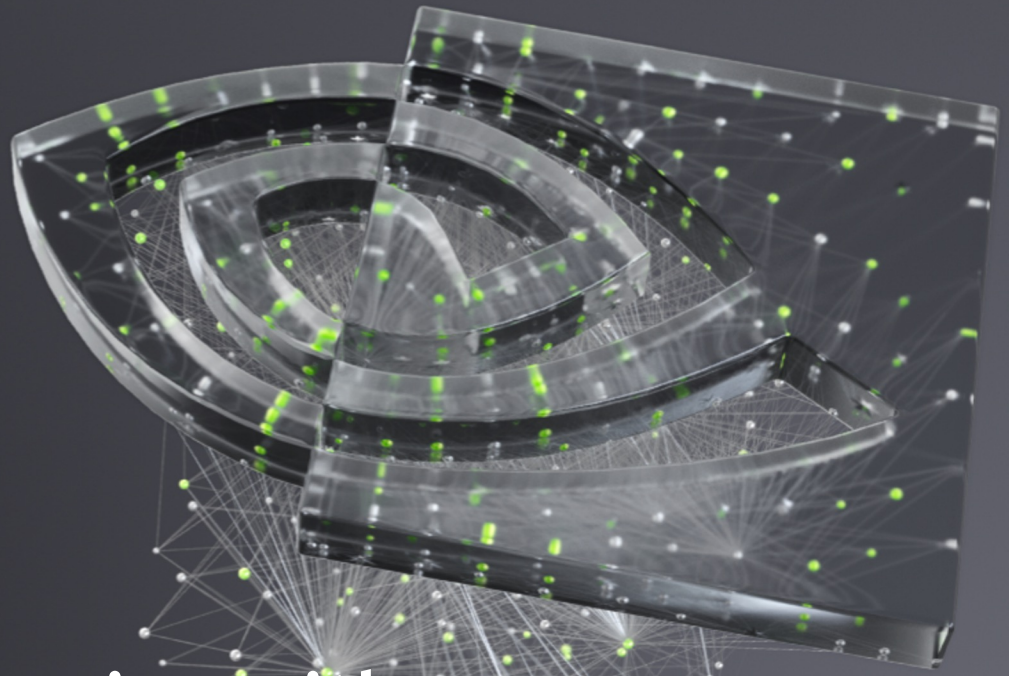


Clara Federated Learning with Homomorphic Encryption

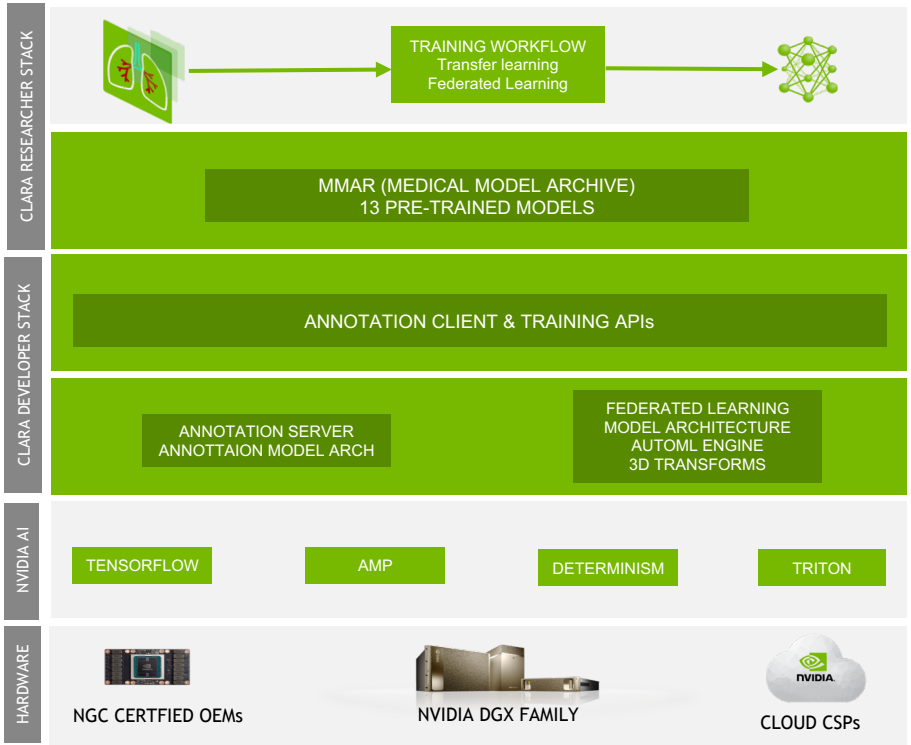
Holger Roth, Senior Applied Research Scientist, Bethesda, MD | Nov 2021

Agenda

1. Clara Train SDK
2. Research projects using Clara Federated Learning
3. Secure Aggregation with Homomorphic Encryption

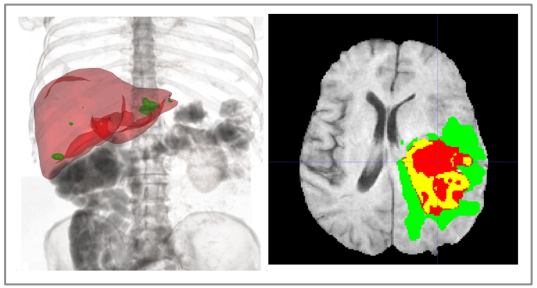
CLARA TRAIN

Domain Optimized Training Framework

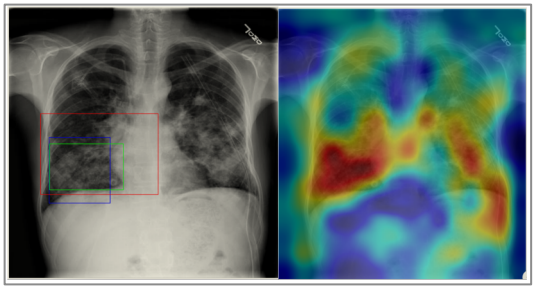


CLARA PRE-TRAINED MODELS

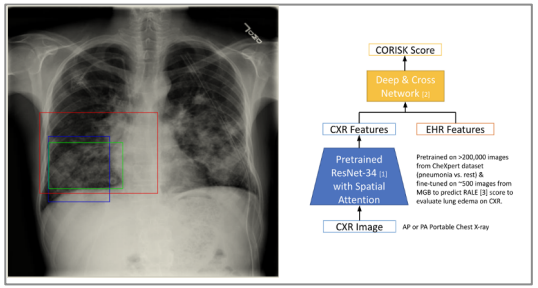
Available on ngc.nvidia.com



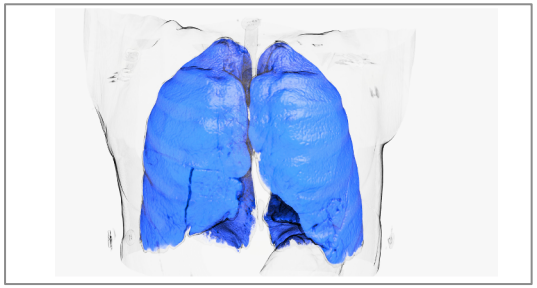
3D Segmentation – AH-Net & Res-UNET
Spleen | Liver Tumor | Brain | Prostate



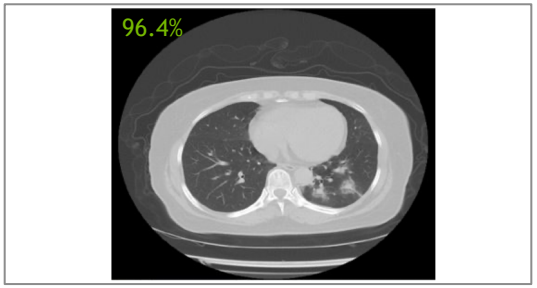
2D Classification – DenseNet121
Chest X-Ray Classification



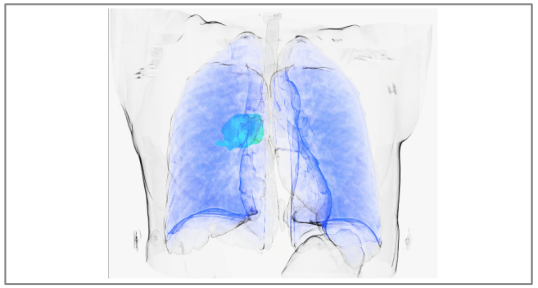
FL4COVID-19 EXAM Model



COVID-19 Lung Segmentation



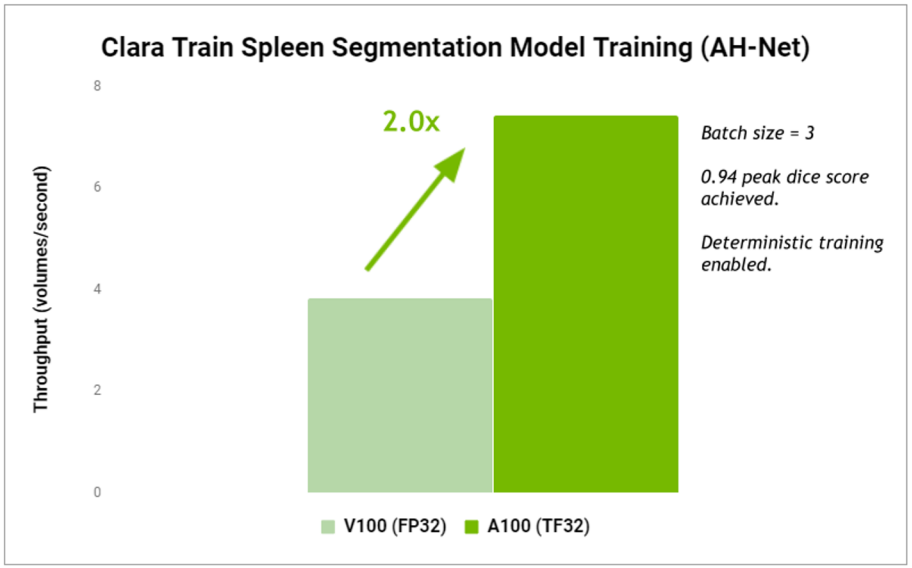
COVID-19 3D Classification
Nature Comm. 2020



