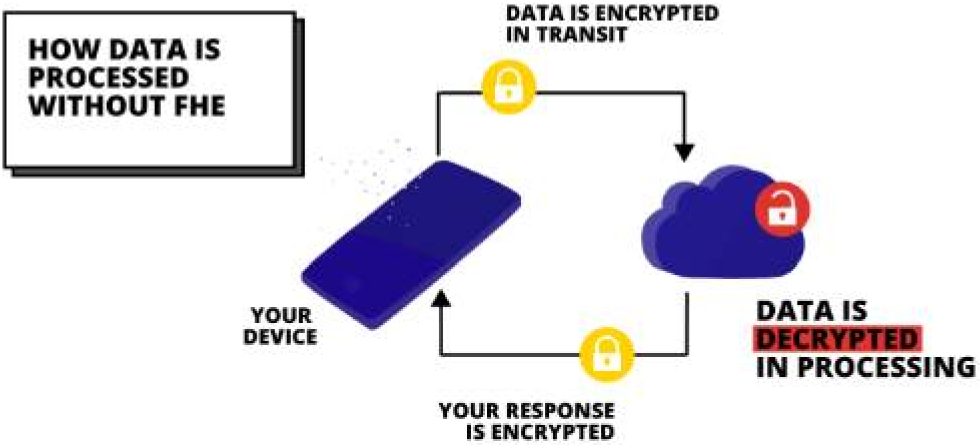
Secure and Efficient Outsourced Matrix Multiplication with Homomorphic Encryption

Aikata, Sujoy Sinha Roy
Graz University of Technology
Austria

aikata@iaik.tugraz.at

20-12-2024

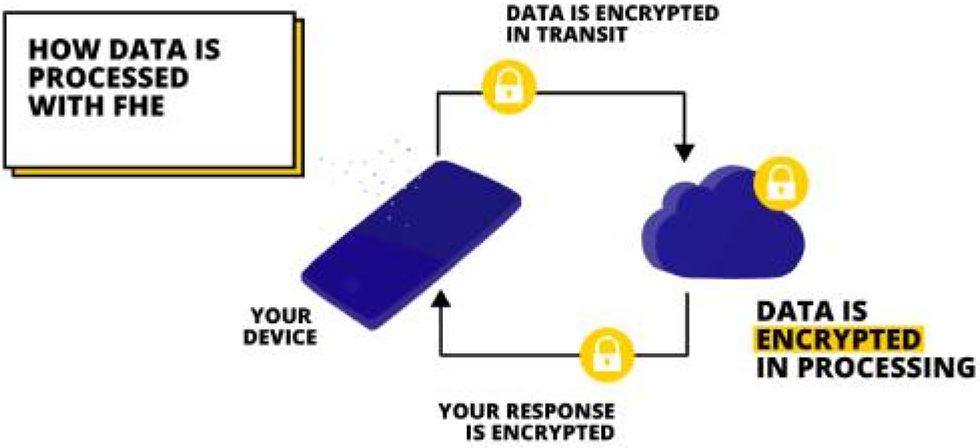
- Motivation
- Fully Homomorphic Encryption
- Machine Learning using FHE
- Our Solution
- Conclusion



Img src: https://www.zama.ai/post/the-revolution-of-fhe

https://huntsmansecurity.com/industries/critical-infrastructure/


New Cache Side Channel Attack Can De-Anonymize Targeted Online Users
Jul 15, 2022 Ravie Lakshmanan
NATIONAL
RITY
BANKING & FINANCE
Over 340 million accounts compromised in data breaches
More than 340 million people have been affected by business data breaches already in the first four months of 2023, according to new research by the Independent Advisor.
FOOD & GROCERY
HEALTH
Nearly 60% of firms have experienced a GDPR-related data breach in the past five years - new data published by iResearch Services - IFA Magazine
This week marks the five year anniversary of the EU's General Data Protection Regulation (GDPR), but new data published today by iResearch Services reveals that the regulation has been unsuccessful in preventing data breaches.
Paper: Stable Diffusion "memorizes" some images, sparking privacy concerns
Benj Edwards - 2/1/2023, 7:37 PM
DATA & CLOUD
Capita hit by new data breach incident
Colchester Council said files including benefits data were found on an unsecured Amazon Data Bucket controlled by the outsourcer
Twitter API security breach exposes 5.4 million users' data
PORT
SP
EDUCATION, RESEARCH & INNOVATION



Img src: https://www.zama.ai/post/the-revolution-of-fhe

- Motivation
- Fully Homomorphic Encryption
- Machine Learning using FHE
- Our Solution
- Conclusion

What is Homomorphic Encryption?

Homomorphism Property

* $\textsc{Additive} \Rightarrow \mathsf{Enc}(a) + \mathsf{Enc}(\mathsf{b}) = \mathsf{Enc}(a + b)$

Homomorphism Property

* Additive $\Rightarrow \mathsf{Enc}(a) + \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a + b)$
* Multiplicative $\Rightarrow \mathsf{Enc}(a) \cdot \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a \cdot b)$

Homomorphism Property

- $*$ Additive $\Rightarrow \mathsf{Enc}(a) + \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a + b)$
- $*$ Multiplicative $\Rightarrow \mathsf{Enc}(a) \cdot \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a \cdot b)$

- RSA, ECC, are only additively homomorphic.

