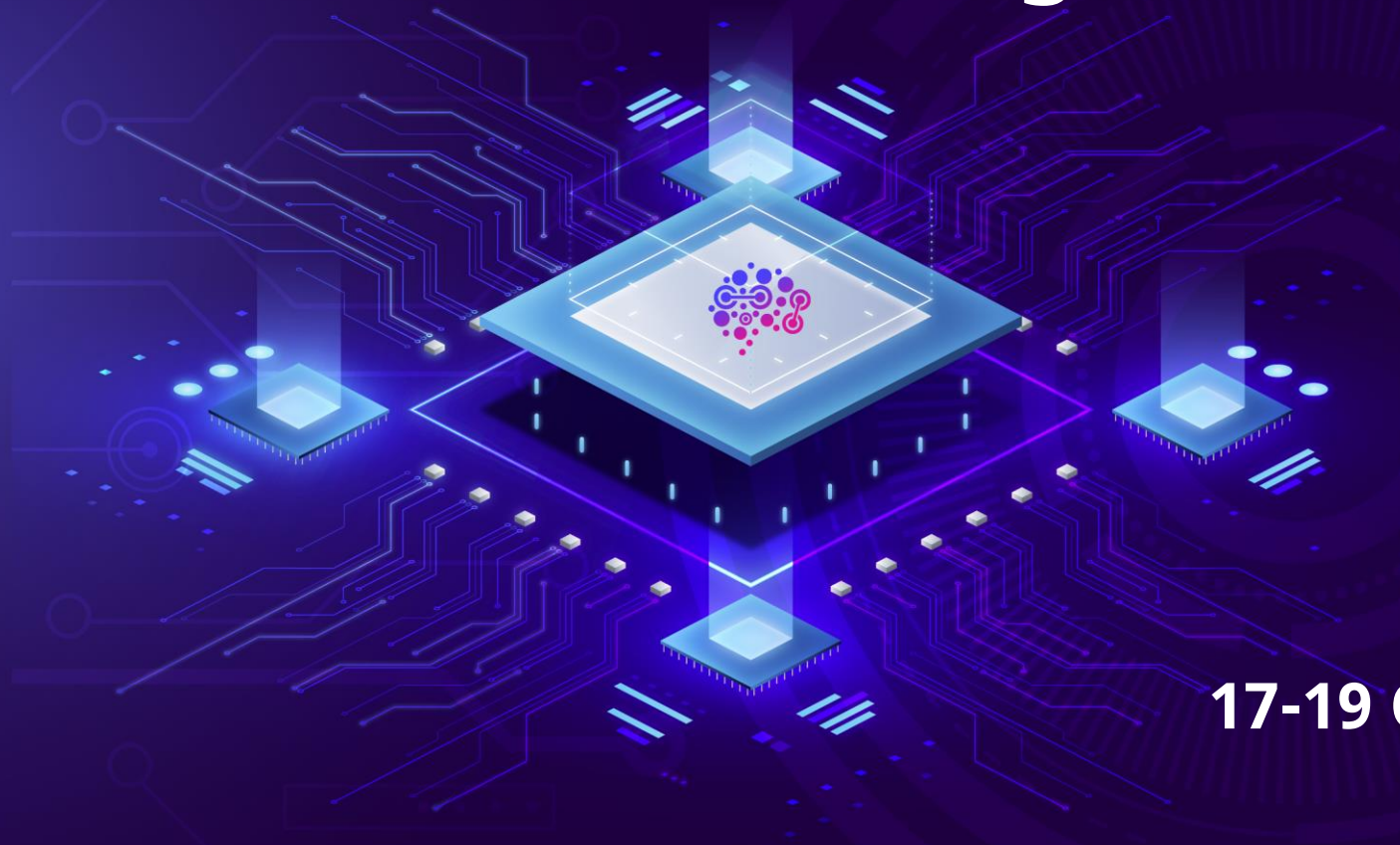
European Conference on EDGE AI Technologies and Applications - EEAI



Advancing emerging edge AI technologies and driving next generation intelligent applications.

17-19 October 2023, Athens, Greece

European Conference on EDGE AI Technologies and Applications - EEAI

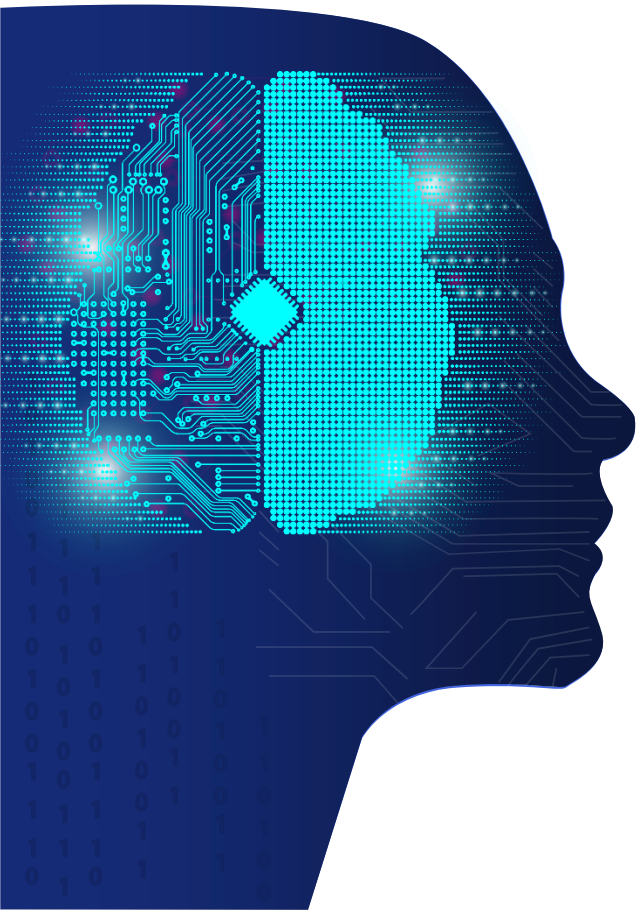
Approximate Computing in a FL Context: Gains beyond Energy

