] &\leftarrow 0 && \text{if ctr} = 1 \\
A^{new}[0] &\leftarrow A^{old}[0] && \text{otherwise}
\end{aligned}
$$

- For all $j \in \{1, \ldots, k\}$ set

$$
\begin{aligned}
A^{new}[j] &\leftarrow A^{old}[j-1] && \text{if ctr} = 1 \\
A^{new}[j] &\leftarrow A^{old}[j] && \text{otherwise}
\end{aligned}
$$

$$\text{ctr} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$



- For all $j = 0$ set

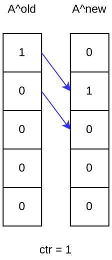
$$\begin{aligned} A^{new}[0] &\leftarrow 0 && \text{if ctr} = 1 \\ A^{new}[0] &\leftarrow A^{old}[0] && \text{otherwise} \end{aligned}$$

- For all $j \in \{1, \ldots, k\}$ set

$$\begin{aligned} A^{new}[j] &\leftarrow A^{old}[j-1] && \text{if ctr} = 1 \\ A^{new}[j] &\leftarrow A^{old}[j] && \text{otherwise} \end{aligned}$$

$$\text{ctr} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

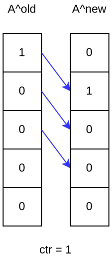
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$\text{ctr} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

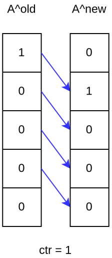
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$\text{ctr} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



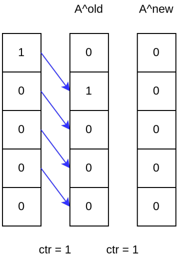
- For all $j = 0$ set

$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$\text{ctr} = 1, s_{2,1} = 1, s_{3,1} = 1, s_{4,1} = 0$$



- For all $j = 0$ set

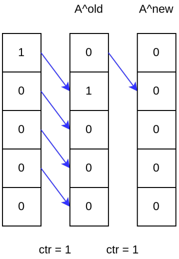
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, \text{ctr} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

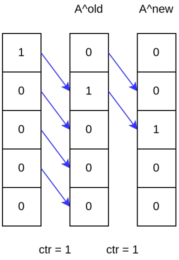
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, \text{ctr} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

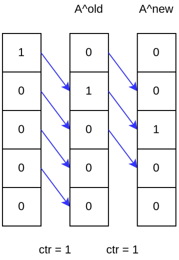
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, \text{ctr} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

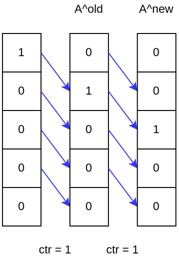
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, \text{ctr} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

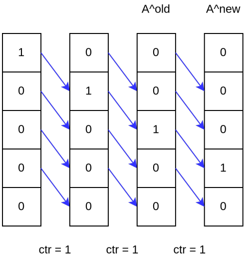
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \dots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, \text{ctr} = 1, s_{3,1} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

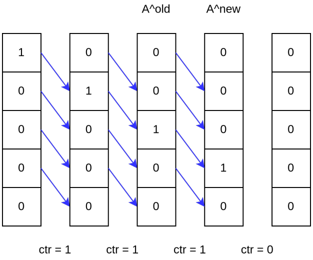
$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, s_{2,1} = 1, \text{ctr} = 1, s_{4,1} = 0$$

Homomorphic Indicator (k = 4)



- For all $j = 0$ set

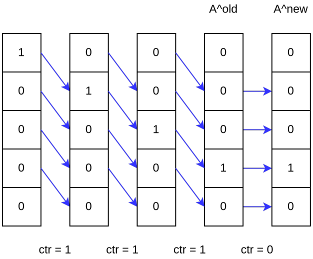
$$A^{new}[0] \leftarrow 0 \quad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \quad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \quad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \quad \text{otherwise}$$

$$s_{1,1} = 1, s_{2,1} = 1, s_{3,1} = 1, \text{ctr} = 0$$

Homomorphic Indicator (k = 4)



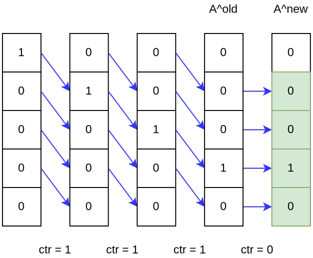
- For all $j = 0$ set

$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, s_{2,1} = 1, s_{3,1} = 1, \text{ctr} = 0$$



- For all $j = 0$ set

$$A^{new}[0] \leftarrow 0 \qquad \text{if ctr} = 1$$
$$A^{new}[0] \leftarrow A^{old}[0] \qquad \text{otherwise}$$

- For all $j \in \{1, \ldots, k\}$ set

$$A^{new}[j] \leftarrow A^{old}[j-1] \qquad \text{if ctr} = 1$$
$$A^{new}[j] \leftarrow A^{old}[j] \qquad \text{otherwise}$$

$$s_{1,1} = 1, s_{2,1} = 1, s_{3,1} = 1, \text{ctr} = 0$$

Homomorphic Indicator

Algorithm 2 Homomorphic Indicator (Hom.Indicator)

Require: $\{\mathbf{C}_i\}_{i \in [m]}, \mathsf{A}^{new}$ and A^{old}.
Ensure: A^{old}.

```
for i ← 1 to k do
    for j ← 1 to k do
        A^new[j] := CMUX_⊠(C_i, A^old[j], A^old[j − 1])
    end for
    A^new[0] := A^old[0] ⊠ (1 − C_i)
    for j ← 0 to k do
        A^old[j] := A^new[j]
    end for
end for
```

Bootstrapping Keys Generation

Algorithm 3 Global bootstrapping key generation

Require: $\{\mathsf{bsk}_i\}_{i \in [k]}, \mathsf{A}^{new}$ and A^{old}.