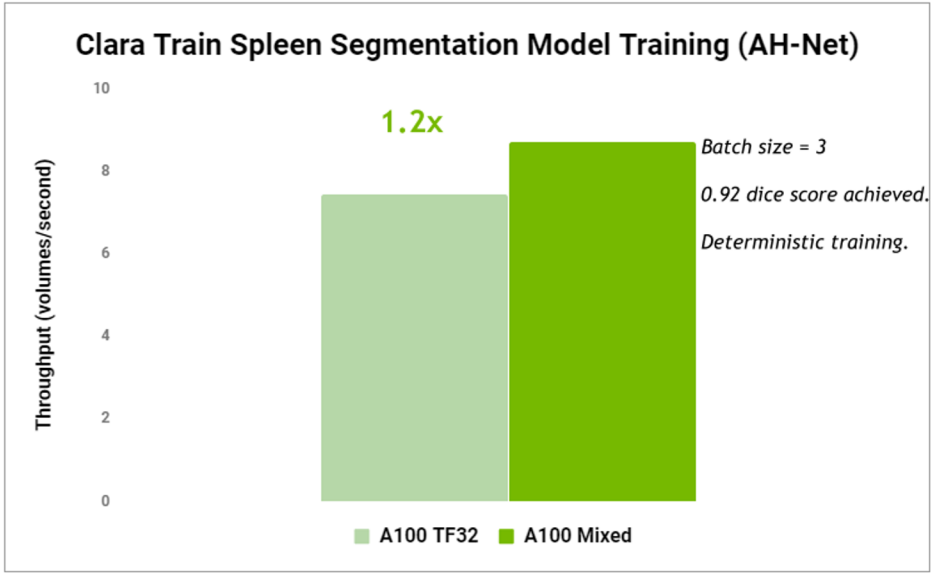
COVID-19 Lesion Segmentation
https://covid-segmentation.grand-challenge.org/

FASTEST MEDICAL AI TRAIN FRAMEWORK

Optimized for NVIDIA A100 Systems



Benchmarks performed on DGX-1 V100 and DGX A100. Training run for 900 epochs



Benchmarks performed on DGX-1 V100 and DGX A100. Training run for 600 epochs

MONAI (Medical Open Network for AI) https://monai.io/

Ease of Integration & Enterprise-grade Software Development

CUSTOMIZABLE

Abstracted for customizable design for varying user expertise

COMPOSIBLE

Portable with ease of integration into existing workflows

DOMAIN SPECIALISED

3D transformations, architecture & workflows for medical imaging

GPU OPTIMIZED

Multi-GPU, CUDA acceleration data & model-parallel processing

REPRODUCIBLE

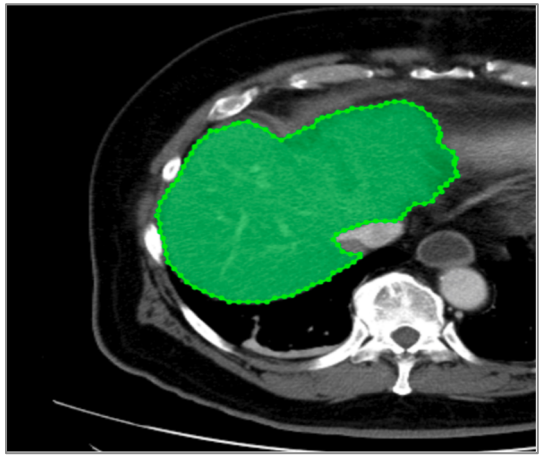
Built for reproducibility and comparison with state of the art

HIGH QUALITY

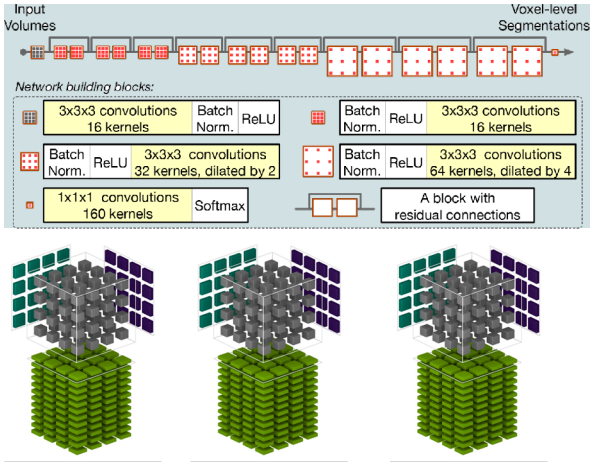
Tutorials for getting started and robust validation & documentation

UNIQUE CHALLENGES OF TRAINING AI MODELS

Data Labeling & Privacy | 3D Networks & Computational Demands



Data Labeling
Expert Knowledge | Time Consuming

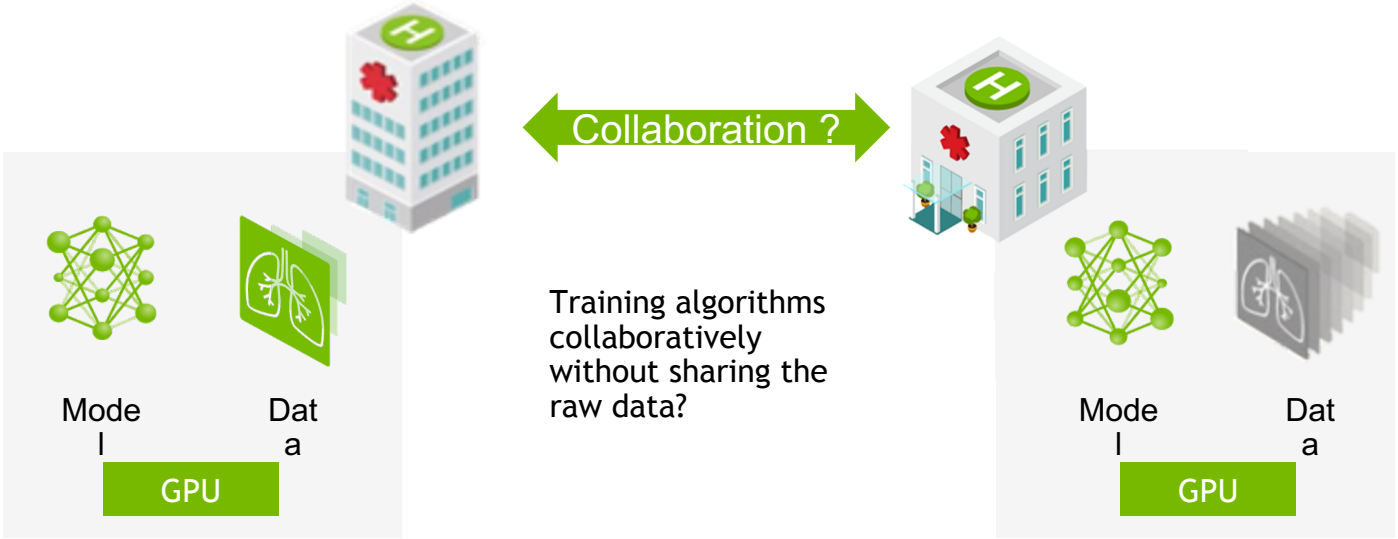


3D Networks
3D Data | High Compute, Memory & I/O Needs

Data Privacy
Patient Privacy | Data Sovereignty

DATA-DRIVEN MEDICINE REQUIRES FEDERATED EFFORTS

Data Governance and Privacy



Possible Solution:

Federated Learning - allow algorithms to learn from non co-located data

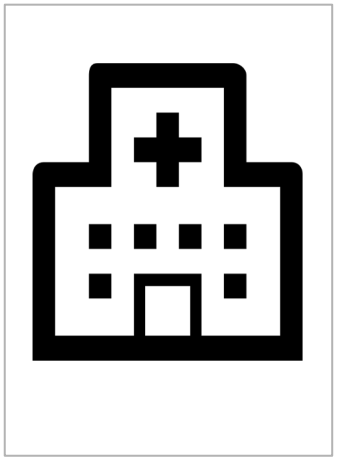
IMPACT OF FEDERATED LEARNING

Increasing the value of AI for all healthcare stakeholders

Clinicians
Accurate assistance tools, Standardization

Patients
Accurate and unbiased AI, Data donor

Researchers
Access to large datasets, Clinical relevant problems



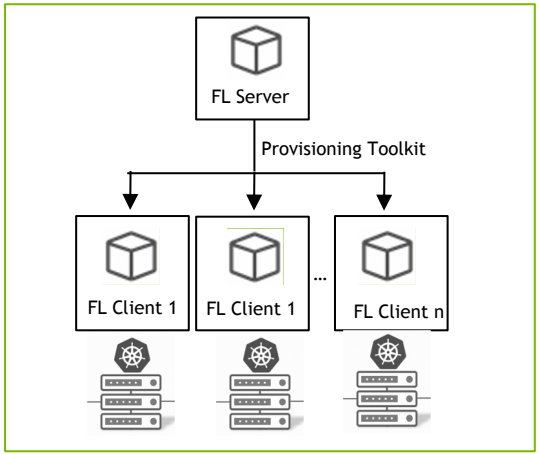
Hospital and Practices
Full control of patient data, Infrastructure

