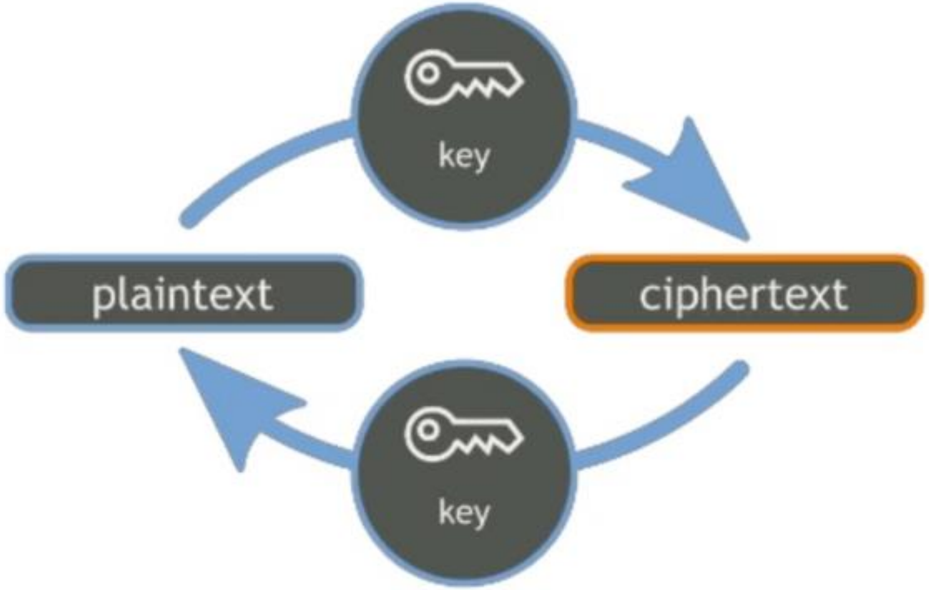
CSE 539
Applied Cryptography
Fall 2024

Ni Trieu (ASU)

Recap: What is Cryptography?

- Cryptography is more than just hiding information (i.e., encryption)
- Cryptography is math
- Crypto definition
  - Idea: compare 2 probability distributions



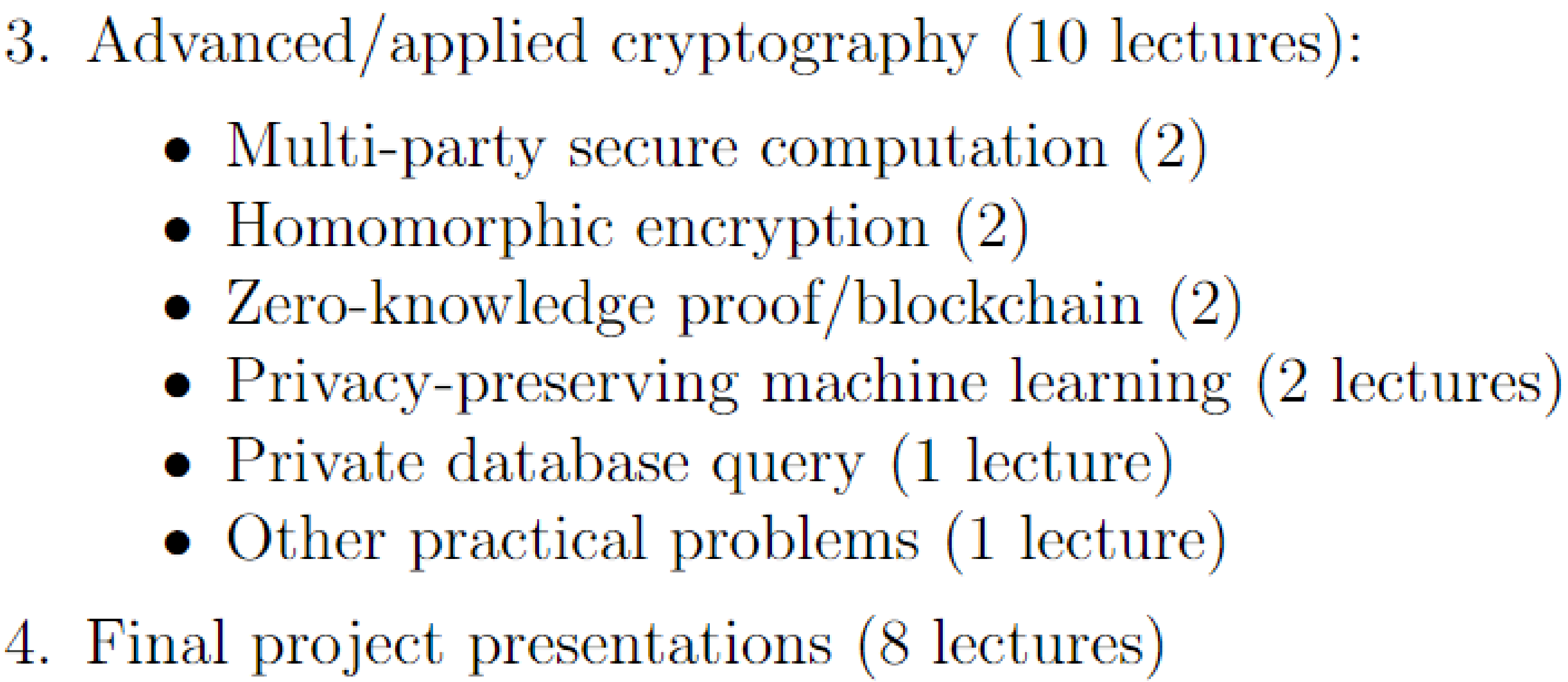
One-time Pad:

- $Enc(k, m) = k \oplus m$
- $Dec(k, c) = k \oplus c$
- $Dec(k, Enc(k, m)) = m$

Lec 2

- ~~Greetings~~
- ~~Syllabus~~
- ~~What Cryptography is~~
- What "Applied" Cryptography is
  - Why cryptography is good for the world?

“Applied” Cryptography

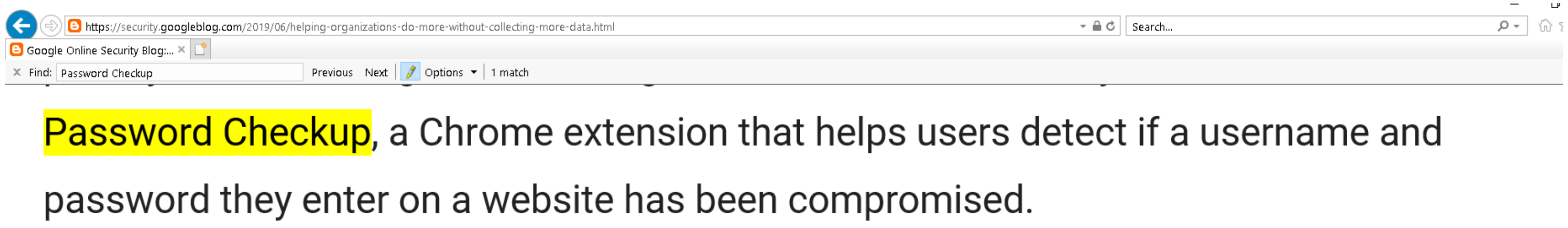


3. Advanced/applied cryptography (10 lectures):
    - Multi-party secure computation (2)
    - Homomorphic encryption (2)
    - Zero-knowledge proof/blockchain (2)
    - Privacy-preserving machine learning (2 lectures)
    - Private database query (1 lecture)
    - Other practical problems (1 lecture)
4. Final project presentations (8 lectures)