Ensure: $\widehat{\mathsf{bsk}}$.

```
for t ← 0 to n − 1 do
    for i ← 1 to k do
        Parse C_{i,t} := bsk_i[t]
    end for
    A := Hom.Indicator({C_{i,t}}_{i∈[k]}, A^new, A^old)
    bsk^[t] := [A[1], . . . , A[k]]
    Refresh A^new and A^old
end for
```

$$
\begin{aligned}
&\textbf{for } t \leftarrow 0 \text{ to } n-1 \textbf{ do}\\
&\quad \textbf{for } i \leftarrow 1 \text{ to } k \textbf{ do}\\
&\quad\quad \text{Parse } \mathbf{C}_{i,t} := \mathsf{bsk}_i[t]\\
&\quad \textbf{end for}\\
&\quad \mathsf{A} := \mathsf{Hom.Indicator}(\{\mathbf{C}_{i,t}\}_{i \in [k]}, \mathsf{A}^{new}, \mathsf{A}^{old})\\
&\quad \widehat{\mathsf{bsk}}[t] := [\mathsf{A}[1], \ldots, \mathsf{A}[k]]\\
&\quad \text{Refresh } \mathsf{A}^{new} \text{ and } \mathsf{A}^{old}\\
&\textbf{end for}
\end{aligned}
$$

Contents

k	N	n	log q	log Q	$\sigma_{\text{rlwe}}(=\theta)$	σ_{lwe}	B	l	Time (in seconds)	Bootstrapping noise	Bsk noise
2	2048	530	32	64	$1.85 \cdot 2^{4.2}$	2^{17}	12	3	**0.20**	56.2 (24.2)	35.91
							6	8	0.48	**45.6 (13.6)**	30.37
4	2048	495	32	64	$1.85 \cdot 2^{4.2}$	2^{17}	11	4	**0.33**	56.12 (24.12)	36.95
							7	7	0.59	**48.97 (16.97)**	32.98
8	2048	495	32	64	$1.85 \cdot 2^{4.2}$	2^{17}	8	4	**0.46**	57.51 (57.51)	40.29
							7	6	0.70	**50.65 (18.65)**	33.85
16	2048	495	32	64	$1.85 \cdot 2^{4.2}$	2^{17}	10	5	**0.90**	58.37 (26.37)	38.02
							7	6	1.06	**52.79 (20.79)**	35.81

Table: Parameter sets recommended achieving at least 110-bit security based on LWE estimator for different number parties k.The last three columns correspond to the average of 500 NAND operations, each performed with a freshly encrypted LWE ciphertext.

Thank you!

- jeongeun.park@esat.kuleuven.be
- sergi.rovira@upf.edu

- Preprint: https://eprint.iacr.org/2023/759

Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs, *Multiparty computation with low communication, computation and interaction via threshold fhe*, Advances in Cryptology – EUROCRYPT 2012 (Berlin, Heidelberg) (David Pointcheval and Thomas Johansson, eds.), Springer Berlin Heidelberg, 2012, pp. 483–501.

Hao Chen, Ilaria Chillotti, and Yongsoo Song, *Multi-key homomorphic encryption from tfhe*, Advances in Cryptology – ASIACRYPT 2019 (Cham) (Steven D. Galbraith and Shiho Moriai, eds.), Springer International Publishing, 2019, pp. 446–472.

Hao Chen, Wei Dai, Miran Kim, and Yongsoo Song, *Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference*, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA), CCS '19, Association for Computing Machinery, 2019, p. 395412.

Long Chen, Zhenfeng Zhang, and Xueqing Wang, *Batched multi-hop multi-key fhe from ring-lwe with compact ciphertext extension*, Theory of Cryptography (Cham) (Yael Kalai and Leonid Reyzin, eds.), Springer International Publishing, 2017, pp. 597–627.

Marc Joye and Pascal Paillier, *Blind rotation in fully homomorphic encryption with extended keys*, Cyber Security, Cryptology, and Machine Learning (Cham) (Shlomi Dolev, Jonathan Katz, and Amnon Meisels, eds.), Springer International Publishing, 2022, pp. 1–18.

Hyesun Kwak, Dongwon Lee, Yongsoo Song, and Sameer Wagh, *A unified framework of homomorphic encryption for multiple parties with non-interactive setup*, IACR Cryptol. ePrint Arch. **2021** (2021), 1412.

Yongwoo Lee, Daniele Micciancio, Andrey Kim, Rakyong Choi, Maxim Deryabin, Jieun Eom, and Donghoon Yoo, *Efficient flew bootstrapping withăsmall evaluation keys, andăapplications toăthreshold homomorphic encryption*, Advances in Cryptology – EUROCRYPT 2023 (Cham) (Carmit Hazay and Martijn Stam, eds.), Springer Nature Switzerland, 2023, pp. 227–256.

Hyang-Sook Lee and Jeongeun Park, *On the security of multikey homomorphic encryption*, Cryptography and Coding (Cham) (Martin Albrecht, ed.), Springer International Publishing, 2019, pp. 236–251.

- Chiara Marcolla, Victor Sucasas, Marc Manzano, Riccardo Bassoli, Frank H.P. Fitzek, and Najwa Aaraj, *Survey on Fully Homomorphic Encryption, Theory, and Applications*.
- Christian Mouchet, Juan Troncoso-Pastoriza, Jean-Philippe Bossuat, and Jean-Pierre Hubaux, *Multiparty homomorphic encryption from ring-learning-with-errors*, Proceedings on Privacy Enhancing Technologies **2021** (2021), 291–311.
- Jeongeun Park, *Homomorphic encryption for multiple users with less communications*, IEEE Access **PP** (2021), 1–1.