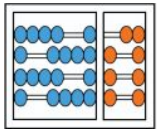
Segurança e Eficiência em Aprendizado Federado Veicular com Criptografia Homomórfica: Otimização de Overhead

UNICAMP

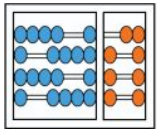
Yuri Dimitre Dias de Faria

Sumário

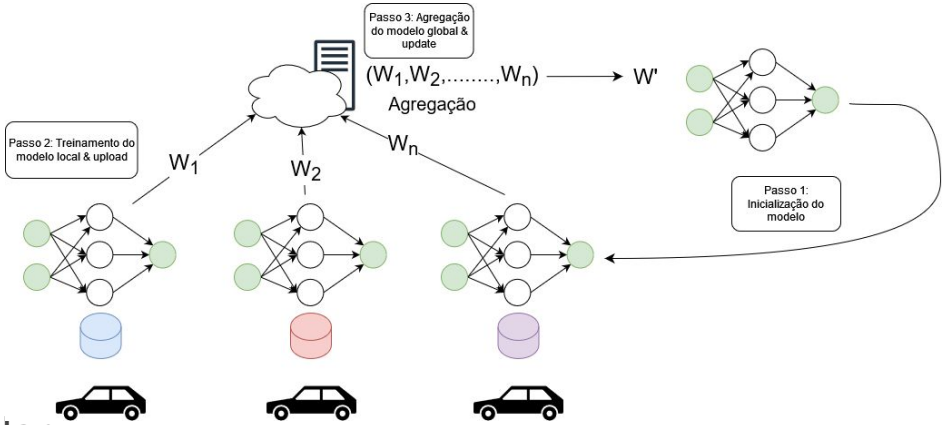


- *Federated Learning.*
- Criptografia Homomórfica.
- Trabalhos Relacionados.
- Objetivo e Proposta.
- Análise dos Resultados.
- Cronograma.
- Resultados Iniciais.

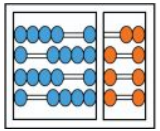
Federated Learning



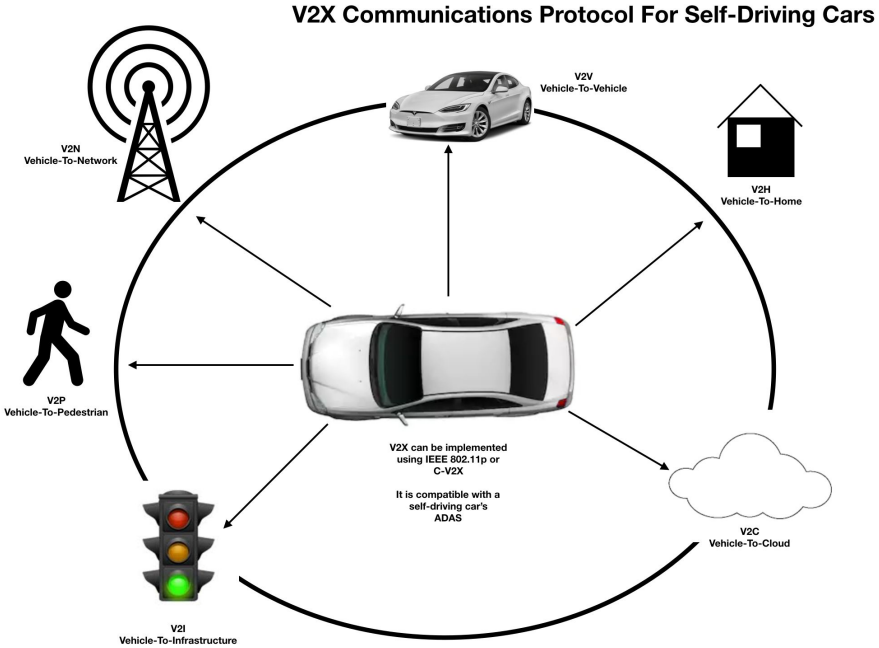
- **Definição**: Aprendizado distribuído, onde os clientes não compartilham os dados.
- **Funcionamento**:
  - Treinamento local
  - Agregação global
  - Atualização global
- **Vantagens**:
  - Preservação de privacidade.
  - Redução de latência.
  - Escalabilidade.
- **Aplicações**: Saúde, Smartphones, Veicular.
- **Problemas pertinentes:**
  - Privacidade em xeque. (Deep Leakage Gradients, Zhu *et al.*)



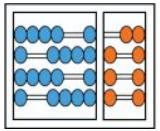
FL em cenário veicular



- **Aplicações:** Detecção de anomalias, previsão de tráfego, assistência à direção e gestão de segurança.
- **Cenários:**
  - V2V, V2N, V2I, V2H, V2C, V2P, V2X.
- **Desafios:**
  - Conectividade Instável e Latência.
  - Variação de Dados.
  - Segurança e Privacidade.
  - Capacidade Computacional Limitada.
- **Soluções Potenciais:**
  - Esparsficação e Quantização de Gradientes.
  - Criptografia Homomórfica.