Ihsen Alouani,
CNRS, France

17-19 October 2023 Athens, Greece

Copyright © 2023

Presentation Outline

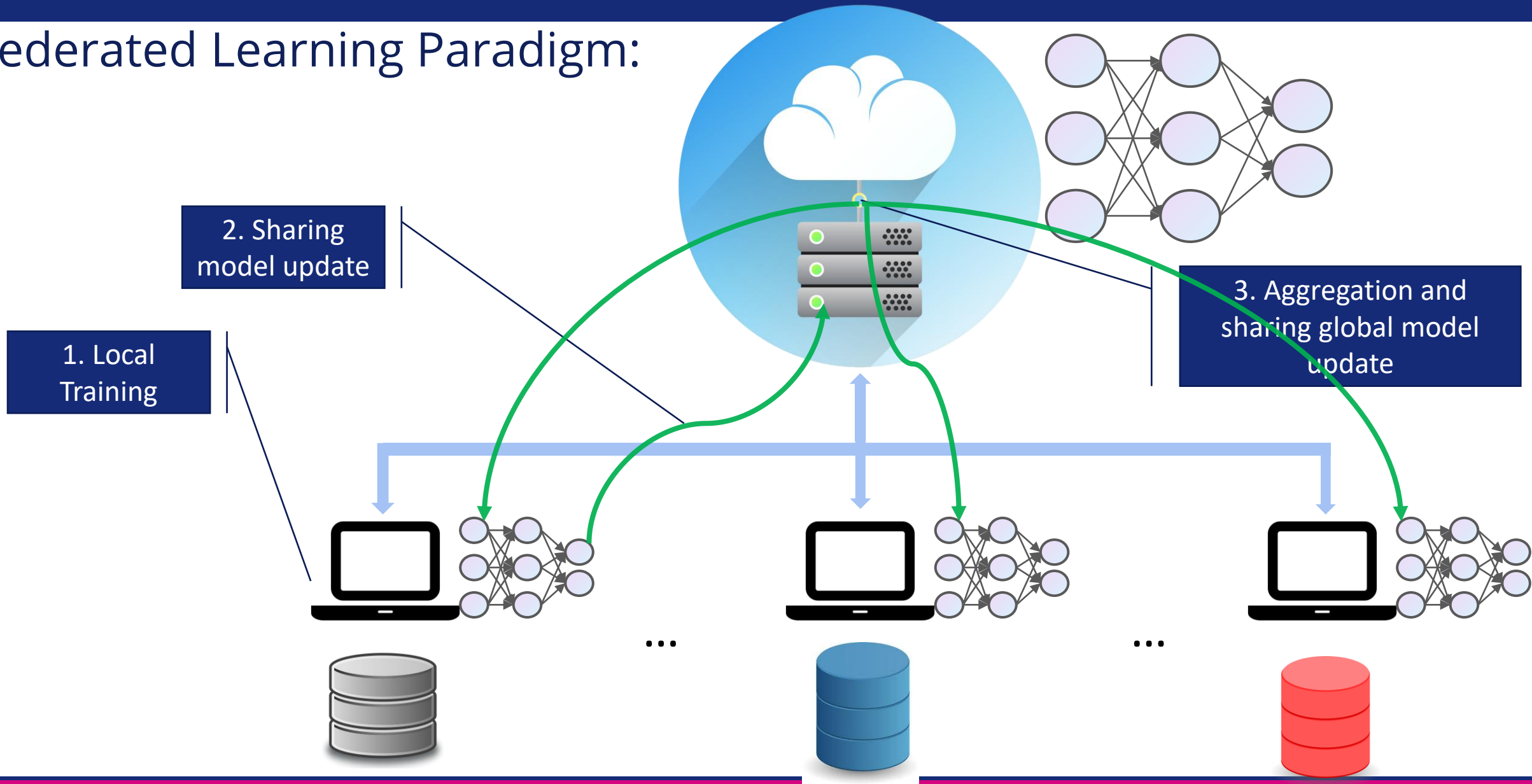


- Introduction
- Threat Model
- Research Goals
- Methodology
- Experimental Results
- Future Research
- Conclusion

Copyright © 2023

Introduction (1)

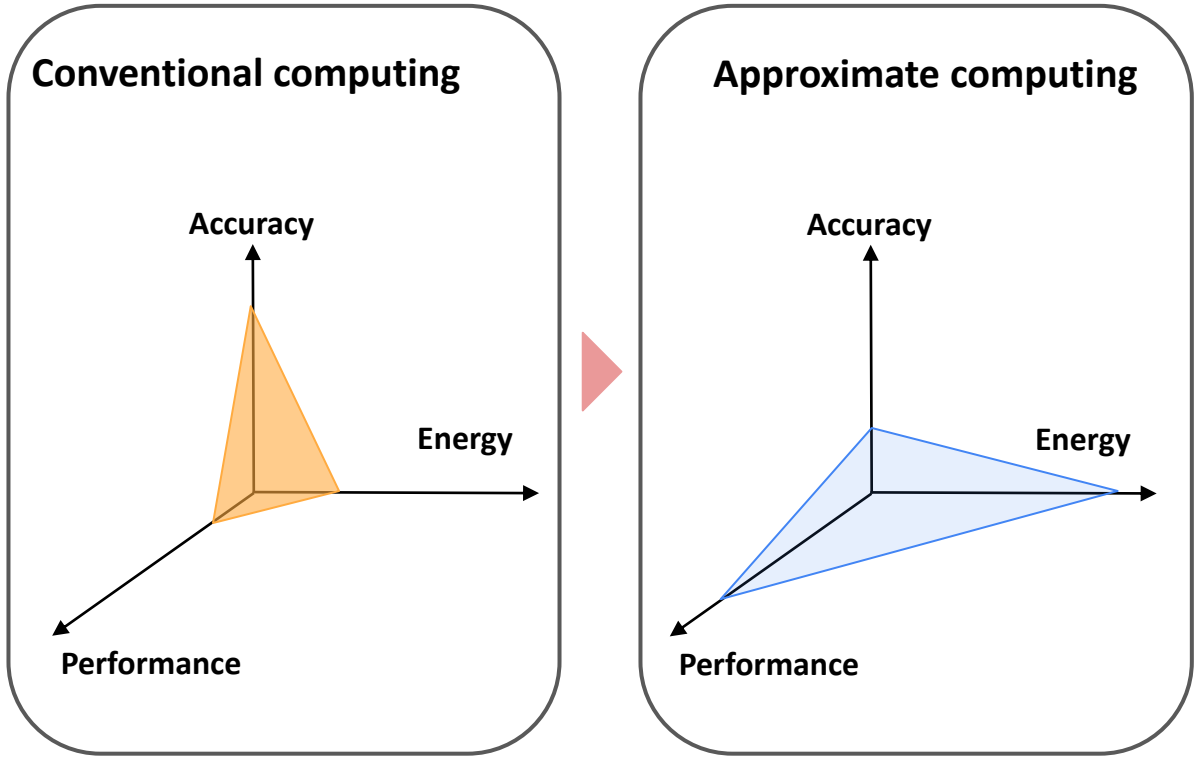
- Federated Learning Paradigm:

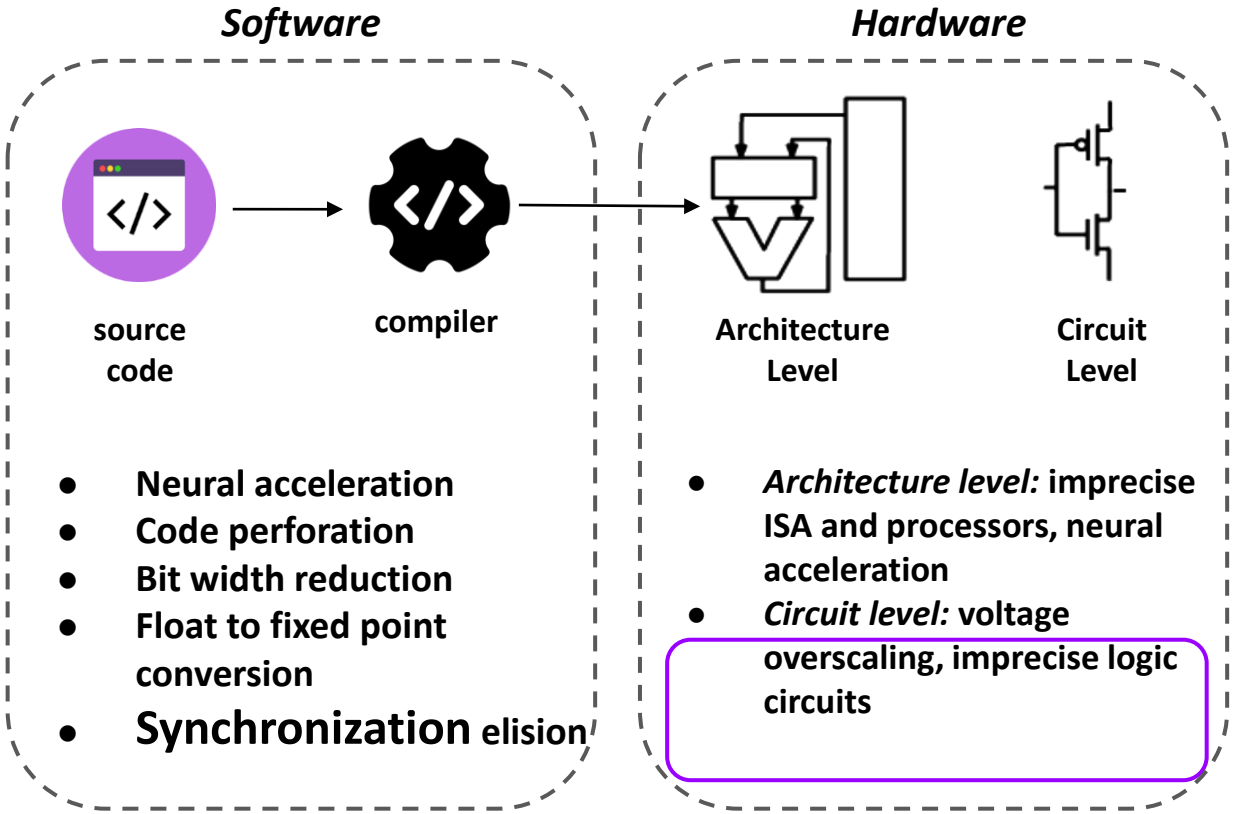


Copyright © 2023

Introduction (2)

- Approximate Computing Paradigm:





→ Allows more effective approximation

Copyright © 2023

Securing the AI is fundamental to develop trustworthy systems

European Union Agency for Cybersecurity (ENISA)
"AI Threat Landscape Report"

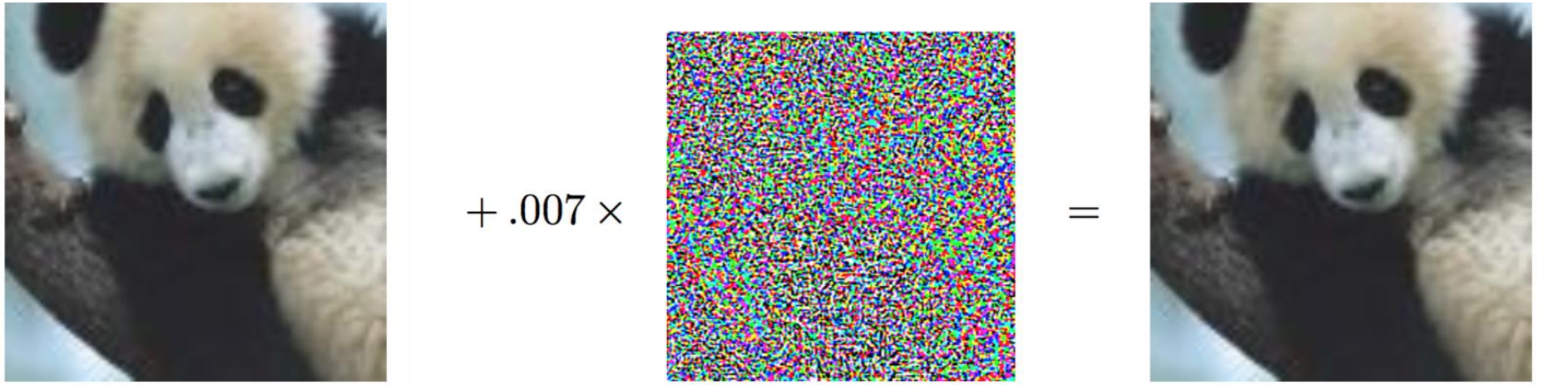
Copyright © 2023

What are Adversarial Attacks?

Copyright © 2023

What are Adversarial Attacks?

Carefully crafted imperceptible noise, that forces the model to misclassify when added to an input



$\boldsymbol{x}$

"panda"
57.7% confidence

$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

"nematode"
8.2% confidence

$\boldsymbol{x} + \epsilon\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

"gibbon"
99.3 % confidence

Copyright © 2023

How Adversarial noise is generated?

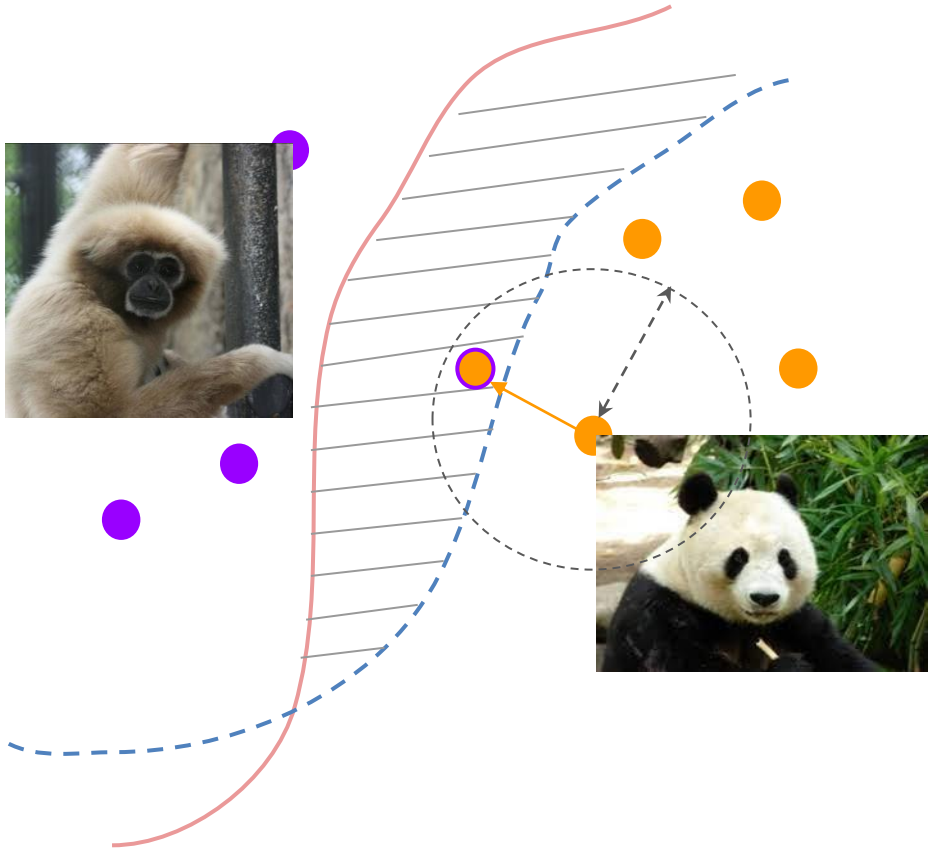
Given a sample *x*, labeled by a classifier $C(x) = l$

Create $x_{adv} = x + \delta$, such that the distance $D(x, x_{adv})$ is minimal AND the classifier assigns a different label than l, i.e.,

$$C(x_{adv}) = C(x + \delta) = l^* \neq l$$

Copyright © 2023

Intuition of Adversarial Examples



- Most attacks try to move inputs across the decision boundary by adding small and carefully crafted noise.
- The resulting image is correctly classified by a human but misclassified by a DL system