Manufacturers
Continuous improvement of ML-based systems

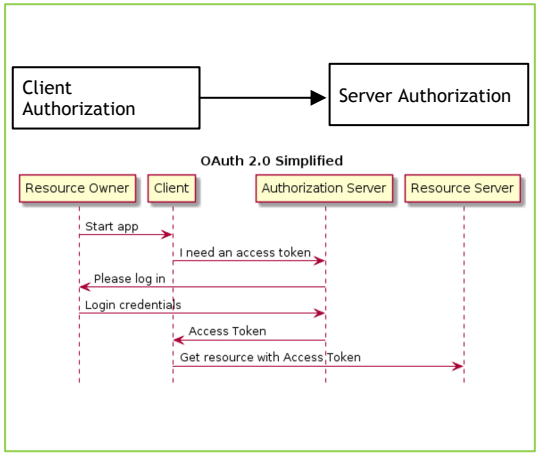
Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H., Albarqouni, S., Bakas, S., Galtier, M. N., Landman, B., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R. M., Trask, A., Xu, D., Baust, M. & Cardoso, M. J. (2020). The Future of Digital Health with Federated Learning. npj Digital Medicine DOI: 10.1038/s41746-020-00323-1

ENTERPRISE FEDERATED LEARNING

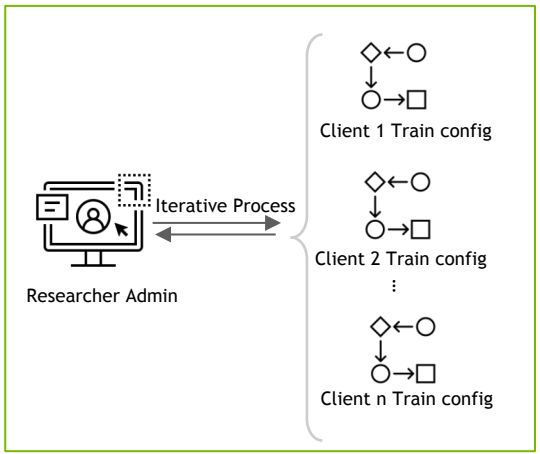
Collaborative Learning – Easy, Secure, Productive



Easy
Simplified Deployment
From days to minutes



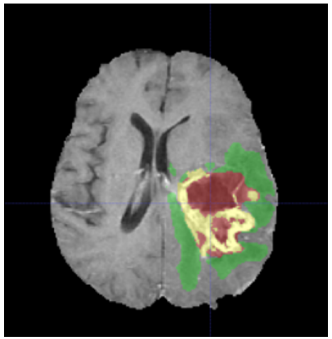
Secure
Flexible Authorization Framework
Improved Security



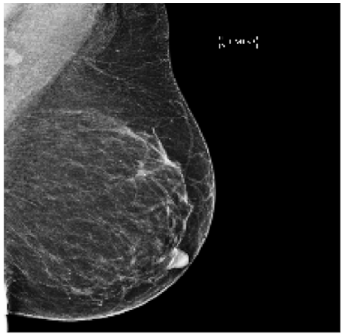
Productive
Maximize Researcher Productivity
10x increase in experimentation


RESEARCH PROJECTS
USING CLARA FL

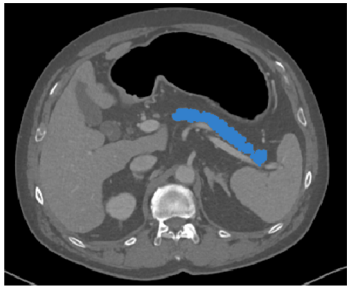
RESEARCH PROJECTS USING CLARA FL



Brain Tumor Segmentation



Mammography

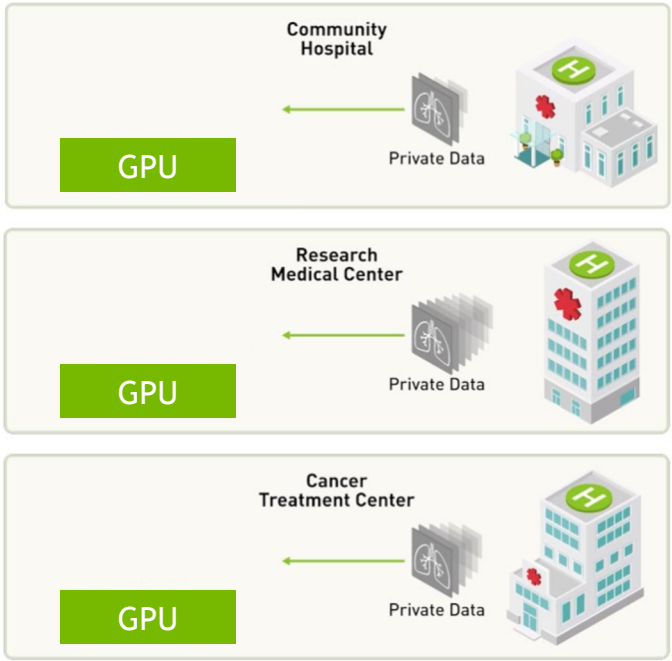


Pancreas Segmentation

COVID-19 Chest X-Ray

SERVER-CLIENT FEDERATED LEARNING

Changing the way AI algorithms are trained

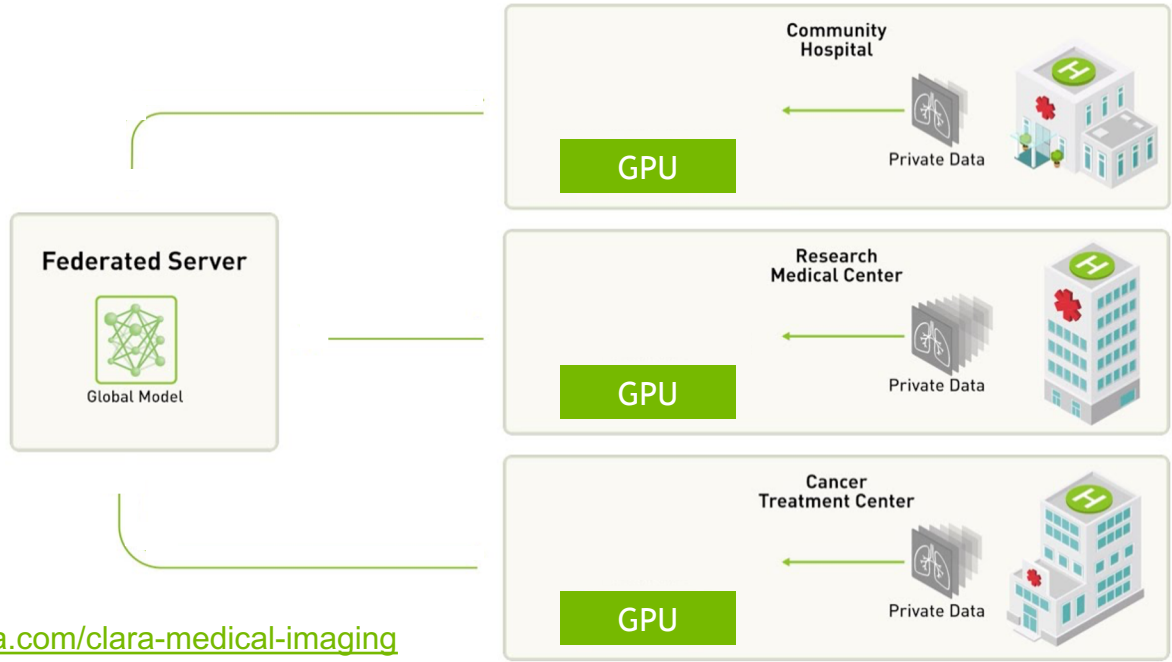


https://developer.nvidia.com/clara-medical-imaging

Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A. (2019, October). Privacy-preserving Federated Brain Tumour Segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer, Cham.

