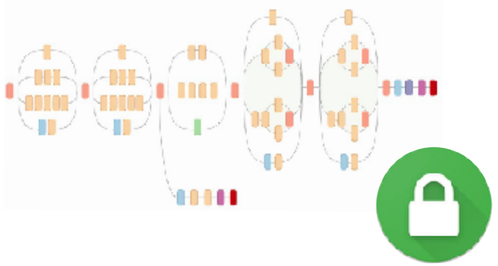
Cryptography behind

Private Machine Learning

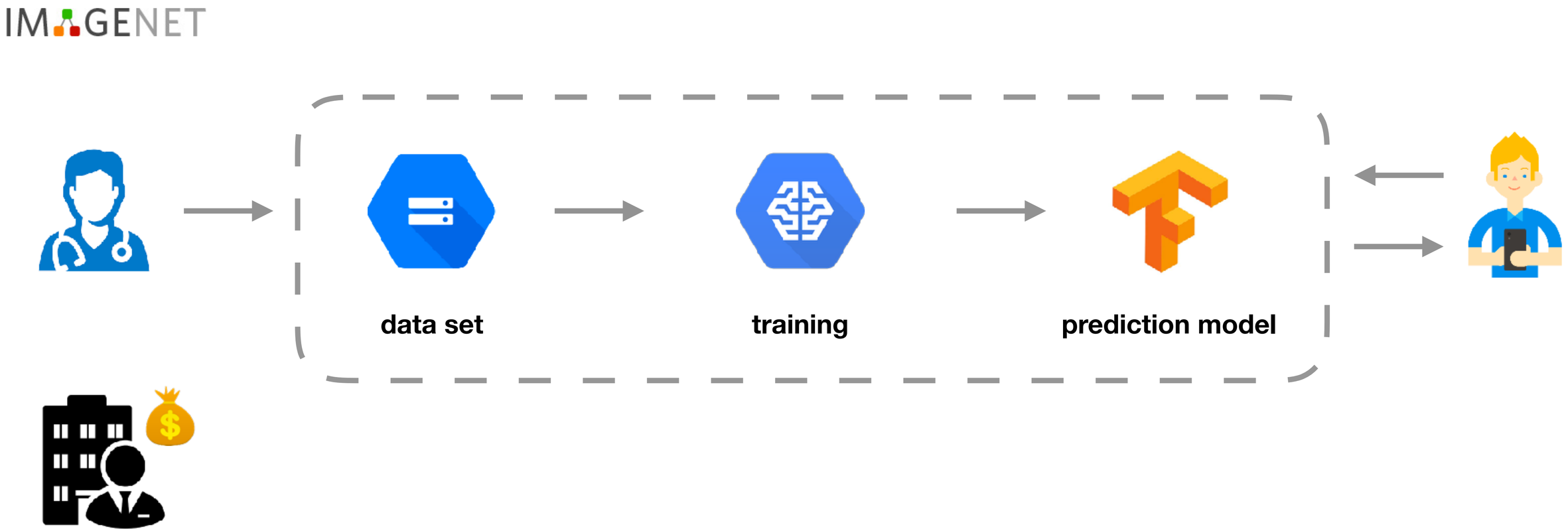


Morten Dahl

(Cyber)Security for Software Engineers meetup, June 2018

Why?