Homomorphism Property

* $*$ ADDITIVE $\Rightarrow \mathsf{Enc}(a) + \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a + b)$
* $*$ MULTIPLICATIVE $\Rightarrow \mathsf{Enc}(a) \cdot \mathsf{Enc}(\mathrm{b}) = \mathsf{Enc}(a \cdot b)$

- RSA, ECC, are only additively homomorphic.
- They are also Post-Quantum **Insecure**. (Thanks to Peter Shor [1994])

The LWE Hard Problem [Oded Regev, Goedel prize 2018]

The LWE Hard Problem [Oded Regev, Goedel prize 2018]

Given $A \in \mathbb{Z}_q^{m \times n}, e \in \mathcal{U}$

Given- $A \cdot s + e$, it is *hard* to retrieve s.

where, $s \in \mathbb{Z}_q^n$

The LWE Hard Problem [Oded Regev, Goedel prize 2018]

Given $A \in \mathbb{Z}_q^{m \times n}, e \in \mathcal{U}$

Given- $A \cdot s + e$, it is *hard* to retrieve s.

where, $s \in \mathbb{Z}_q^n$

✓ This problem remains secure in a Post-Quantum scenario.

Fully Homomorphic Encryption

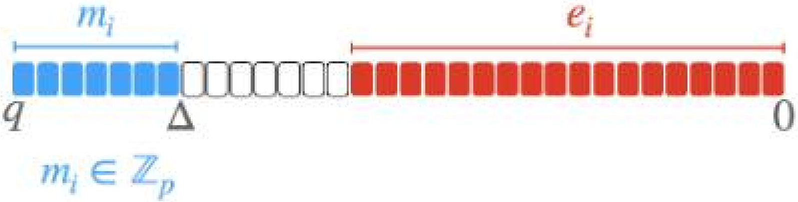
- LWE sample: $A \cdot s + e$

Fully Homomorphic Encryption

- LWE sample: $A \cdot s + e$
- Encryption: $A \cdot s + e + m \cdot \Delta$

Fully Homomorphic Encryption

- LWE sample: $A \cdot s + e$
- Encryption: $A \cdot s + e + m \cdot \Delta$



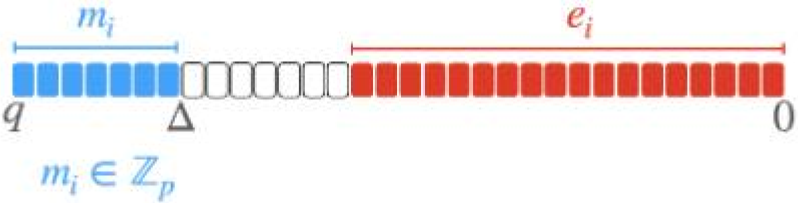
Img src: https://www.zama.ai/

Fully Homomorphic Encryption

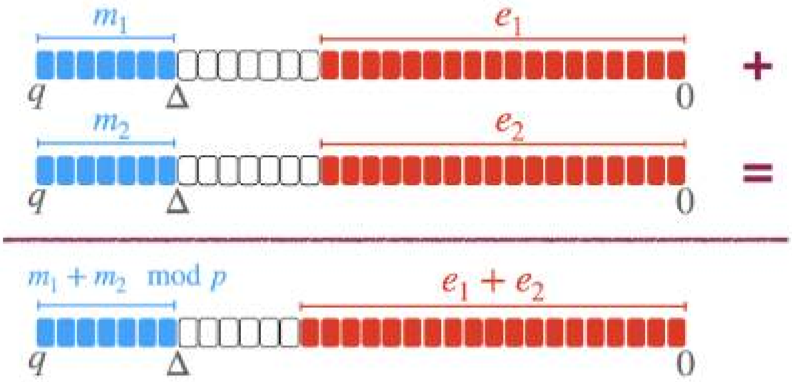
- LWE sample: $A \cdot s + e$
- Encryption: $A \cdot s + e + m \cdot \Delta$
- **Ciphertext**: $\{-A, A \cdot s + e + m \cdot \Delta\}$

Fully Homomorphic Encryption

- LWE sample: $A \cdot s + e$
- Encryption: $A \cdot s + e + m \cdot \Delta$
- **Ciphertext**: $\{-A, A \cdot s + e + m \cdot \Delta\}$
- Decryption: $\mathrm{rnd}(\{-A \cdot s + A \cdot s + \mathbf{e} + \mathbf{m} \cdot \Delta\})$