SERVER-CLIENT FEDERATED LEARNING

Changing the way AI algorithms are trained

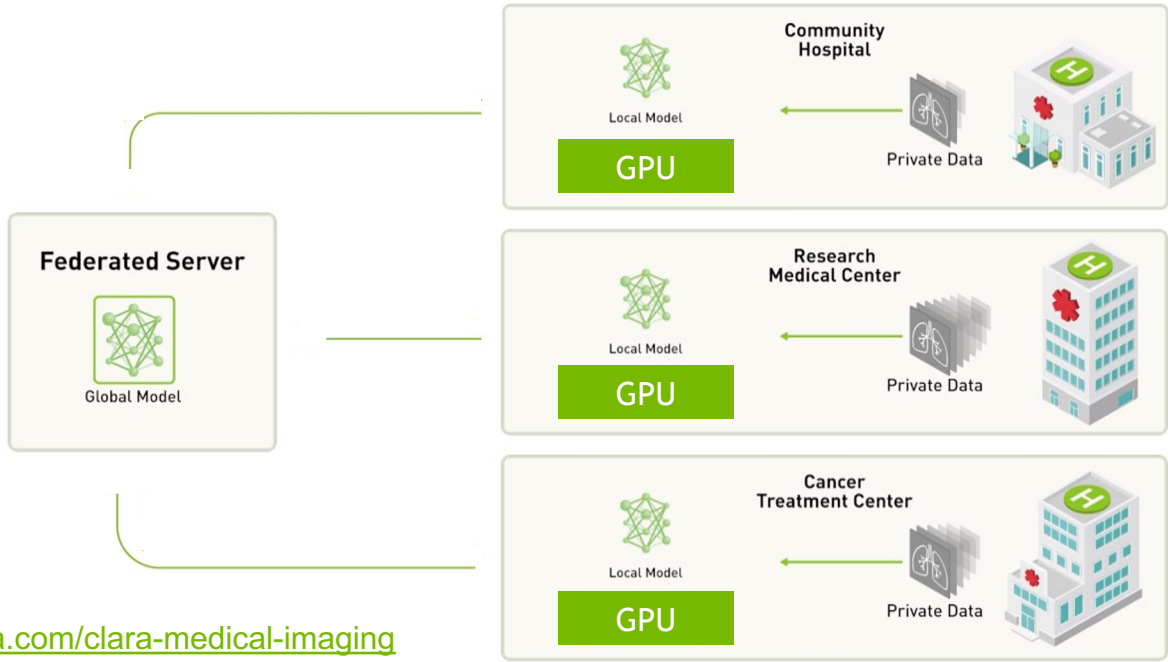


https://developer.nvidia.com/clara-medical-imaging

Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A. (2019, October). Privacy-preserving Federated Brain Tumour Segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer, Cham.

SERVER-CLIENT FEDERATED LEARNING

Changing the way AI algorithms are trained

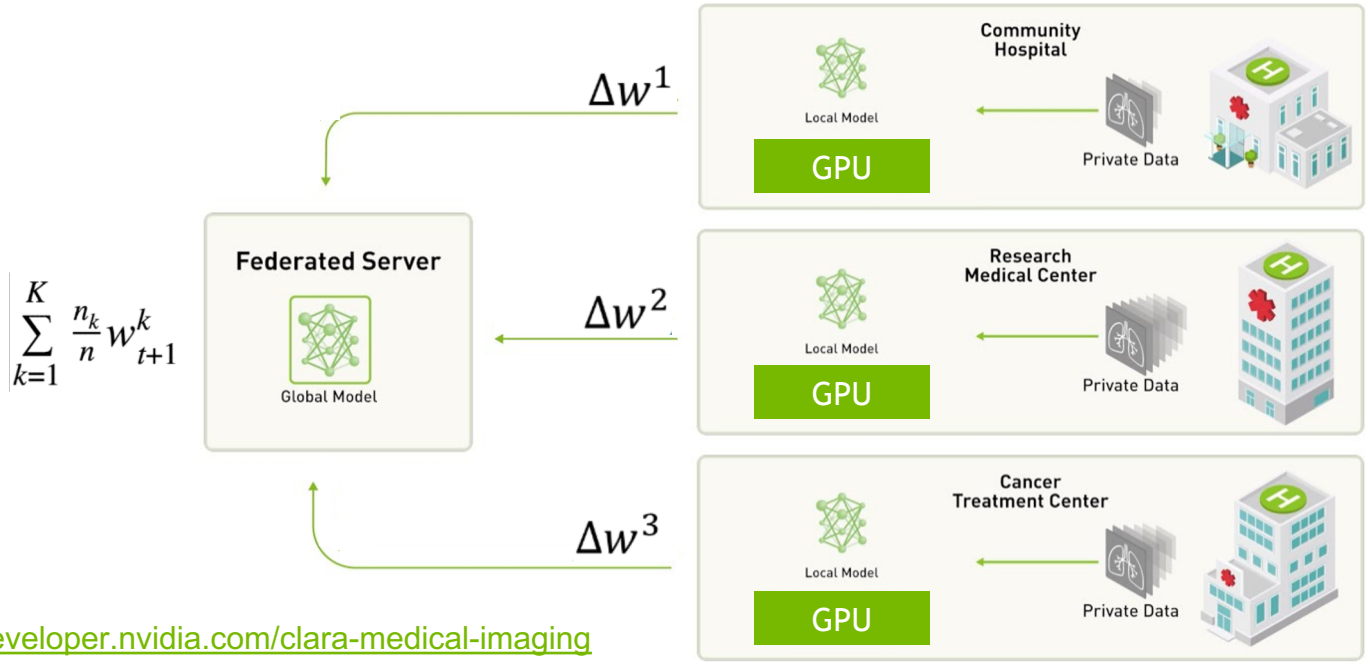


https://developer.nvidia.com/clara-medical-imaging

Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A. (2019, October). Privacy-preserving Federated Brain Tumour Segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer, Cham.

SERVER-CLIENT FEDERATED LEARNING

Changing the way AI algorithms are trained

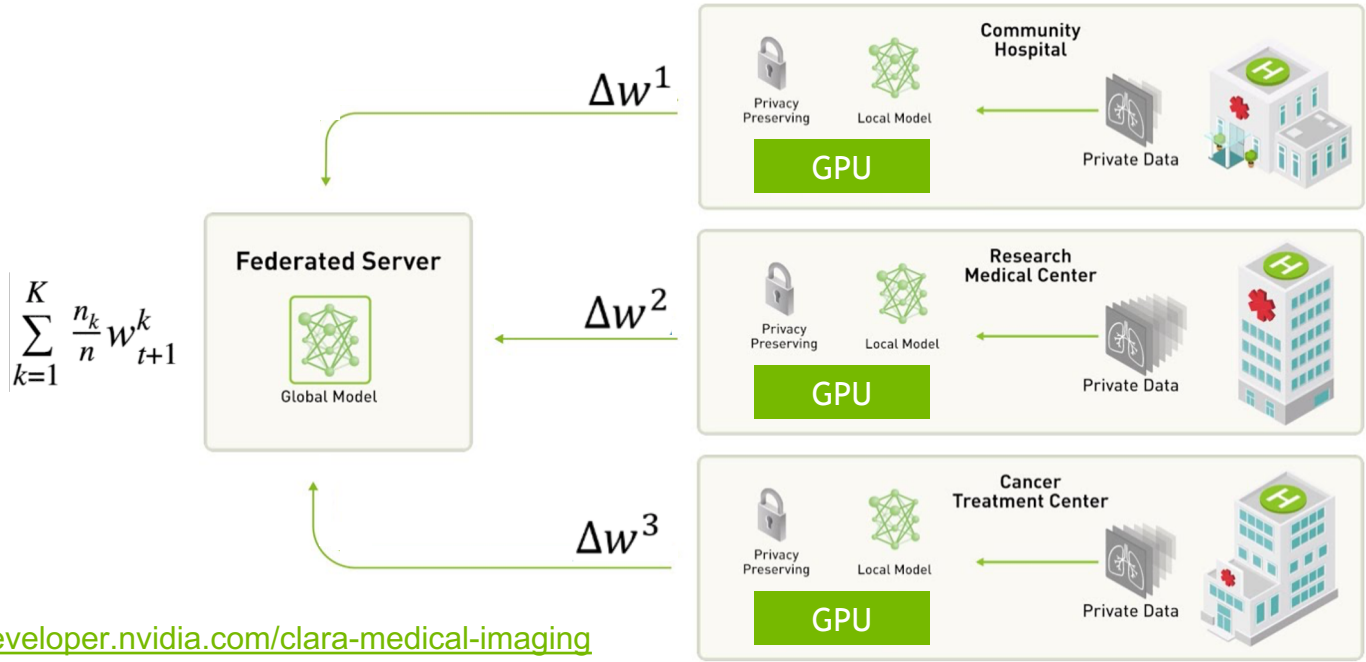


https://developer.nvidia.com/clara-medical-imaging

Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A. (2019, October). Privacy-preserving Federated Brain Tumour Segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer, Cham.