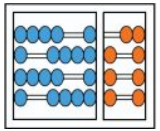


Criptografia Homomórfica



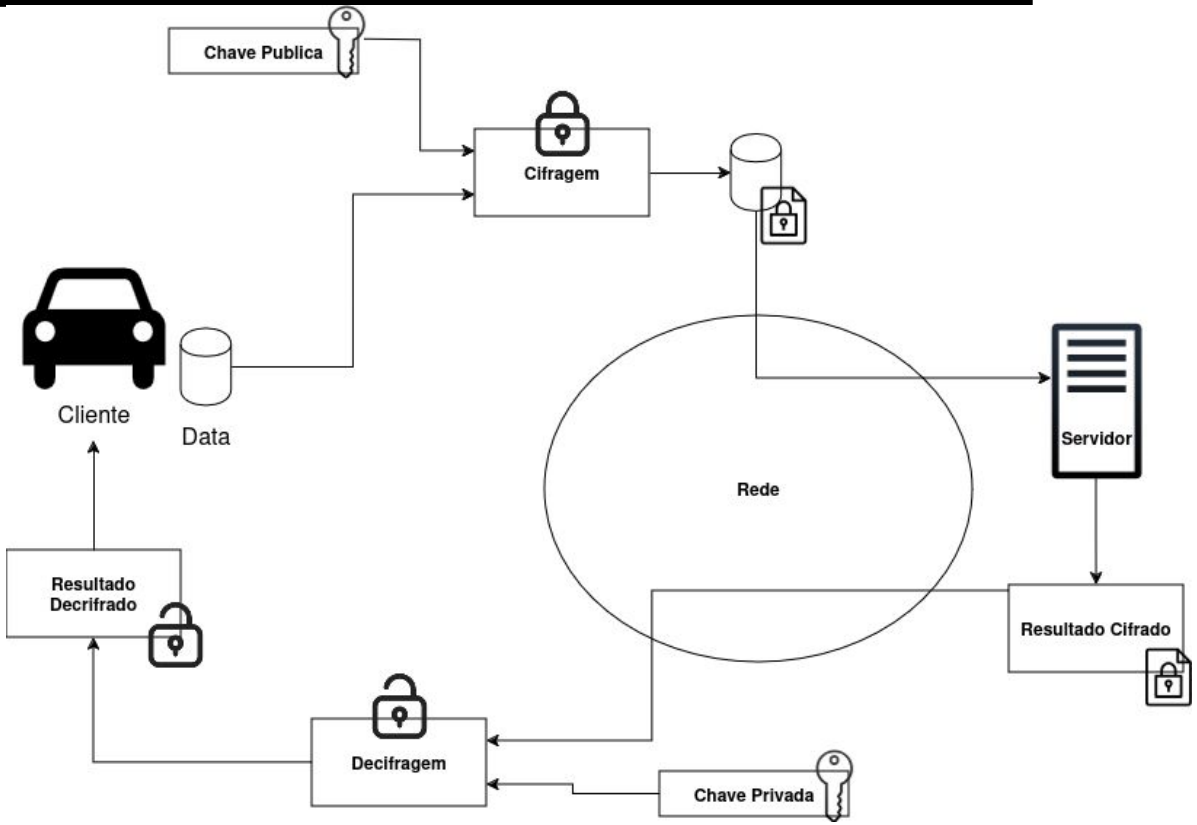
- Técnica criptográfica que permite realizar cálculos diretamente sobre dados criptografados sem necessidade de decriptá-los.
- **Homomorfismo:** Preservação da estrutura algébrica em operações entre duas estruturas.
  - $f(a+b) = f(a)+f(b)$
  - $\text{Enc}(a+b) = \text{Enc}(a)+\text{Enc}(b) \longrightarrow \text{Disc}(\text{Enc}(a+b)) = a+b$
- Os resultados permanecem criptografados e podem ser descriptografados somente pela parte autorizada, garantindo a privacidade dos dados.
- **Criptografia Assimétrica:** Par chave Publica/Privada.
- **Tipos Principais:**
  - **Criptografia Parcialmente Homomórfica (PHE)**: Suporta operações limitadas (adição ou multiplicação).
  - **Criptografia Homomórfica Leve (SHE)**: Suporta um número fixo de operações aritméticas limitadas.
  - **Criptografia Homomórfica Completa (FHE)**: Permite qualquer operação aritmética em dados criptografados, mas é computacionalmente mais intensa.