Machine Learning Process



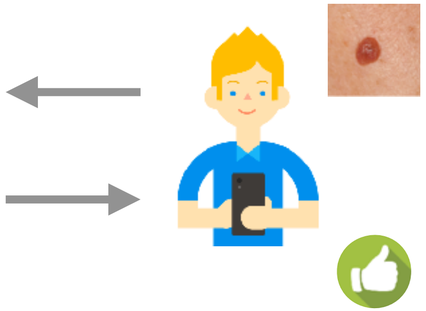
Skin Cancer Image Classification

Brett Kuprel

12:30-12:40pm

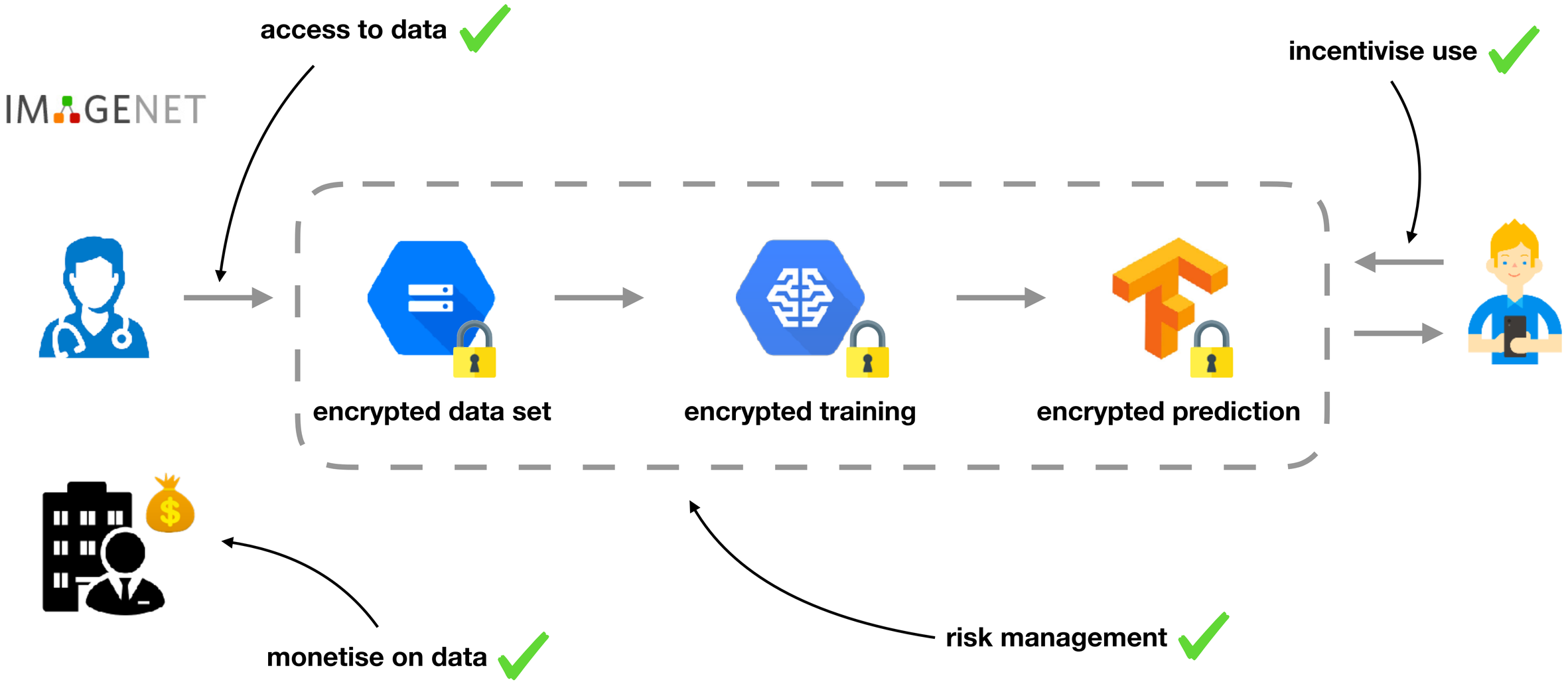
Join Brett Kuprel, and see how TensorFlow was used by the artificial intelligence lab and medical school of Stanford to classify skin cancer images. He'll describe the project steps: from acquiring a dataset, training a deep network, and evaluating of the results. To wrap up, Brett will give his take on the future of skin cancer image classification.

clinical photos → **transfer learning** → **CNN**



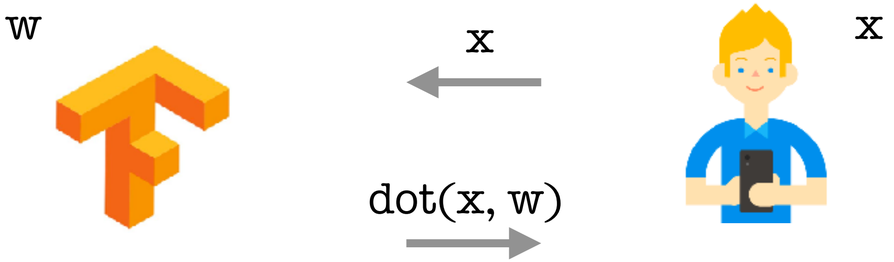
machine learning on sensitive information could make a big impact

