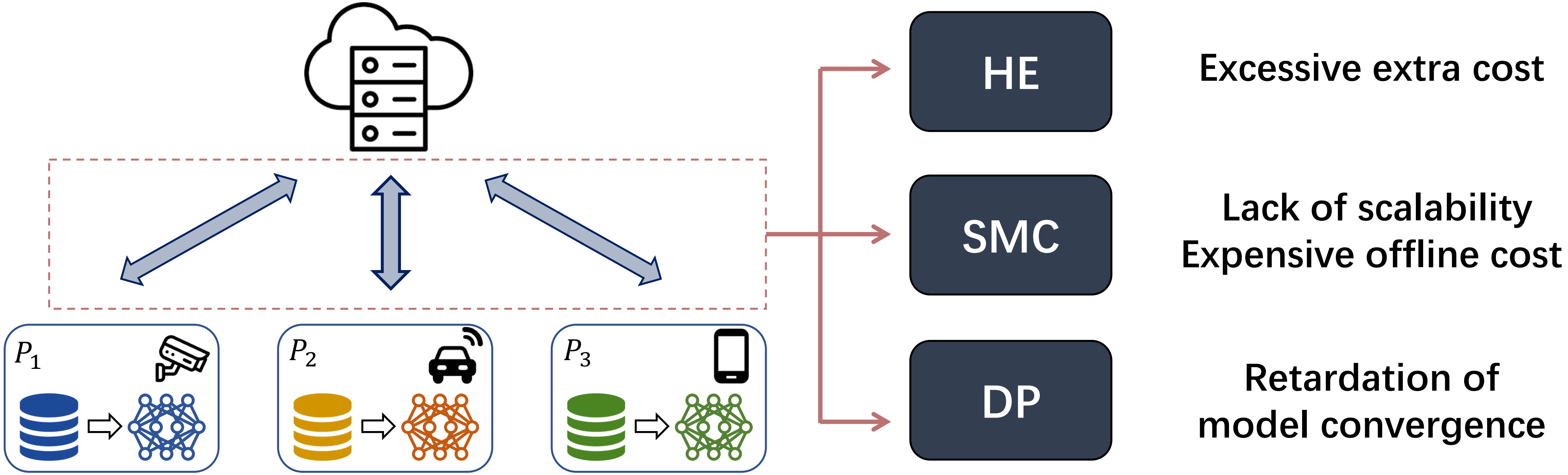
# FLSwitch: Towards Secure and Fast Model Aggregation for Federated Deep Learning with a Learning State-Aware Switch

*Yunlong Mao*, Ziqin Dang, Yu Lin*, Tianling Zhang, Yuan Zhang, Jingyu Hua and Sheng Zhong

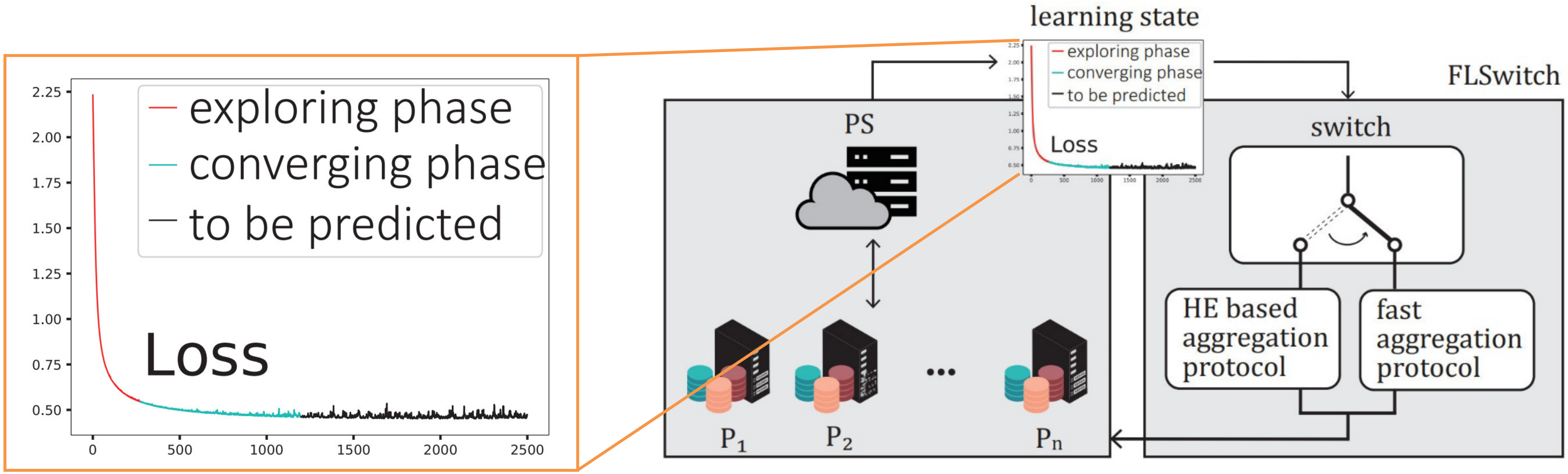
State Key Laboratory for Novel Software Technology, Nanjing University
Nanjing, China
*ByteDance Ltd. Shenzhen, China