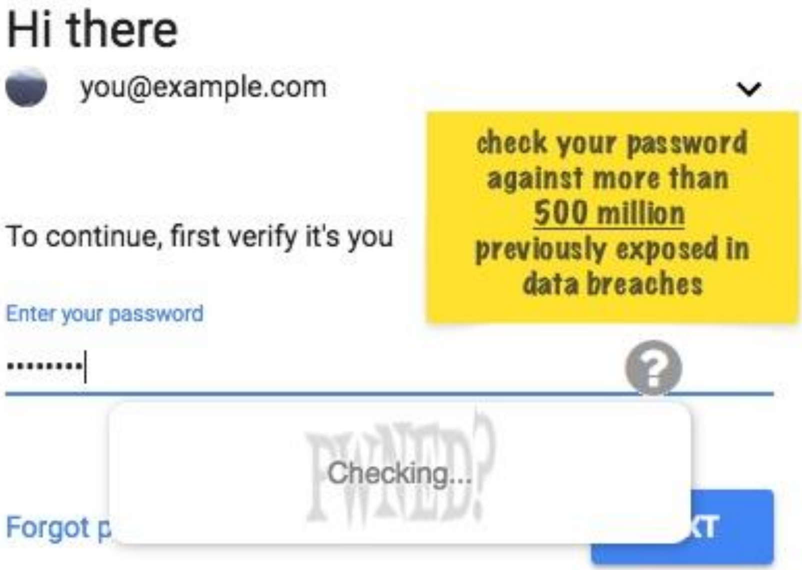
- Secure Password Checkup
- Privacy Preserving Machine Learning

Secure Password Checkup

Credit by Google Security Blog


https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html
Search...
Google Online Security Blog:...
Find: Password Checkup
Previous
Next
Options
1 match

Password Checkup, a Chrome extension that helps users detect if a username and password they enter on a website has been compromised.


Hi there

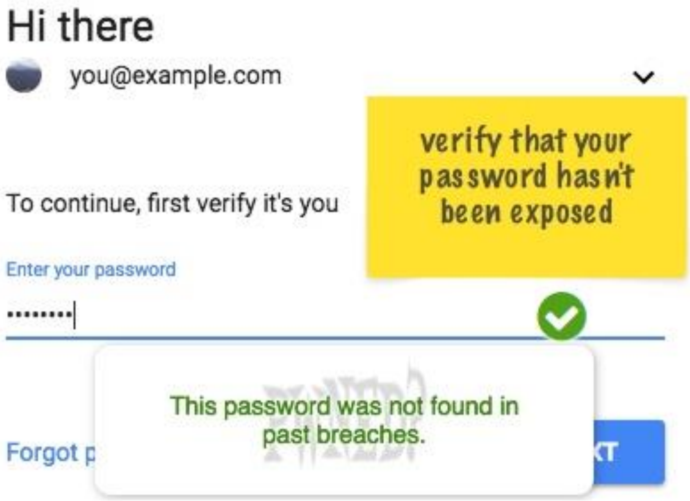
you@example.com

check your password against more than 500 million previously exposed in data breaches

To continue, first verify it's you

Enter your password

Checking...


Hi there

you@example.com

verify that your password hasn't been exposed

To continue, first verify it's you

Enter your password

This password was not found in past breaches.