Potential Bottlenecks



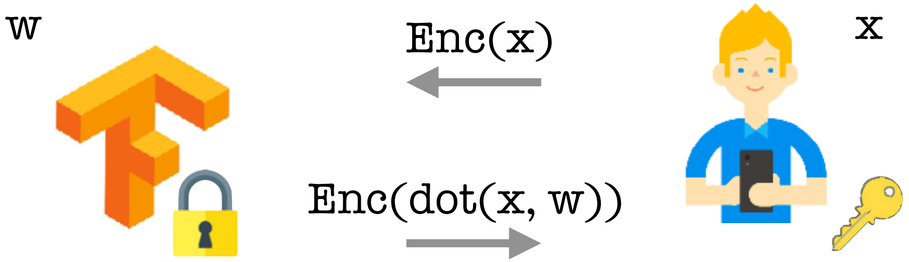
Prediction

Unencrypted Prediction



dot(x0 x1 x2 , w0 w1 w2) = x0*w0 + x1*w1 + x2*w2

Prediction on Encrypted Data



homomorphic encryption scheme

public multiplication

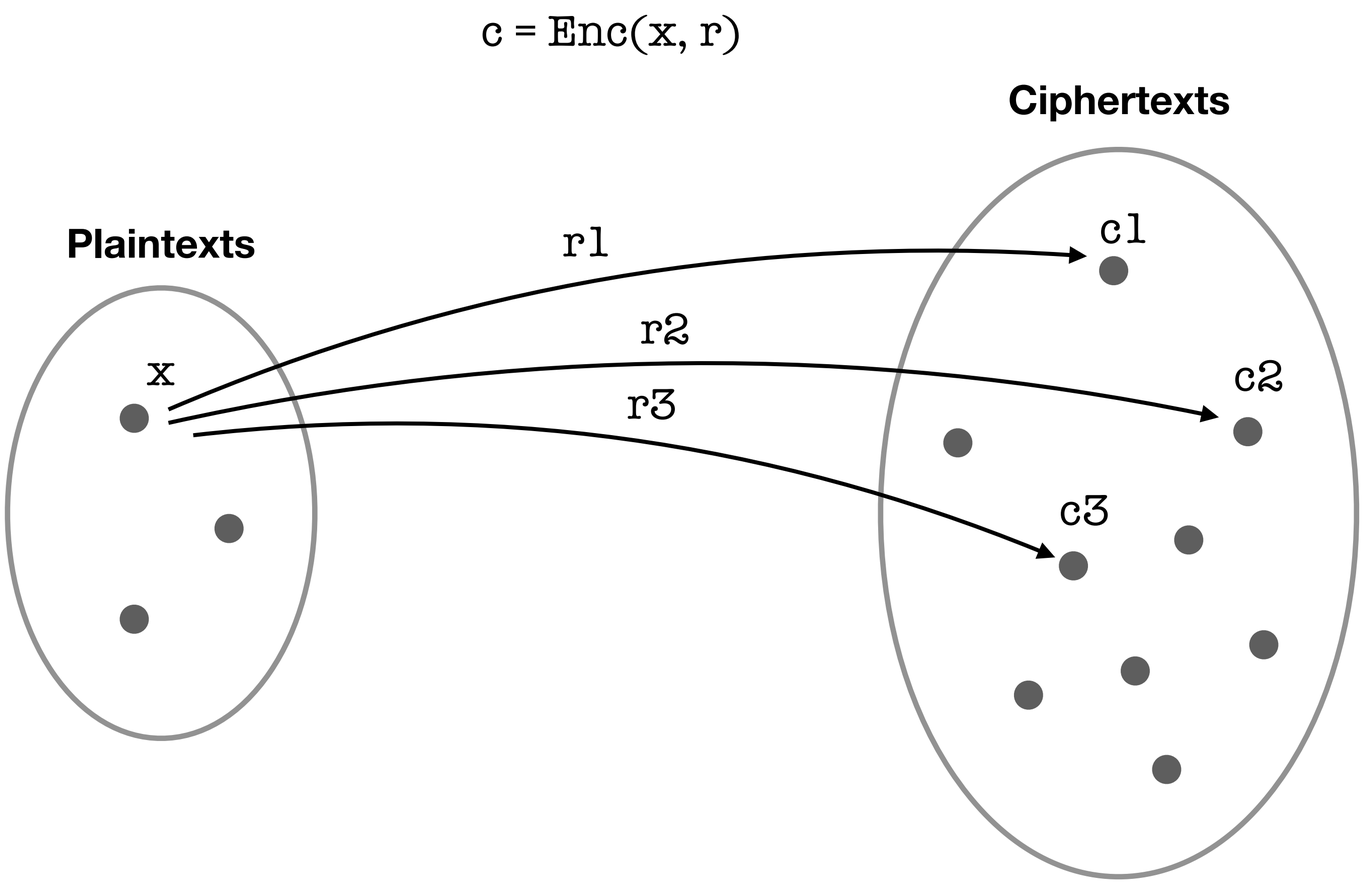
private addition

dot(Enc(x0) Enc(x1) Enc(x2) , w0 w1 w2) = Enc(x0)*w0 + Enc(x1)*w1 + Enc(x2)*w2

= Enc(x0*w0) + Enc(x1*w1) + Enc(x2*w2)

= Enc(x0*w0 + x1*w1 + x2*w2)

Paillier Encryption



Paillier Encryption

public encryption key

$$c = Enc(x, r) = g^x * r^n \bmod n^2$$

$g = 36$
$n = 35$
$n^2 = 1225$

$Enc(5, 2) = 36^5 * 2^{35} \bmod 1225 = 718$

$Enc(5, 4) = 36^5 * 4^{35} \bmod 1225 = 674$

Private Addition

Enc(x, r) * Enc(y, s)

= (g^x * r^n mod n^2) * (g^y * s^n mod n^2)

= g^(x + y) * (r * s)^n mod n^2

= Enc(x+y, r*s)

Enc(5, 2) * Enc(5, 4)
= 718 * 674
= 57
= 36^10 * 8^35
= Enc(10, 8)

Public Multiplication

Enc(x, r) ^ w

= (g^x * r^n mod n^2) ^ w

= g^(x*w) * (r^w)^n mod n^2

= Enc(x*w, r^w)

Enc(5, 2) ^ 2
= 718 * 718
= 1024
= 36^10 * 4^35
= Enc(10, 4)

What’s Next?