# Related Work



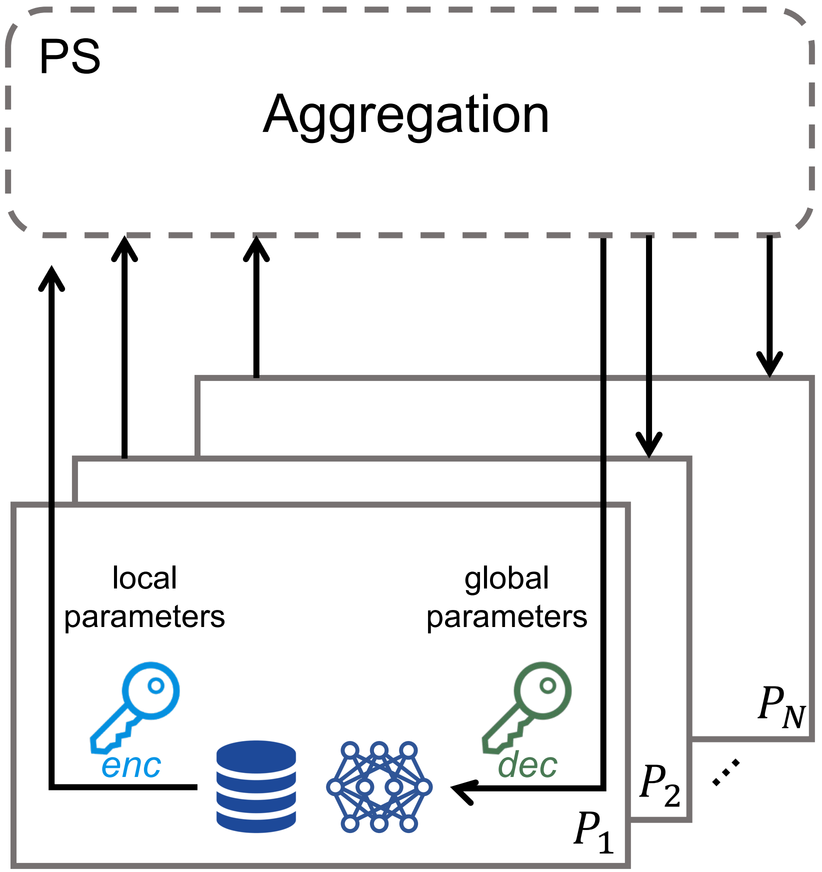
# FLSwitch

- **Overview**




Secure Model Aggregation (SMA)

# Threat Model




- semi-honest PS and participants
- secure communication channel
- no collusion allowed between the adversarial PS and any participant
- collusion of up to N −2 adversarial participants is allowed

# Our Work

- We propose a residual encoding based HE protocol (RBPHE), outperforming the existing solutions in single instruction multiple data operation (SIMD).
- We propose a fast SMA protocol by utilizing FL characteristics and lightweight cryptographical tools for further efficiency improvement, which significantly speeds up conventional SMA designs.
- We design a switch model based on meta-learning, monitoring FL tasks and switching between protocols dynamically.

# RBPHE

- RBPHE provides a flexible encoding range extension method.
- RBPHE reduces the precision loss of updated parameters via dynamic range extension.
- RBPHE achieves more efficient batching and takes less amortized overhead for critical operations.