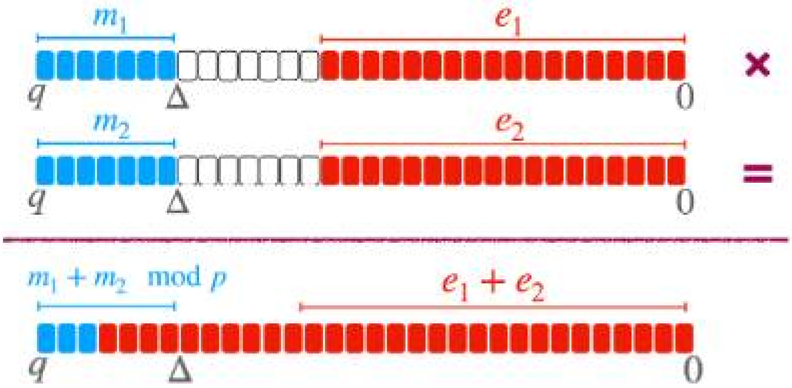


Additive Homomorphism

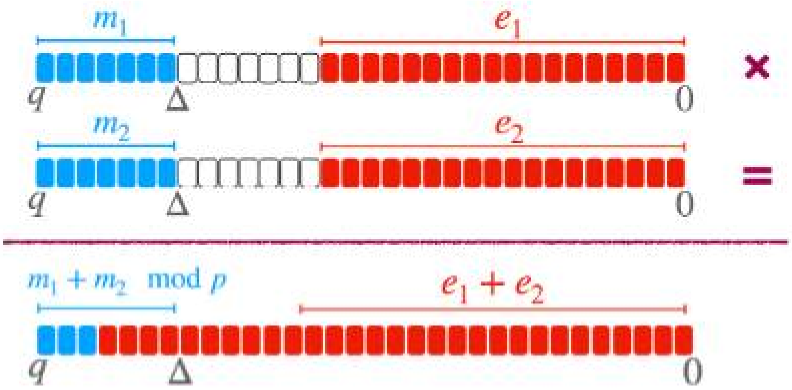


Img src: https://www.zama.ai/

Multiplicative Homomorphism



Multiplicative Homomorphism



KeySwitching+Scaling is done to restore the en/decryption+message-error barrier.

Img src: https://www.zama.ai/

Multiplicative Homomorphism

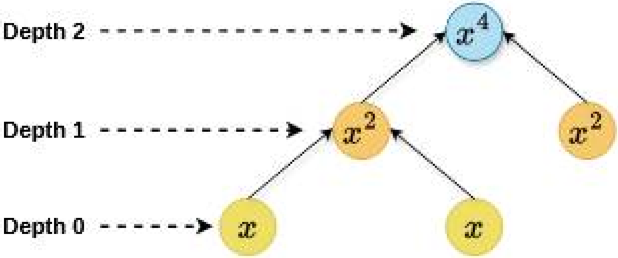
- KeySwitching is **expensive**.

Multiplicative Homomorphism

- KeySwitching is **expensive**.
- Scaling reduces the **computation depth**.

Multiplicative Homomorphism

- KeySwitching is **expensive**.
- Scaling reduces the **computation depth**.



Fully Homomorphic Encryption in Practice

Schemes used: [CKKS'17], [BGV'14], [Bra12, FV12] (RingLWE)

Fully Homomorphic Encryption in Practice

Schemes used: **[CKKS'17]**, [BGV'14], [Bra12, FV12] (RingLWE)

Operation supported: $+, \{\times, \ll, \gg\} \to \text{KeySwitch}$

Fully Homomorphic Encryption in Practice

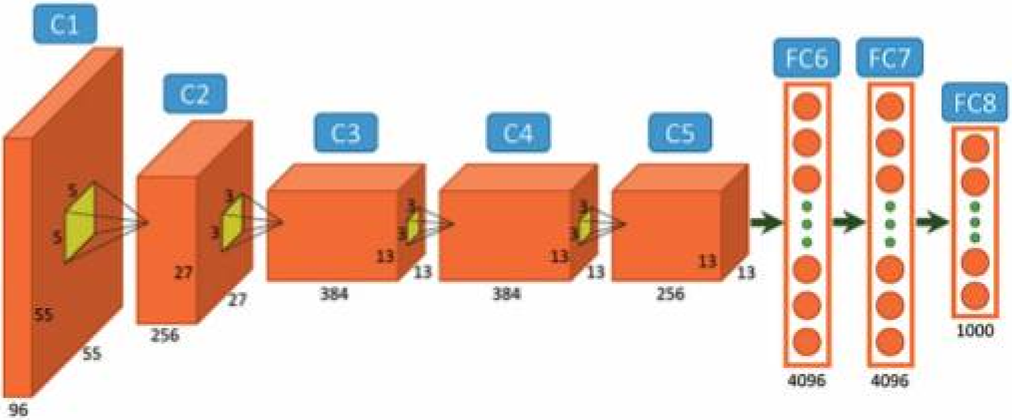
Schemes used: **[CKKS'17]**, [BGV'14], [Bra12, FV12] (RingLWE)

Operation supported: $+$, $\{\times, \ll, \gg\} \rightarrow$ KeySwitch

Application Goal: Reduce Depth consumption and #KeySwitch operations.