SERVER-CLIENT FEDERATED LEARNING

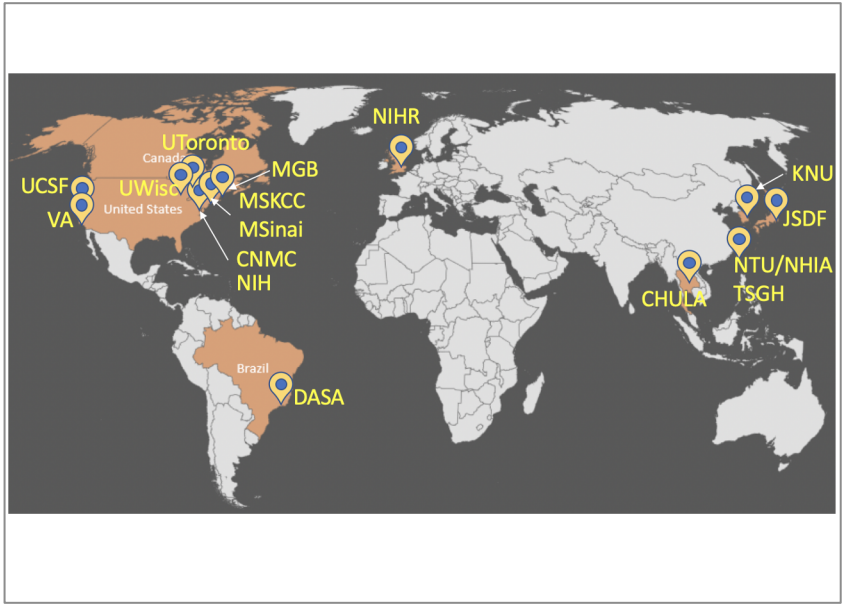
Changing the way AI algorithms are trained



https://developer.nvidia.com/clara-medical-imaging

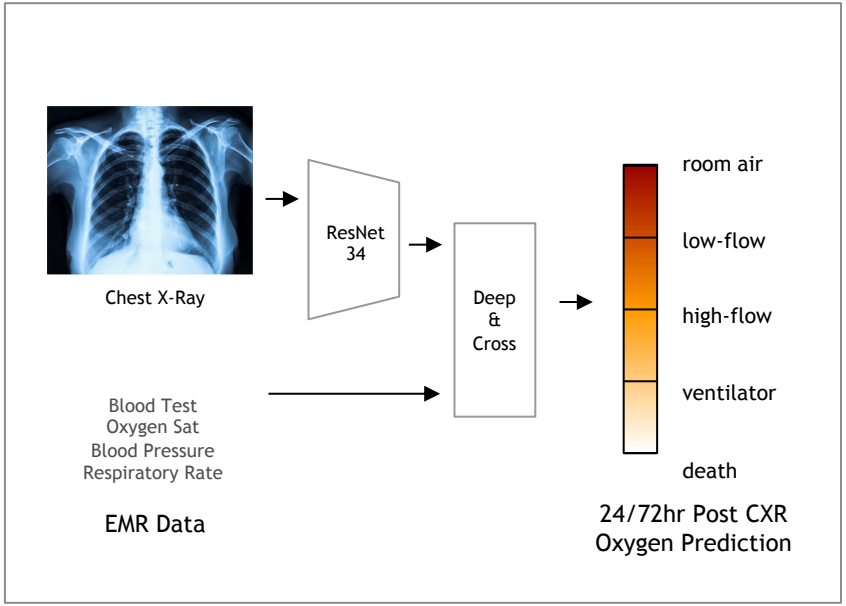
Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A. (2019, October). Privacy-preserving Federated Brain Tumour Segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer, Cham.

CLARA FEDERATED LEARNING FOR COVID-19 PATIENT CARE "EXAM" AI MODEL



Clara Federated Learning

20 Sites | 8 Countries
COVID-19 Oxygen Prediction



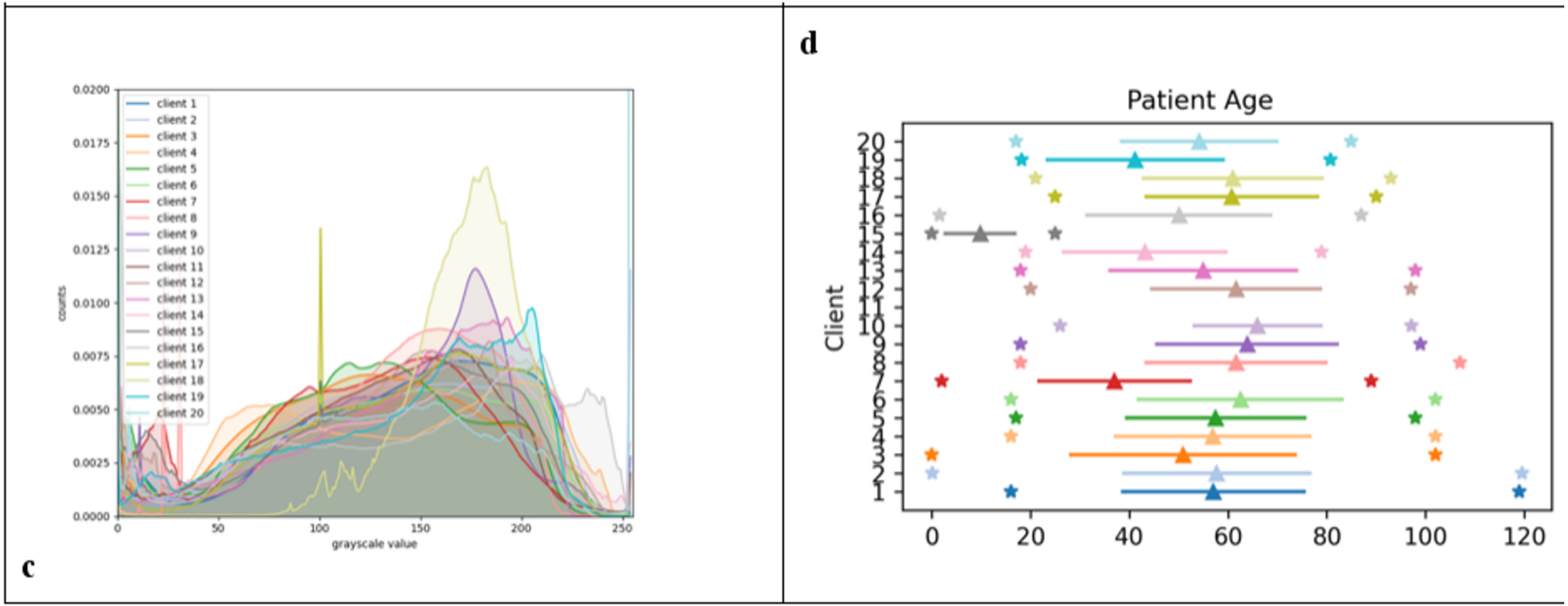
Collaborative Training of Model

Every Site Benefited Regardless of Dataset Size

Hospitals Build AI Model that Predicts Oxygen Needs of COVID-19 Patients | NVIDIA Blog

I. Dayan et al. Nature Medicine 2021

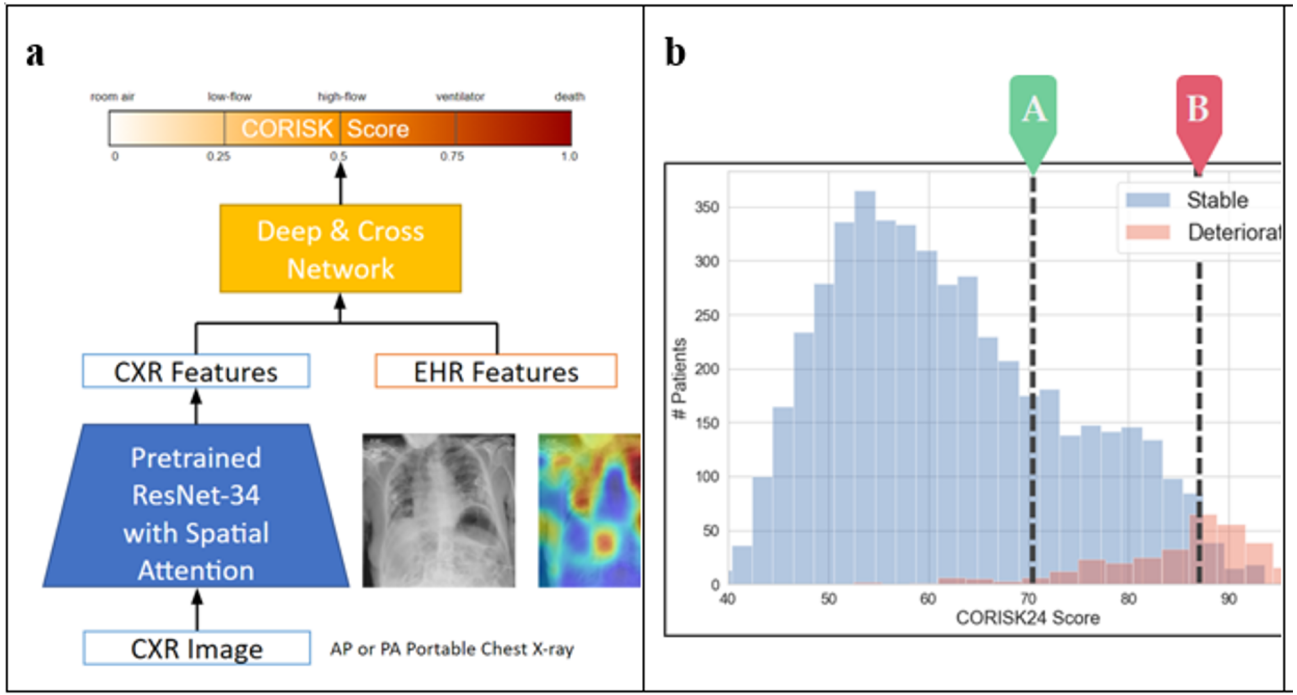
DATA DISTRIBUTIONS



c, CXR intensity distributions at each client site **d,** Age of patients included at each client-site showing the min. and max. ages (asterisks) and mean and standard deviation (length of bars).