Google Password Checkup

Password Checkup extension

Offered by: google.com

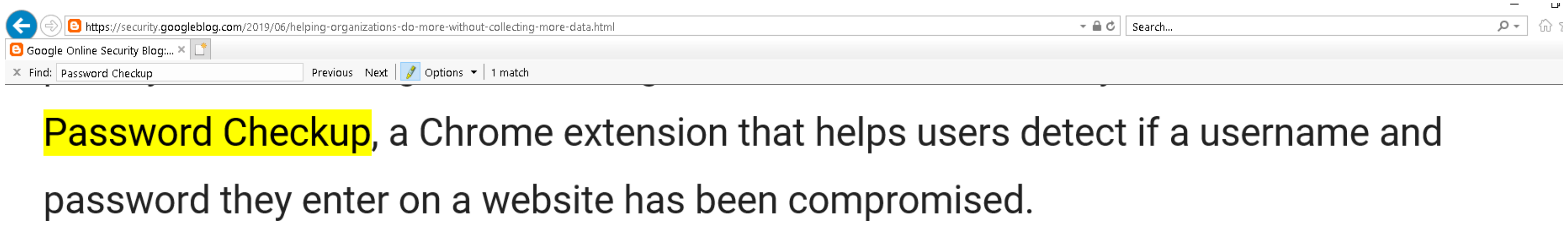
Password Checker

Offered by: David Hunt

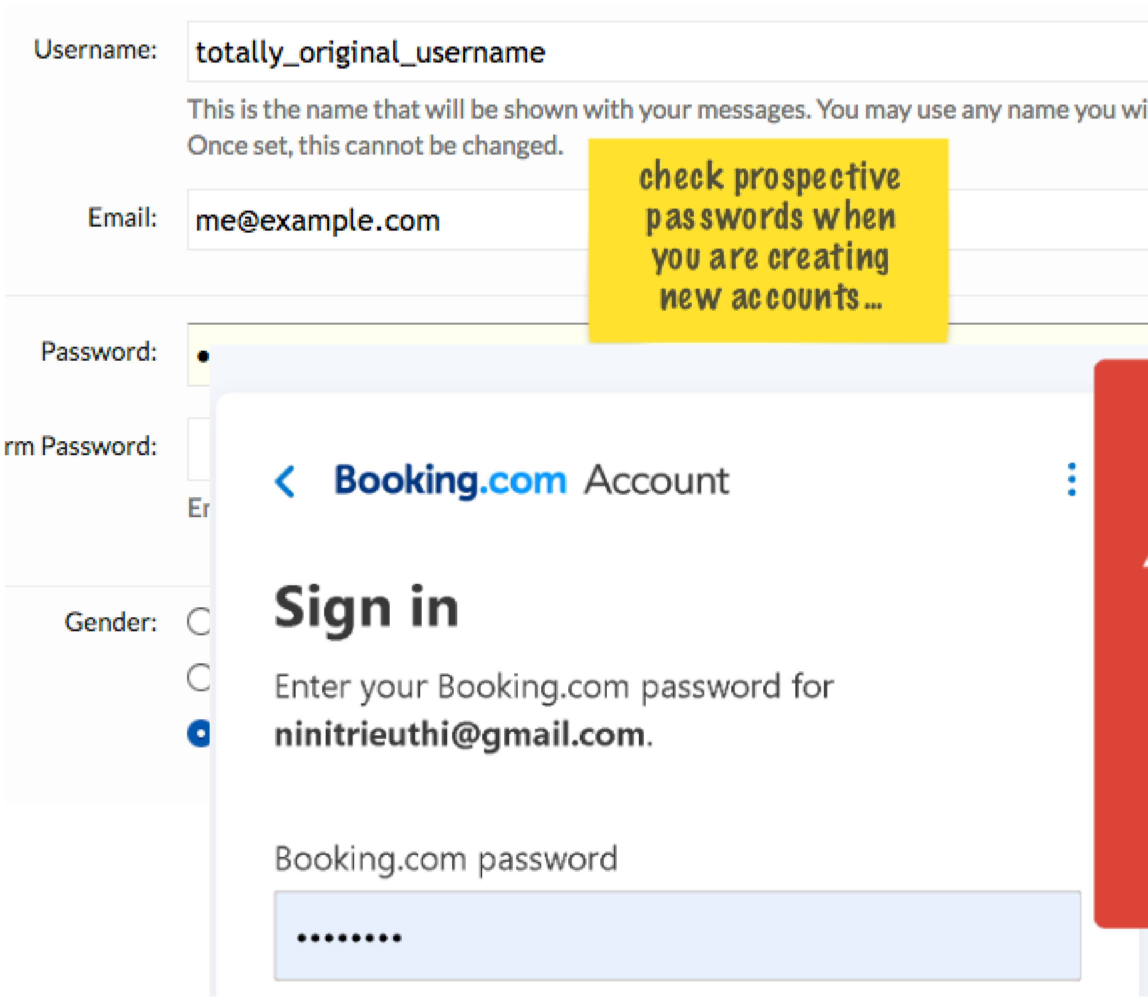
Secure Password Checkup

Credit by Google Security Blog

Google Password Checkup


https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html
Search...
Google Online Security Blog:...
Find: Password Checkup
Previous
Next
Options
1 match

Password Checkup, a Chrome extension that helps users detect if a username and password they enter on a website has been compromised.



Username: totally_original_username

This is the name that will be shown with your messages. You may use any name you wish. Once set, this cannot be changed.

Email: me@example.com

Password: •

rm Password:

Er

Gender: ○ ○ ●

check prospective passwords when you are creating new accounts...

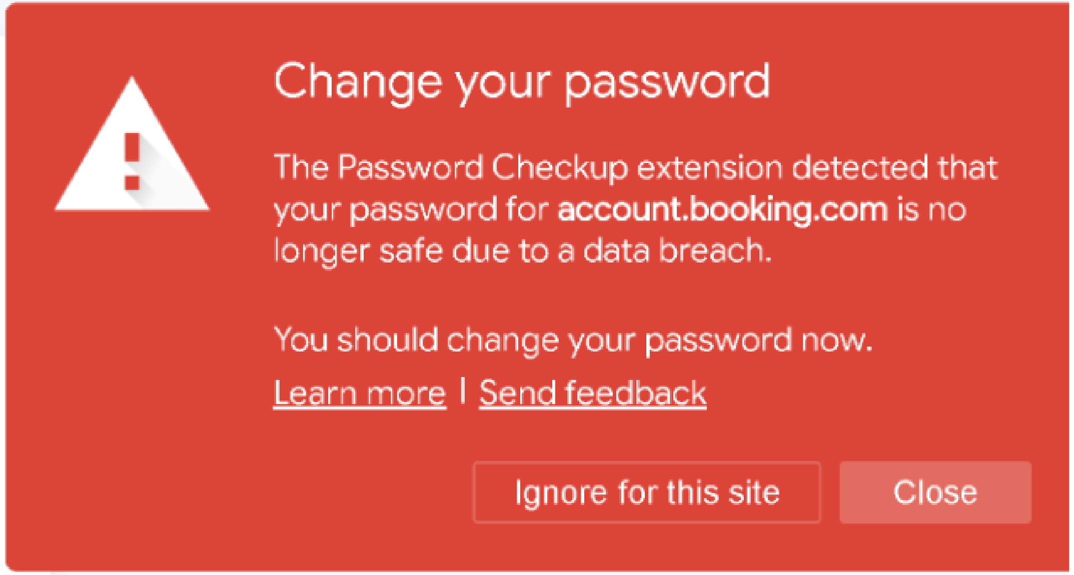
Booking.com Account

Sign in

Enter your Booking.com password for **ninitrieuthi@gmail.com**.

Booking.com password

•••••••••



Change your password

The Password Checkup extension detected that your password for **account.booking.com** is no longer safe due to a data breach.

You should change your password now.