- Motivation
- Fully Homomorphic Encryption
- Machine Learning using FHE
- Our Solution
- Conclusion

Matrix Multiplication and Neural Networks

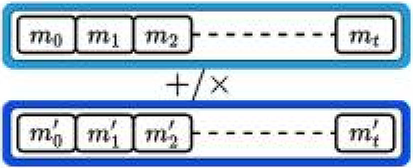


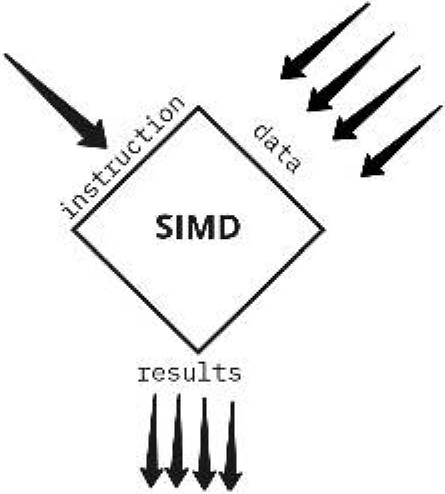
Img src:https://viso.ai/deep-learning/alexnet/

Prior Works

Methodology	Packing	# ct-ct Mult	# Rotations	Depth
Naive	1	$\mathcal{O}(d^3)$	-	2
[WaH19,LKS17]	d	$\mathcal{O}(d^2)$	$\mathcal{O}(d^2 \log_2 d)$	2
[RizT22]	d^3	$\mathcal{O}(1)$	$\mathcal{O}(d)$	2
[JKLS18]	d^2, d^3	$\mathcal{O}(d)$	$\mathcal{O}(d)$	3
[CKY18]	d^2	$\mathcal{O}(d)$	$\mathcal{O}(d \log_2 d)$	2

Encrypted Matrix Multiplication





Encrypted Matrix Multiplication

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} e & f \\ g & h \end{bmatrix} \longrightarrow \begin{bmatrix} a & a \\ c & c \end{bmatrix} \bullet \begin{bmatrix} e & f \\ e & f \end{bmatrix} + \begin{bmatrix} b & b \\ d & d \end{bmatrix} \bullet \begin{bmatrix} g & h \\ g & h \end{bmatrix}$$

Encrypted Matrix Multiplication [RizT22]

a	b	c	d

Encrypted Matrix Multiplication [RizT22]

$$\begin{array}{|c|c|c|c|}\hline a & b & c & d \\ \hline\end{array} \quad \bullet \quad \begin{array}{|c|c|c|c|}\hline 1 & 0 & 0 & 0 \\ \hline\end{array}$$

Encrypted Matrix Multiplication [RizT22]

$$
\begin{array}{ccc}
\boxed{a}\boxed{b}\boxed{c}\boxed{d} & \cdot & \boxed{1}\boxed{0}\boxed{0}\boxed{0} \\
\boxed{a}\boxed{b}\boxed{c}\boxed{d} & \cdot & \boxed{0}\boxed{1}\boxed{0}\boxed{0} \\
\vdots & & \vdots
\end{array}
$$

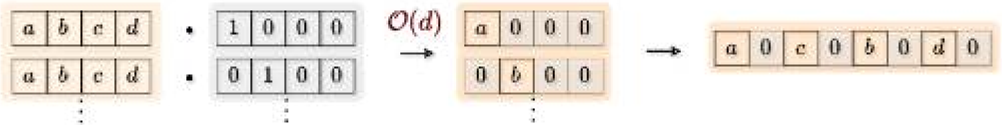
Encrypted Matrix Multiplication [RizT22]

$$\begin{matrix}
\begin{array}{|c|c|c|c|}\hline a & b & c & d \\ \hline\end{array} & \cdot & \begin{array}{|c|c|c|c|}\hline 1 & 0 & 0 & 0 \\ \hline\end{array} & & \begin{array}{|c|c|c|c|}\hline a & 0 & 0 & 0 \\ \hline\end{array} \\
\begin{array}{|c|c|c|c|}\hline a & b & c & d \\ \hline\end{array} & \cdot & \begin{array}{|c|c|c|c|}\hline 0 & 1 & 0 & 0 \\ \hline\end{array} & \longrightarrow & \begin{array}{|c|c|c|c|}\hline 0 & b & 0 & 0 \\ \hline\end{array} \\
\vdots & & \vdots & & \vdots
\end{matrix}$$

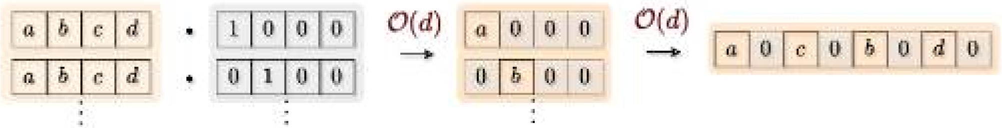
Encrypted Matrix Multiplication [RizT22]

$$
\begin{array}{ccccc}
\boxed{a \mid b \mid c \mid d} & \cdot & \boxed{1 \mid 0 \mid 0 \mid 0} & \xrightarrow{\mathcal{O}(d)} & \boxed{a \mid 0 \mid 0 \mid 0} \\
\boxed{a \mid b \mid c \mid d} & \cdot & \boxed{0 \mid 1 \mid 0 \mid 0} & & \boxed{0 \mid b \mid 0 \mid 0} \\
\vdots & & \vdots & & \vdots
\end{array}
$$