I. Dayan et al. Nature Medicine 2021

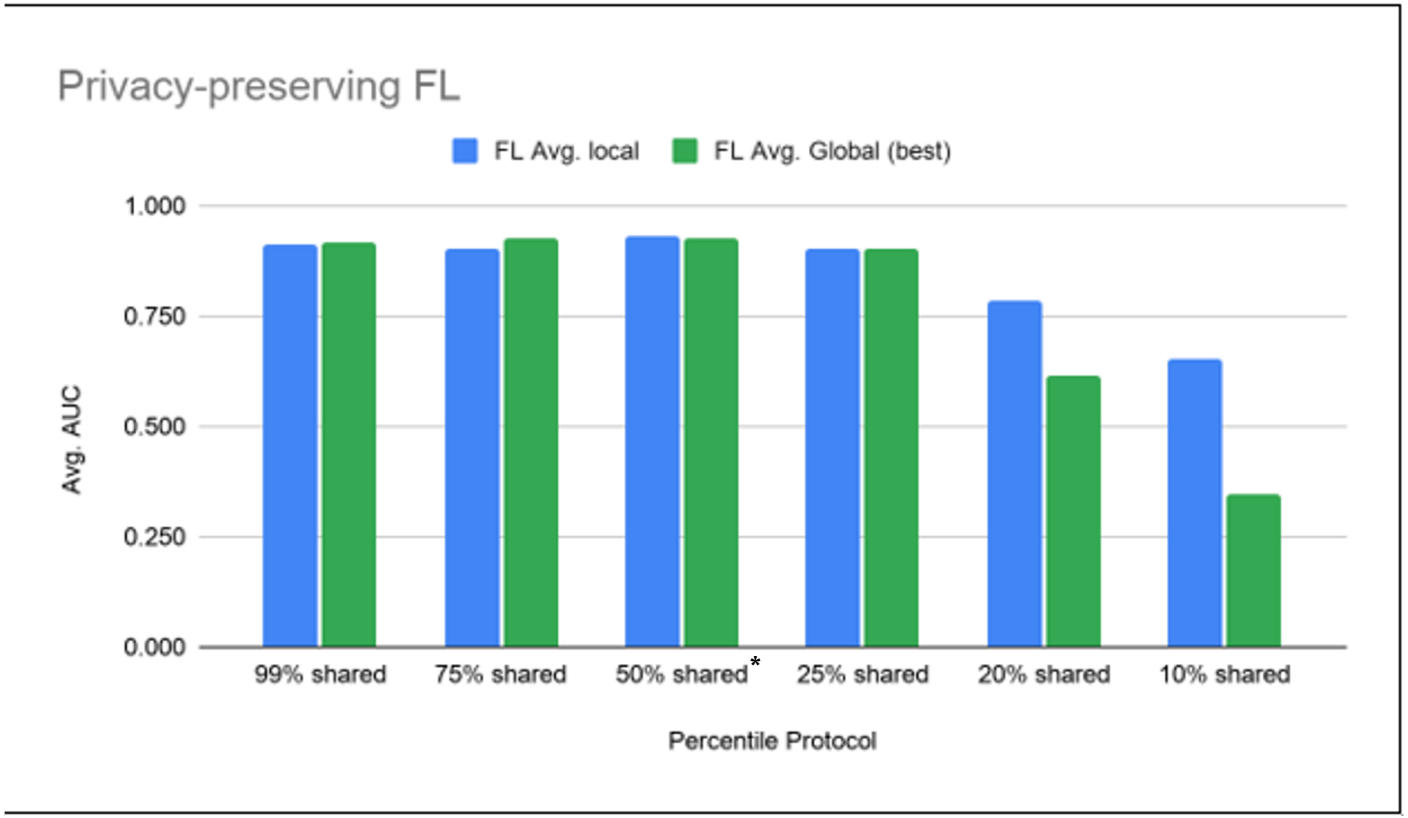
CLINICAL APPLICATION



(a) Our proposed model to predict a COVID risk score, **(b)** Histogram of CORISK results at MGB, with an illustration of how the score can be used for patient triage, in which 'A' is an example threshold for safe discharge that has 99.5% negative predictive value, and 'B' is an example threshold for ICU admission that has 50.3% positive predictive value

CORISK paper: Zhong, A. *et al.* Deep Metric Learning-based Image Retrieval System for Chest Radiograph and its Clinical Applications in COVID-19. *arXiv [eess.IV]* (2020). arxiv Preprint 2012.03663

I. Dayan et al. Nature Medicine 2021



*used for published ngc model

I. Dayan et al. Nature Medicine 2021

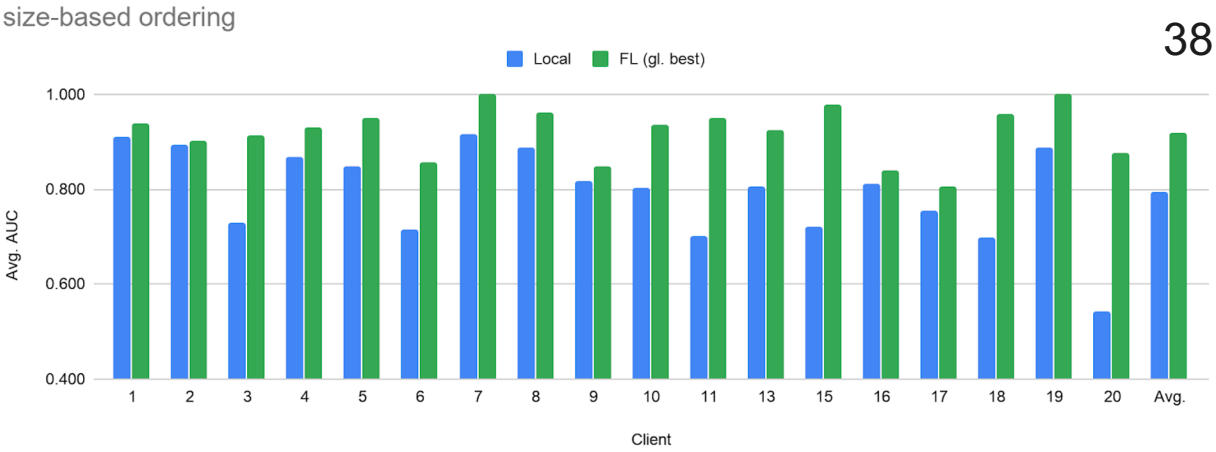
CLARA FL FOR COVID-19

FL resulted on average in

16% performance improvement

38% generalizability improvement

(3 repeated runs)



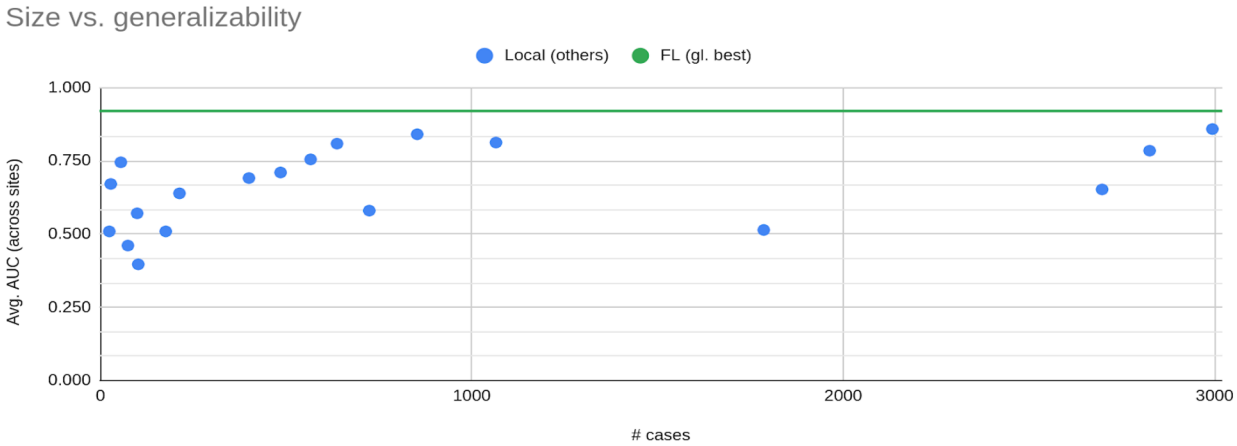
EXAM Model:

24h avg. AUC: **0.94**

72h avg. AUC: **0.91**

Available on NGC:

https://ngc.nvidia.com/catalog/models/nvidia:med:clara_train_covid19_exam_ehr_xray



I. Dayan et al. Nature Medicine 2021


Secure Aggregation with
Homomorphic Encryption

HOMOMORPHIC ENCRYPTION (HE)

What if I don't trust the server?