Copyright © 2023

Adversarial attacks IRL

The adversarial noise is now constrained by:

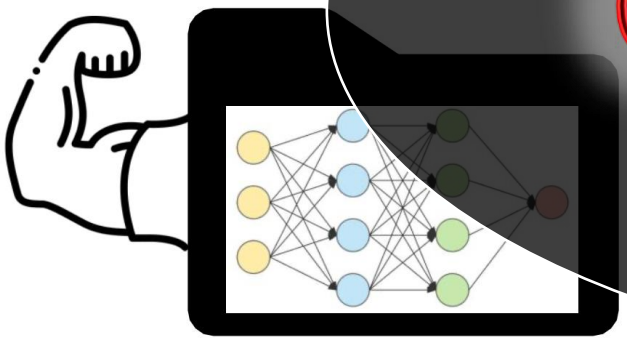
- Limitation in space
- Printability

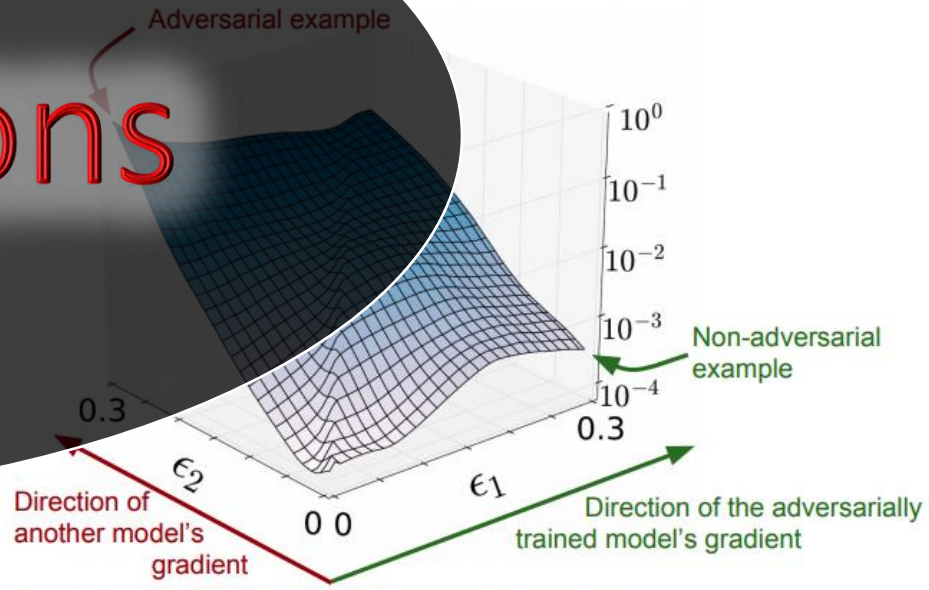
Copyright © 2023

Defense Mechanisms

- Adversarial Training
- Input Filtering
- Gradient Masking

Costly Solutions





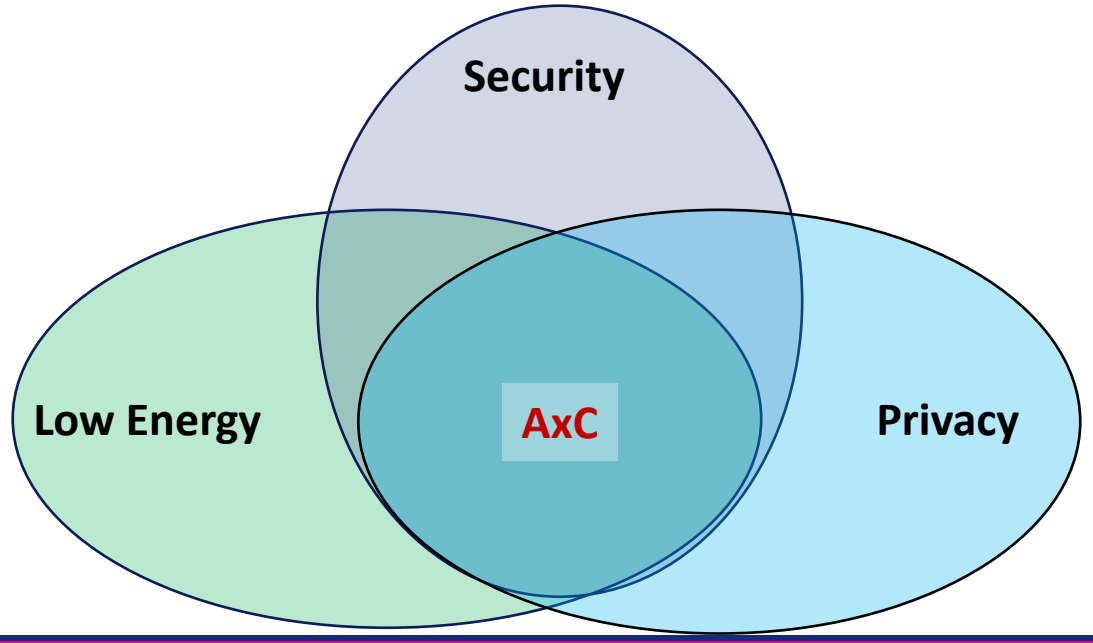
Tramèr et al. *Ensemble Adversarial Training: Attacks and Defenses*
Illustration adapted from slides by Florian Tramèr

Copyright © 2023

Research Objective

- We ask the following research questions:

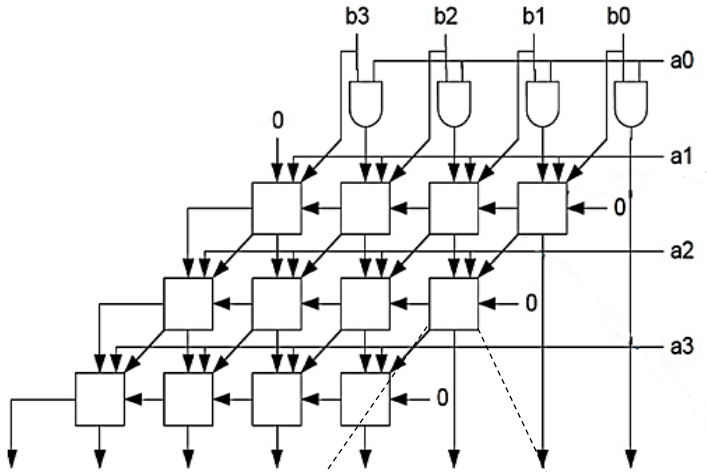
1. Can FL still converge if some of the nodes (or all) are approximate?
2. Can we obtain higher privacy-preserving in FL with AxC ?
3. Can we have more robust (global) models with AxC ?