computationally expensive

4096 bit modulus

data expansion

available operations

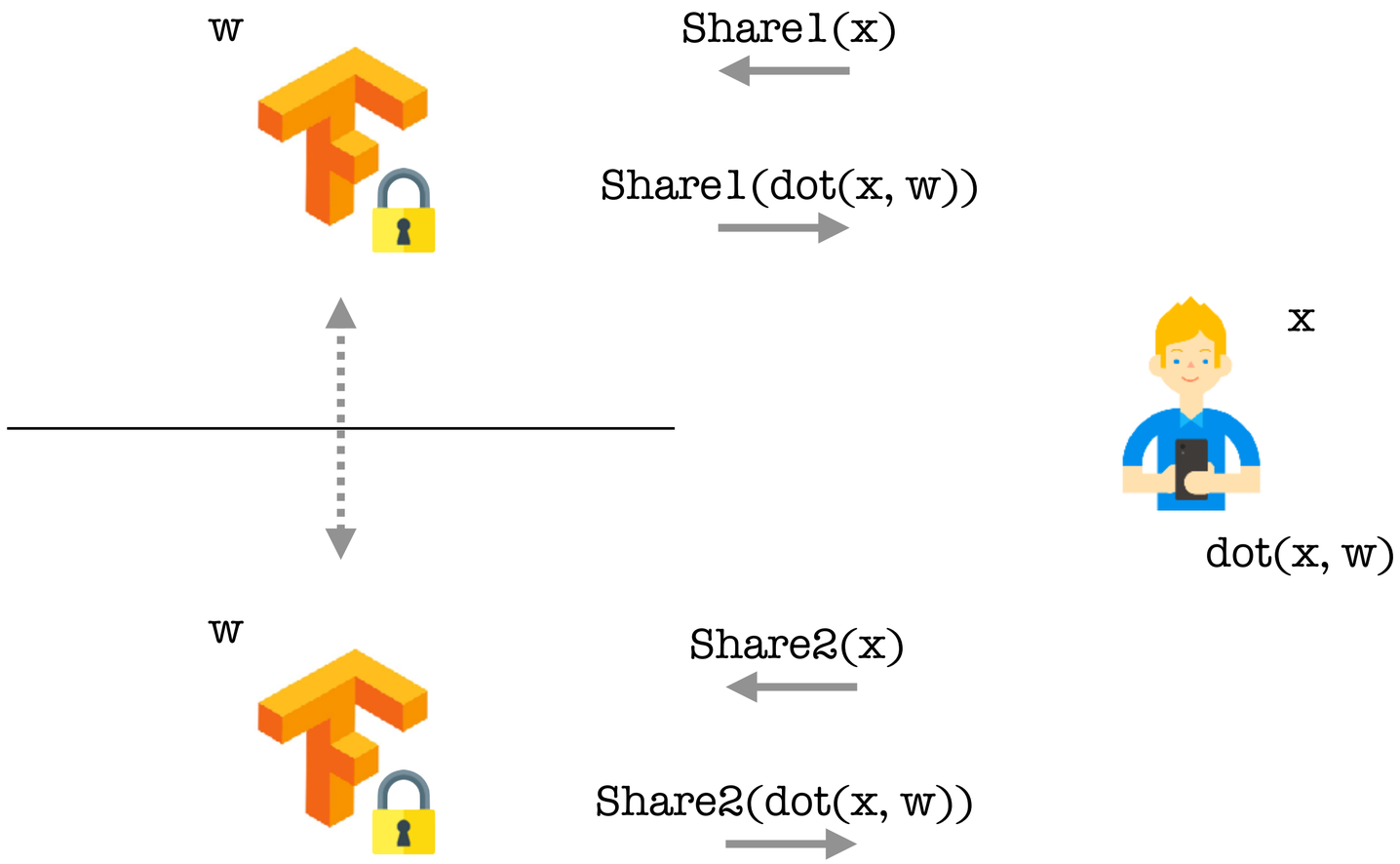
private multiplication

…

Secret Sharing

replace computation with communication

Prediction on Secret Shared Data



Secret Sharing in SPDZ

public parameter

$$x1 = \text{Share1}(x, r) = r \bmod m$$

$$x2 = \text{Share2}(x, r) = x - r \bmod m$$

$$x1 + x2 = x \bmod m$$

$m = 10$

$$\text{Share1}(5, 7) = 7 \bmod 10 = 7$$

$$\text{Share2}(5, 7) = 5 - 7 \bmod 10 = 8$$

Private Addition

$x1$ $\quad$ $y1$ $\quad$ $z1 = x1 + y1$

$x2$ $\quad$ $y2$ $\quad$ $z2 = x2 + y2$

$x1 + x2 = x$ $\quad$ $y1 + y2 = y$

$$
\begin{aligned}
& z1 + z2 \\
& \quad = (x1 + y1) + (x2 + y2) \\
& \quad = (x1 + x2) + (y1 + y2) \\
& \quad = x + y
\end{aligned}
$$

Public Multiplication

$x1$ w $z1 = x1 * w$

$x2$ w $z2 = x2 * w$

$x1 + x2 = x$

$$
\begin{aligned}
z1 + z2 \\
&= (x1 * w) + (x2 * w) \\
&= (x1 + x2) * w \\
&= x * w
\end{aligned}
$$