Método CKKS (Cheon-Kim-Kim-Song)

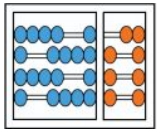


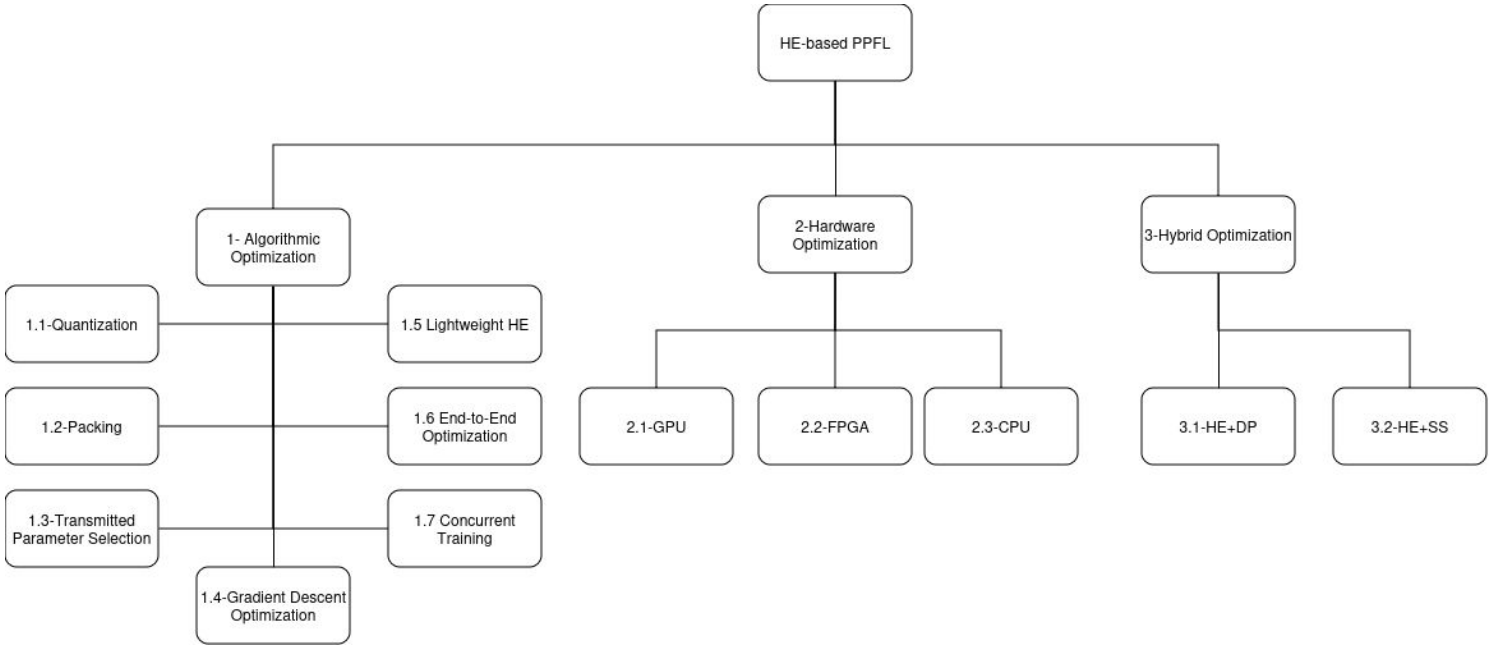
- Um esquema de criptografia homomórfica focado em realizar operações em números reais e complexos.
- **Eficiência:** Mais eficiente que outros métodos (BGV e BFG, *e.g.*) em cenários que não necessitam de operações exatas, tornando-o ideal para aplicações em deep learning.
- **Redução de Erro:** Minimiza erros acumulados em cálculos iterativos, mantendo uma precisão prática para muitos algoritmos de aprendizado.
- **Parâmetros de Configuração:**
  - **Grau do Polinômio (n):** Define o grau do polinômio subjacente usado no esquema (quanto o grau mais seguro e mais caro é a cifragem)
  - **Modulo de Chave (q):** Determina a faixa de valores que as operações são realizadas e controla a precisão e a capacidade de realizar operações.
  - **Parâmetro de Escala (Δ):** Controla a precisão dos valores reais representados.