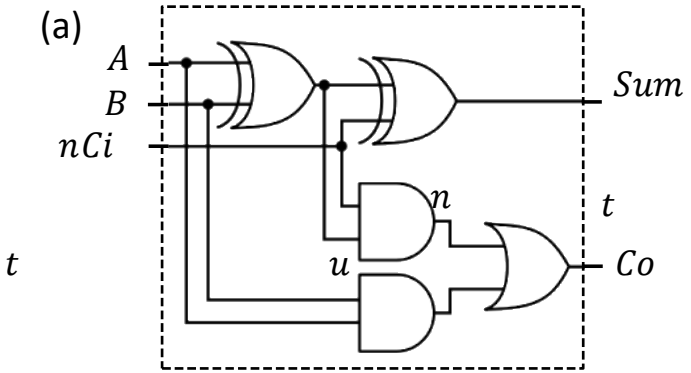


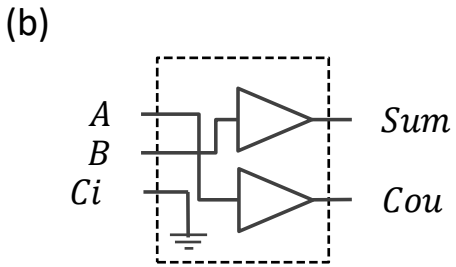
Copyright © 2023

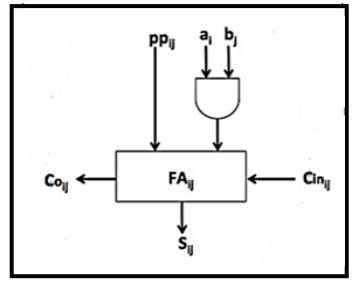
Floating Point Multiplier

- A 24x24-bit Array Multiplier for the **Mantissa**
- Relatively high resource utilization and energy consumption





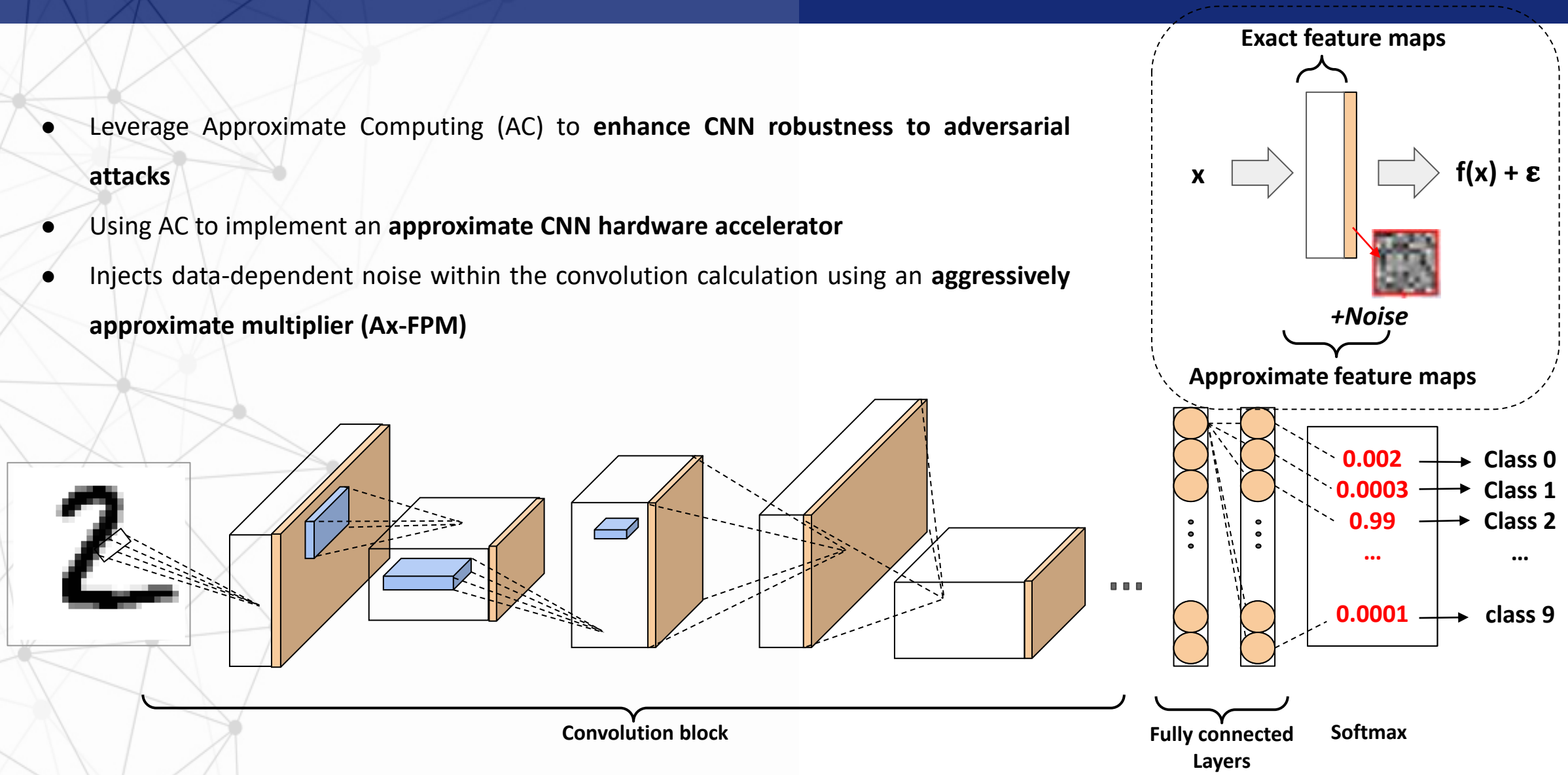




Copyright © 2023

Proposed Defense Mechanism

- Leverage Approximate Computing (AC) to **enhance CNN robustness to adversarial attacks**
- Using AC to implement an **approximate CNN hardware accelerator**
- Injects data-dependent noise within the convolution calculation using an **aggressively approximate multiplier (Ax-FPM)**



Copyright © 2023

Robustness Results (1 node)

Attack success rate for MNIST

Attack method	Exact LeNet-5	Approximate LeNet-5
FGSM	100%	22%
PGD	100%	0%
C&W	100%	0%
DF	100%	25%
LSA	100%	26%
HSJ	100%	0%

Transferability results for CIFAR-10

Attack	Exact AlexNet	Approximate AlexNet
FGSM	100%	38%
PGD	100%	31%
C&W	100%	17%
DF	100%	35%
LSA	100%	36%
HSJ	100%	12%

Copyright © 2023

Performance Results

Impact on Model Accuracy

Used Multiplier	MNIST	CIFAR-10
Float32	97.93%	81%
Approximate (DA)	97.67%	80%
Fully quantized	-	80%
Weight-only quantized	-	80%
BFloat16	97.93%	81%

Minimal to negligible impact on model accuracy

- Up to **51%** energy saving
- Up to **71%** reduction in delay

Reduced Energy

Reduced Latency

Copyright © 2023

Road Ahead: Approximate Computing in FL

- Instead of conventional nodes, we are using approximate nodes in a FL setting
- We are studying the learning of aggregated model as a function of the number of approximate nodes
- Considering **Privacy attacks** (Membership Inference, Leakage from Gradient, etc.)
- Consider Approximate **Quantized** nodes

Copyright © 2023

Conclusion

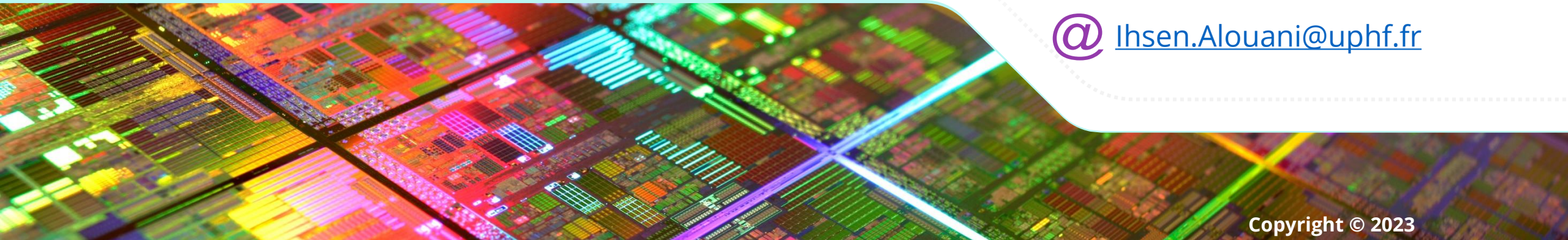
- We aim for Edge-compatible Trustworthy ML solutions
- We consider 3 objectives in our design
  - Security
  - Privacy
  - Low power
- Approximate Computing scope is wide and ground needs to be broken in this direction for Edge