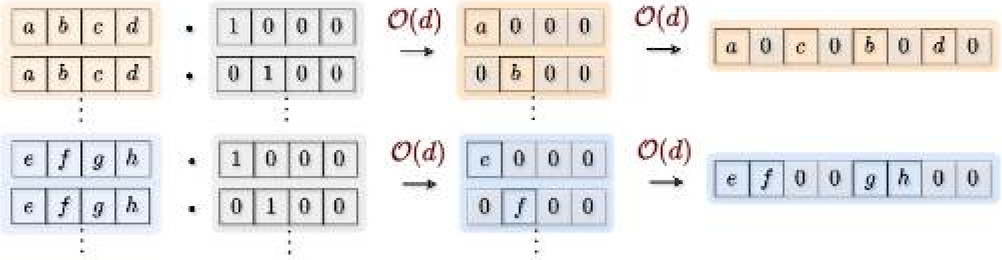
Encrypted Matrix Multiplication [RizT22]



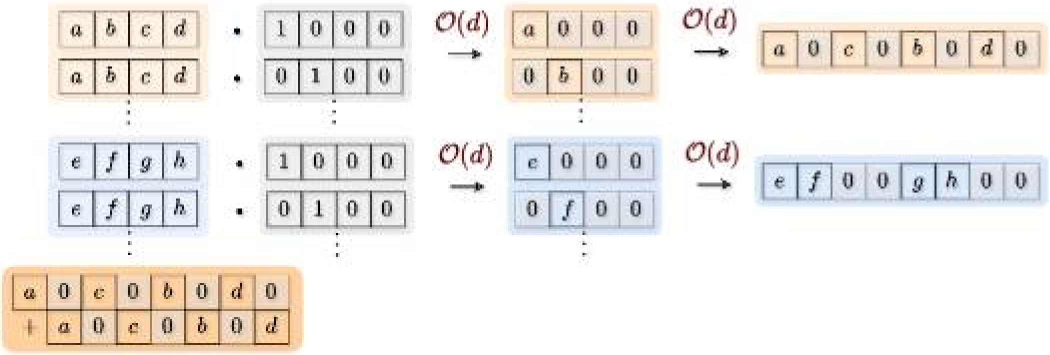
Encrypted Matrix Multiplication [RizT22]



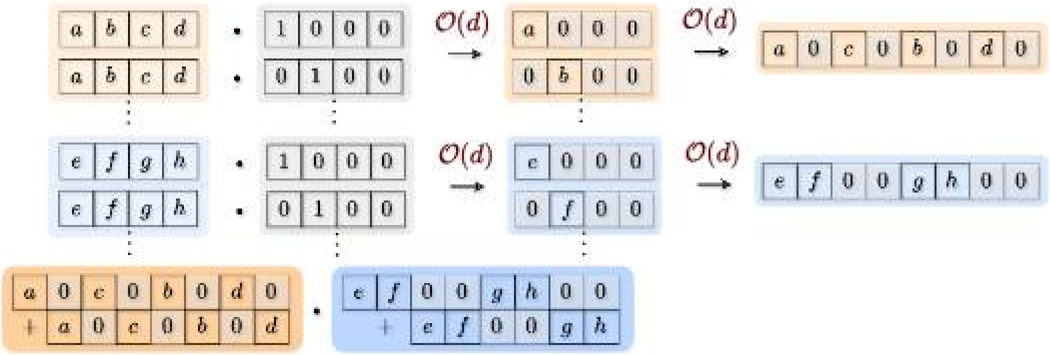
Encrypted Matrix Multiplication [RizT22]



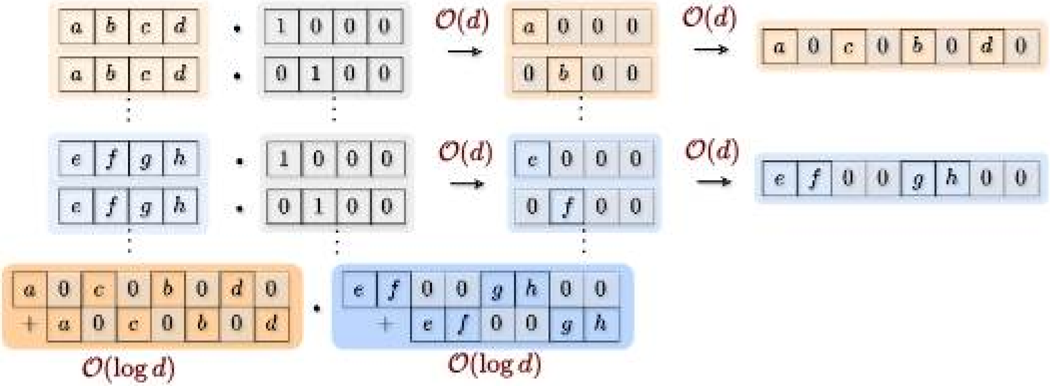
Encrypted Matrix Multiplication [RizT22]