# RBPHE

- **Comparison of HE-based SMA solutions**

| Input Size | Scheme* | Size (KB) | Enc (ms) | Dec (ms) | Add (ms) | Mul (ms) |
|---|---|---|---|---|---|---|
| 4096 | CKKS (16bit) | 1280.1 | 16 | 6 | 0.6 | 1 |
| | BatchCrypt (8bit) | 16.6 | 350 | 105 | 1 | / |
| | BatchCrypt (16bit) | 25.7 | 528 | 157 | 2 | / |
| | **RBPHE** (8bit) | 19.1 | 261 | 79 | 1 | 0.8 |
| | **RBPHE** (16bit) | 30.3 | 411 | 122 | 2 | 1 |
| 65536 | CKKS (16bit) | 10241.1 | 127 | 44 | 5 | 8 |
| | BatchCrypt (8bit) | 256.8 | 5442 | 1633 | 24 | / |
| | BatchCrypt (16bit) | 403.3 | 8275 | 2452 | 36 | / |
| | **RBPHE** (8bit) | 297.8 | 4142 | 1254 | 17 | 13 |
| | **RBPHE** (16bit) | 479.9 | 6497 | 1916 | 28 | 21 |

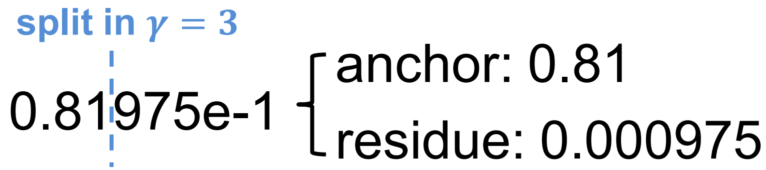
* We use the implementation of CKKS in the SEAL library. The implemention of BatchCrypt and RBPHE is based on python-paillier.

