CryptoNets

Applying Neural Networks to Encrypted Data with High Throughput and Accuracy

ICML 2016, New York

Ran-Gilad Bachrach, Nathan Dowlin*, Kim Laine, Kristin Lauter,
Michael Naehrig, John Wernsing

Microsoft Research, WA

* Princeton University, NJ

Prediction as a Service

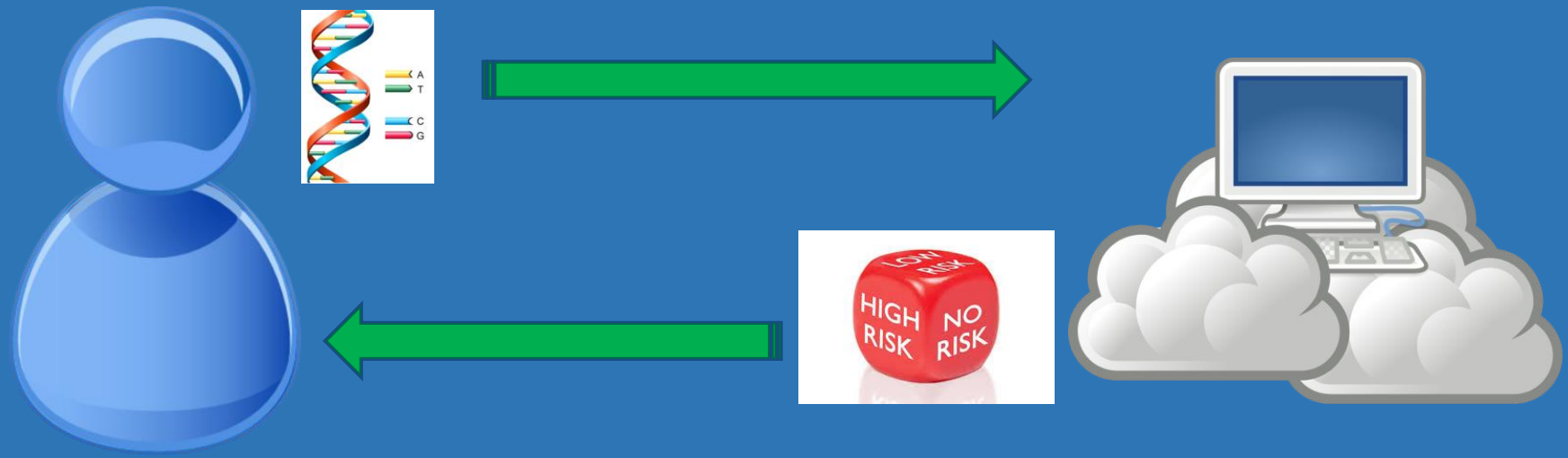
Prediction as a Service

Medical

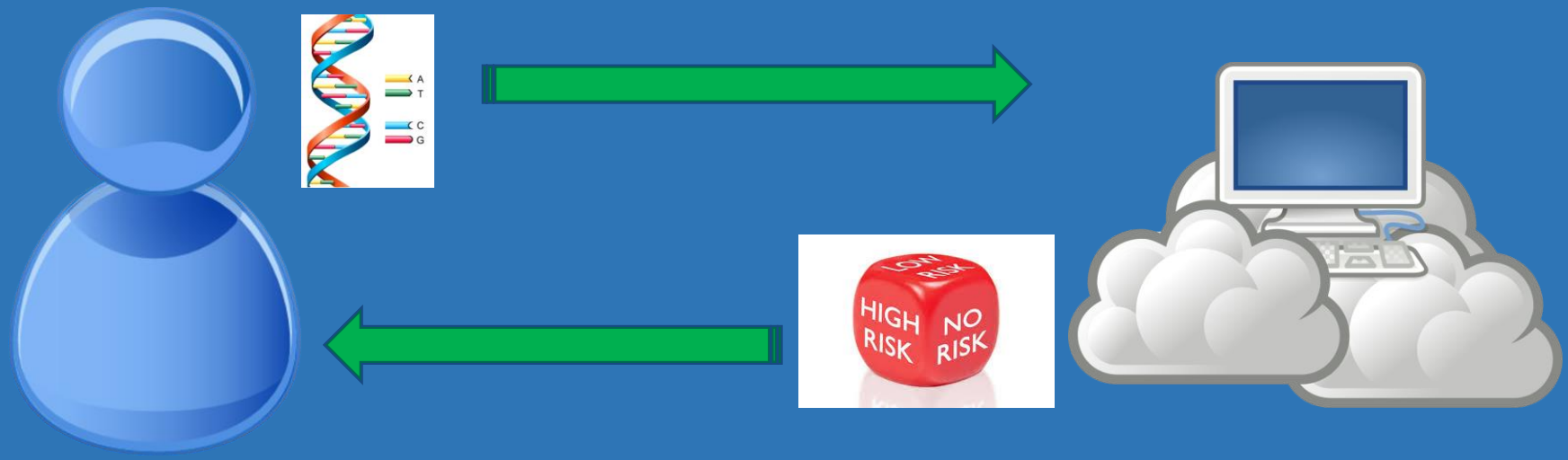
Genomic

Financial