Learn more | Send feedback

Password Checkup extension

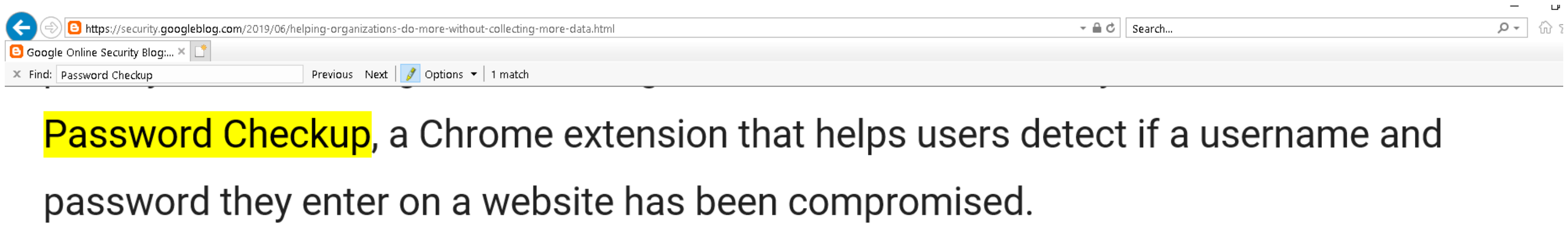
Offered by: google.com

Password Checker

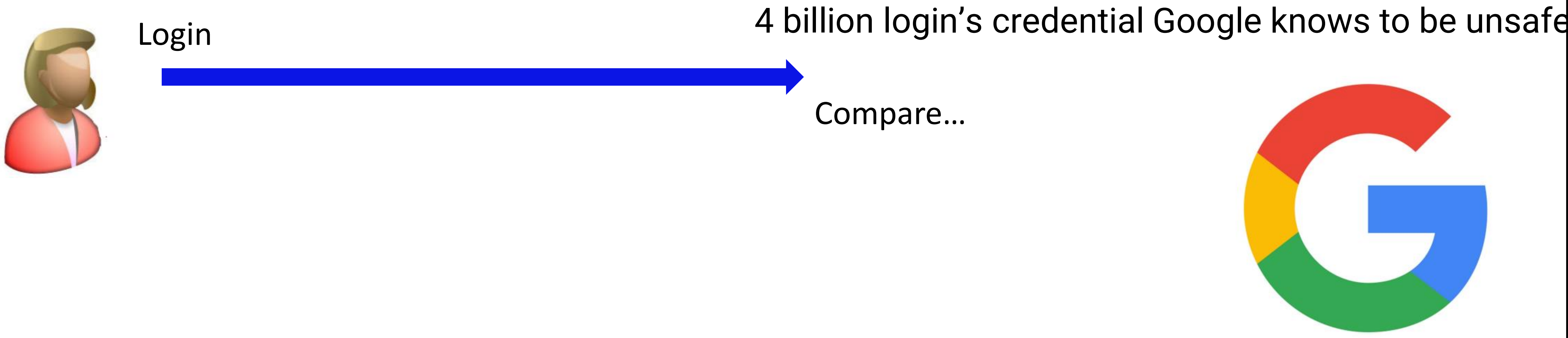
Offered by: David Hunt

Secure Password Checkup

Credit by Google Security Blog

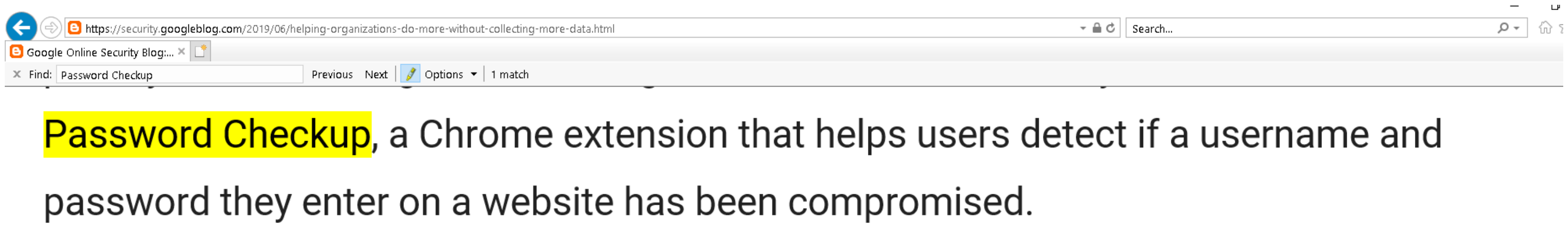

https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html
Search...
Google Online Security Blog:...
Find: Password Checkup
Previous
Next
Options
1 match

Password Checkup, a Chrome extension that helps users detect if a username and password they enter on a website has been compromised.



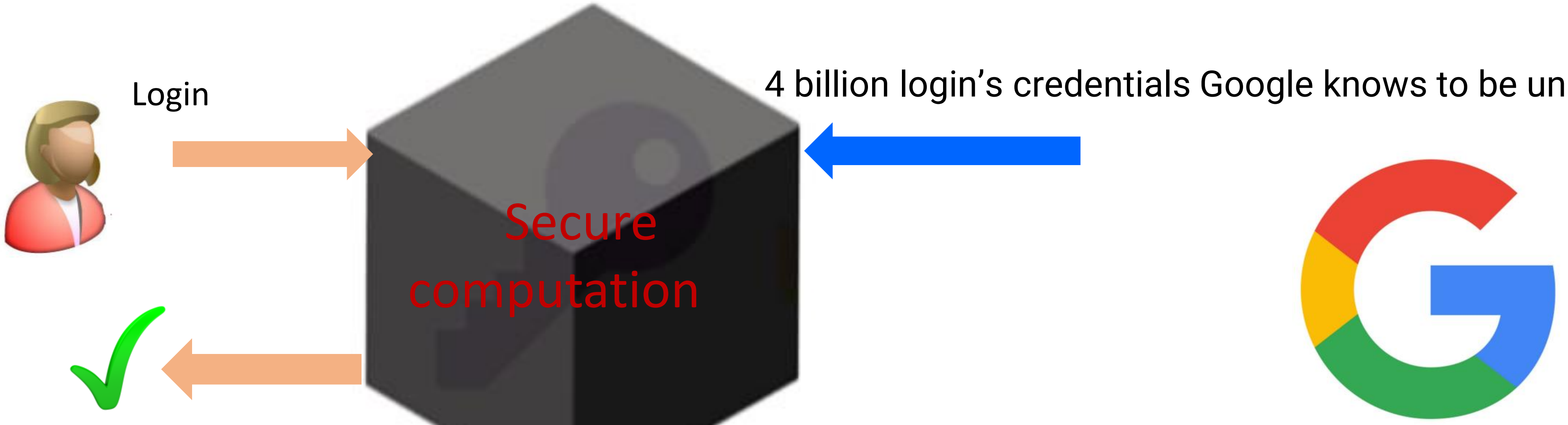
Secure Password Checkup

Credit by Google Security Blog



https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html
Search...
Google Online Security Blog:...
Find: Password Checkup
Previous
Next
Options
1 match

Password Checkup, a Chrome extension that helps users detect if a username and password they enter on a website has been compromised.