Homomorphic encryption (HE)

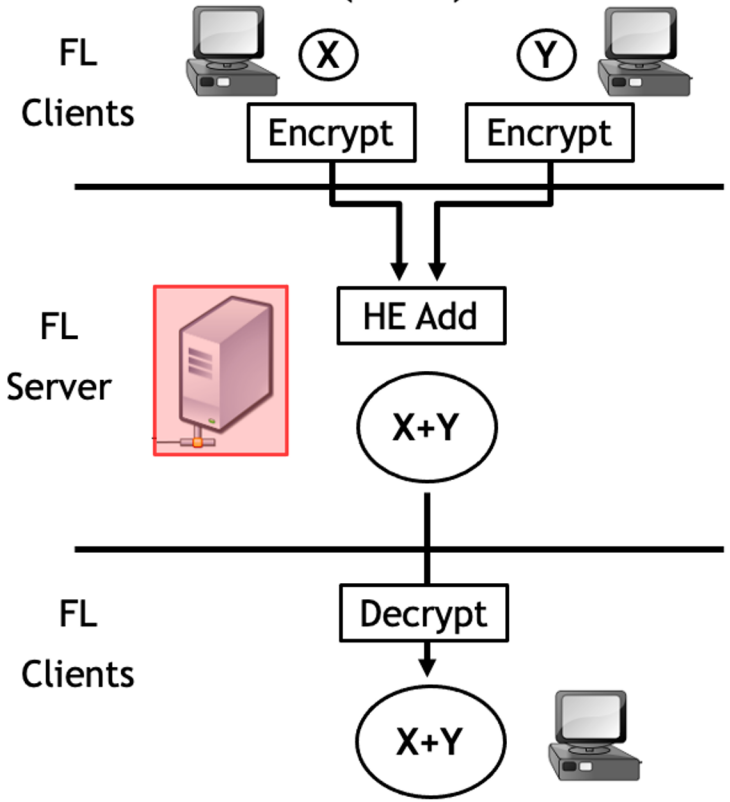
- Form of encryption that permits users to perform computations on encrypted data

Secure Aggregation with Homomorphic Encryption

- Protecting gradient/model inversion or attacks on untrusted server

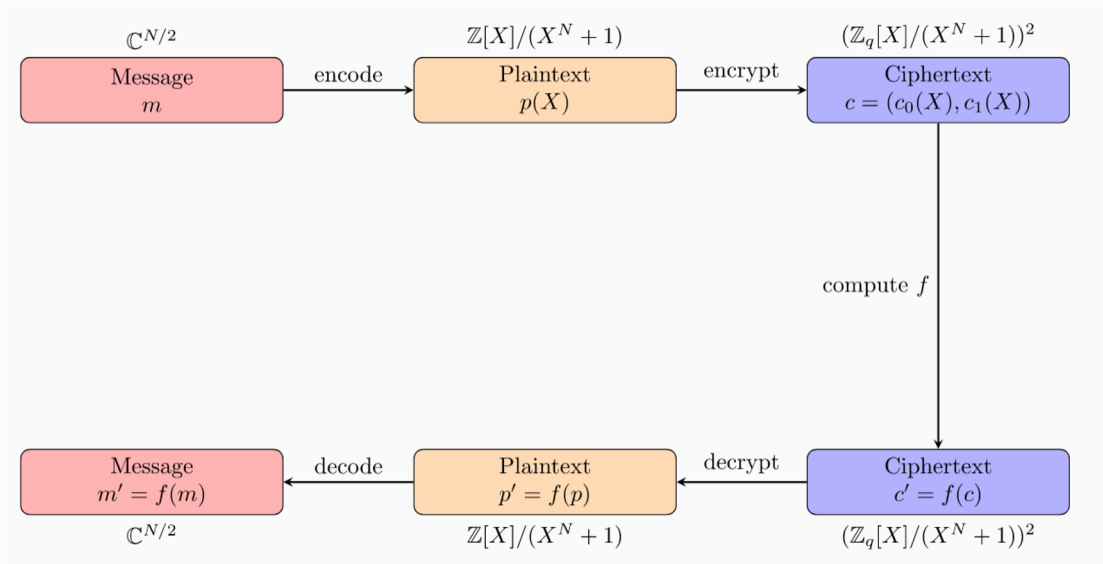
Clients have symmetric key for encryption/decryption

- Server can only save the encrypted model
- Secret keys for decryption are owned by clients



TenSEAL library (based on Microsoft SEAL)

High level view of CKKS



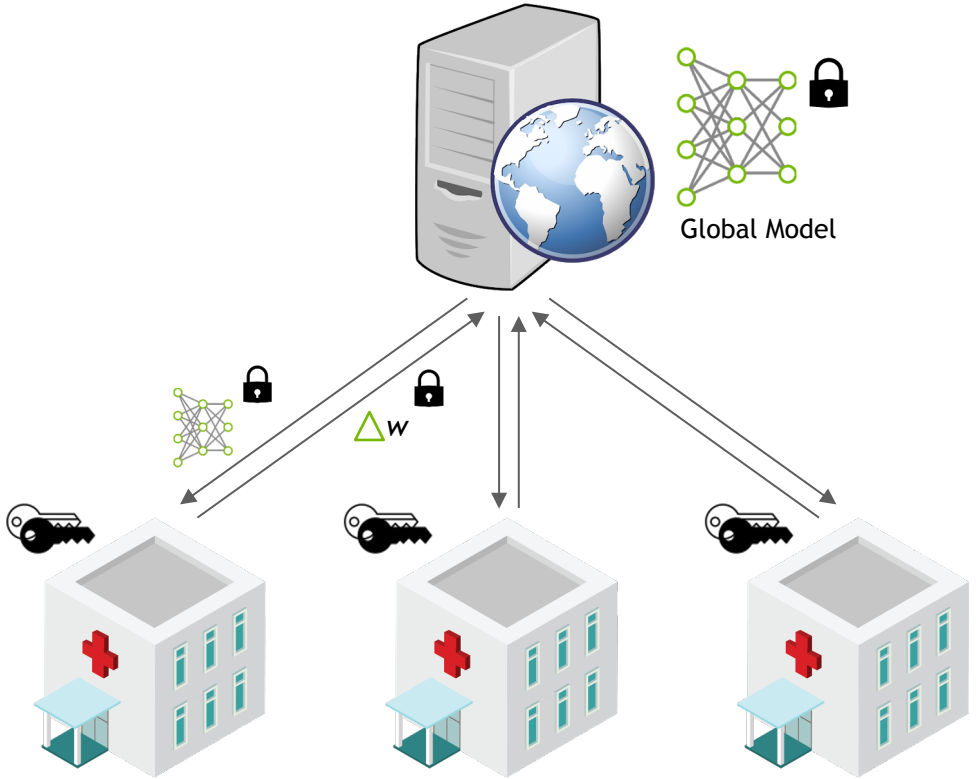
- CKKS encodes the data into polynomials
- Utilizes the properties of integer polynomial rings
- Proposed as a solution for encrypted machine learning (works with approximate floating point numbers)

Source: https://blog.openmined.org/ckks-explained-part-1-simple-encoding-and-decoding/

HE in Clara Train 4.0

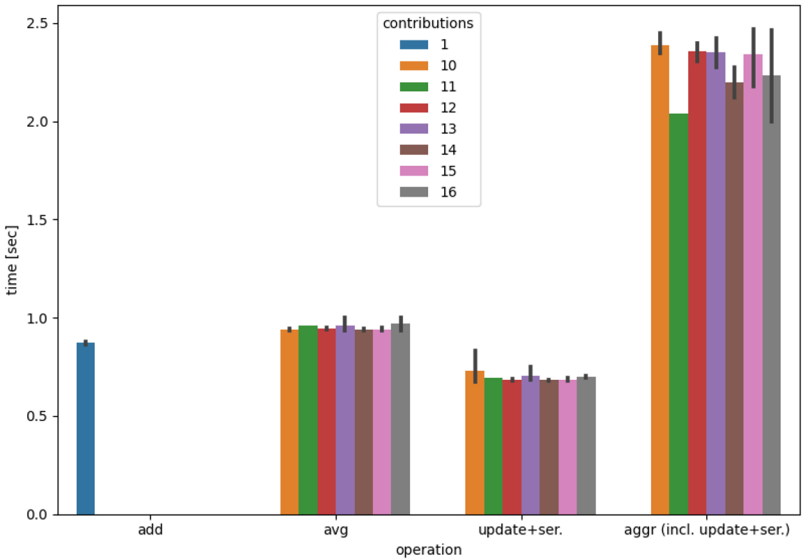
The clients all have a copy of the **same** symmetric key (assumes trust between clients)

Provisioning tool is used to generate those keys and securely distribute them to the hospitals (one-time process before using FL).

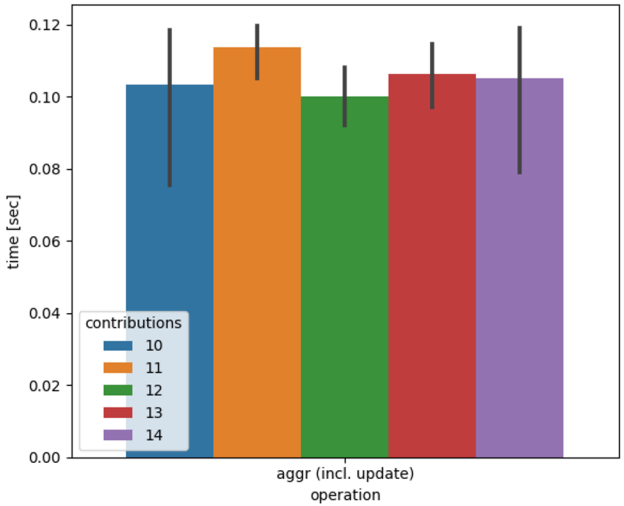


Symmetric key

HE vs. Raw (server-side, just in time aggregation)