# Anchor negotiation

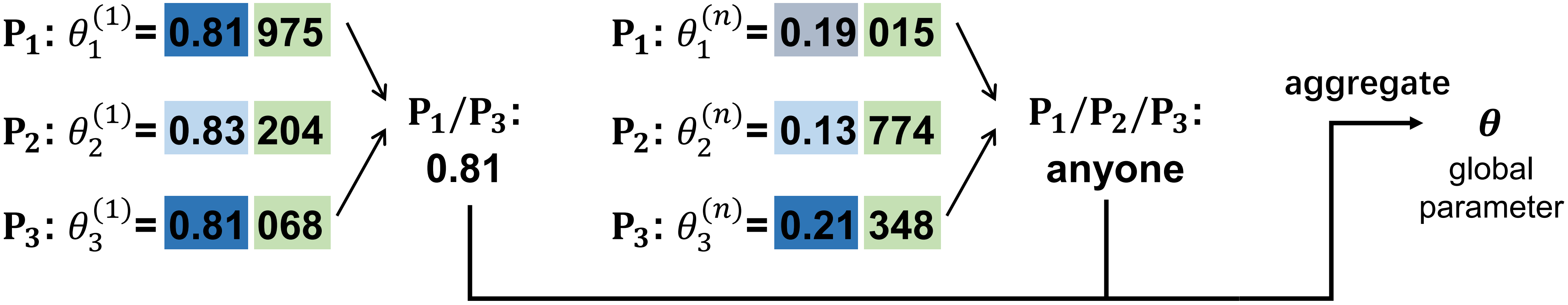
- **parameter split**

$$\theta = a \cdot 10^{-\gamma} + r$$

anchor residue

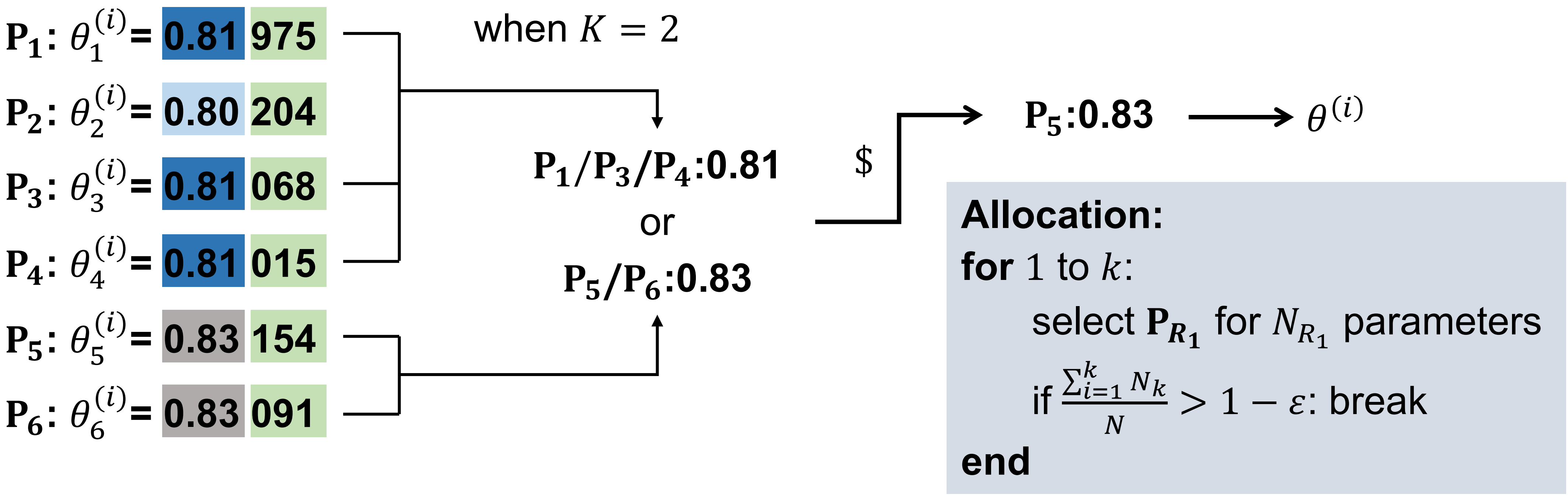



- **select representatives**

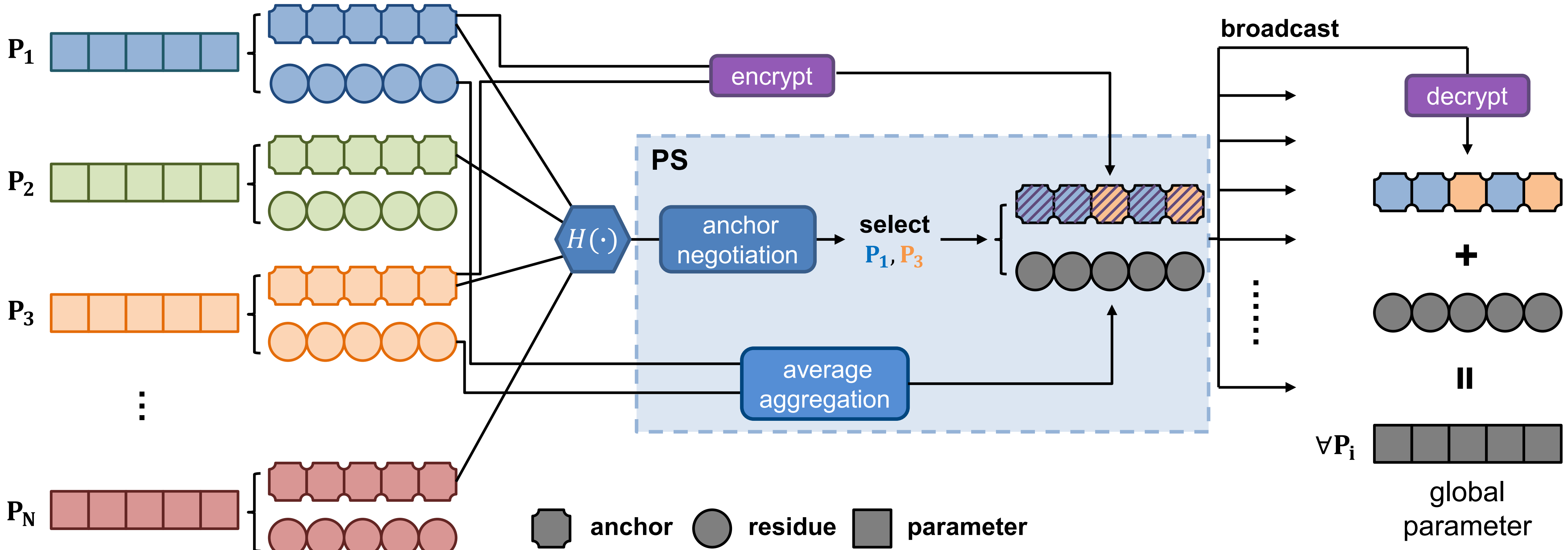


# Anchor negotiation

- **anchorK**



# Fast SMA



P1
P2
P3
PN
encrypt
broadcast
decrypt
PS
H(·)
anchor negotiation
select
P1, P3
average aggregation
+
=
∀Pi
global parameter
anchor
residue
parameter

# Analysis of Fast SMA

- **cost analysis**

  Compuation: $N\mathrm{enc}(\boldsymbol{\theta}) \rightarrow K\mathrm{enc}(\boldsymbol{\theta}) + O(|\boldsymbol{\theta}|NlogK)$

