Flamingo: Multi-Round Single-Server Secure Aggregation with Applications to Private Federated Learning

Yiping Ma\textsuperscript{1} Jess Woods\textsuperscript{1} Sebastian Angel\textsuperscript{1,2} Antigoni Polychroniadou\textsuperscript{3} Tal Rabin\textsuperscript{1}

\textsuperscript{1}University of Pennsylvania
\textsuperscript{2}Microsoft Research
\textsuperscript{3}J.P. Morgan AI Research & AlgoCRYPT CoE
Data-driven applications nowadays

Service providers collect and analyze user data in order to provide customized functionalities.
Data-driven applications nowadays

Simply put, to protect users at scale, we rely on machine learning powered by user feedback to catch spam and help us identify patterns in large data sets—making it easier to adapt quickly to ever-changing spam tactics. Gmail employs a number of AI-driven filters that determine what gets marked as spam. These filters look at a variety of signals, including characteristics of the IP address, domains/subdomains, whether bulk senders are authenticated, and user input. User feedback, such as when a user marks a certain email as spam or signals they want a sender’s emails in their inbox, is key to this filtering process, and our filters learn from user actions.
Centralized vs. decentralized training

Centralized

Decentralized

Data never leaves user devices!

“Federated learning” [McMahan et al. in 2016]

Many clients (users) collaboratively train a model under the orchestration of a central server (service provider).
Centralized vs. decentralized training

Centralized

```
Centralized = \text{Train}\left(\begin{array}{l}
\text{("hacked", spam)} \\
\text{("hotel", not spam)} \\
\text{("malicious", spam)}
\end{array}\right)
```

```
= \text{Train}\left(\begin{array}{l}
\text{("hacked", spam)} \\
\text{("hotel", not spam)} \\
\text{("malicious", spam)}
\end{array}\right)
```

Decentralized

```
Decentralized = \text{Update}\left(\begin{array}{l}
\text{("hacked", spam)}
\end{array}\right)
```

```
= \text{Update}\left(\begin{array}{l}
\text{("malicious", spam)}
\end{array}\right)
```

```
= \text{Update}\left(\begin{array}{l}
\text{("hotel", not spam)}
\end{array}\right)
```

Local weights
Centralized vs. decentralized training

**Centralized**

Centralized training involves:

- **Train**: 
  
  \[ \text{Train} \left( \begin{array}{c}
  \text{"hacked", spam} \\
  \text{"hotel", not spam} \\
  \text{"malicious", spam}
  \end{array} \right) \]

**Decentralized**

Decentralized training involves:

- **Global weights**: 

  \[ \text{Global weights} \]

  \[ \text{Update} \left( \begin{array}{c}
  \text{"hacked", spam} \\
  \text{"malicious", spam} \\
  \text{"hotel", not spam}
  \end{array} \right) \]

  - Update ("hacked", spam)
  - Update ("malicious", spam)
  - Update ("hotel", not spam)
Centralized vs. decentralized training

Centralized

Train

("hacked", spam)
("hotel", not spam)
("malicious", spam)
("apple", not spam)
("dog", not spam)
("lottery", spam)
("random", spam)

= A few hundreds to a few thousands of clients

Decentralized

= + +

---

7
Centralized vs. decentralized training

**Centralized**

\[
\text{Train} = \begin{cases} 
\text{("hacked", spam)} \\
\text{("hotel", not spam)} \\
\text{("malicious", spam)} \\
\text{("apple", not spam)} \\
\text{("dog", not spam)} \\
\text{("lottery", spam)} \\
\text{("random", spam)} 
\end{cases}
\]

**Decentralized**

\[
\text{= } + +
\]
Centralized vs. decentralized training

Centralized

Train:

- (“hacked”, spam)
- (“hotel”, not spam)
- (“malicious”, spam)
- (“apple”, not spam)
- (“dog”, not spam)
- (“lottery”, spam)
- (“random”, spam)

Decentralized

= + +
Federated learning: steps forward

• Weights do not necessarily hide data: inference attack [Zhu et al. 2019]

• Training does not need individual weights; only the sum is needed ("hacked", spam)
Federated learning: steps forward

• Weights do not necessarily hide data: inference attack
  [Zhu et al. 2019]

  ("hacked", spam)

• Training does not need individual weights; only the sum is needed
Secure aggregation for federated learning

• Secure aggregation (A special case of MPC [Yao 1986])

- Only learns $x_1 + x_2 + x_3$

Many works under different communication models, cryptographic assumptions, etc.

