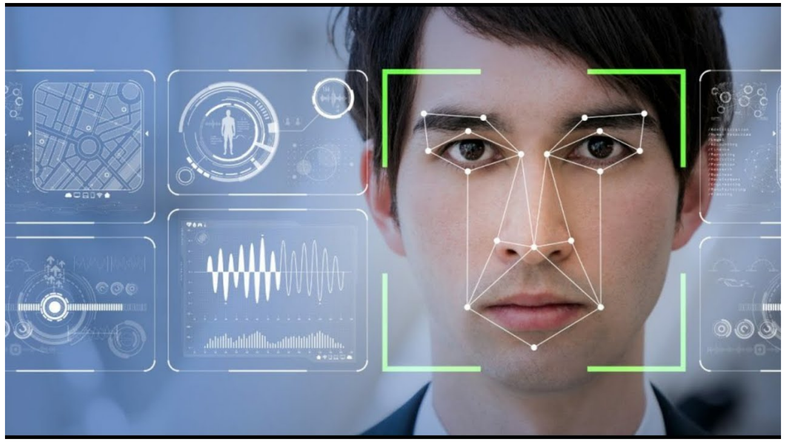
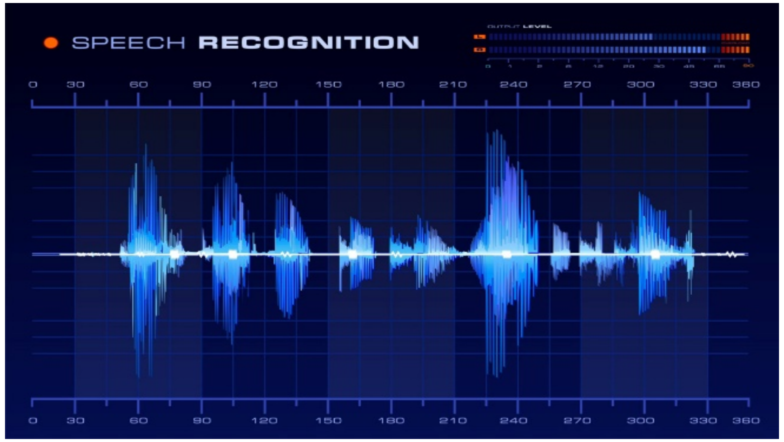
Privacy-preserving Machine Learning