Private Multiplication

random triple

(a1 , b1 , c1) x1 y1 x - a y - b

z1 = (x - a)*(y - b)
+ (x - a)*b1
+ (y - b)*a1
+ c1

(a2 , b2 , c2) x2 y2 x - a y - b

z2 = (x - a)*b2
+ (y - b)*a2
+ c2

a1 + a2 = a

b1 + b2 = b

c1 + c2 = a * b

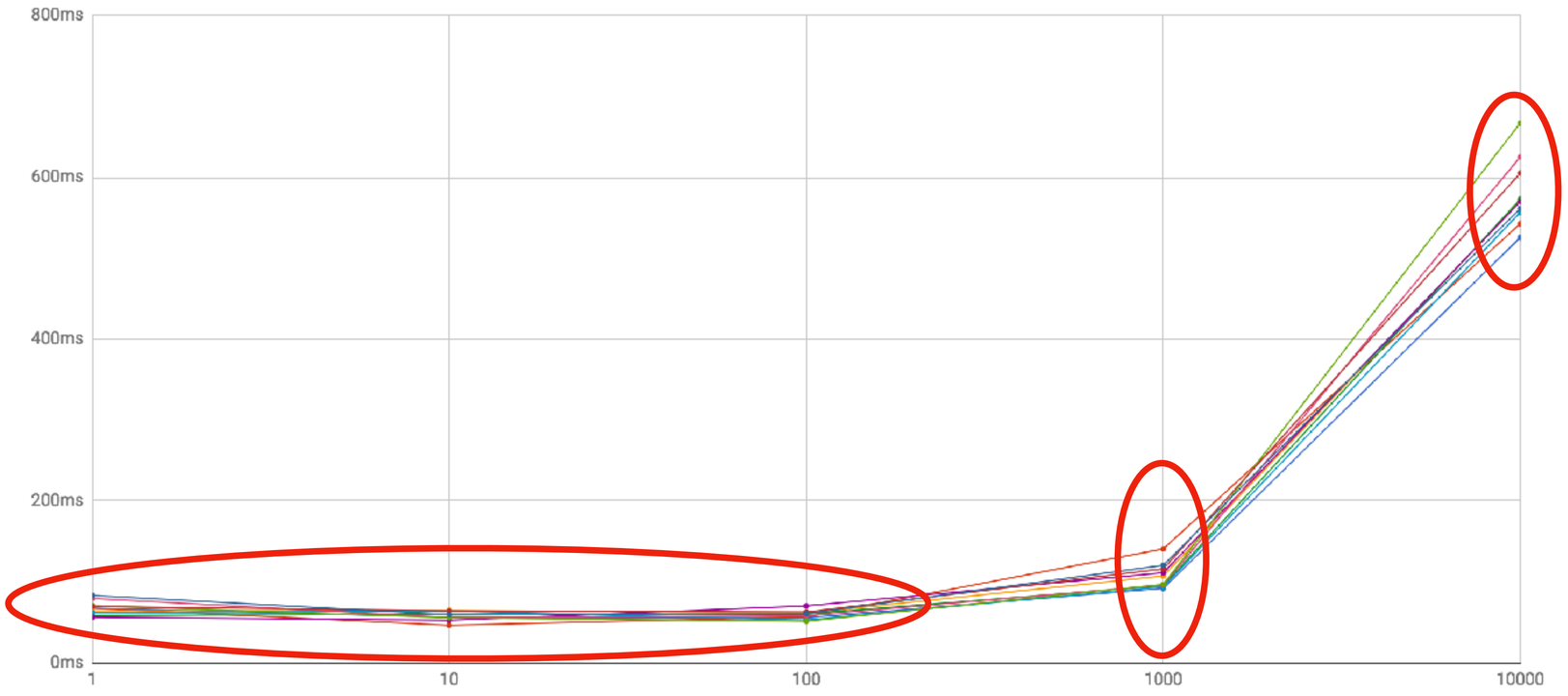
x1 + x2 = x y1 + y2 = y

z1 + z2
= ...
= x * y

Performance

logistic regression

Sigmoid evaluation, 100 features, servers on Google cloud (2 vCPU, 10 GB)