Copyright © 2023

EDGE AI

Thank You

For your attention



@ Ihsen.Alouani@uphf.fr

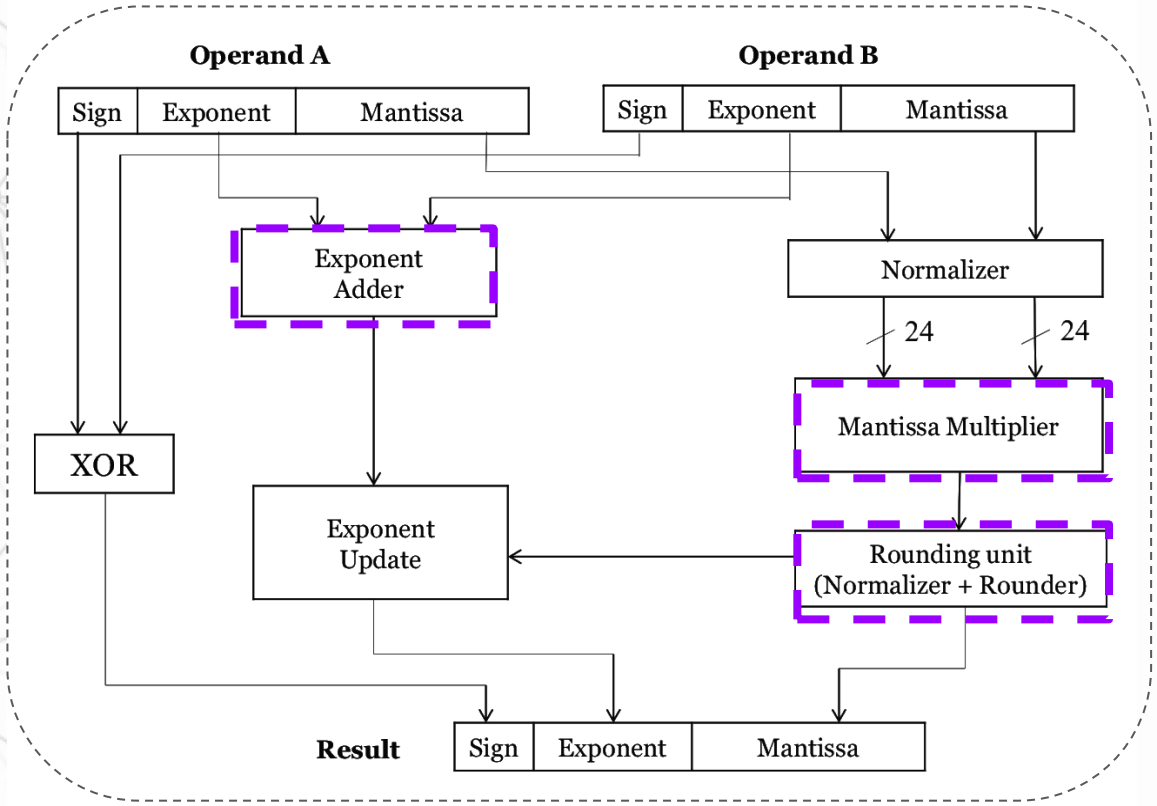
Copyright © 2023

Floating Point Multiplier

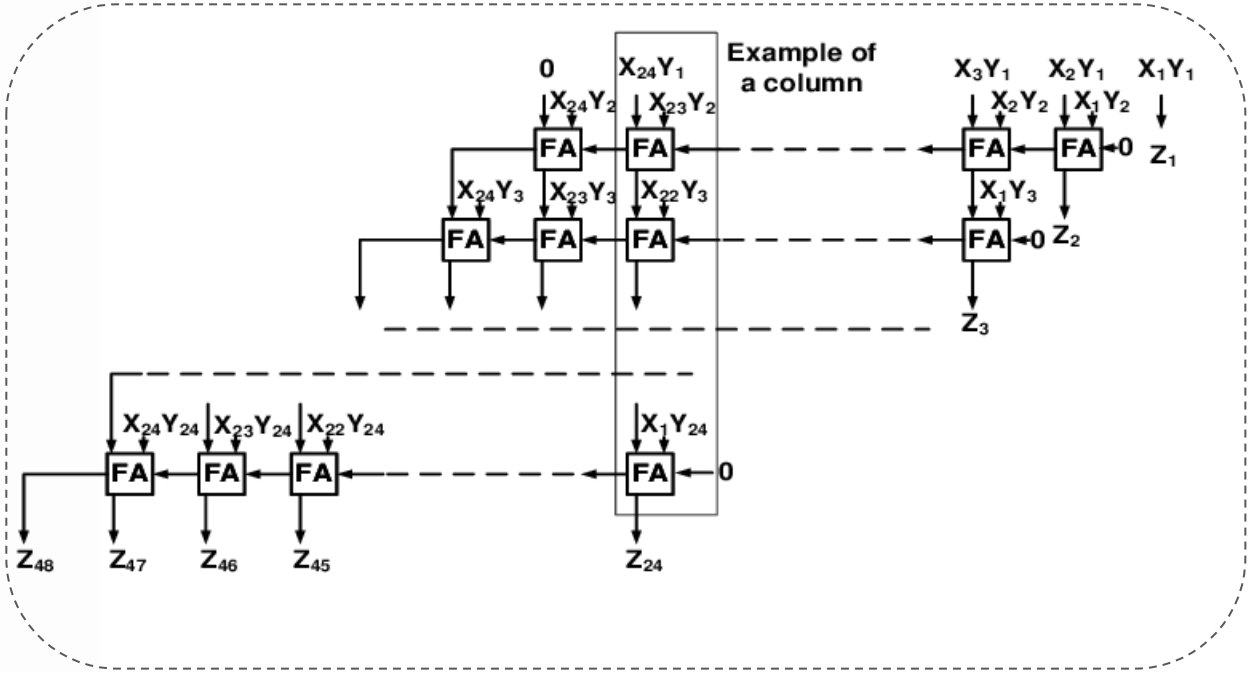
Decimal Number: -7.5

IEEE 754 single precision FP Representation: 1 (Sign) 10000001 (Exponent) 11100000000000000000000 (Mantissa)

Floating Point Multiplier Architecture



24-bit mantissa multiplier (array architecture)