Machine Learning

Image processing



Speech recognition

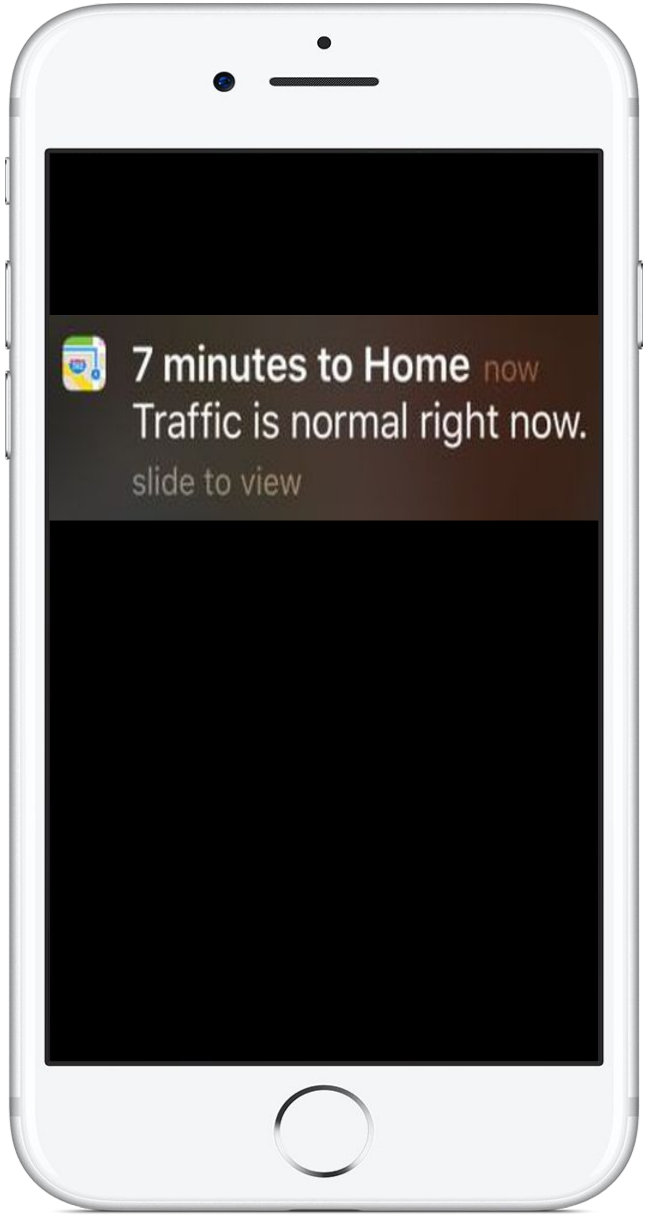


Playing Go

OpenAI

More data → Better Models

Map Predictions

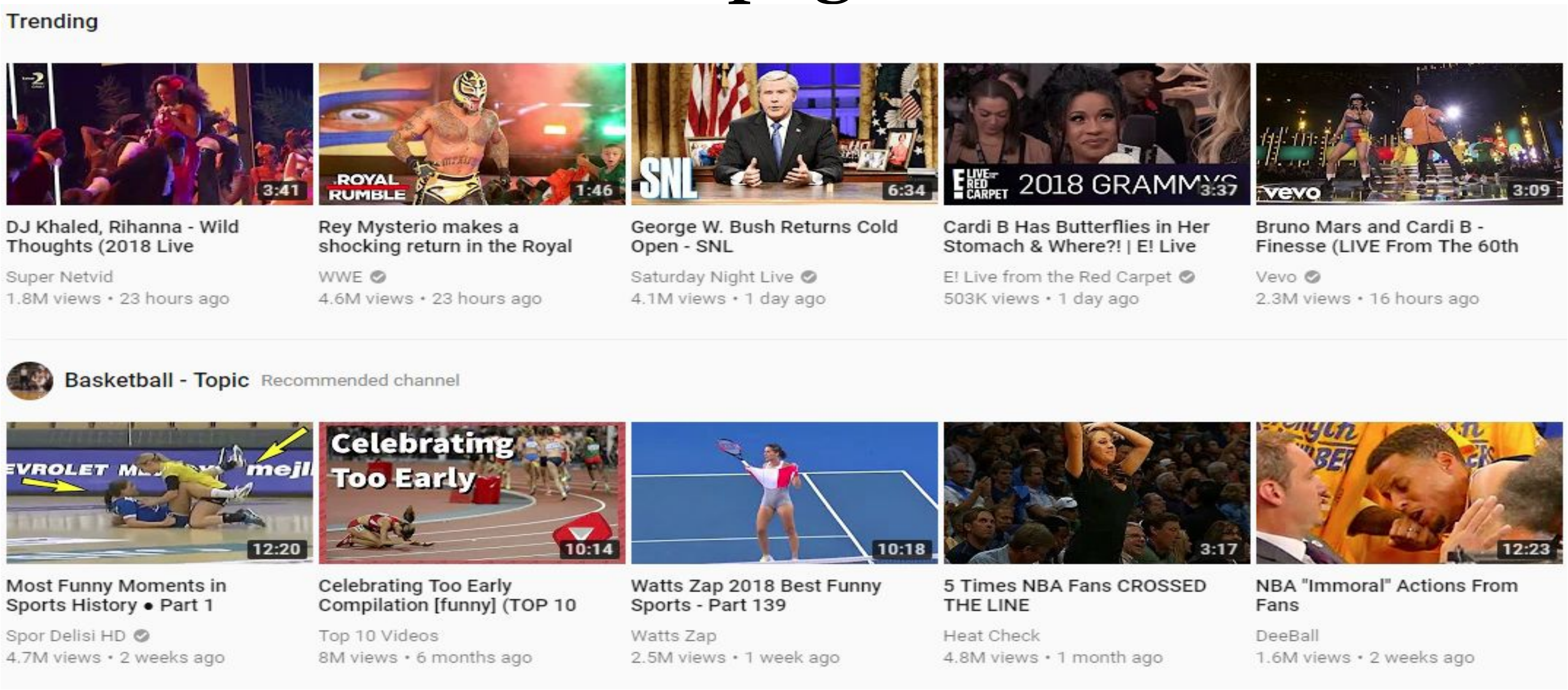


7 minutes to Home now

Traffic is normal right now.

slide to view

Customized Homepage



Trending

DJ Khaled, Rihanna - Wild Thoughts (2018 Live
Super Netvid
1.8M views • 23 hours ago

Rey Mysterio makes a shocking return in the Royal
WWE
4.6M views • 23 hours ago

George W. Bush Returns Cold Open - SNL
Saturday Night Live
4.1M views • 1 day ago

Cardi B Has Butterflies in Her Stomach & Where?! | E! Live
E! Live from the Red Carpet
503K views • 1 day ago

Bruno Mars and Cardi B - Finesse (LIVE From The 60th
Vevo
2.3M views • 16 hours ago

Basketball - Topic Recommended channel

Most Funny Moments in Sports History • Part 1
Spor Delisi HD
4.7M views • 2 weeks ago

Celebrating Too Early Compilation [funny] (TOP 10
Top 10 Videos
8M views • 6 months ago