Getting Involved

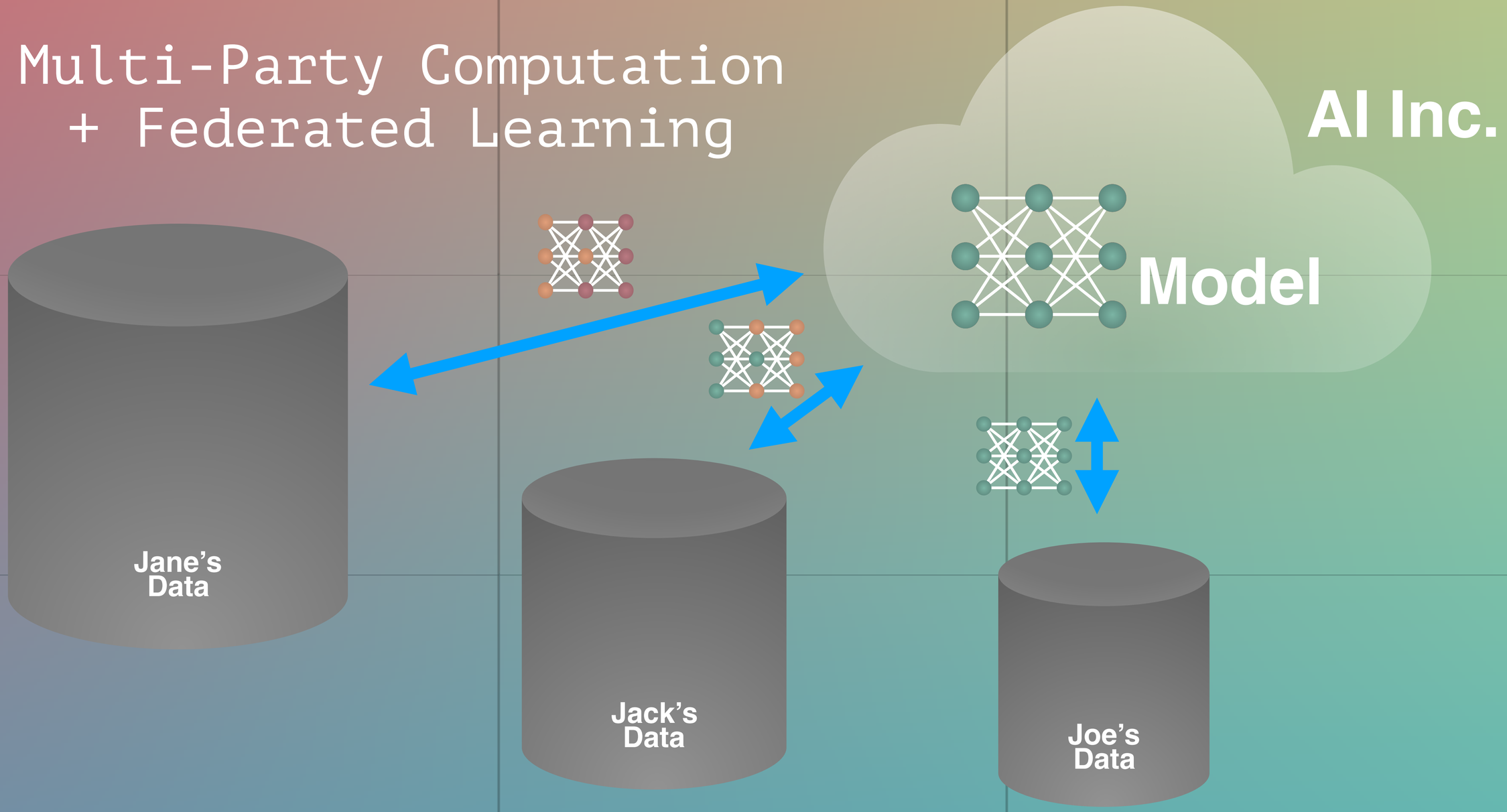
Tools for Safe AI

- Federated Learning
- Homomorphic Encryption
- Multi-Party Computation
- Gradient Validation Markets

OpenMined

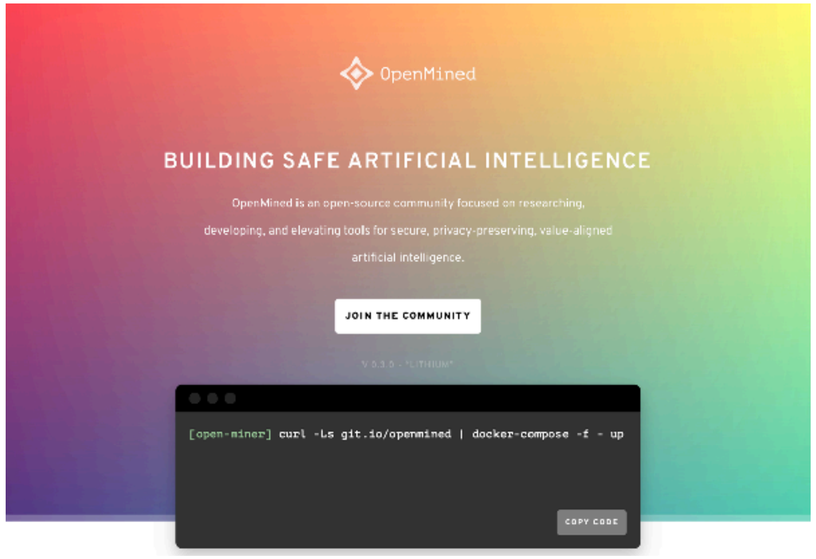
Slides originally by Andrew Trask

Multi-Party Computation + Federated Learning



@mortendahlcs

mortendahl.github.io



@openminedorg

openmined.org

Thank you