Private and Reliable Neural Network Inference

Nikola Jovanović  Marc Fischer  Samuel Steffen  Martin Vechev

ETH Zurich, Switzerland

{nikola.jovanovic, marc.fischer, samuel.steffen, martin.vechev}@inf.ethz.ch
Motivation: ML as a Service

- Privacy-preserving inference
- Inference with reliability guarantees

FHE

fairness

robustness
This Work

- FHE
- Phoenix
- Randomized Smoothing
- Argmax Approximation
- FHE Optimizations
- fairness
- robustness
- private+reliable inference
Guarantees of Phoenix

- **Client Data Privacy**
  - Lock icon

- **Reliability Guarantees**
  - Checkmark icon

- **Fairness**

- **Robustness**

- **Private + Reliable Inference**

- **FHE**

- **Phoenix**
Background: Randomized Smoothing

\[ x \rightarrow x_1 \rightarrow x_2 \rightarrow \ldots \rightarrow x_n \]

Logits: \([0.1, 2.4, 0.3, \ldots]\)

Predictions: \([0, 1, 0, \ldots]\)

Counts: \([13, 81, 6, \ldots]\)

Prediction ("Cat")

**Probabilistic Reliability Guarantee**

("The prediction is robust.")
Overview of Phoenix

Prior Work (Batched Inference)

Key Challenge!

Rotate + Add + Optimizations

Soft Counting Heuristic

Rewrite of BinPValue

1 Ciphertext
Argmax Approximation

Cheon et al. (ASIACRYPT ’20)

Bound P(violation)

Conditions + Rescale

\[ [a, 1] \rightarrow [1 - 2^{-b}, 1] \]

Full algorithm in our paper
Available on GitHub: eth-sri/phoenix

Consistency

The results are equivalent to the ones obtained in non-private evaluation

Efficiency

Viable latencies and communication costs
Summary: **Phoenix**

- **Client Data Privacy**
- **Reliability Guarantees**

![Diagram of Phoenix system](image)