CaPC: from proof-of-concept to real-world applications

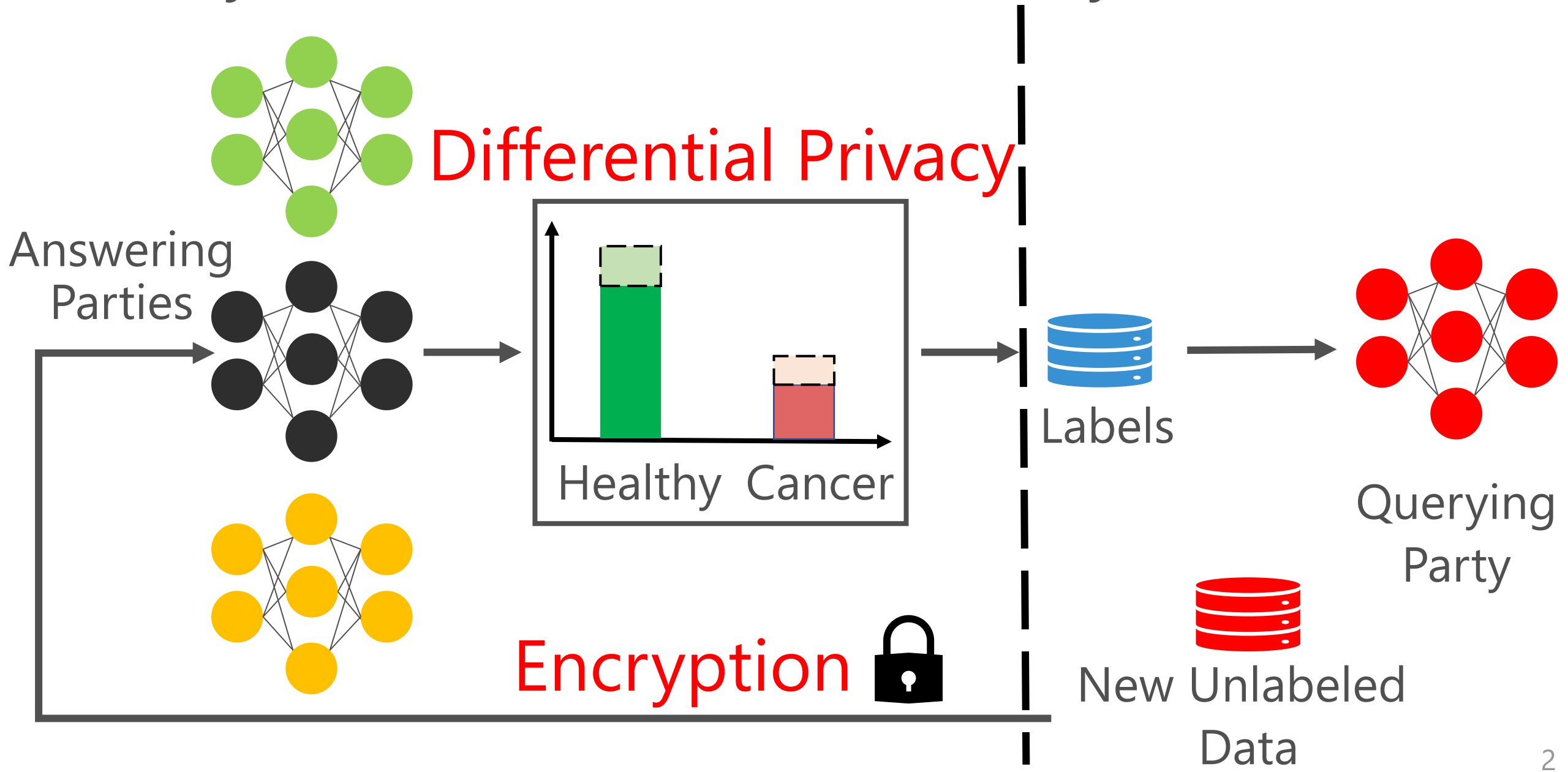
Adam Dziedzic
Nicolas Papernot

Intel Private AI
November 4th, 2021

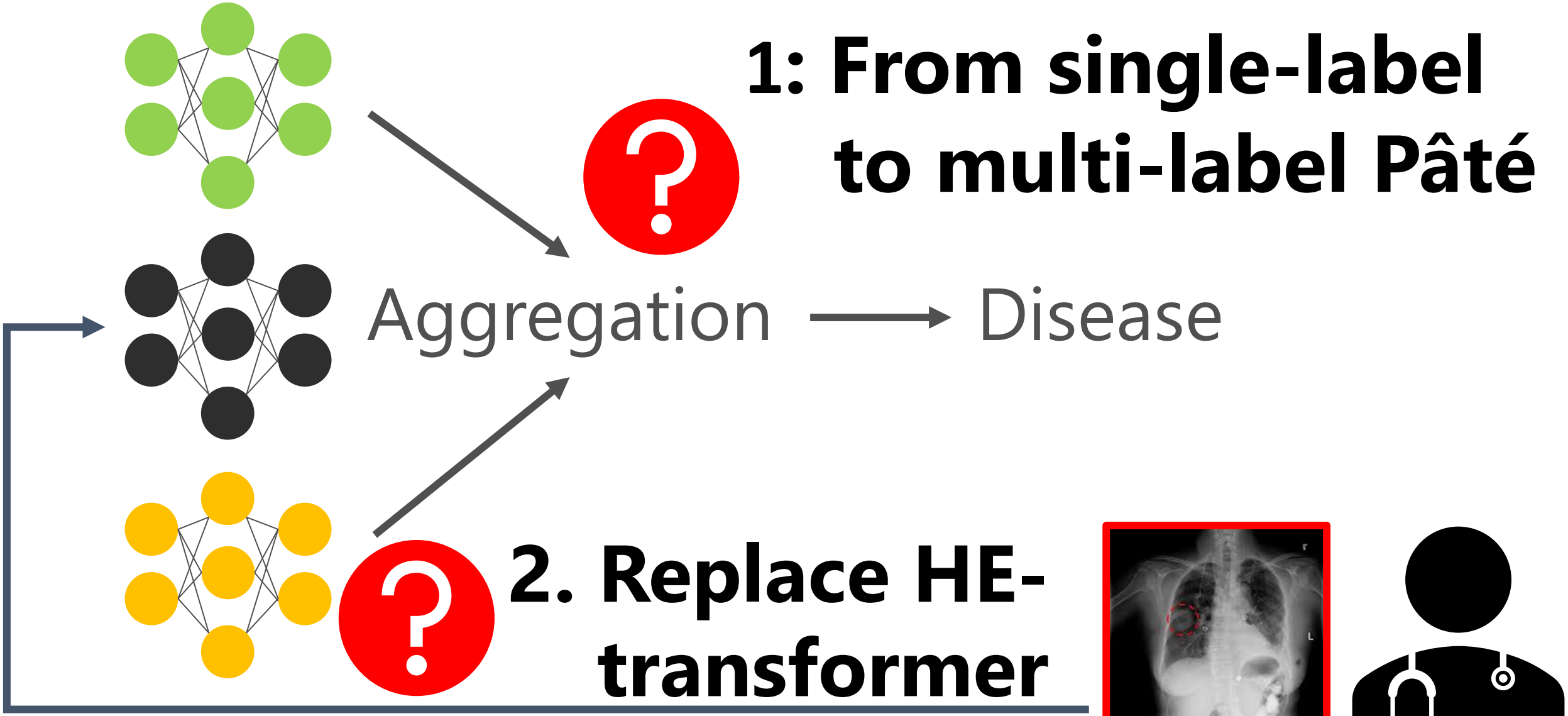
VECTOR INSTITUTE