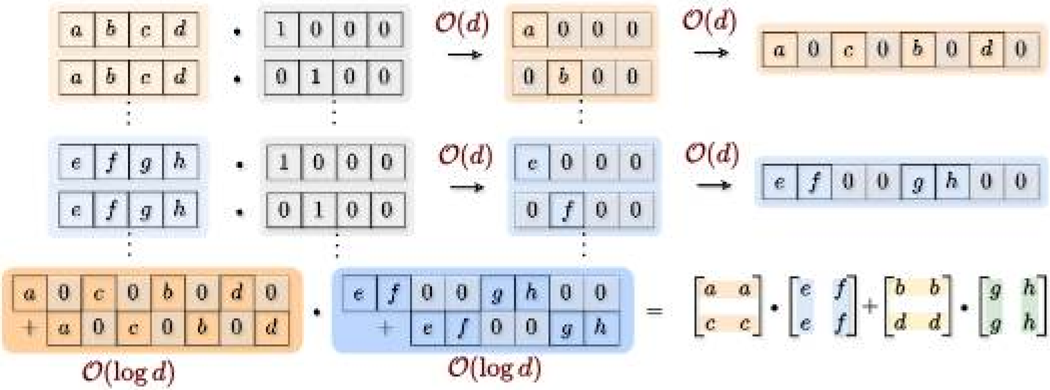
Encrypted Matrix Multiplication [RizT22]



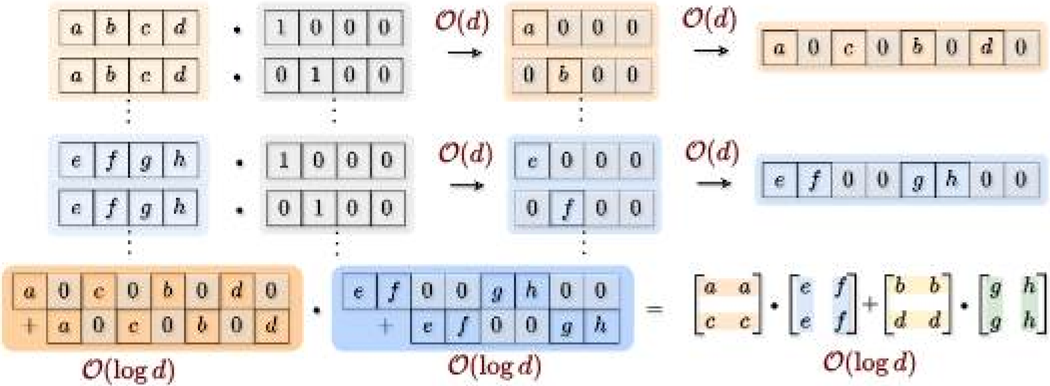
Encrypted Matrix Multiplication [RizT22]



Encrypted Matrix Multiplication [RizT22]



Encrypted Matrix Multiplication [RizT22]



- Motivation
- Fully Homomorphic Encryption
- Machine Learning using FHE
- **Our Solution**
- Conclusion

Encrypted Matrix Multiplication

a	b	c	d

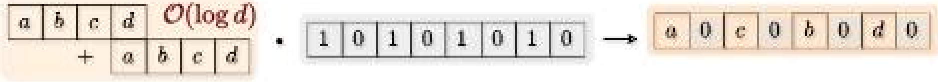
Encrypted Matrix Multiplication

a	b	c	d			
		$+$	a	b	c	d

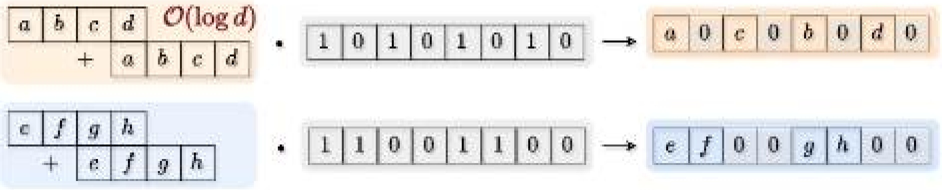
Encrypted Matrix Multiplication

$$\begin{array}{ccccccc} a & b & c & d & & & \\ & & + & a & b & c & d \end{array} \cdot \begin{bmatrix}1&0&1&0&1&0&1&0\end{bmatrix} \longrightarrow \begin{bmatrix} a&0&c&0&b&0&d&0\end{bmatrix}$$