Login

4 billion login’s credentials Google knows to be unsafe

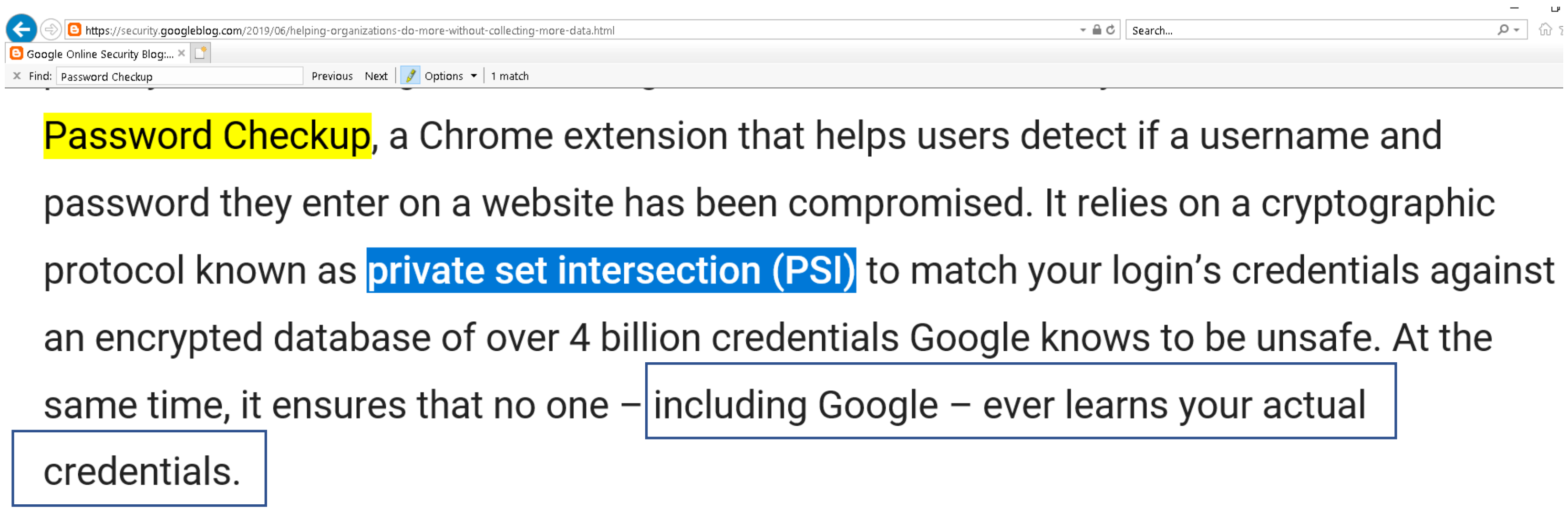
Secure computation

Learns nothing about Google’s database

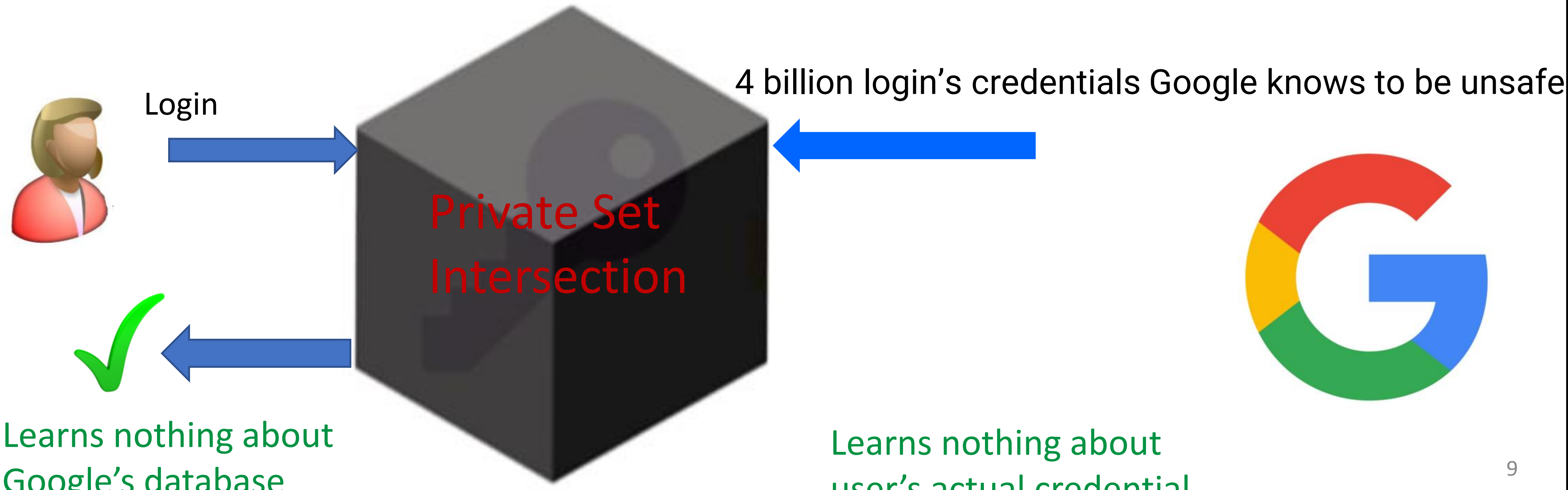
Learns nothing about user’s actual credential

Secure Password Checkup

Credit by Google Security Blog


https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html
Search...
Google Online Security Blog:...
Find: Password Checkup
Previous
Next
Options
1 match

Password Checkup, a Chrome extension that helps users detect if a username and password they enter on a website has been compromised. It relies on a cryptographic protocol known as private set intersection (PSI) to match your login's credentials against an encrypted database of over 4 billion credentials Google knows to be unsafe. At the same time, it ensures that no one – including Google – ever learns your actual credentials.