Wait. What about privacy?

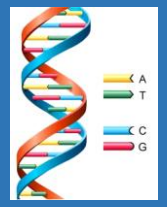

A
T
C
G
LOW RISK
HIGH RISK
NO RISK

Who else is going to see your DNA sequence and the prediction?



Who else is going to see your DNA sequence and the prediction?

"Sorry, your DNA does not match this job description."

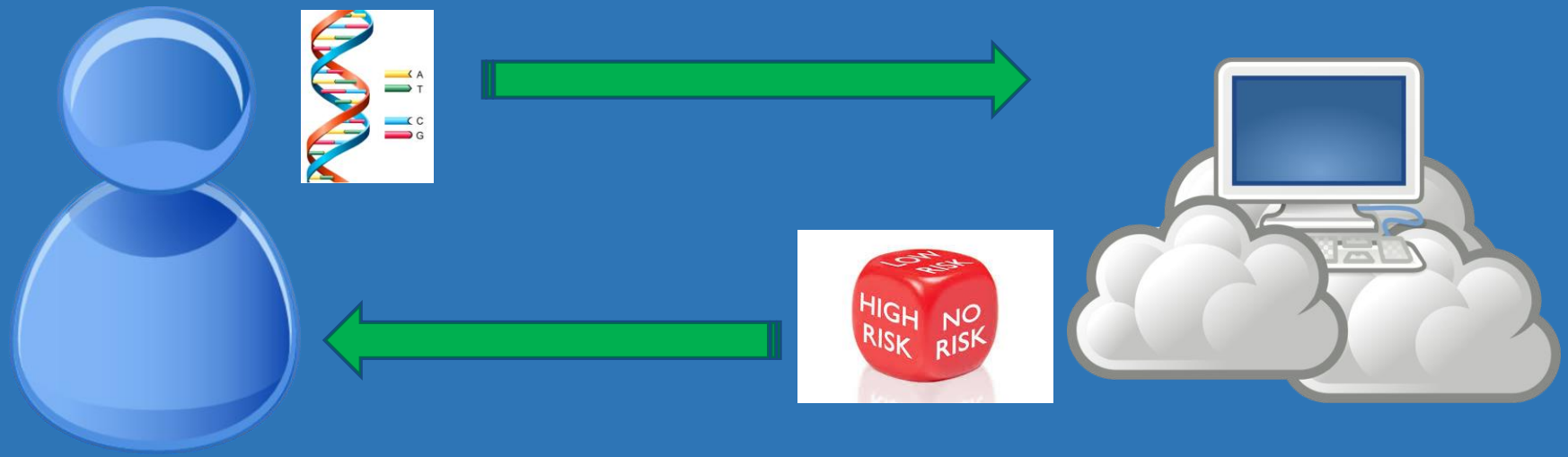


"Here is an advertisement that according to your DNA you will not be able to resist."