Watts Zap 2018 Best Funny Sports - Part 139
Watts Zap
2.5M views • 1 week ago

5 Times NBA Fans CROSSED THE LINE
Heat Check
4.8M views • 1 month ago

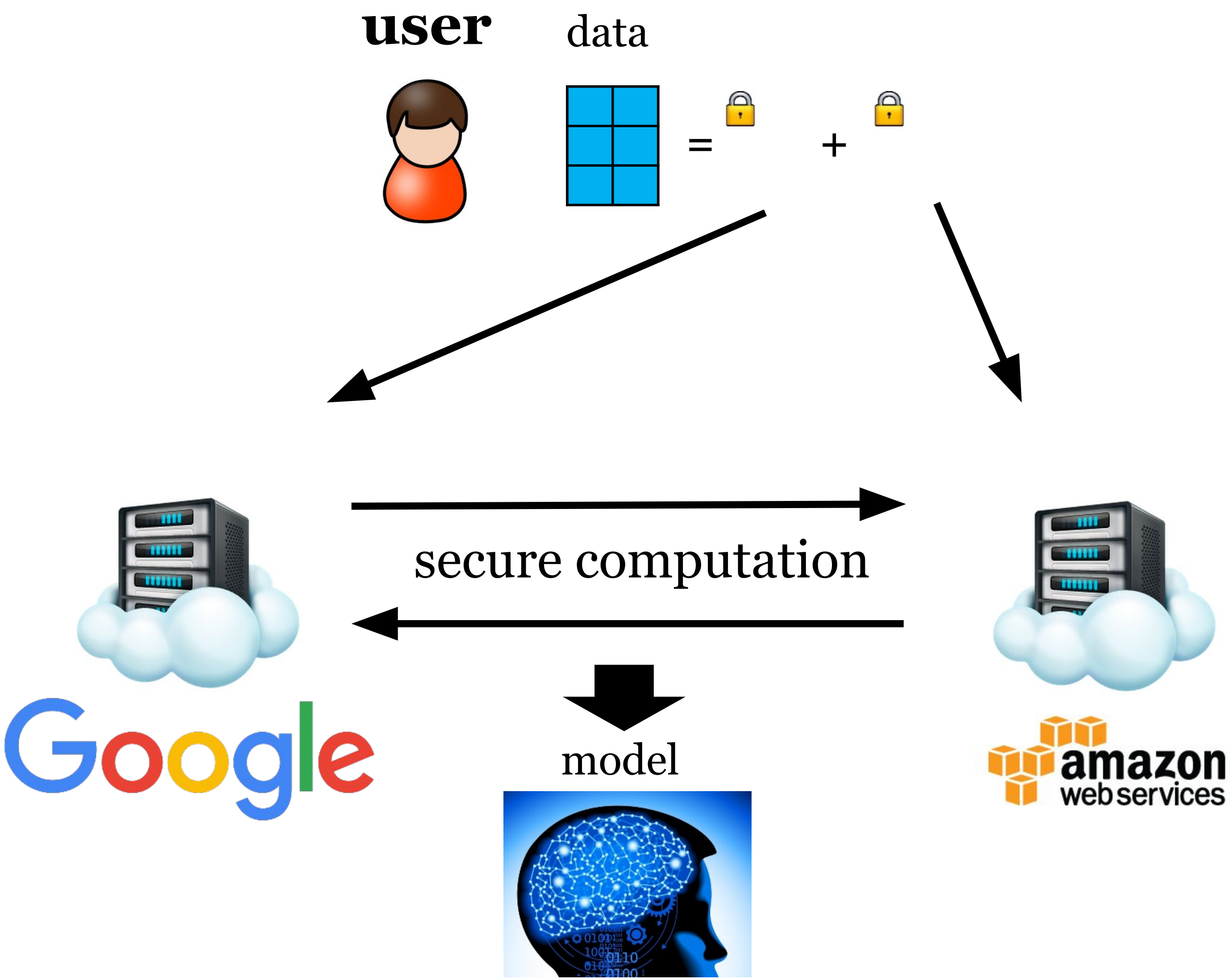
NBA "Immoral" Actions From Fans
DeeBall
1.6M views • 2 weeks ago

✔ Nice machine learning applications benefiting our lives

× Models trained on sensitive data

Can companies train the models without learning our data

Privacy-preserving Machine Learning



Use Case for Companies: Fraud detection

VISA

Card #	Time	Location	Amount
xxxxxxx	8/8/2016	CA, USA	xx.xx
……			

MasterCard

xxxxxxx	x/xx/xxxx	xx,xxx	xx.xx
……			

Name	SSN
Alice	xxxxx
……	
Alice	xxxxx
…..	