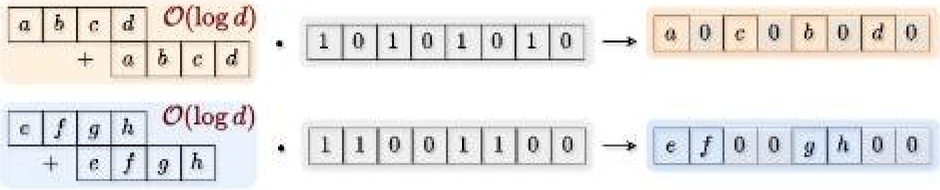
Encrypted Matrix Multiplication



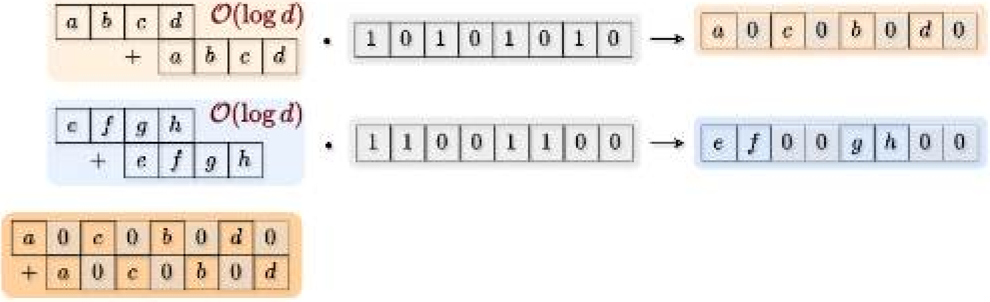
Encrypted Matrix Multiplication



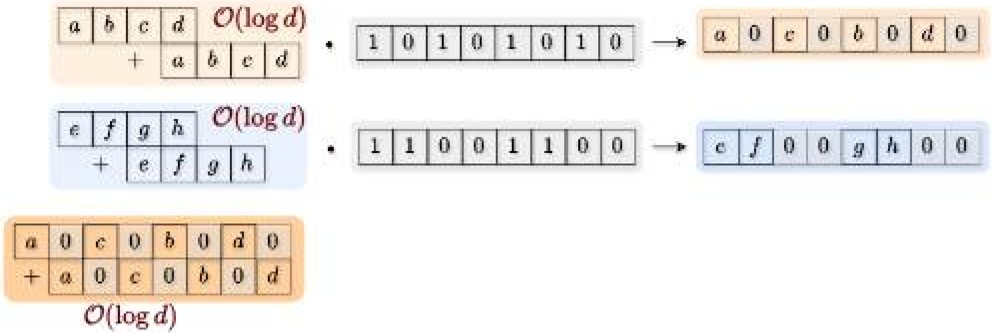
Encrypted Matrix Multiplication



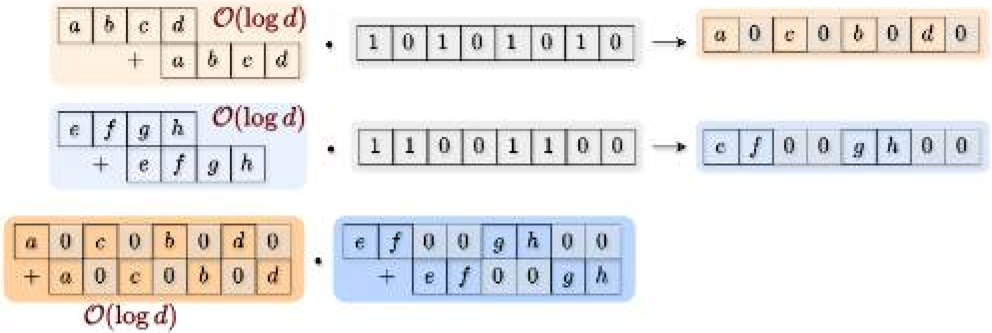
Encrypted Matrix Multiplication



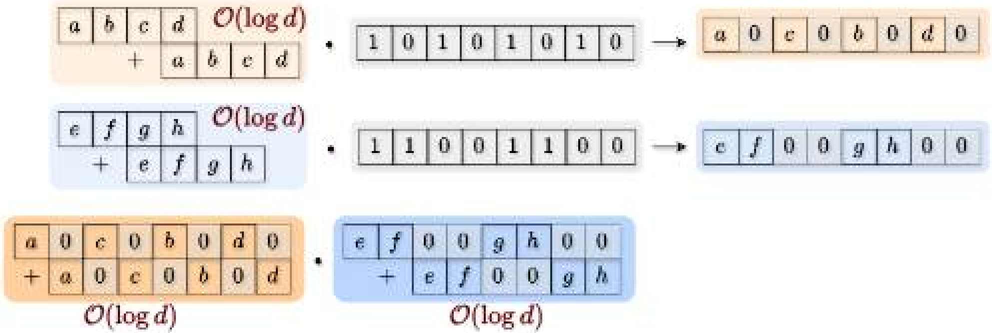
Encrypted Matrix Multiplication



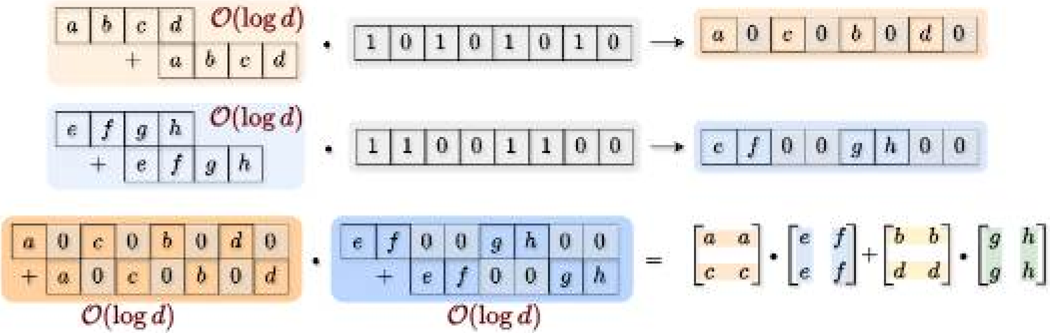
Encrypted Matrix Multiplication



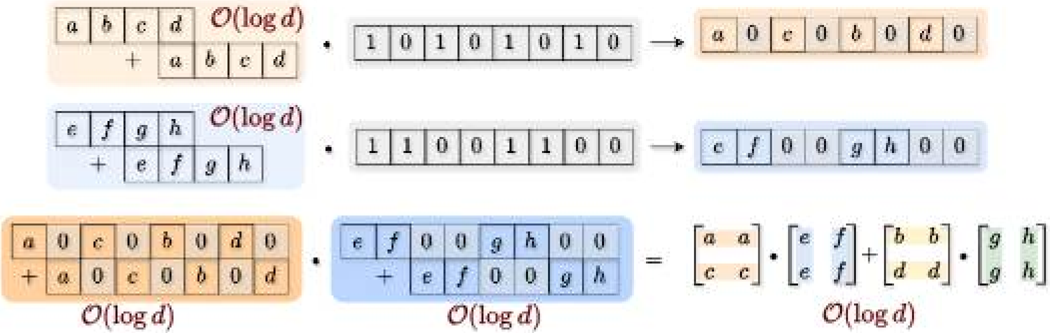
Encrypted Matrix Multiplication



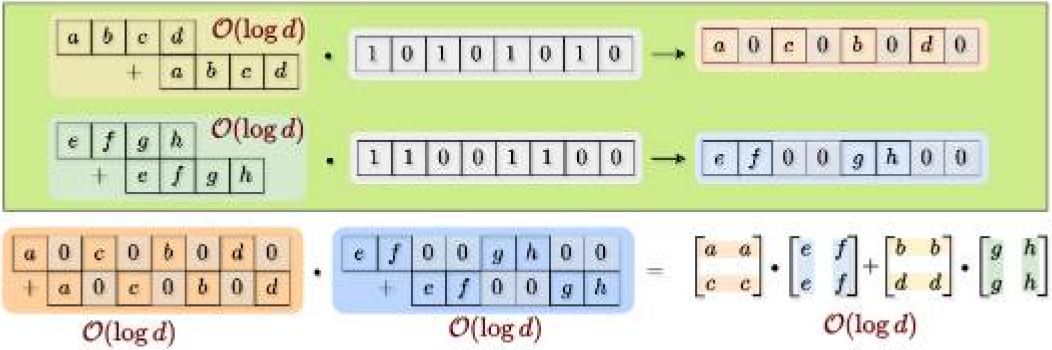
Encrypted Matrix Multiplication



Encrypted Matrix Multiplication



Encrypted Matrix Multiplication



Results

Packing	#pt-ct Mult	#ct-ct Mult	#Rotations	Depth
d^2	$2 \cdot d$	d	$2 \cdot d(1 + \log_2 d) - 2$	2
$2 \cdot d^2$	d	$\frac{d}{2}$	$d(1 + \log_2 d) + 1$	2
$4 \cdot d^2$	$\frac{d}{2}$	$\frac{d}{4}$	$\frac{d}{2}(1 + \log_2 d) + 4$	2
d^3	2	1	$5 \cdot \log_2 d$	2

Comparisons

Methodology	Packing	# ct-ct Mult	# Rotations	Depth
Naive	1	$\mathcal{O}(d^3)$	-	2
[WaH19,LKS17]	d	$\mathcal{O}(d^2)$	$\mathcal{O}(d^2 \log_2 d)$	2
This Work	$\mathbf{d^2}$	$\mathcal{O}(\mathbf{d})$	$\mathcal{O}(\mathbf{d} \log_2 \mathbf{d})$	**2**
[RizT22]	d^3	$\mathcal{O}(1)$	$\mathcal{O}(d)$	2
This Work	$\mathbf{d^3}$	$\mathcal{O}(\mathbf{1})$	$\mathcal{O}(\log_2 \mathbf{d})$	**2**
[JKLS18]	d^2, d^3	$\mathcal{O}(d)$	$\mathcal{O}(d)$	3
[CKY18]	d^2	$\mathcal{O}(d)$	$\mathcal{O}(d \log_2 d)$	2

Matrix Multiplication

The article details the solution provided by the winner of the Matrix Multiplication Challenge.