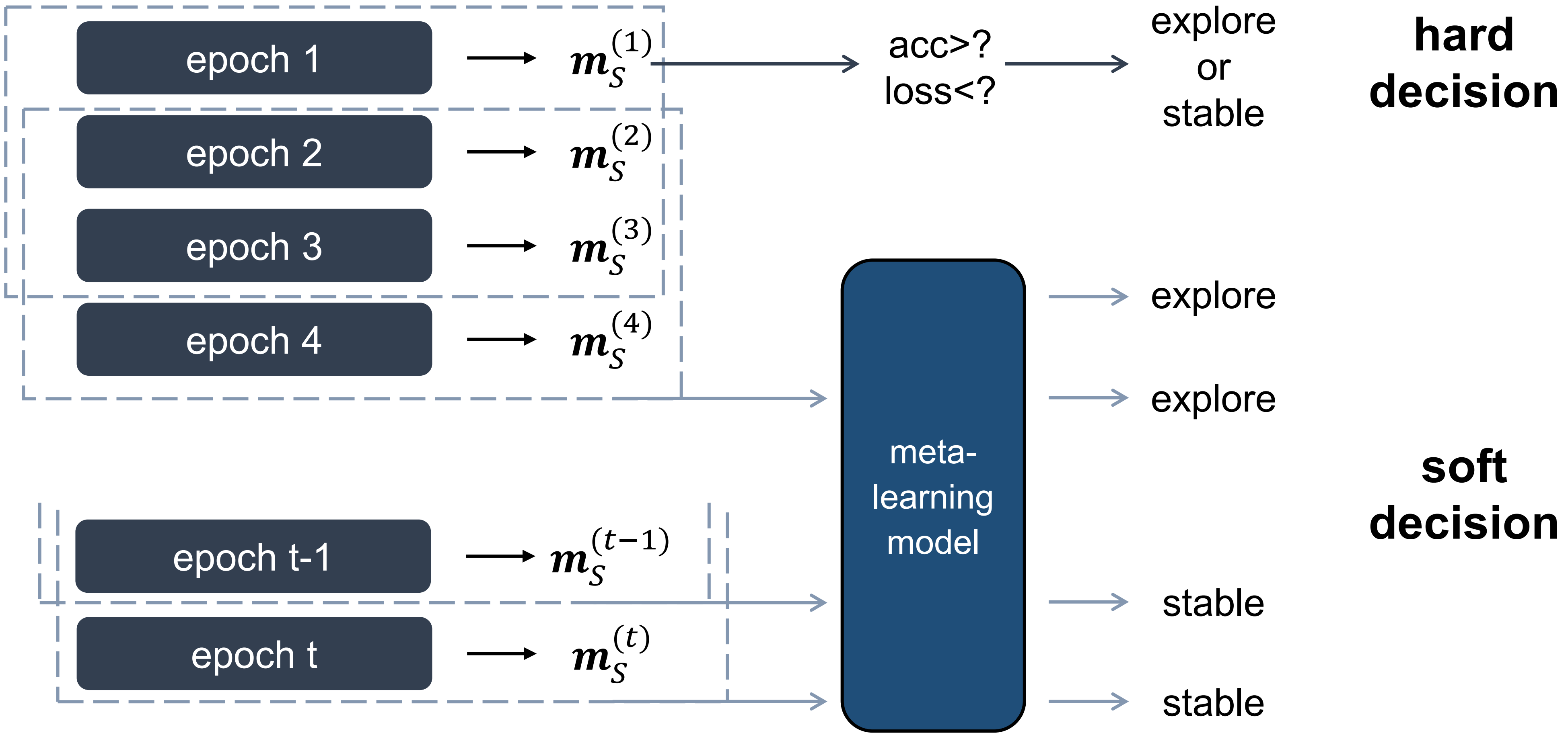
  Communication: $N|\boldsymbol{c}| \rightarrow K|\boldsymbol{c}| + K|\boldsymbol{r}|$