Login

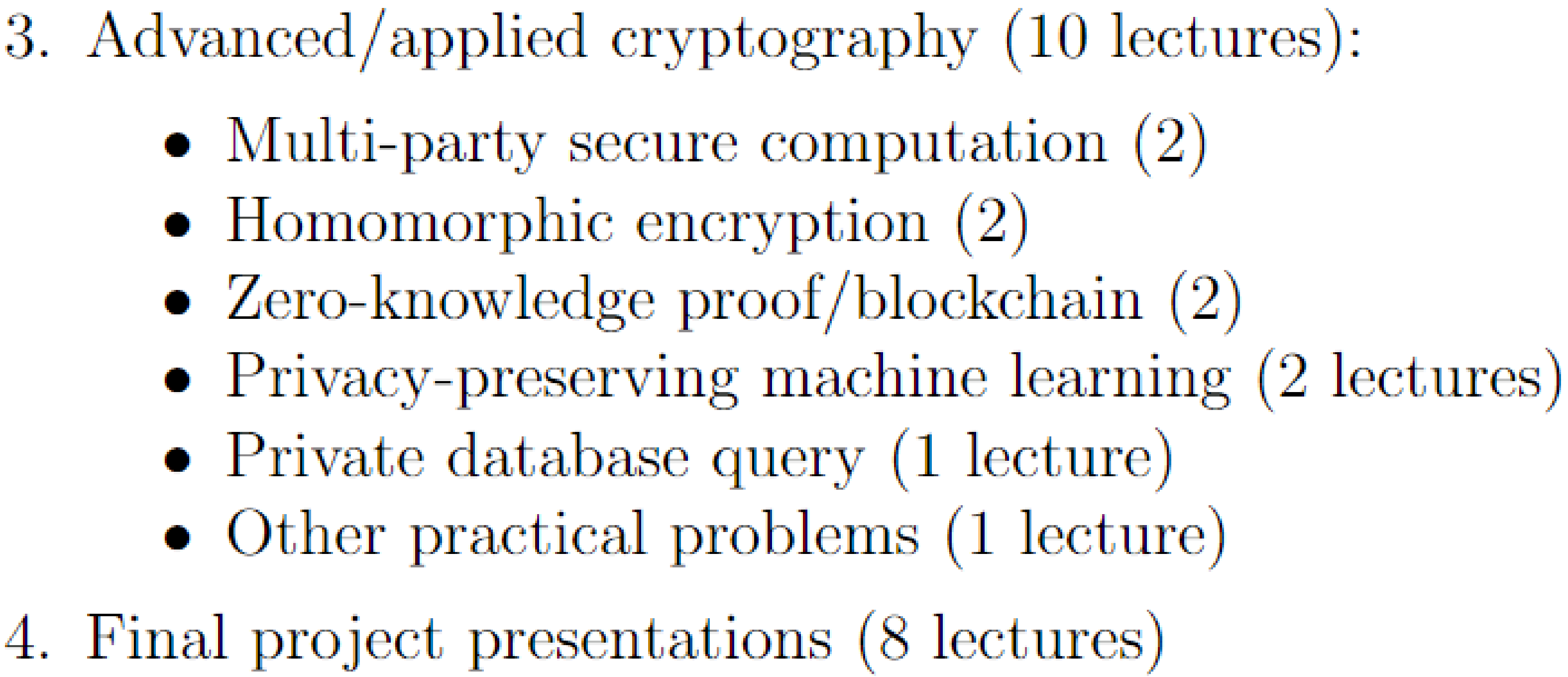
Private Set Intersection

4 billion login's credentials Google knows to be unsafe

Learns nothing about Google's database

Learns nothing about user's actual credential

“Applied” Cryptography

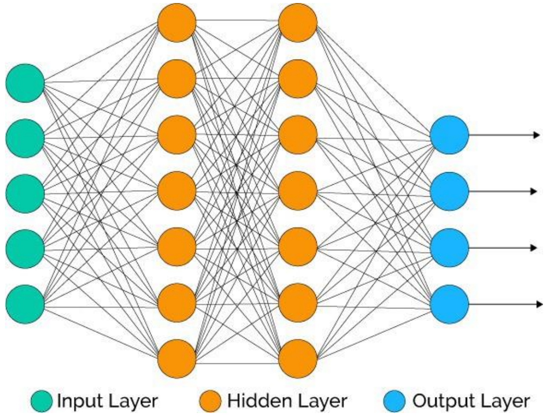


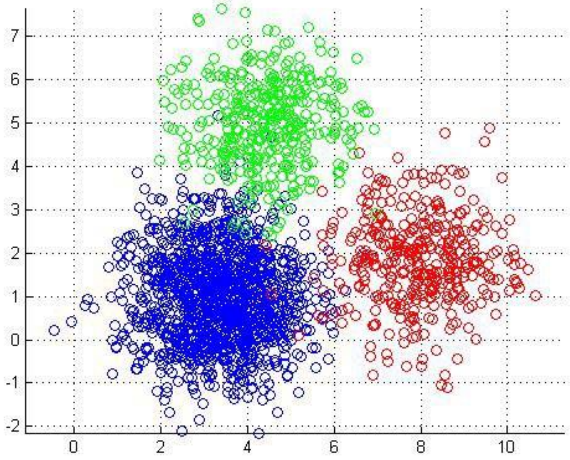
3. Advanced/applied cryptography (10 lectures):
   - Multi-party secure computation (2)
   - Homomorphic encryption (2)
   - Zero-knowledge proof/blockchain (2)
   - Privacy-preserving machine learning (2 lectures)
   - Private database query (1 lecture)
   - Other practical problems (1 lecture)
4. Final project presentations (8 lectures)

- ~~Secure Password Checkup~~
- Privacy Preserving Machine Learning

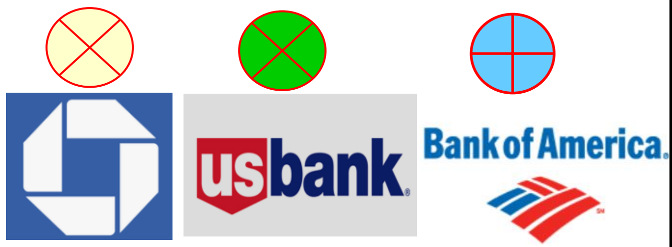
What is Machine Learning (ML)?

- “**Machine learning** (**ML**) is the study of computer algorithms that improve automatically through experience. It is seen as a subset of artificial intelligence. Machine learning algorithms build a model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so.” (source: https://en.wikipedia.org/wiki/Machine_learning)

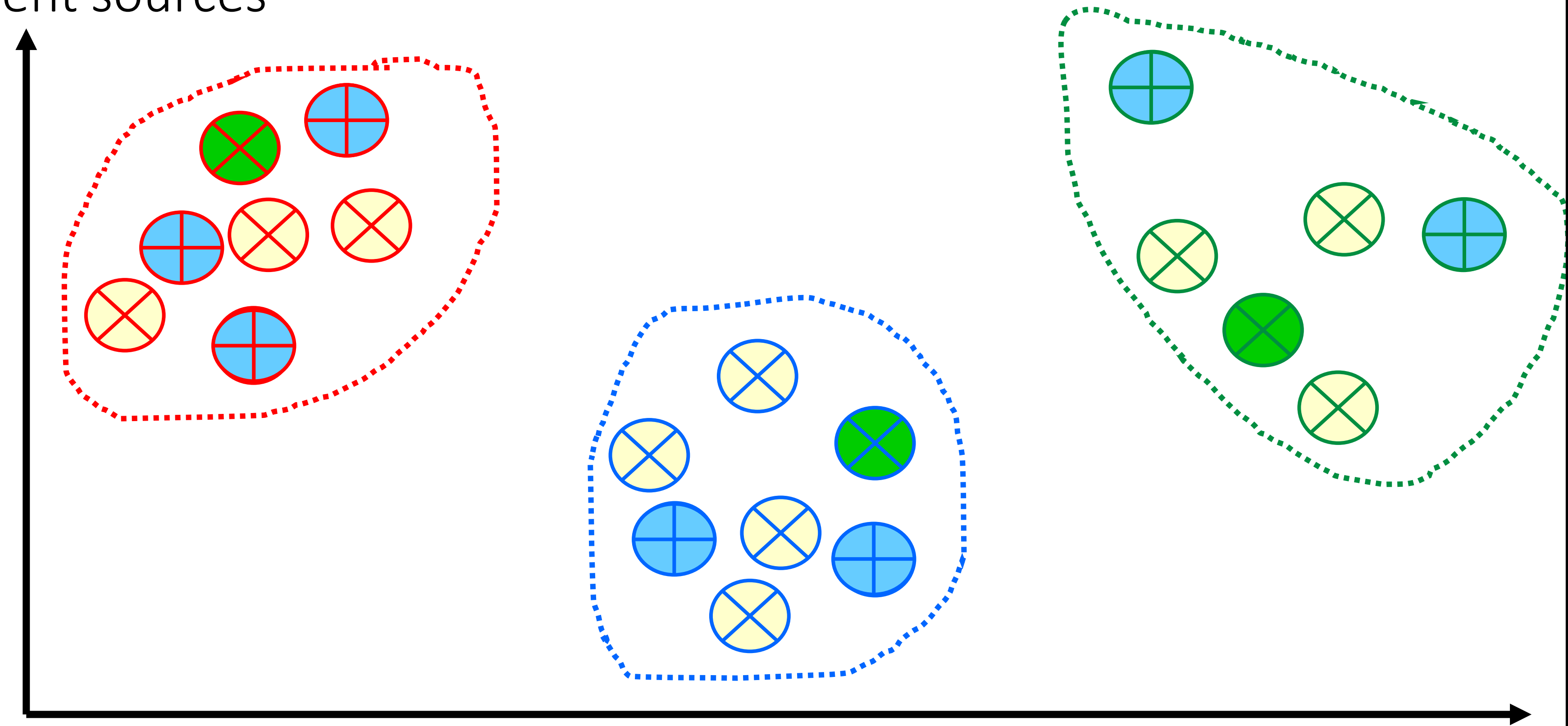




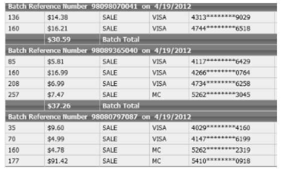
Why need Secure Computation for ML?