UNIVERSITY OF TORONTO

Privacy of Train & Confidentiality of Test Data

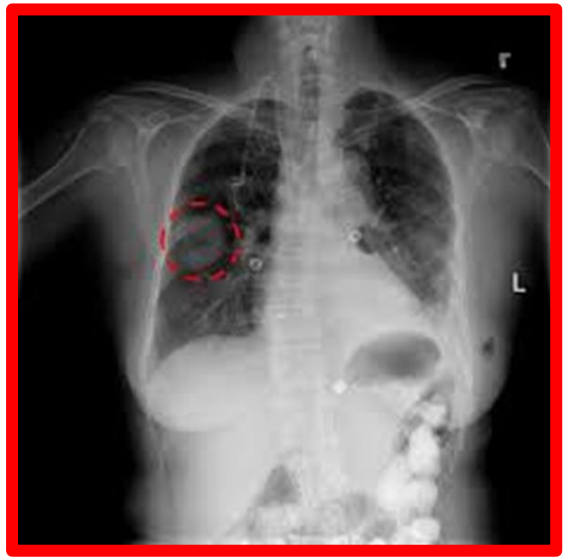


CaPC for X-rays & histological images



Single-label classification

airplane	automibile	bird	cat	deer	dog	frog	horse	ship	truck
0	0	0	0	0	0	0	0	0	**1**



Multi-label classification

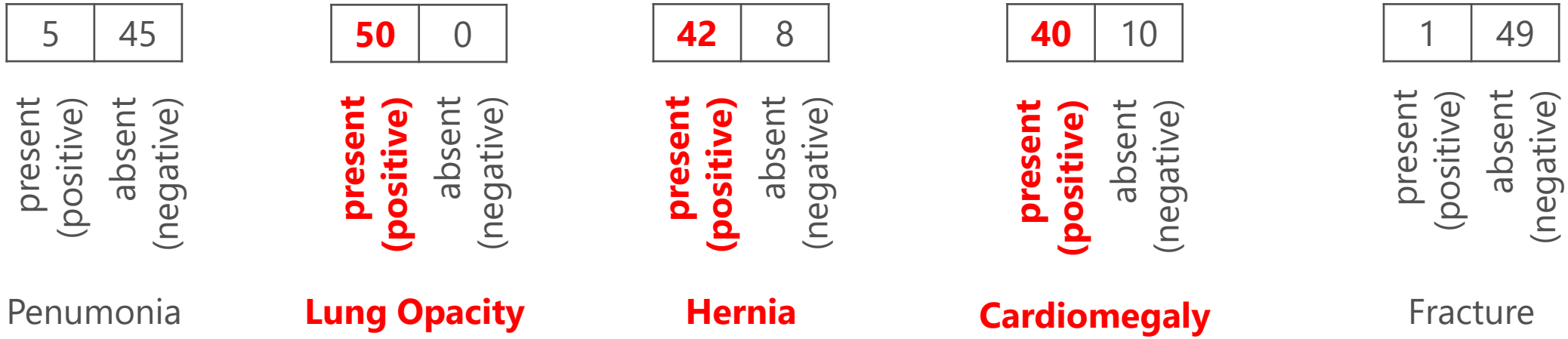
Pneumonia	**Lung Opacity**	**Hernia**	**Cardiomegaly**	Fracture
0	**1**	**1**	**1**	0