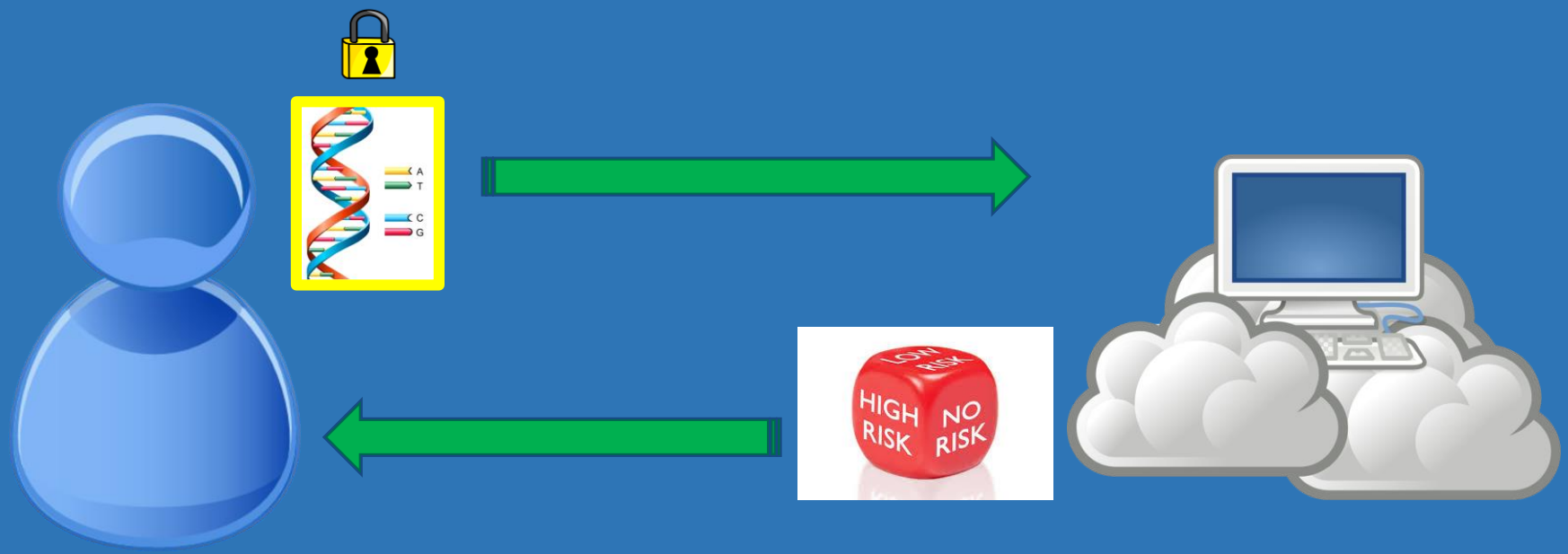
"We are not giving you this loan because it is not in your DNA to pay it back."