Bank of America

Use Case for Hospitals

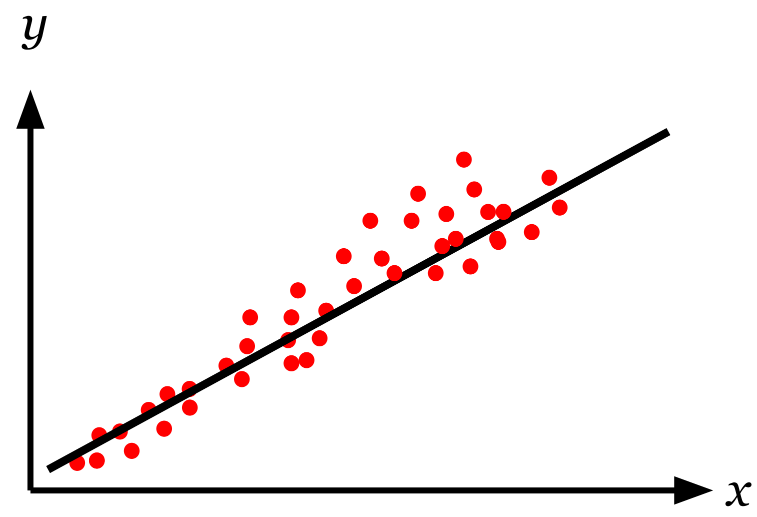
ID	Name	Sex	DOB	Disease xxx
101	Alice	F	1976-2-23	N
102	Bob	M	1992-10-12	N
103	Charlie	M	1983-1-15	N
104	David	M	2005-4-30	Y
…	…	…	…	N

In theory, there is no difference between theory and practice;

In practice, there is.

Linear Regression

Linear Regression



Input: data value pairs (x, y)s

Output: model w

$$y^* = \sum_i w_i x_i = w \cdot x \approx y$$

Cost function (Loss function)