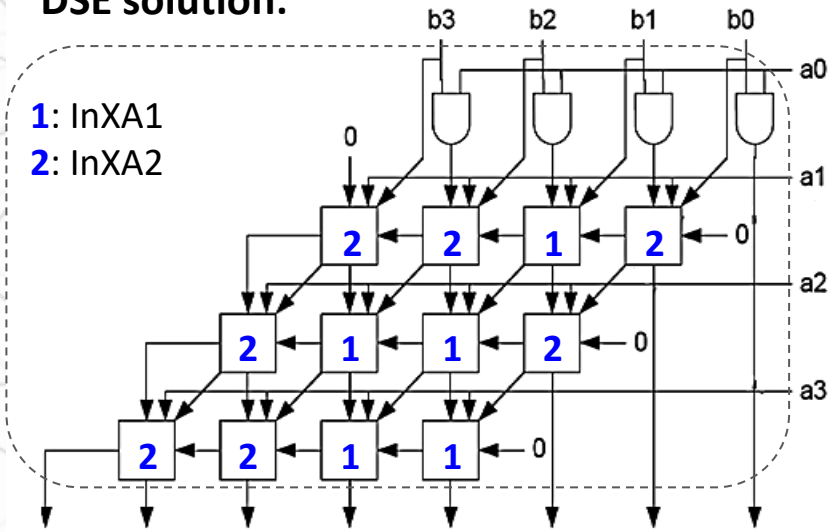


➔ Consumes **81%** of the whole multiplier power consumption

Copyright © 2023

Experimental Results: Approximate Mantissa Multiplier

DSE solution:

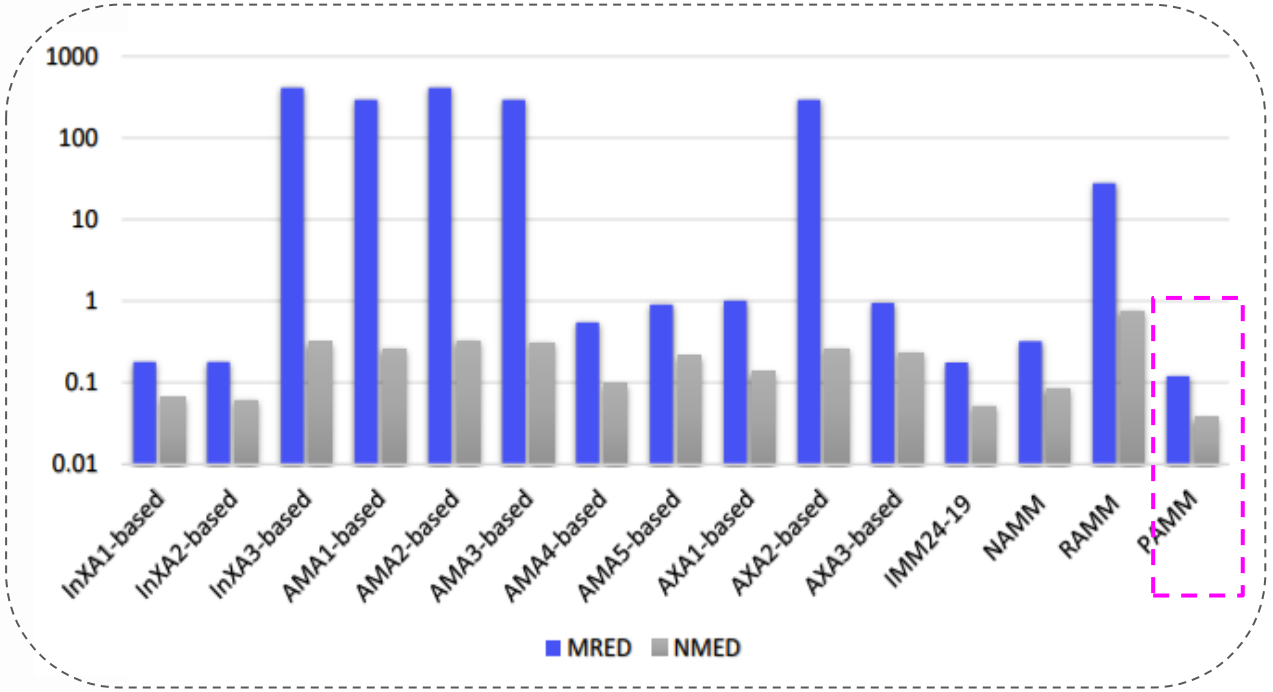


Mean Relative Error Distance:

$$MRED = \frac{1}{n}\sum_{i=1}^{n}\frac{|\hat{Y} - Y|}{Y}$$

Normalized Mean Error Distance:

$$NMED = \frac{1}{n}\sum_{i=1}^{n}\frac{|\hat{Y} - Y|}{(2^k - 1)^2}$$



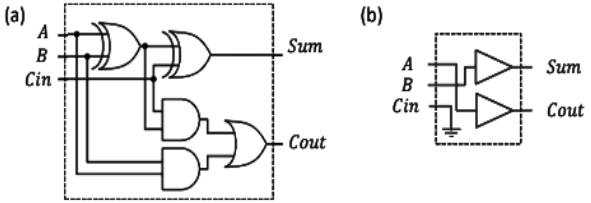
- **IMM24-19:** inexact mantissa multiplier with 24-bit truncation and 19-bit inexact design in partial product
- **NAMM:** inexact mantissa multiplier neglecting an additional term
- **RAMM:** replacing mantissa multiplication with mantissa addition
- **PAMM:** proposed approximate mantissa multiplier

Copyright © 2023

Proposed Defense Mechanism

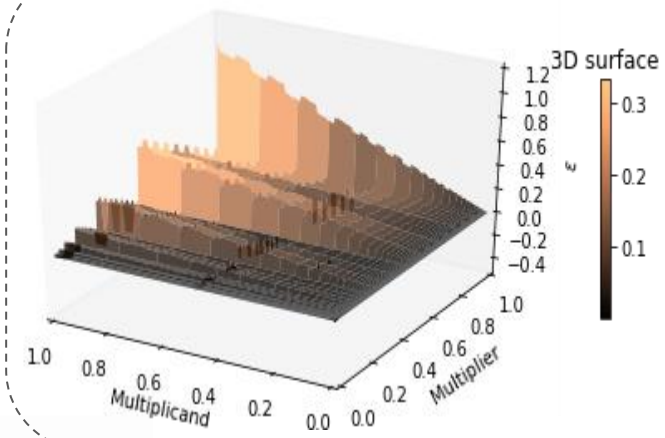
Approximate Full Adder

- Injecting significant noise
- Keeping the cumulative noise magnitude under control to avoid affecting the CNN's accuracy