Inference Over Encrypted Data

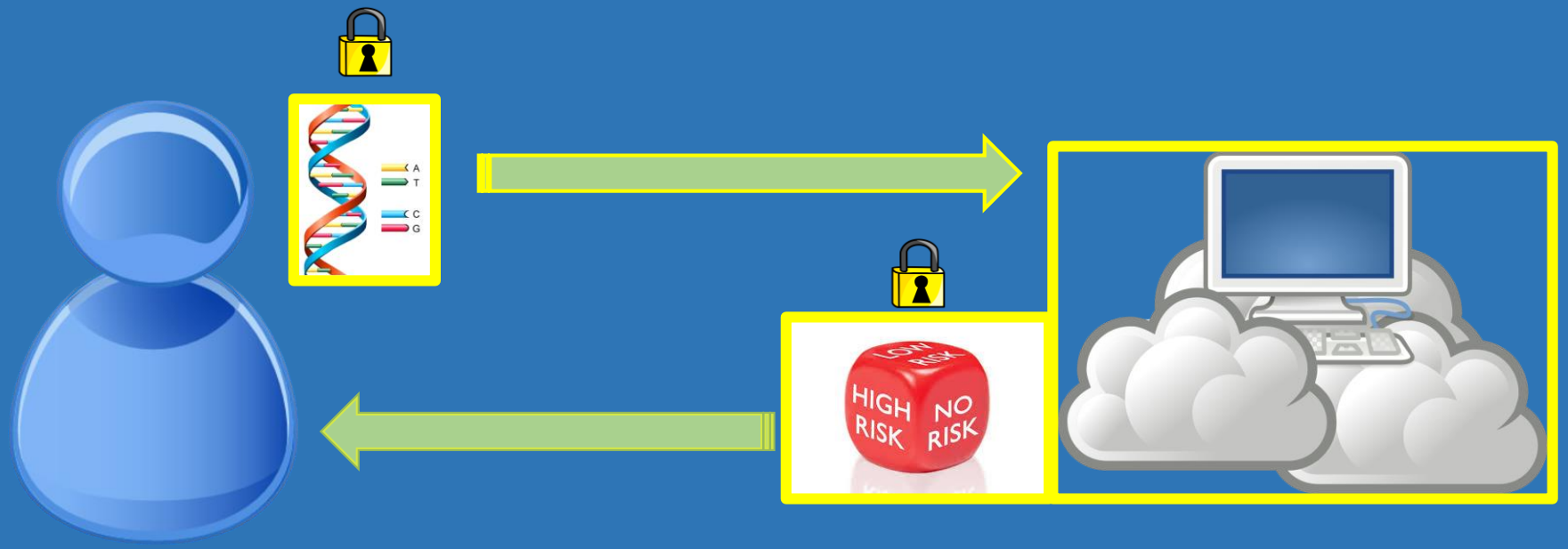
Inference Over Encrypted Data



Inference Over Encrypted Data



Inference Over Encrypted Data



Homomorphic Encryption

Fully Homomorphic Encryption Using Ideal Lattices

Craig Gentry
Stanford University and IBM Watson
cgentry@cs.stanford.edu