Single-label classification: standard Pâté

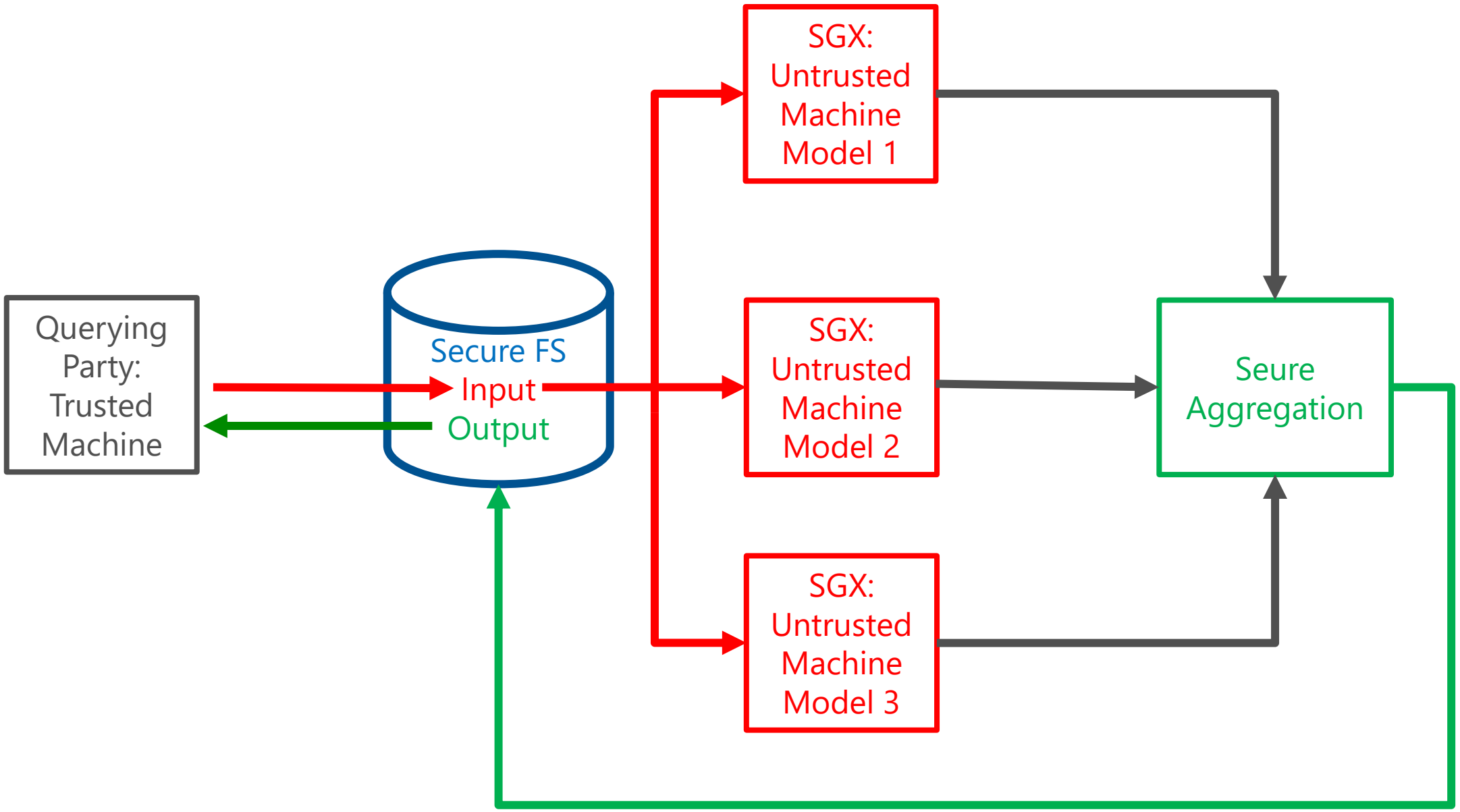
# of votes:

airplane	automibile	bird	cat	deer	dog	frog	horse	ship	**truck**
0	0	0	0	0	0	0	1	15	**34**

Multi-label classification: binary Pâté per label



Replace HE-transformer with SGX



CaPC from proof-of-concept to applications

- CaPC for private and confidential collaboration.
- Privacy of train data protected with differential privacy.
- Confidentiality of test data is achieved via encryption.
- Pâté for other ML tasks: multi-label classification on medical data. Privacy analysis for the multi-label classification with Pâté.
- Better system for private inference, such as via SGX or CrtypGPU.

Thank you

https://arxiv.org/abs/2102.05188
https://github.com/cleverhans-lab/capc-demo