- Secret sharing
  [KRKR 2020], [DSQG+ 2022], ...
- Threshold homomorphic encryption
  [SGA 2021], [SHYL+ 2022], ...
- Pairwise masking
  [BIKM+ 2017], [BBGLR 2020], ...
- Other styles
  [SSVR+ 2022], [GPSBB 2022], ...
Secure aggregation for federated learning

• Secure aggregation (A special case of MPC [Yao 1986])

Only learns $x_1 + x_2 + x_3$

Many works under different communication models, cryptographic assumptions, etc.

Concrete efficiency but not asymptotics

[SGA 2021], [SHYL+ 2022], ...  
• Pairwise masking  
[BIKM+ 2017], [BBGLR 2020], ...  
• Other styles  
[SSVR+ 2022], [GPSBB 2022], ...
Federated learning has complex setting

• From the federation side—restricted clients (mobile devices)
  • Limited computation power
  • Unstable network connection

• From the machine learning side—large parameters
  • Inputs: model weights, e.g., ~500K in popular models for CIFAR100
  • Participants: 100-5000 per iteration
  • Training: many iterations, e.g., ~300 for CIFAR100
Federated learning has complex setting

• From the federation side—restricted clients (mobile devices)
  • Limited computation power
  • Unstable network connection

  • Lightweight client computation
  • Tolerate dropouts at any point

• From the machine learning side—large parameters
  • Inputs: model weights, e.g., ~500K in popular models for CIFAR100
  • Participants: 100-5000 per iteration
  • Training: many iterations, e.g., ~300 for CIFAR100
Federated learning has complex setting

• From the federation side—restricted clients (mobile devices)
  • Limited computation power
  • Unstable network connection

• From the machine learning side—large parameters
  • Inputs: model weights, e.g., ~500K in popular models for CIFAR100
  • Participants: 100-5000 per iteration
  • Training: many iterations, e.g., ~300 for CIFAR100
Prior designs are not the best fit for a full training

- From the federation side—restricted clients (mobile devices)
  - Limited computation power
  - Unstable network connection

- From the machine learning side—large parameters
  - Inputs: model weights, e.g., ~500K in popular models for CIFAR100
  - Participants: **100-5000 per iteration**
  - Training: many iterations, e.g., ~300 for CIFAR100

One summation: multiple round trips, some of which are expensive
Having fewer round trips is important

- Reduce bias and improve quality
- Reduce run time

Will discuss in evaluation section why round trips matter a lot
We propose Flamingo

• From the federation side—restricted clients (mobile devices)
  • Limited computation power
  • Unstable network connection

  Lightweight client computation
  Tolerate dropouts at any point

• From the machine learning side—large parameters
  • Inputs: model weights, e.g., ~500K in popular models for CIFAR100
  • Participants: 100-5000 per iteration
  • Training: many iterations, e.g., ~300 for CIFAR100

Can practically run for a full training session

Same threat model as in prior work: a malicious adversary controlling the server and a subset of the clients
Flamingo has two key ideas

• A fault-tolerant private sum protocol based on pairwise secrets and threshold decryption

• A way to reuse pairwise secrets over many iterations
A fault-tolerant private sum protocol

**Pairwise secrets**

BIKM+ 2017, BBGLR 2020

Take some cost to set them up

Take some cost to set them up

\[ v_1 = x_1 + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \]
A fault-tolerant private sum protocol