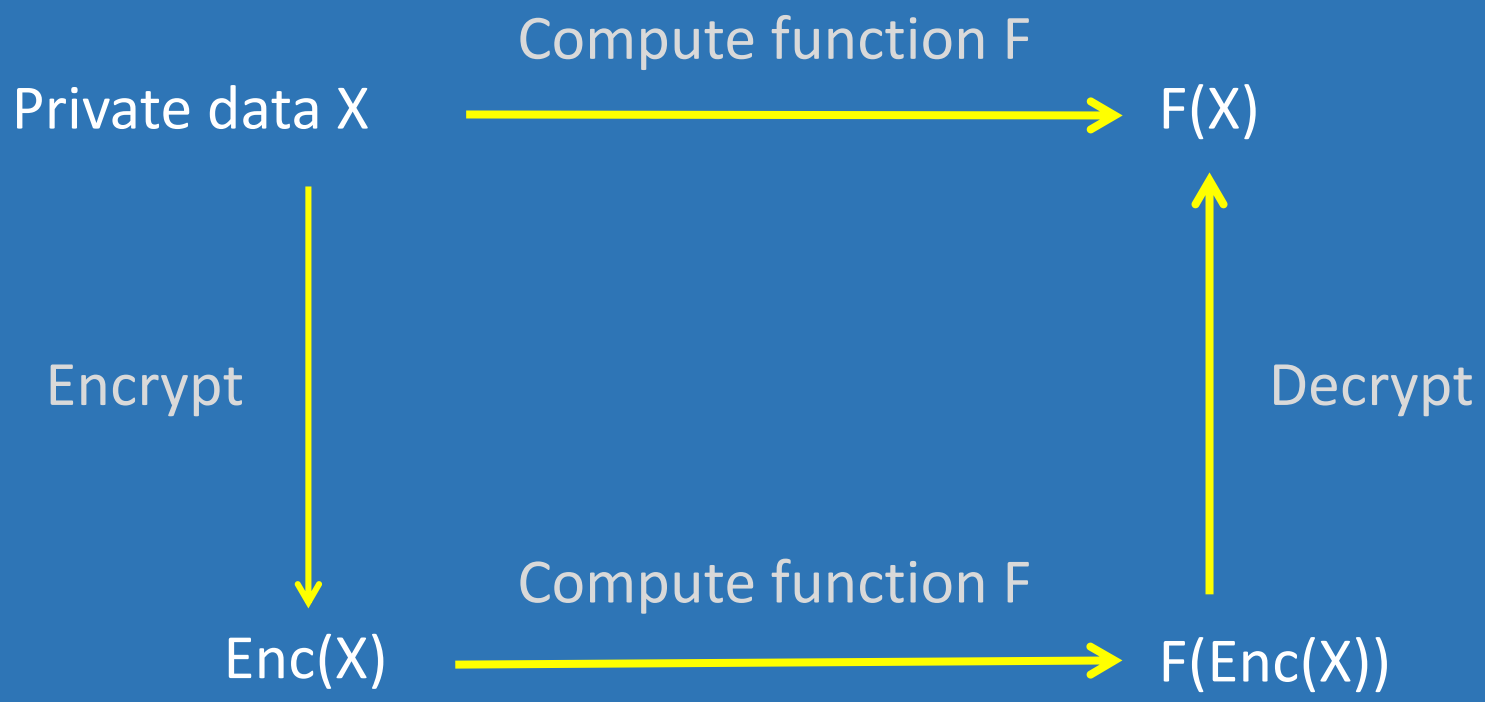
ABSTRACT

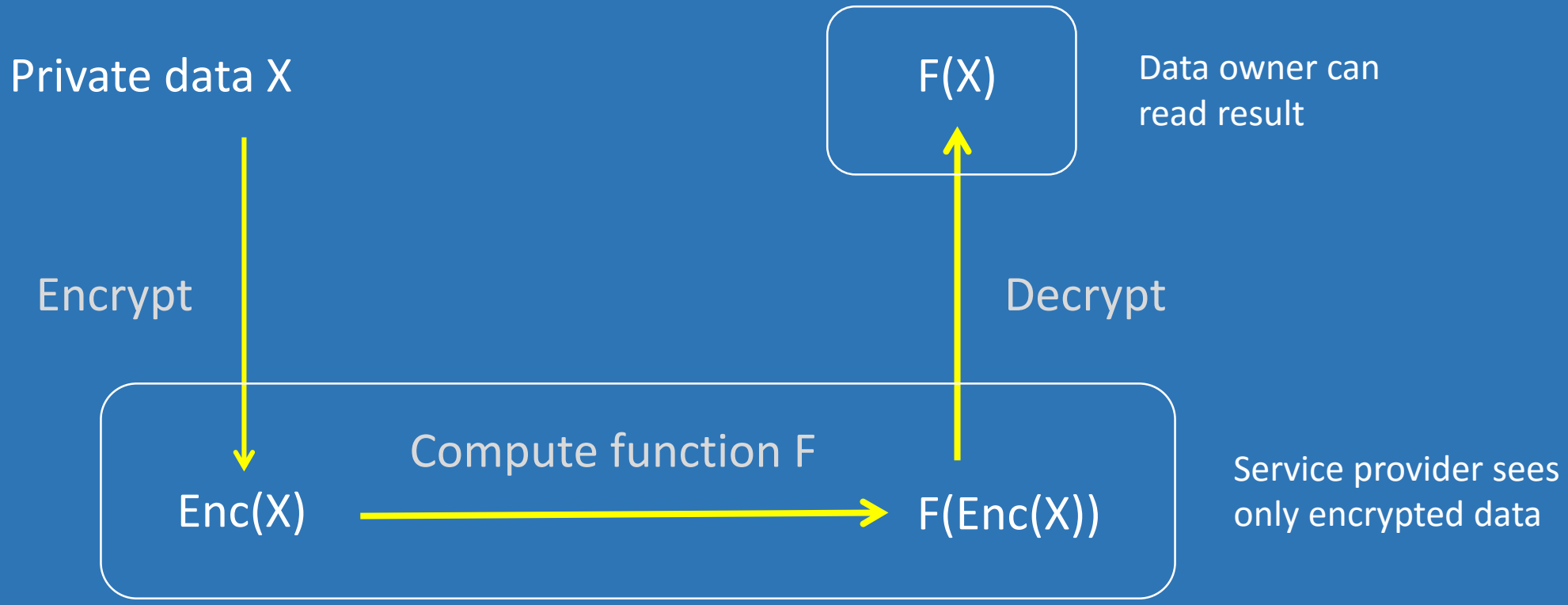
We propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of *arbitrary circuits*, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its *own decryption circuit*; we call a scheme that can evaluate its (augmented) decryption circuit *bootstrappable*.