Exemplo de fluxo de HE com FL

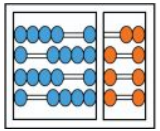


Trabalhos relacionados



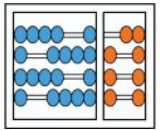


Trabalhos relacionados



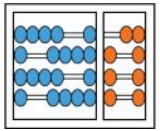
- **Quantização:** Processo de aproximação de valores contínuos para um conjunto menor de valores discretos.
  - **Exemplo:**
    - **8 bit:** representação de peso de 32 bits em 8 bits.
    - **Binaria:** Converte valores para 0 ou 1.
- **Seleção de parâmetros transmitidos (Esparsificação):** Envio de apenas uma parte dos parâmetros que representam as mudanças significativas.
  - **Exemplos:**
    - **Thresholding:** Apenas parâmetros que excedem um certo valor limiar são enviados
    - **Top-K:** Seleciona K valores para serem transmitidos.

Trabalhos relacionados



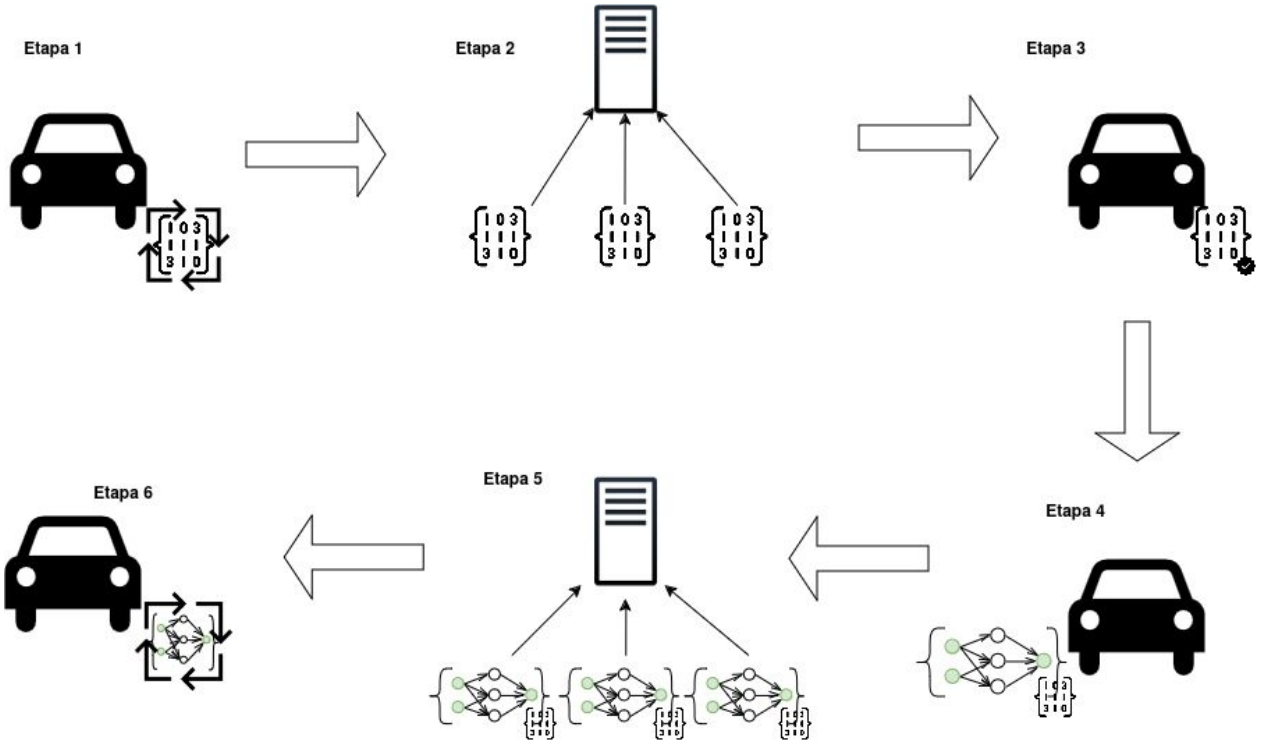
- **Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning**
  - *Batch encoding:* codifica os gradientes em lotes de inteiros longos
  - Cortam os valores do gradiente em distribuição uniforme de faixa simétrica para evitar problemas de precisão.
  - Representabilidade de complemento de dois, dois bits de sinal para valores quantizados.
- **Efficient asynchronous vertical federated learning via gradient prediction and double-end sparse compression**
  - Esparsificação de ponta dupla (cliente/servidor).
  - Mudanças significativas são transmitidas, demais são acumuladas.
  - Outros trabalhos estendem, utilizando PCA e *autoencoders,* por exemplo…