- **security analysis**

  Anchors are protected via HE

  Meaningless hijacked residues without anchors

# Learning State-Aware Switch



# Experiment Setup

- **Dataset**

  MNIST, FASHION-MNIST, CIFAR10 and CIFAR100

- **Model**

  For MNIST family:  3-layer fully-connected NN

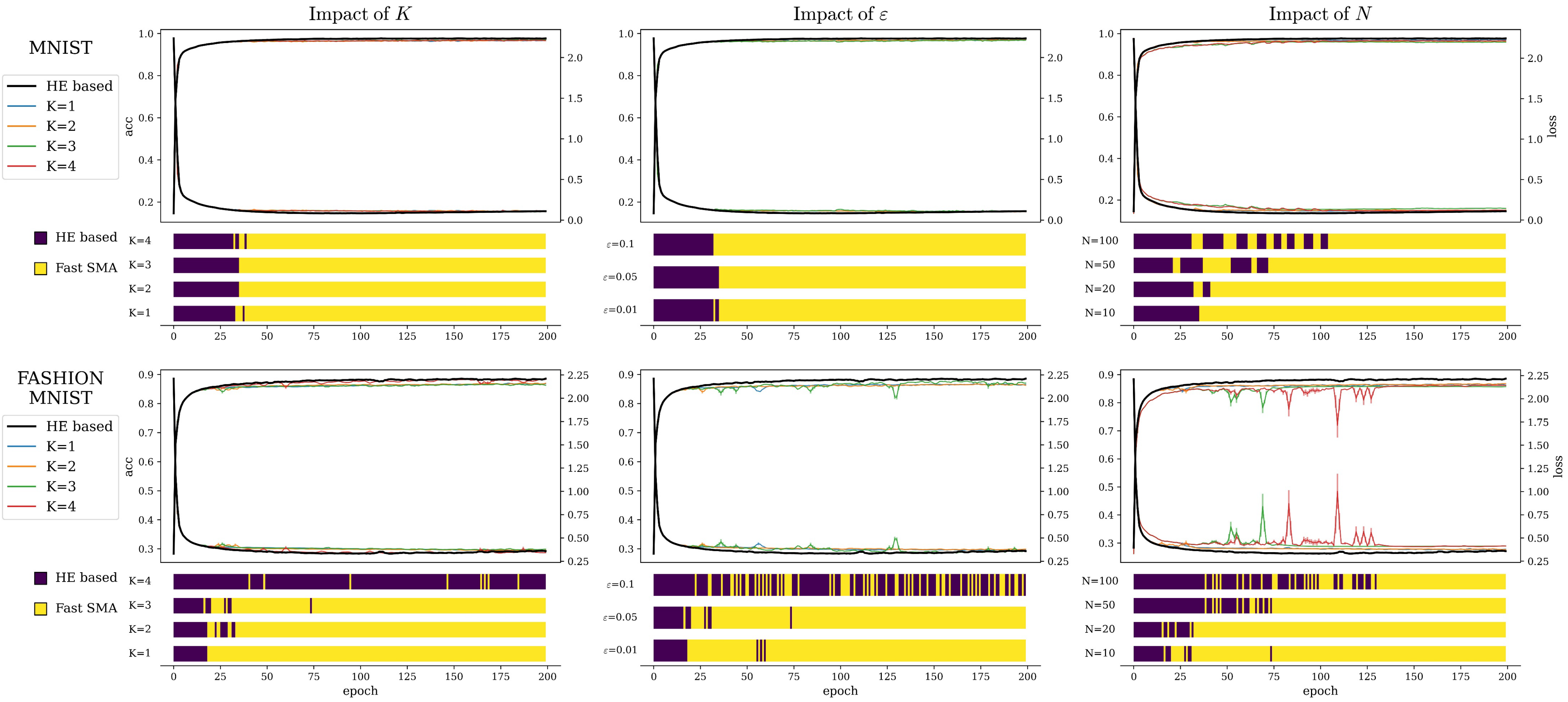
  For CIFAR family: 20-layer ResNet

- **HE algorithms**

  Paillier, Batchcrypt, CKKS and our RBPHE

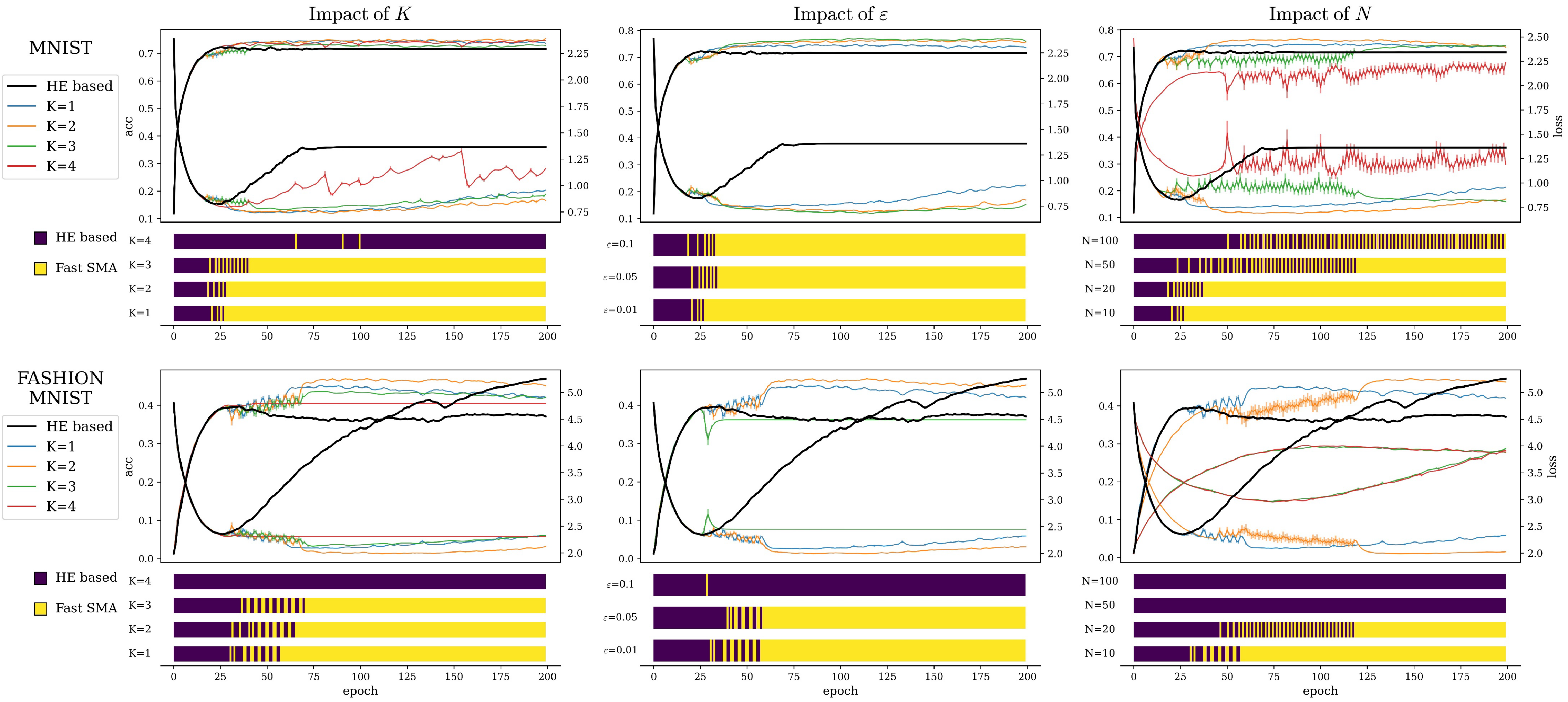
# Experiments

- **MNIST**



# Experiments

- **CIFAR**



# Experiments

## Execution time

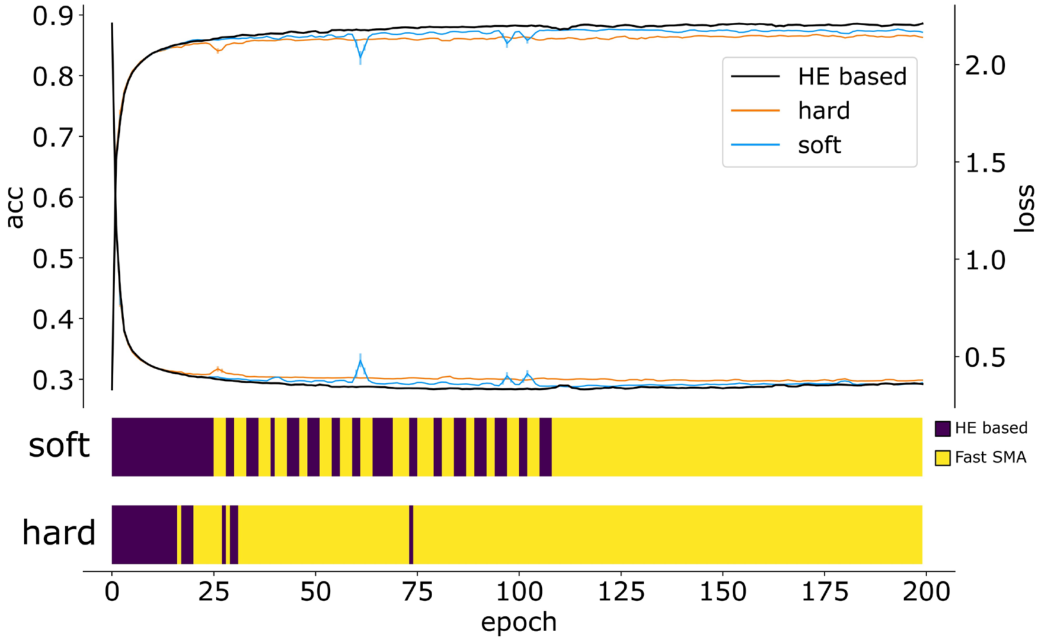
| Dataset | Protocol | Clients10 | | Clients50 | | Clients100 | |
|---|---|---|---|---|---|---|---|
| | | Client | Server | Client | Server | Client | Server |
| FASHION MNIST | **FastAgg** | 2.22 | 2.36 | 5.03 | 13.48 | 28.21 | 3.79 |
| | **RBPHE** | 8.64 | 0.19 | 23.68 | 1.04 | 47.15 | 2.08 |
| | Paillier | 8.72 | 0.07 | 25.53 | 0.41 | 52.69 | 0.86 |
| | Batchcrypt | 9.64 | 0.26 | 26.24 | 1.48 | 51.83 | 3.06 |
| CIFAR10 | **FastAgg** | 24.92 | 17.91 | 56.83 | 26.38 | 165.74 | 19.23 |
| | **RBPHE** | 43.17 | 0.95 | 122.21 | 5.12 | 233.03 | 10.28 |
| | Paillier | 47.10 | 0.35 | 130.46 | 2.24 | 263.89 | 4.45 |
| | Batchcrypt | 48.59 | 1.20 | 131.27 | 6.65 | 266.74 | 14.98 |