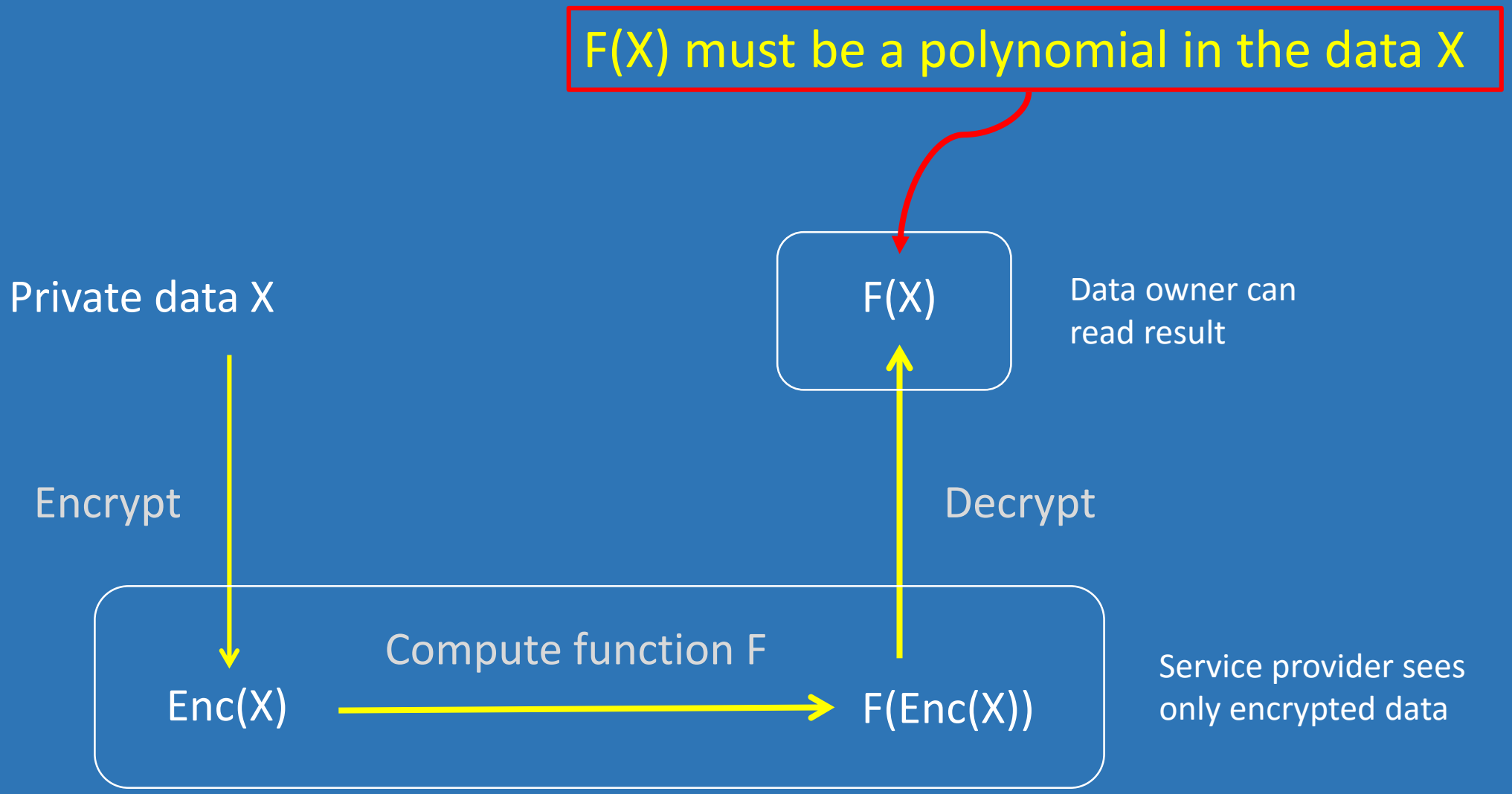
Next, we describe a public key encryption scheme using *ideal lattices* that is *almost* bootstrappable. Lattice-based cryptosystems typically have decryption algorithms with low

duced by Rivest, Adleman and Dertouzos [54] shortly a
ter the invention of RSA by Rivest, Adleman and Sham
[55]. Basic RSA is a multiplicatively homomorphic encry
tion scheme – i.e., given RSA public key $\mathrm{pk} = (N, e)$ an
ciphertexts $\{\psi_i \leftarrow \pi_i^e \bmod N\}$, one can efficiently compu
$\prod_i \psi_i = (\prod_i \pi_i)^e \bmod N$, a ciphertext that encrypts t
product of the original plaintexts. Rivest et al. [54] ask
a natural question: What can one do with an encrypti
scheme that is *fully* homomorphic: a scheme $\mathcal{E}$ with an ef
cient algorithm $\mathsf{Evaluate}_{\mathcal{E}}$ that, for any valid public key p
any circuit C (not just a circuit consisting of multiplicati
gates), and any ciphertexts $\psi_i \leftarrow \mathsf{Encrypt}_{\mathcal{E}}(\mathrm{pk}, \pi_i)$, outpu

$$\psi \leftarrow \mathsf{Evaluate}_{\mathcal{E}}(\mathrm{pk}, C, \psi_1, \ldots, \psi_t) ,$$


Compute function F
Private data X
F(X)
Encrypt
Decrypt
Compute function F
Enc(X)
F(Enc(X))


Private data X
F(X)
Data owner can read result
Encrypt
Decrypt
Compute function F
Enc(X)
F(Enc(X))
Service provider sees only encrypted data


F(X) must be a polynomial in the data X
Private data X
F(X)
Data owner can read result
Encrypt
Decrypt
Compute function F
Enc(X)
F(Enc(X))
Service provider sees only encrypted data