$$y^* = \sum_i w_i x_i = w \cdot x \approx y$$

-

$$C_x(w) = \frac{1}{2}(y^* - y)^2$$

$$C(w) = \frac{1}{n}\sum_x C_x(w)$$

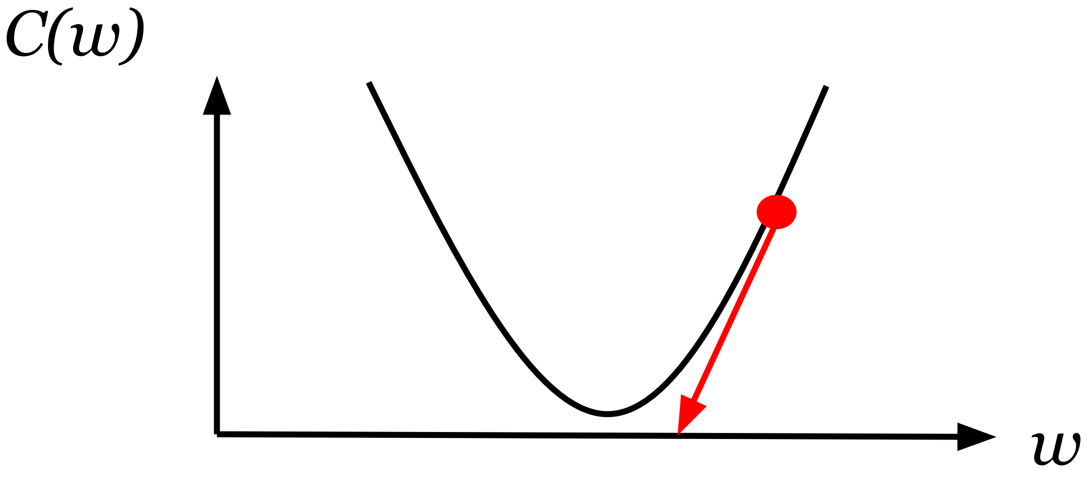
$$\arg\min_w C(w)$$

Closed-form solution for linear regression

- $w = (X^T X)^{-1} X^T y$

O(n^3), slow for large datasets

Gradient decent



$$y^* = \sum_i w_i x_i = w \cdot x$$

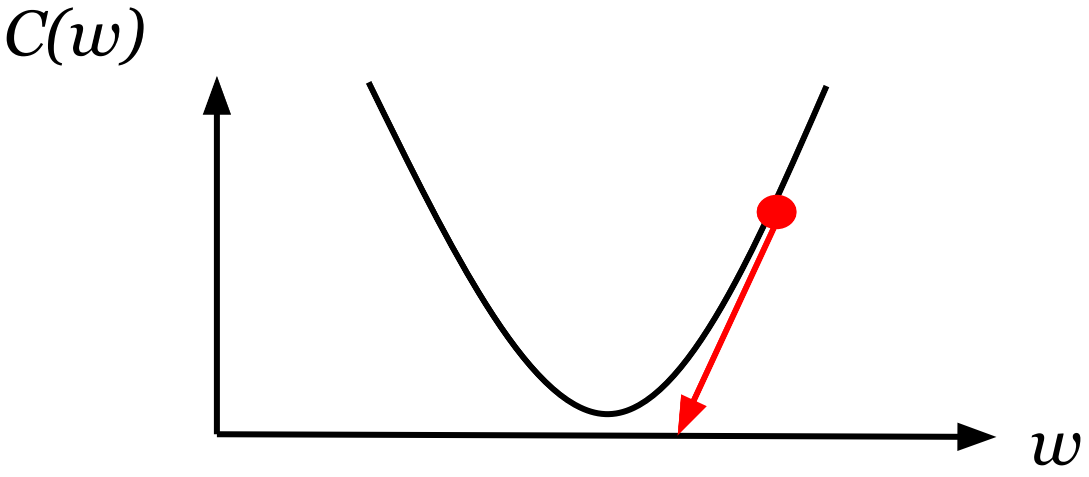
$$C_x(w) = \frac{1}{2}(y^* - y)^2$$

$$C(w) = \frac{1}{n}\sum_x C_x(w)$$

1. Initialize *w* randomly
2. Compute derivative of *C(w)*
3. Update *w*

$$w = w - \alpha \frac{1}{n}\sum_x (x \cdot w - y)x \qquad w_i = w_i - \alpha \frac{1}{n}\sum_x (x \cdot w - y)x_i$$

Stochastic gradient decent (SGD)

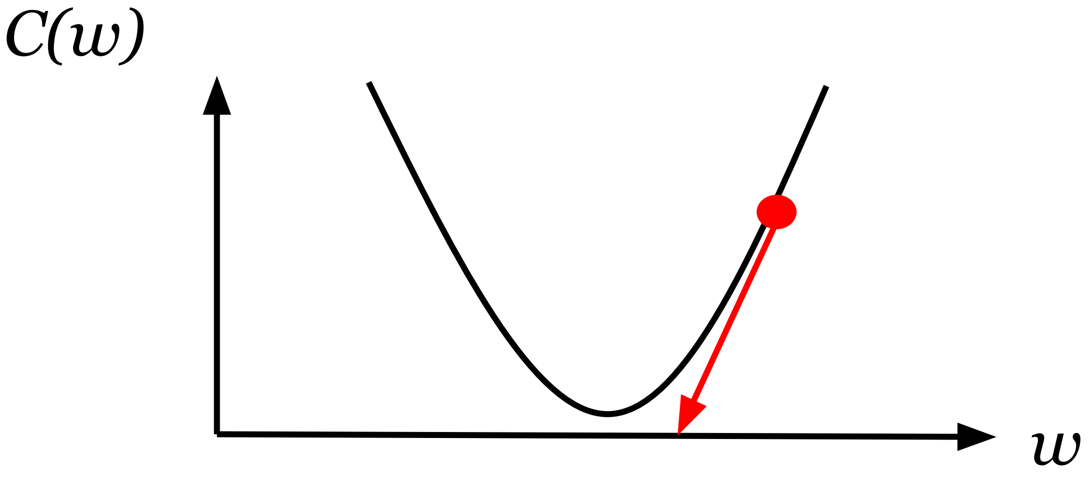


1. Initialize w randomly
2. Select a random sample (x, y), compute derivative of $C_x(w)$
3. Update w

$$w = w - \alpha(x \cdot w - y)x$$

$$w_i = w_i - \alpha(x \cdot w - y)x_i$$

Mini-batch SGD



1. Initialize w randomly
2. Select a batch of random samples (x, y), compute derivative
3. Update w

$$w = w - \alpha \frac{1}{|B|} \sum_{x \in B} (x \cdot w - y) x$$

Mini-batch SGD

- Epoch: randomly shuffle all the data, select |B| samples each round

- Vectorization:

$$w = w - \alpha \frac{1}{|B|} \sum_{x \in B} (x \cdot w - y) x$$

$$w = w - \frac{\alpha}{|B|} \cdot X^{\mathrm{T}} \times (X \times w - y)$$

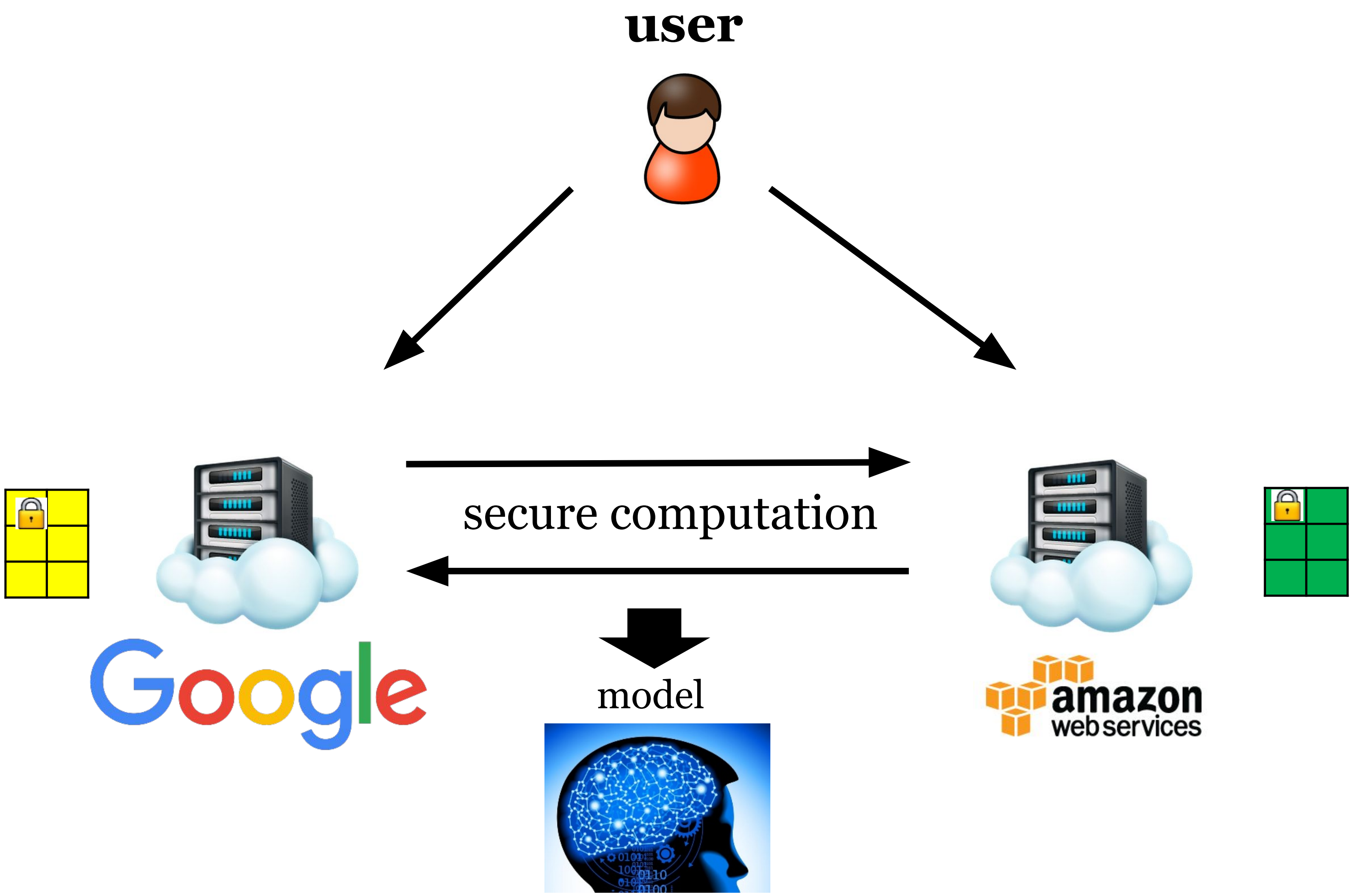
Other variants

$$y^* = \sum_i w_i x_i + b = \mathbf{w} \cdot \mathbf{x} + b$$

Ridge regression: $C_x(w) = \frac{1}{2}(y^* - y)^2 + \lambda||w||_2^2$

Adaptive learning rate α