- ML is data hungry
- Data comes from different sources
- E.g. Fraud Detection
- Privacy concern

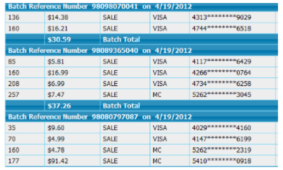


~~Privacy Preserving~~ ML Model



Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

Trans. records

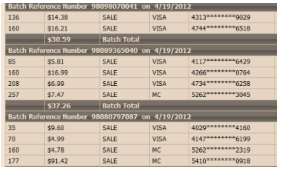


Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

=====>

Server

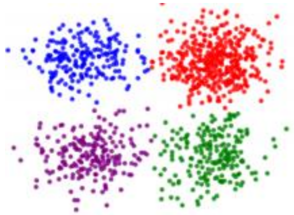
<=====



Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

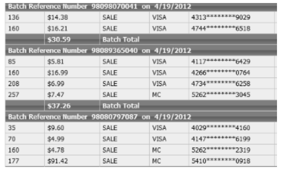
Training

Model



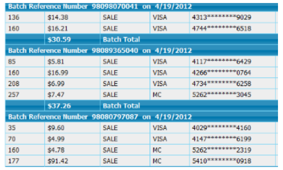
<=====

~~Privacy Preserving~~ ML Model



Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

Trans. records



Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

=====>

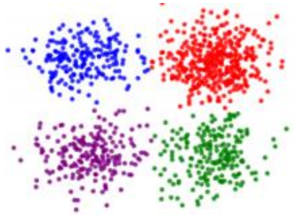
Server

<=====

Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

Training

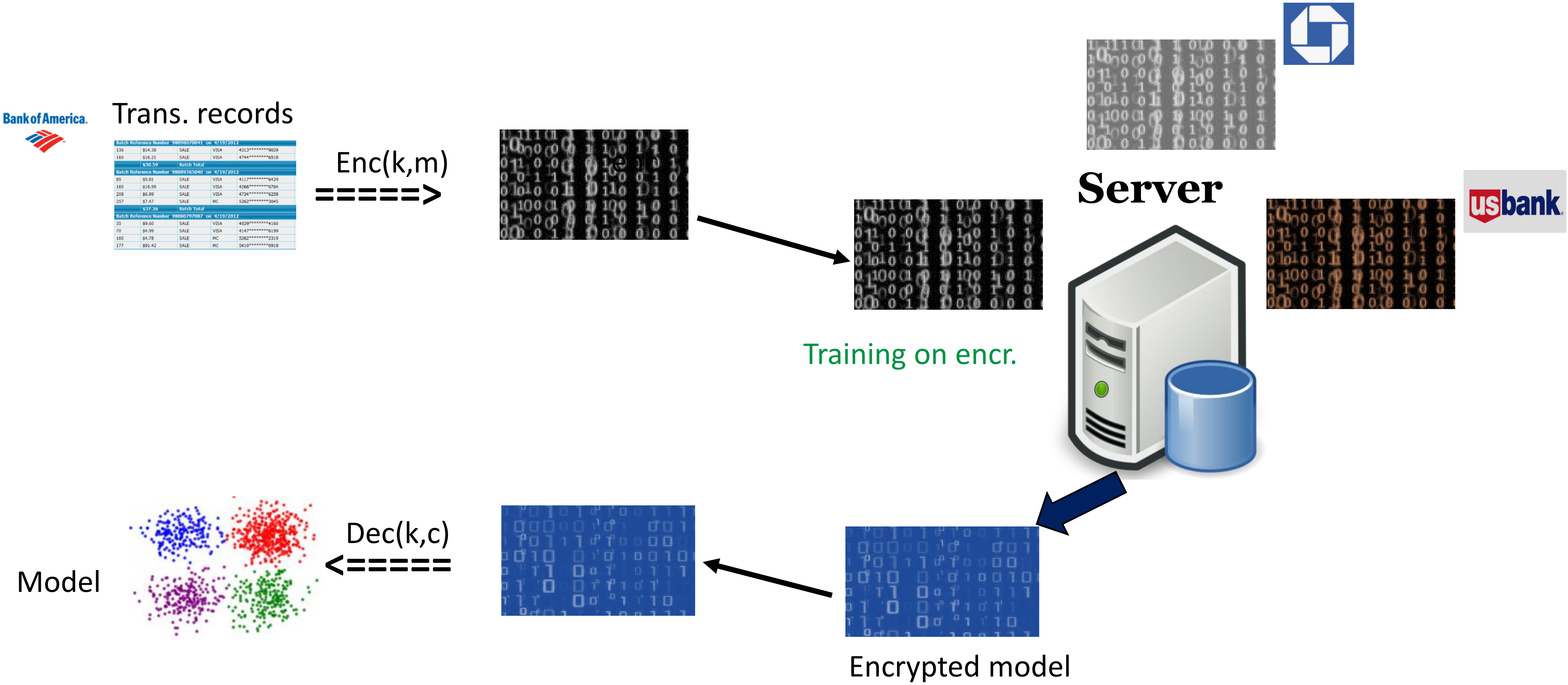
Model



<=====

What if the server is malicious?

Privacy Preserving ML Model



Trans. records

Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

Enc(k,m)

=====>

Server

Training on encr.

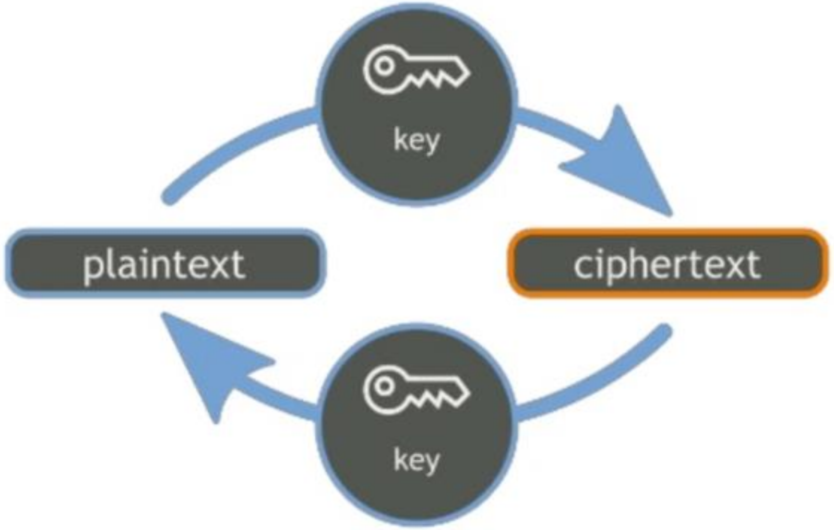
Encrypted model

Dec(k,c)

