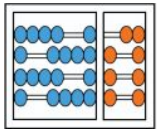
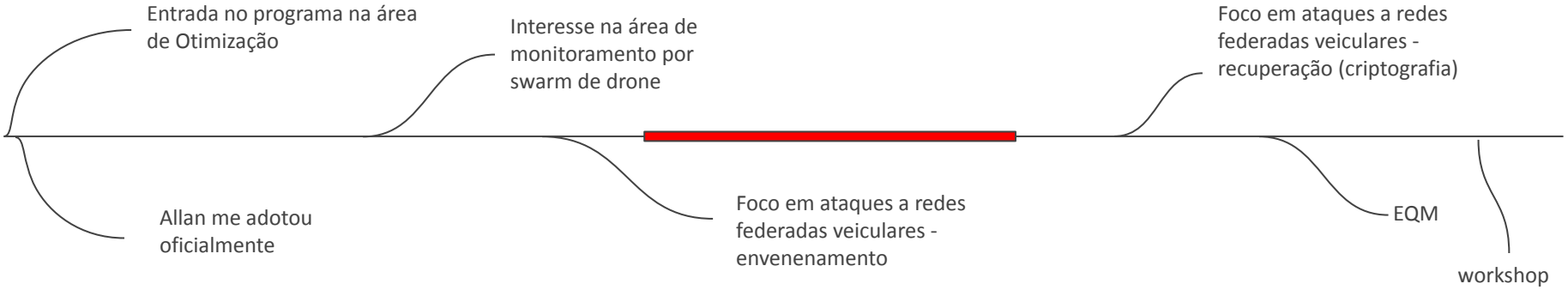
Workshop: Resumão do ano

UNICAMP

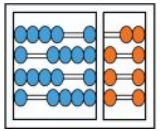
Yuri Dimitre Dias de Faria

Linha do tempo



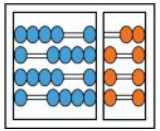


Criptografia Homomórfica



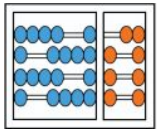
- Técnica de criptografia que permite realizar operações em dados criptografados sem precisar de descriptografá-los.
- Os dados permanecem seguros enquanto as operações são feitas diretamente sobre o texto cifrado.
- Desafios:
  - Alto custo computacional.
  - Complexidade na implementação.

Desafios: Redução de *Overhead* para FL



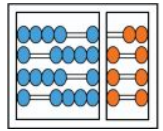
- HE traz alto custo computacional e produz um cifro texto com alto consumo de memória
  - Isso impacta no treinamento, transmissão e agregação dos dados
- Técnicas comuns de redução do Overhead:
  - Quantização
  - Seleção de parâmetros
  - Seleção de clientes
- Artigos *state of the art:*
  - Batchcrypt (paillier): Quantização por meio de distribuição uniforme e representação binaria com complemento de dois.
  - FedPHE: Empacotamento, esparcificação, clusterização, *Sketching* para seleção de clientes

Exame de Qualificação de Mestrado



- Loureiro
  - Trocar aplicação de ITS
  - Recursos computacionais → começar o trabalho por um cenário menos restritivo, avaliar até onde as soluções podem ser restringida em relação a recursos.
  - Algoritmos de agregação devem ser considerados -> Como os agregadores podem ser utilizados com FHE
  - Discussão do HE em relação aos algoritmos de agregação
  - Discutir requisitos cenários
- Hilder:
  - Entender cenário → Compartilhamento de Chave → Protocolo de compartilhamento para cenário mais controlado
  - Definição de cenário→ semi-honesto, bizantino.
  - Definir modelo de ameaça → ataque passivo/ativo/honesto, mas curioso - cenário plausível
  - Verificar PHE/FHE

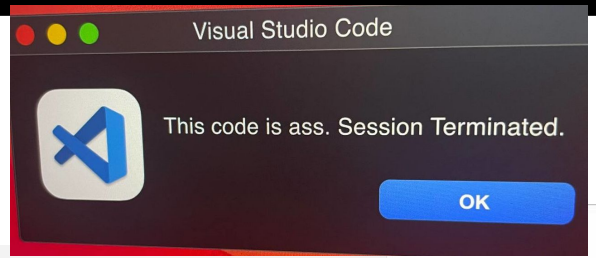
Projeto FAPESP e SBRC

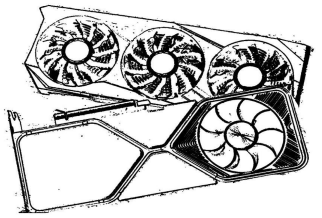


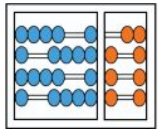
- Mudança de cenário, sair do veicular para um mais amplo.
- Considerar mais técnicas do que apenas esparcificação por meio de máscaras.
    - Seleção de clientes, ponderamento da acurácia, envio de informações encriptadas e seleção por meio desse dado.
    - Representação do dado, empacotamento, LoRa (Low-Rank Adaptation of Large Language Models).
- **SBRC:**
    - Literatura considera majoritariamente FedAvg
    - Diferentes tipos de agregadores podem trabalhar melhor com determinadas configurações de HE.
    - Executar testes com chaves conhecidas, verificar as melhores candidatas para cada agregador padrão do Flower e outros da literatura.

Encryption Type	Scheme Type	Polynomial modulus	Coefficient modulus sizes	Saved keys	Context serialized size
symmetric	ckks	8192	[40, 21, 21, 21, 21, 21, 21, 40]	all	263.02 KB
symmetric	ckks	8192	[40, 21, 21, 21, 21, 21, 21, 40]	Secret key	263.02 KB
symmetric	ckks	8192	[40, 21, 21, 21, 21, 21, 21, 40]	Galois keys	86.87 MB
symmetric	ckks	8192	[40, 21, 21, 21, 21, 21, 21, 40]	Relin keys	3.63 MB
symmetric	ckks	8192	[40, 21, 21, 21, 21, 21, 21, 40]	none	112.0 B
symmetric	ckks	8192	[40, 20, 40]	all	124.71 KB
symmetric	ckks	8192	[40, 20, 40]	Secret key	124.71 KB
symmetric	ckks	8192	[40, 20, 40]	Galois keys	11.89 MB
symmetric	ckks	8192	[40, 20, 40]	Relin keys	503.79 KB
symmetric	ckks	8192	[40, 20, 40]	none	91.0 B
symmetric	ckks	8192	[20, 20, 20]	all	79.39 KB
symmetric	ckks	8192	[20, 20, 20]	Secret key	79.38 KB
symmetric	ckks	8192	[20, 20, 20]	Galois keys	7.48 MB
symmetric	ckks	8192	[20, 20, 20]	Relin keys	317.27 KB
symmetric	ckks	8192	[20, 20, 20]	none	85.0 B
symmetric	ckks	8192	[17, 17]	all	44.21 KB
symmetric	ckks	8192	[17, 17]	Secret key	44.2 KB

Obrigado







BORN TO TRAIN
RAINFORESTS ON FIRE
布赫BACKPROP SINCE 1987
I am $\text{softmax}(\frac{QK^T}{\sqrt{d_k}})V$
410,757,864,350 TFLOPS

AI app developers

AI model trainers