Author: Aikata, Ph.D. student at TU Graz

Matrix multiplication is a crucial aspect of advanced mathematics and plays a central role in machine learning, especially in Neural Networks. Certain network components, like fully connected layers or filter/kernel, rely on matrix multiplication. Though there are efficient algorithms like Strassen's algorithm for plaintext operations, conducting matrix multiplication in an encrypted domain is a newer research area. This has gained attention because it enables encrypted ML training or inference

Blog: `https://hackmd.io/iuy3lJX2RfCHJJs03pLc5w`

- Motivation
- Fully Homomorphic Encryption
- Machine Learning using FHE
- Our Solution
- Conclusion

Conclusion

1. **Efficiency and Generalization**: This work significantly reduces key-switch complexity to $\mathbb{O}(\log d)$, enhancing computational efficiency and generalizing secure matrix multiplication across diverse packing scenarios.

Conclusion

1. **Efficiency and Generalization:** This work significantly reduces key-switch complexity to $\mathcal{O}(\log d)$, enhancing computational efficiency and generalizing secure matrix multiplication across diverse packing scenarios.

2. **Foundation for Privacy-Preserving Applications:** The proposed techniques optimize FHE component routines, enabling scalable and efficient solutions for secure neural network evaluations and similar privacy-centric computations.

Secure and Efficient Outsourced Matrix Multiplication with Homomorphic Encryption

Aikata, Sujoy Sinha Roy
Graz University of Technology
Austria

aikata@iaik.tugraz.at

20-12-2024