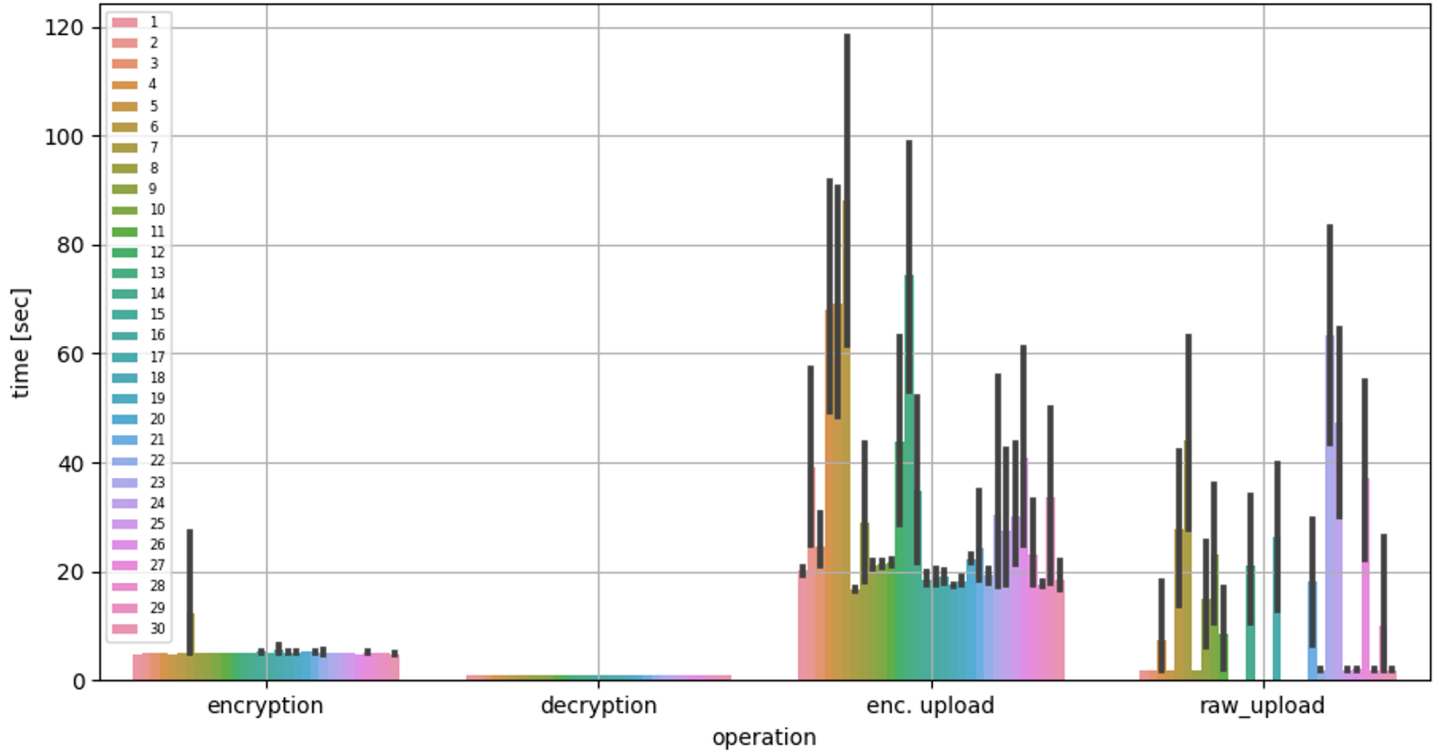
HE



Raw

Note: min. nr. clients is 10 (JIT), up to 30 clients connected, server on AWS. Aggr includes saving on server
SegResNet (U-Net), ~5 Million parameters, CT spleen segmentation, 100 rounds, 10 local epochs (V100, cuDNN benchmark, determ. diff. seeds);

HE vs. raw (client-side)



times
avg. encryption time: 5.01 +- 1.18 sec.
avg. decryption time: 0.95 +- 0.04 sec.
avg. enc. upload time: 38.00 +- 71.70 sec.
avg. raw upload time: 21.57 +- 74.23 sec.

Enc 283 MB
Raw 19 MB

HE benchmarking in 4.0

Setting	Message size [MB]	Nr. clients	Training time	Best global Dice	Best epoch	Rel. increase in training time
Raw	19	2	4:57:26	0.951	931	-
Raw	19	4	5:11:20	0.956	931	-
Raw	19	8	5:18:00	0.943	901	-
HE full	283	2	5:57:05	0.949	931	20.1%
HE full	283	4	6:00:05	0.946	811	15.7%
HE full	283	8	6:21:56	0.963	971	20.1%
HE conv layers	272	2	5:54:39	0.952	891	19.2%
HE conv layers	272	4	6:06:13	0.954	951	17.6%
HE conv layers	272	8	6:28:16	0.948	891	22.1%
HE three layers	43	2	5:12:10	0.957	811	5.0%
HE three layers	43	4	5:15:01	0.939	841	1.2%
HE three layers	43	8	5:19:02	0.949	971	0.3%

SegResNet (U-Net), ~5 Million parameters, CT spleen segmentation, 100 rounds, 10 local epochs (V100, cuDNN benchmark, determ. diff. seeds); Half of clients each with half of the training data and half of the validation data (reporting total training time and best average validation score of the global model)

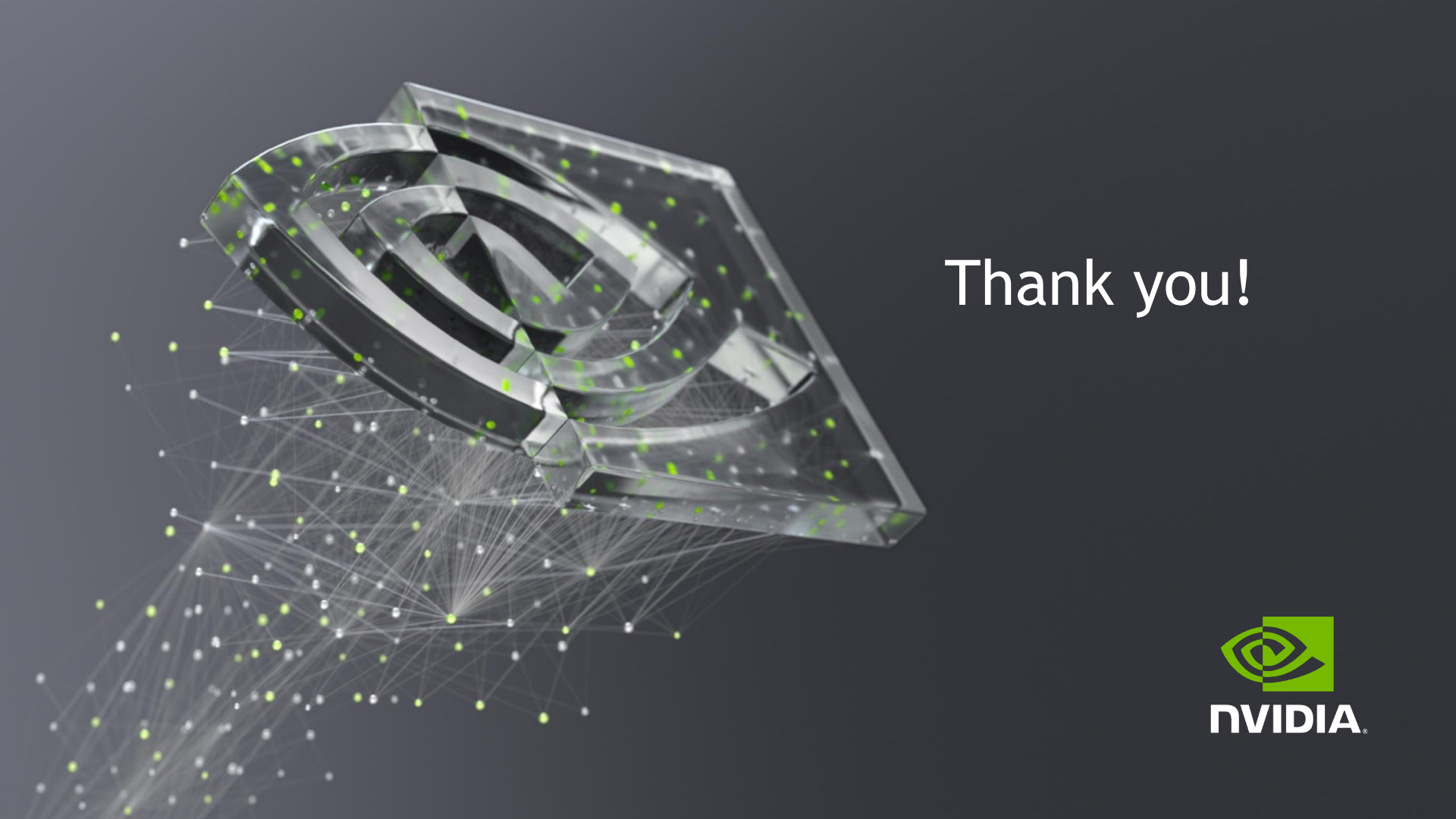
Considerations

- What is the optimal parameter setting for HE?
  - CKKS benchmarking by TenSEAL
  - Every setting that runs is considered secure (guaranteed 128 bits of security; following http://homomorphicencryption.org)
  - Our default setting increases message size by ~15x
    - full model encryption for large models might be impractical
- Partial model encryption might be enough to protect against gradient inversion
  - Differential privacy still needed to avoid subsequent model inversion

Resources

Standards: http://homomorphicencryption.org/
Talk: Practical Applications of Homomorphic Encryption
Slides: Building Applications with Homomorphic Encryption
Thesis: On the Explanation and Implementation of Three Open-Source Fully Homomorphic Encryption Libraries
Tutorials: https://blog.openmined.org/ckks-explained-part-1-simple-encoding-and-decoding/
TenSEAL tutorial on the CKKS scheme

Clara Train HE notebook: https://github.com/NVIDIA/clara-train-examples/blob/master/PyTorch/NoteBooks/FL/Homomorphic_Encryption.ipynb


Thank you!
NVIDIA