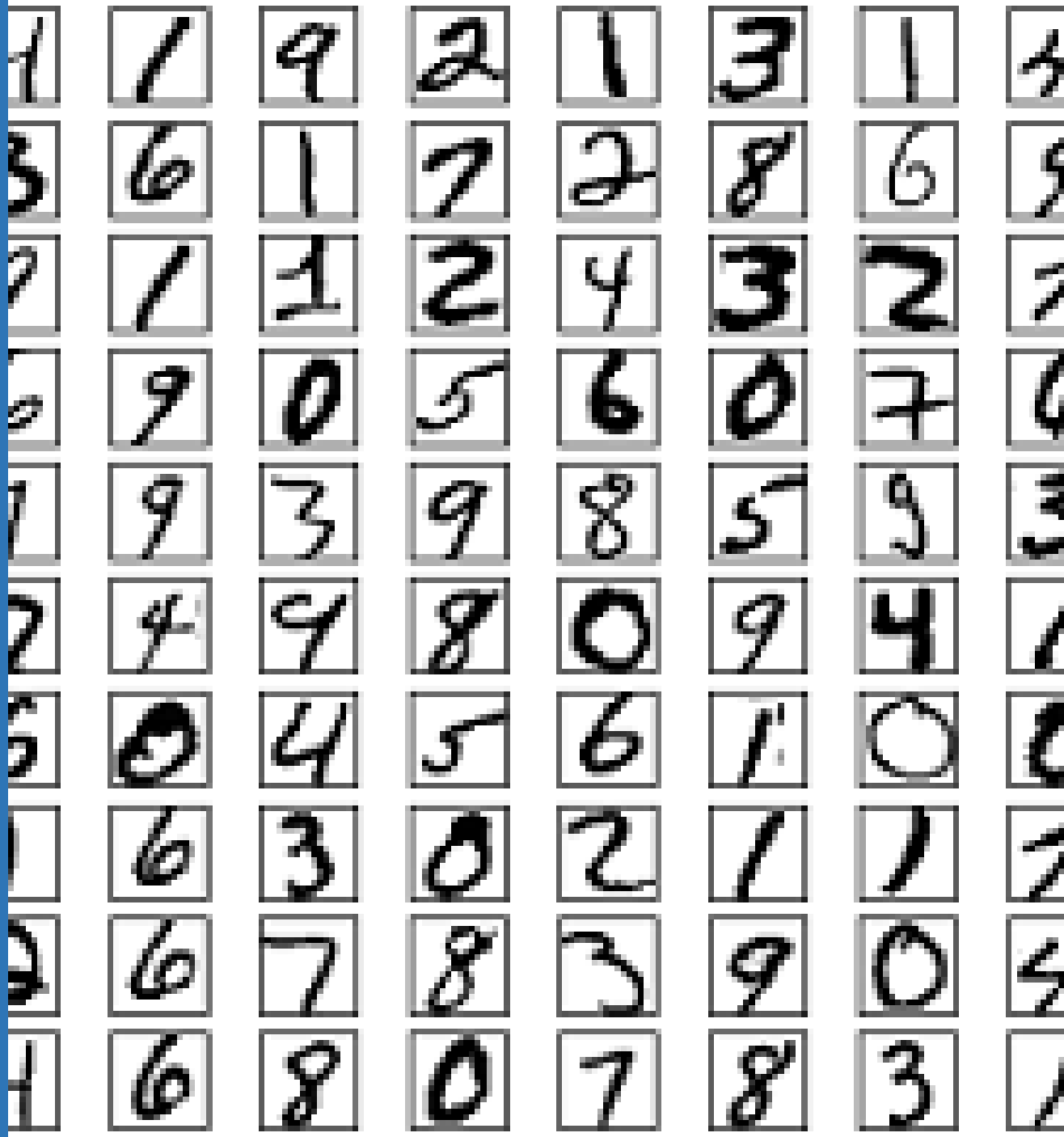
Why Neural Networks?