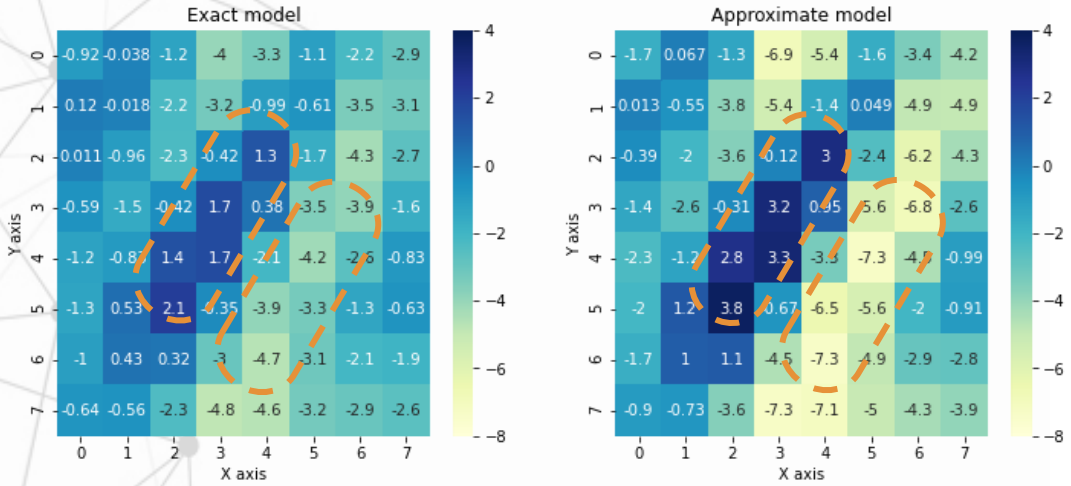
(a) Conventional FA (b) AMA5

Approximate Multiplier



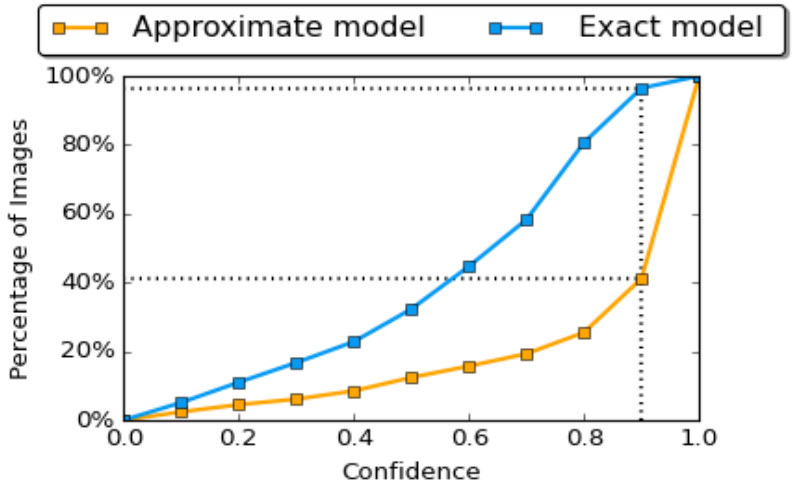
- Data-dependent noise
- Higher noise for higher similarity between the input and the kern
- lower noise for lower similarity

Approximate Convolution



- Further highlighted important features

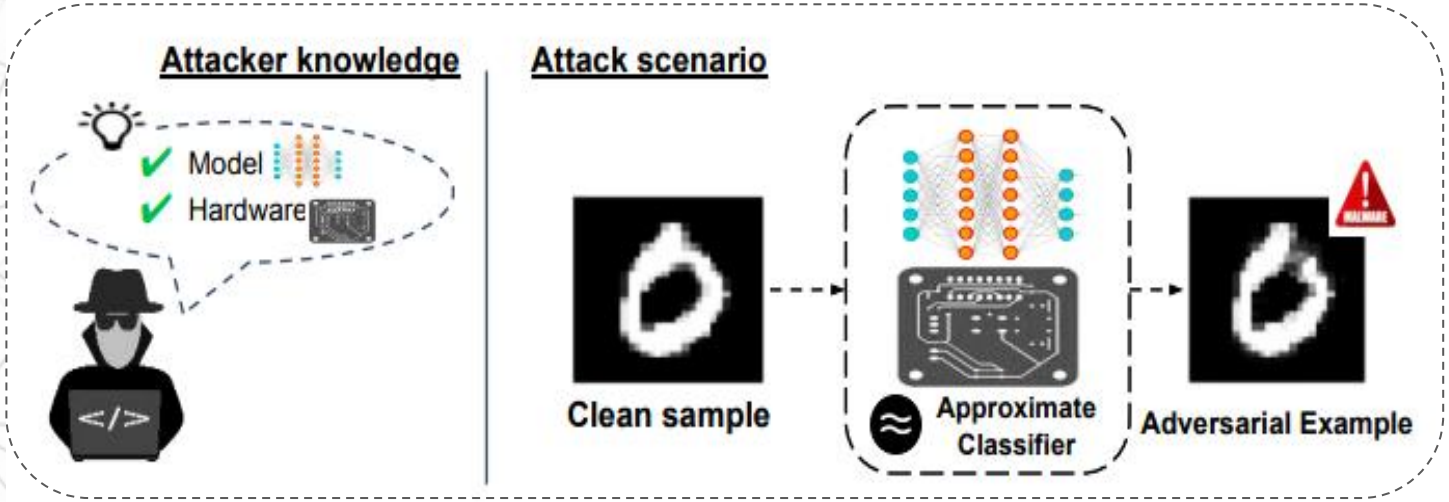
Approximate Model



- Higher confidence for the predicted class

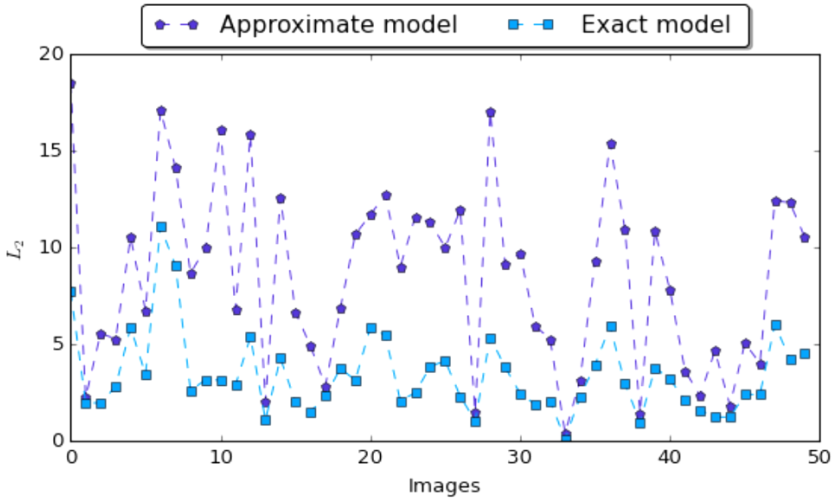
Copyright © 2023

Can We Attack an Approximate CNN?

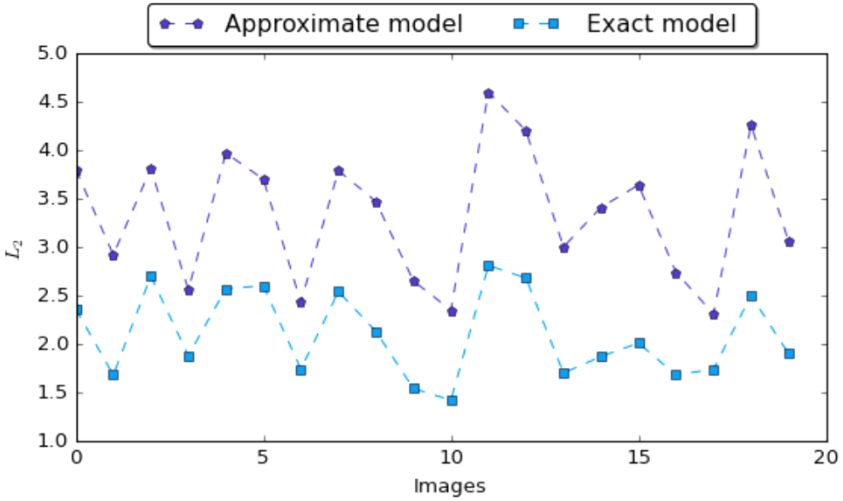


- A **powerful attacker** who has **full knowledge** of the victim classifier's **architecture** and **hyper-parameters**
- The attacker uses this knowledge to create AEs

DeepFool Attack on MNIST



C&W Attack on MNIST



Copyright © 2023