Objetivo e Proposta

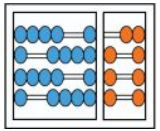


- **Objetivo:** Reduzir *Overhead* causado ao utilizar criptografia homomórfica em arquiteturas *Federated Learning*
- **Objetivo (Trabalhos relacionados):** Problema de escalabilidade.
- **Proposta:**
  - Utilizar máscaras para reduzir a dimensão dos gradientes cifrados.
  - Aplicar técnicas hibridas de seleção de parâmetros.

Fluxo da proposta

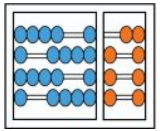


Análise dos Resultados



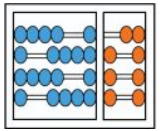
- **Dataset:** VeRi dataset
- **Cenário ITS:** centralizado
- **Cenário bizantino:** servidor adversário.
- **Modelo**
  - Acurácia e perda.
- **Privacidade**
  - Inversão do gradiente e reconstrução dos dados.
    - MAE e MSE
- **Recursos**
  - CPU
  - GPU
  - Memoria Principal (RAM)
  - Latência
  - Transmissão de bytes

Cronograma



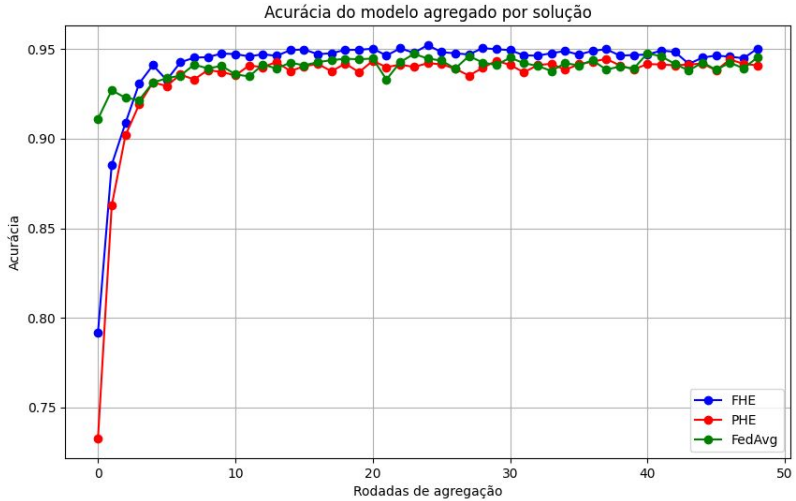
Atividades	Out-Dez 2024	Jan - Mar 2025	Abr - Maio 2025	Jun - Set 2025	Out-Nov 2025
Criação de um ambiente para desenvolvimento.	X				
Implementação de máscara de esparcificação	X	X	X		
Implementação de seleção de atributos				X	X
Técnicas hibridas					X
Testes, análises e validações.			X		X
Elaborar artigos			X		X