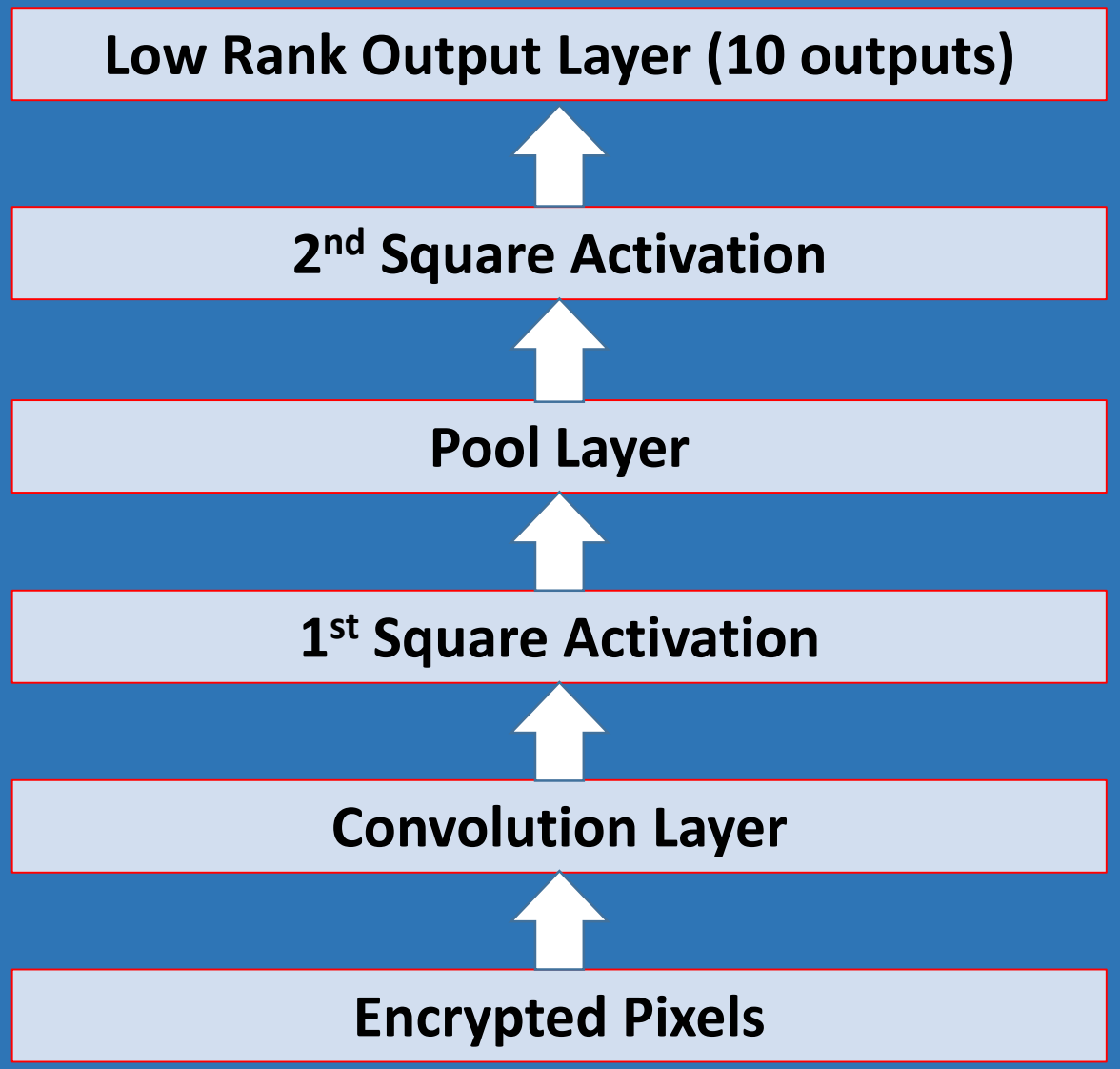
1. Challenging
2. High accuracy for difficult problems
3. Easily converted to polynomial predictor (polynomial activation function)

Simple Encrypted Arithmetic Library - SEAL

http://sealcrypto.codeplex.com

MNIST dataset




Low Rank Output Layer (10 outputs)
2nd Square Activation
Pool Layer
1st Square Activation
Convolution Layer
Encrypted Pixels

Method/Trick	Accuracy	Latency seconds	Amortized Latency sec/instance	Throughput instances/hr	Amortized Memory Footprint
Square Activation Network	97.3%	1360	1360	2.65	16000x
Plain Multiplication	97.3%	24	24	150	16000x
Chinese Remainder Theorem	97.6%	60	60	60	16000x
Convolution Network	99.0%	3976	3976	0.91	196000x
Skipping Relinearization	99.0%	590	590	6.1	196000x
Pre-Computing Linear Layers	99.0%	538	538	6.32	196000x
Splitting Plaintext Ring	99.0%	538	.065	51739	24x
Improved parameters	99.0%	250	.061	58982	15x

Future Directions

New techniques in homomorphic encryption

Other Machine Learning models?

How to do rectified linear?

Crypto + ML + Engineering lead to success

Thank You!

Questions?

Kim Laine
kim.laine@microsoft.com

Ran Gilad-Bachrach
rang@microsoft.com