Privacy-preserving linear regression



user

secure computation

model

Privacy-preserving linear regression

SGD: $w_i = w_i - \alpha(x \cdot w - y)x_i$

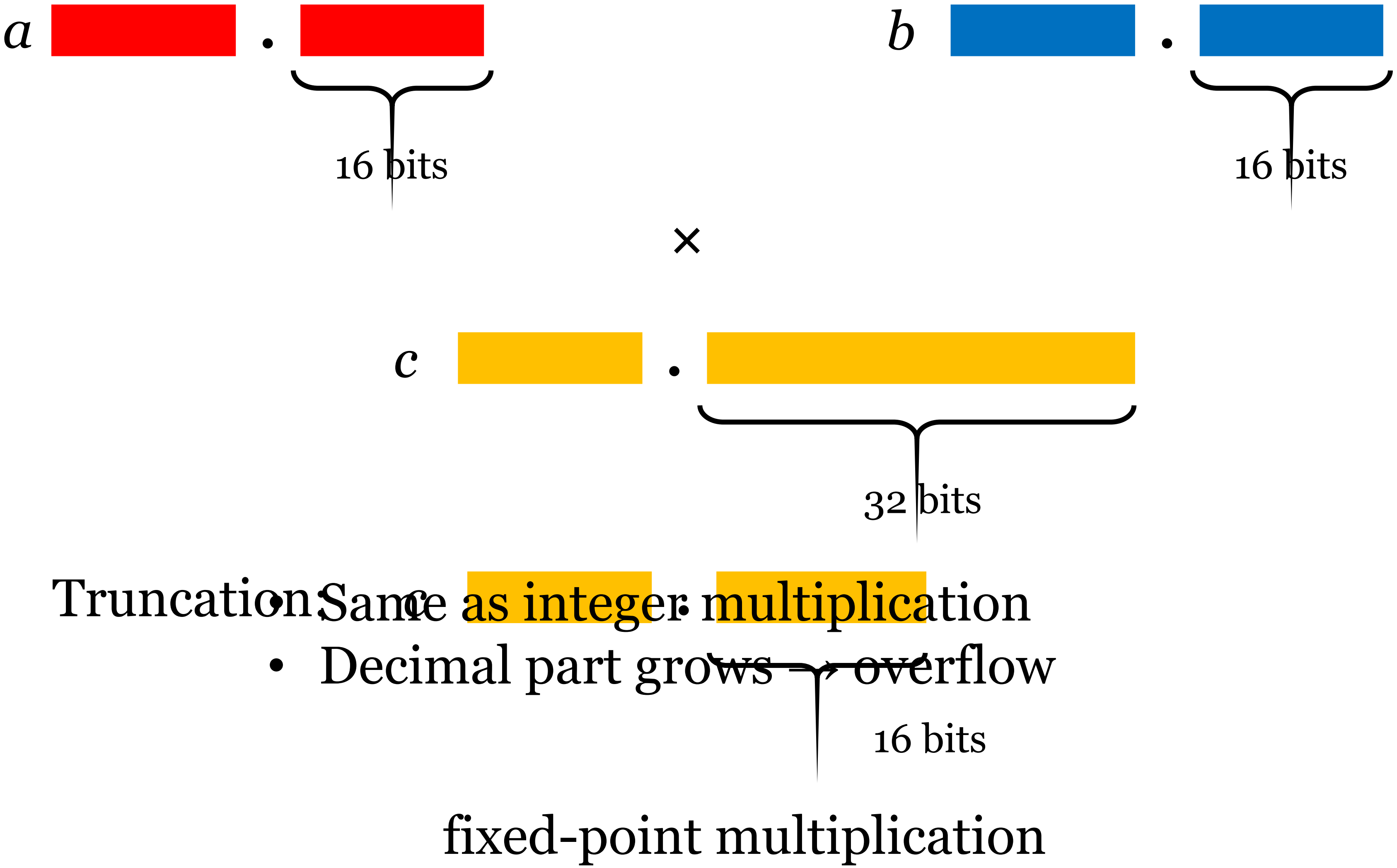
1. Users secret share data and values (x,y)

2. Servers initialize and secret share the model w

3. Run SGD using GMW protocol

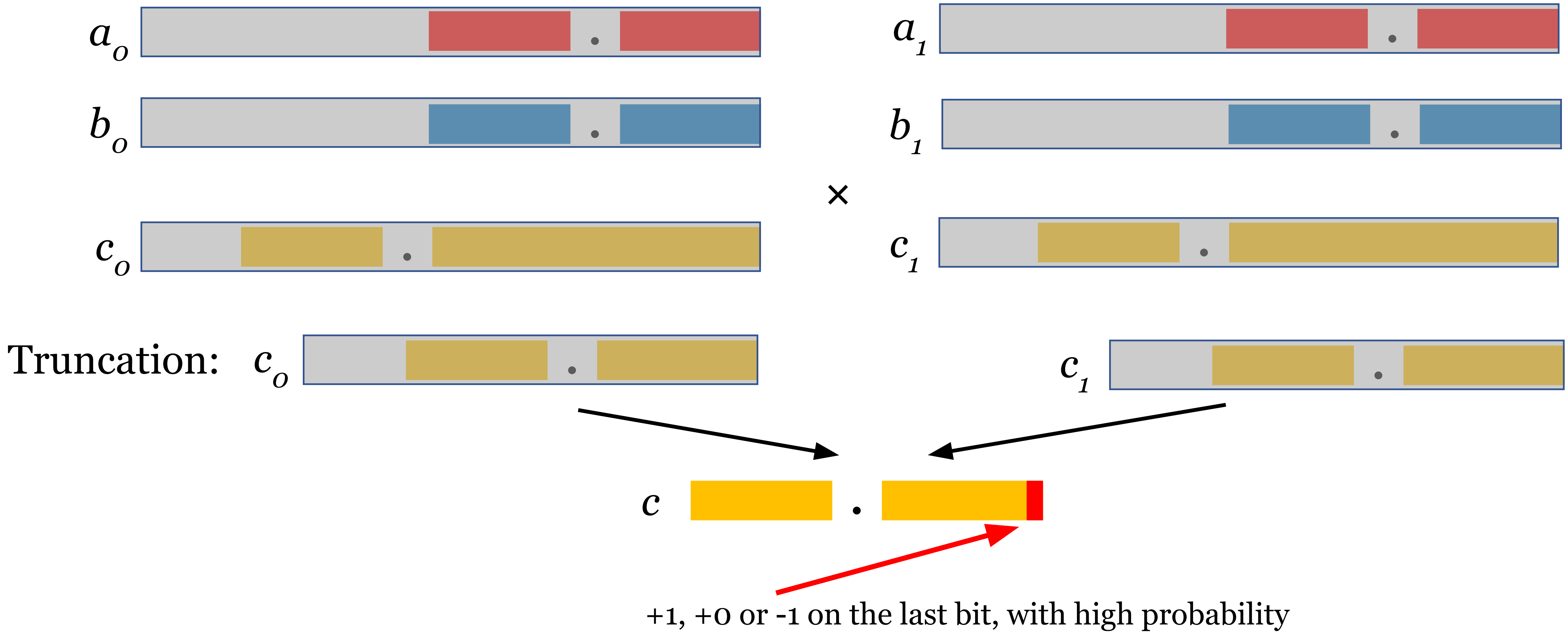
Decimal number?