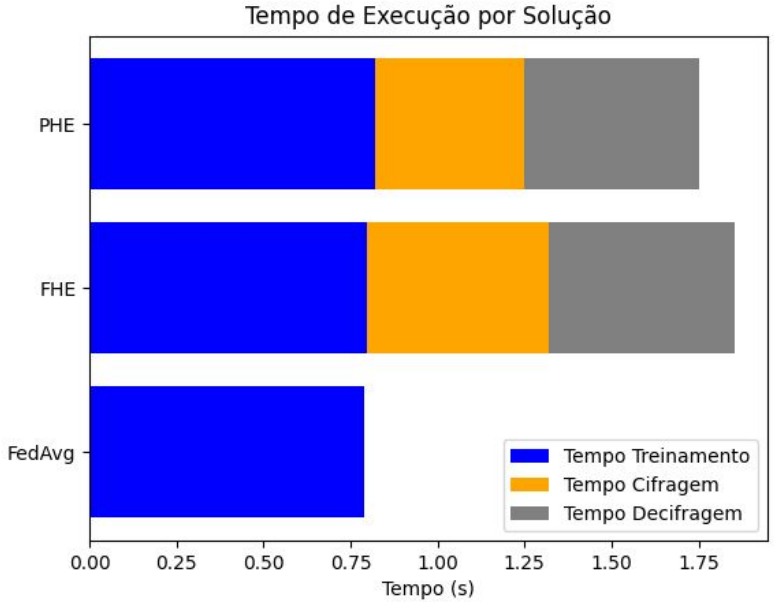
Resultados iniciais



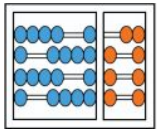
- Experimentos com FHE e PHE.
- Cenário Bizantino: Servidor adversário.
- PHE: Paillier.
- FHE: CKKS
  - Grau do Polinômio: 8192
  - Modulo de chave: 60,40,40,60
  - Parâmetro de escala: 2^40
- Modelo: 32x16x10.
- Dataset: Mnist.
- FedAvg.
- Número de clientes: 2.
- Camadas encriptadas: 2 ultimas.
- Camadas enviadas: 2 ultimas.

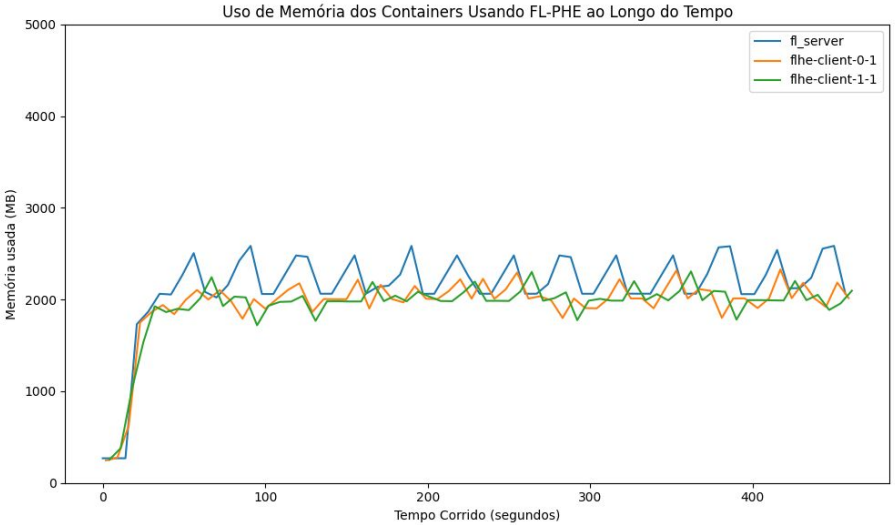
Resultados iniciais

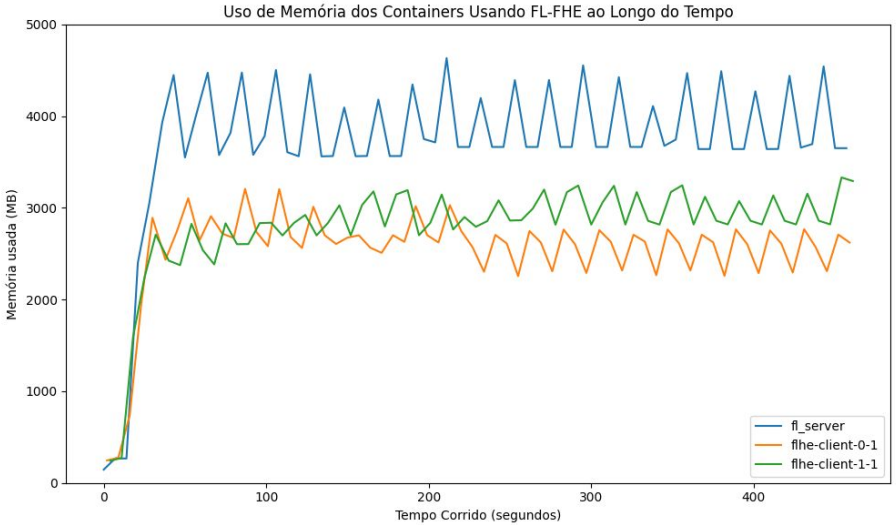


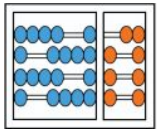


Resultados iniciais









Obrigado!