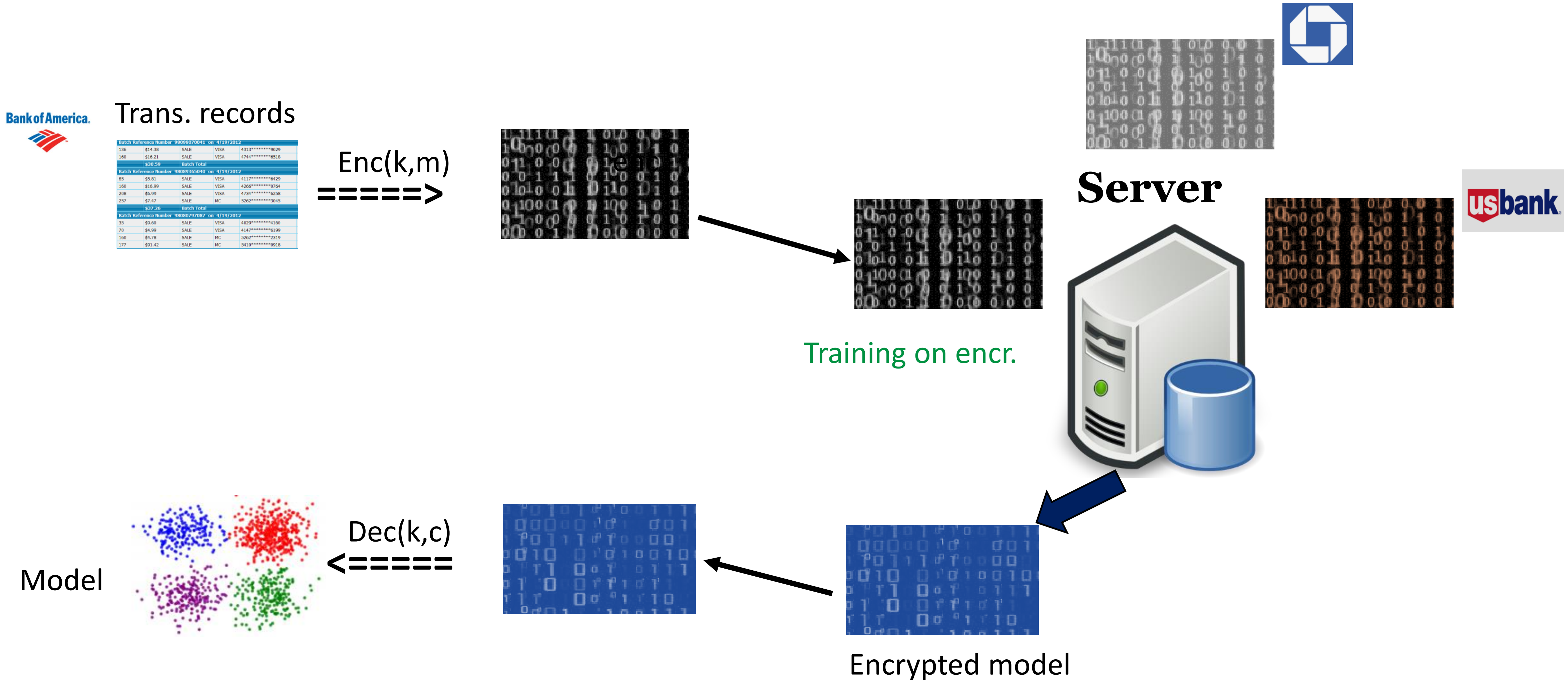
<=====

Model

- $Enc(k, m) = c$
- $Dec(k, c) = m$
- $f(Enc(k, m)) = Enc(k, f(m))$



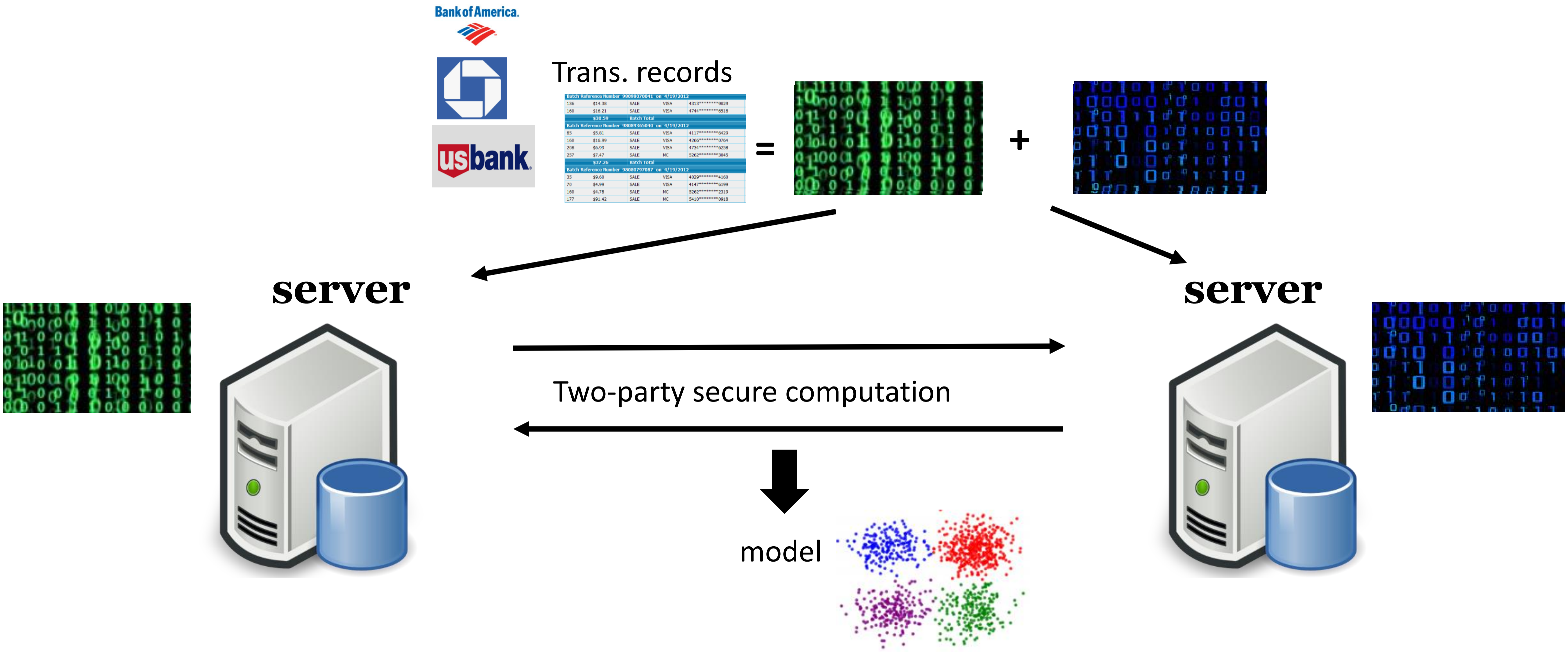
Privacy Preserving ML Model



Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918

Expensive solution because of 1) training on encrypted data
2) requiring different keys

Privacy Preserving ML Model



Trans. records

Batch Reference Number 98098070041 on 4/19/2012				
136	$14.38	SALE	VISA	4313********9029
160	$16.21	SALE	VISA	4744********6518
	$30.59	Batch Total		
Batch Reference Number 98089365040 on 4/19/2012				
85	$5.81	SALE	VISA	4117********6429
160	$16.99	SALE	VISA	4266********0764
208	$6.99	SALE	VISA	4734********6258
257	$7.47	SALE	MC	5262********3045
	$37.26	Batch Total		
Batch Reference Number 98080797087 on 4/19/2012				
35	$9.60	SALE	VISA	4029********4160
70	$4.99	SALE	VISA	4147********6199
160	$4.78	SALE	MC	5262********2319
177	$91.42	SALE	MC	5410********0918