Fixed-point multiplication



- Same as integer multiplication
- Decimal part grows → overflow

Truncation on shared values



+1, +0 or -1 on the last bit, with high probability

Privacy-preserving linear regression

SGD: $w_i = w_i - \alpha(x \cdot w - y)x_i$

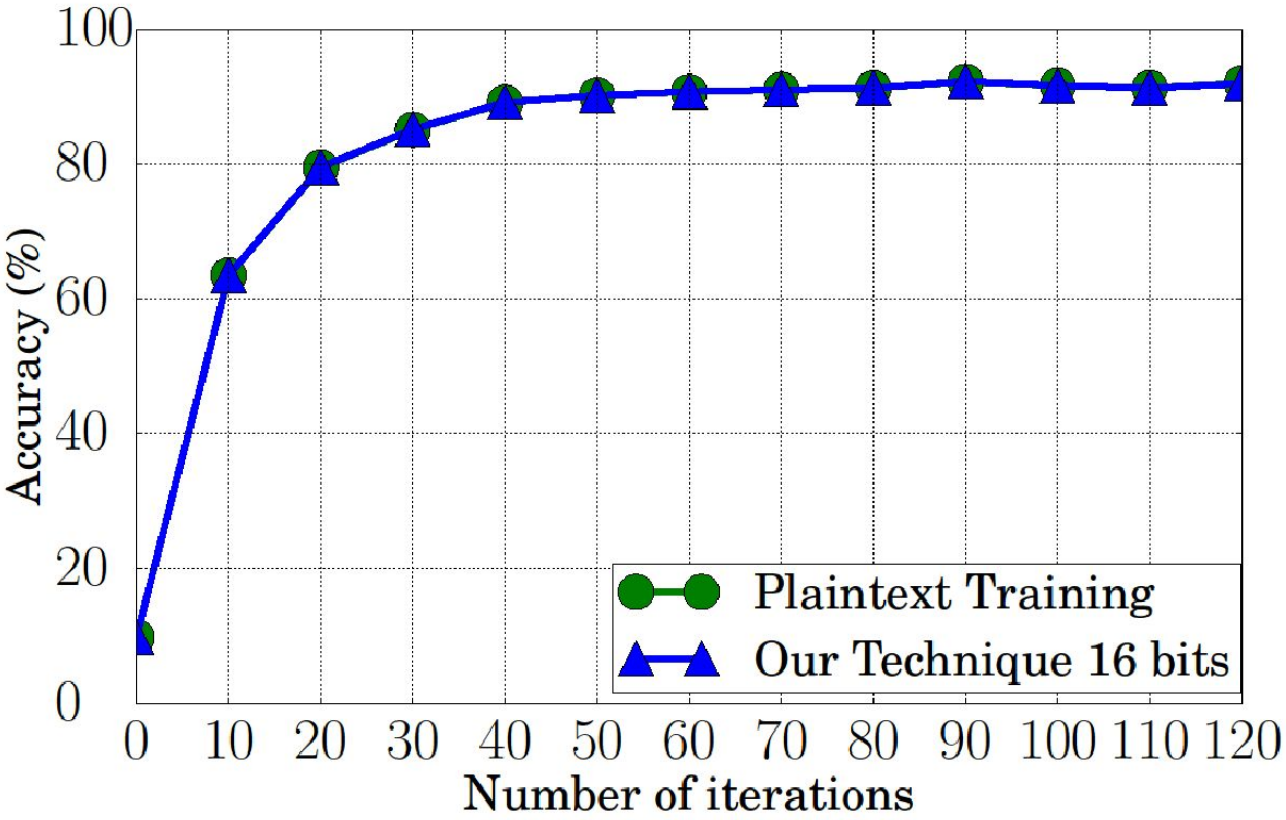
1. Users secret share data and values (x,y)

2. Servers initialize and secret share the model w

3. Run SGD using GMW protocol

4. Truncate the shares after every multiplication

Effects of truncation



- 4-8× faster than fix-point multiplication garbled circuit