## Communication cost

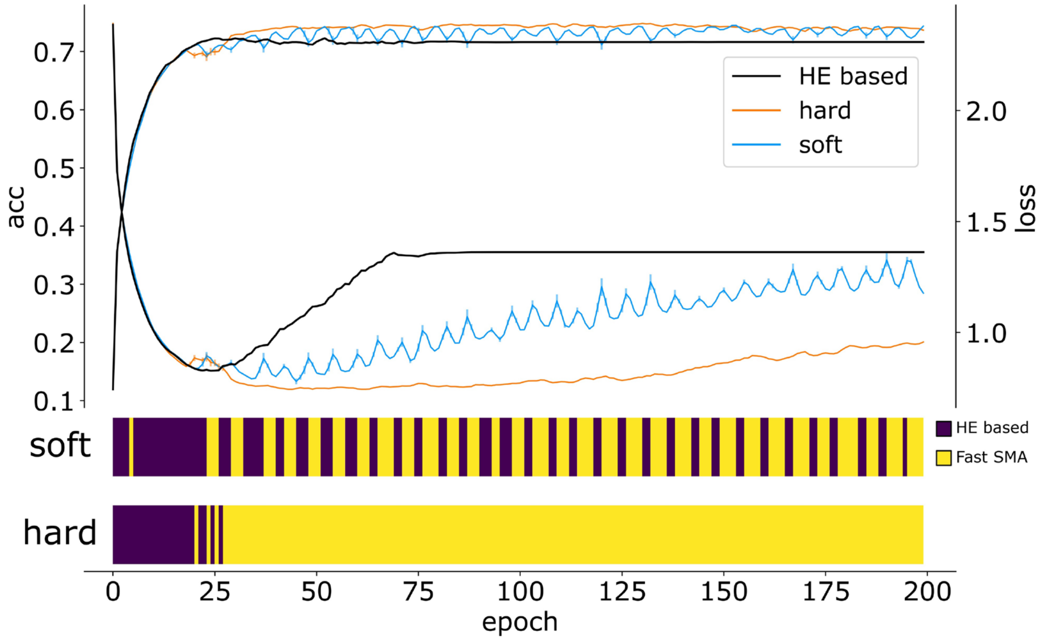
| Dataset | Protocol | Clients10 | | Clients50 | | Clients100 | |
|---|---|---|---|---|---|---|---|
| | | Client | Server | Client | Server | Client | Server |
| FASHION MNIST | **FastAgg** | 0.64 | 7.88 | 0.53 | 33.34 | 0.48 | 59.59 |
| | **RBPHE** | 0.37 | 3.65 | 0.37 | 18.26 | 0.37 | 36.51 |
| | Paillier | 0.28 | 2.82 | 0.31 | 15.56 | 0.32 | 32.22 |
| | Batchcrypt | 0.29 | 2.94 | 0.29 | 14.68 | 0.29 | 29.39 |
| CIFAR10 | **FastAgg** | 4.02 | 43.79 | 2.62 | 163.82 | 2.21 | 260.33 |
| | **RBPHE** | 1.80 | 18.01 | 1.80 | 90.07 | 1.80 | 180.1 |
| | Paillier | 1.52 | 15.23 | 1.68 | 83.82 | 1.74 | 173.68 |
| | Batchcrypt | 1.44 | 14.49 | 1.44 | 72.46 | 1.44 | 144.86 |

# Experiments

- **State-aware switch model**




FASHION-MNIST




CIFAR10

# Thanks!

# question?