Pairwise secrets

\[
\begin{align*}
\overrightarrow{x}_1 &= \overrightarrow{v}_1 + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \\
\overrightarrow{v}_2 &= \overrightarrow{v}_2 - \text{PRG}(s_{12}) + \text{PRG}(s_{23}) \\
\overrightarrow{v}_3 &= \overrightarrow{v}_3 - \text{PRG}(s_{13}) - \text{PRG}(s_{23})
\end{align*}
\]

Take some cost to set them up

Semi-honest
A fault-tolerant private sum protocol

Pairwise secrets

BIKM+ 2017, BBGLR 2020

Pairwise secrets

Efficient despite large inputs

\[
\sum_{i=1}^{3} v_i = \sum_{i=1}^{3} x_i
\]

\[
\begin{align*}
\overrightarrow{v_1} &= \overrightarrow{x_1} + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \\
\overrightarrow{v_2} &= \overrightarrow{x_2} - \text{PRG}(s_{12}) + \text{PRG}(s_{23}) \\
\overrightarrow{v_3} &= \overrightarrow{x_3} - \text{PRG}(s_{13}) - \text{PRG}(s_{23})
\end{align*}
\]
A fault-tolerant private sum protocol

Pairwise secrets

\[ \vec{v}_1 = \vec{x}_1 + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \]
\[ \vec{v}_2 = \vec{x}_2 - \text{PRG}(s_{12}) + \text{PRG}(s_{23}) \]

Reveal the secrets to the server!

Went offline...
A fault-tolerant private sum protocol

Threshold decryption

\[
\mathbf{v}_1 = \mathbf{x}_1 + \text{PRG}(s_{12}) + \text{PRG}(s_{13})
\]
A fault-tolerant private sum protocol

Threshold decryption

A random (small) subset of clients

Recovery is lightweight

Semi-honest
A fault-tolerant private sum protocol

Threshold decryption

\[ \overrightarrow{v_1} = \overrightarrow{x_1} + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \]
\[ \overrightarrow{v_2} = \overrightarrow{x_2} - \text{PRG}(s_{12}) + \text{PRG}(s_{23}) \]
A fault-tolerant private sum protocol

Threshold decryption

\[
\begin{align*}
\vec{v}_1 &= \vec{x}_1 + \text{PRG}(s_{12}) + \text{PRG}(s_{13}) \\
\vec{v}_2 &= \vec{x}_2 - \text{PRG}(s_{12}) + \text{PRG}(s_{23}) \\
&\quad - \text{PRG}(s_{13}) - \text{PRG}(s_{23})
\end{align*}
\]

\[
\vec{v}_1 + \vec{v}_2 - \text{PRG}(s_{13}) - \text{PRG}(s_{23}) = \vec{x}_1 + \vec{x}_2
\]
Reusing the secrets

Essentially OTP

\[ x_1 \]

Alice

\[ x_2 \]

Bob

\[ x_3 \]

Charlie

Simple idea, but cannot work for [BBGLR 2020] due to a crucial design difference for fault tolerance

\[ \bar{v}_1 = \bar{x}_1 + \text{PRG}(s_{12}^t) + \text{PRG}(s_{13}^t) \]

Iteration \( t \): \( s_{12}^t = \text{PRF}(s_{12}, t) \)

\[ \text{Enc}(PK, s_{12}^t) \]

\[ \text{Enc}(PK, s_{13}^t) \]
With the two key ideas →

Do the costly setup once,
and run the lightweight sum many times
More details in the paper

• How decryptors work
  • Selection
  • Sharing of $SK$
  • Switching decryptors over time

• How setup is done

• How to achieve malicious security

• Efficient instantiation of cryptographic primitives, system-level optimizations
Evaluation results

• What is the right factor to look at?
  • Computation cost was the focus: [BIKM+ 2017] → [BBGLR 2020]
  • When computation is made cheap, what matters is the “waiting time”
Evaluation results

• What is the right factor to look at?
  • Computation cost was the focus: [BIKM+ 2017] → [BBGLR 2020]
  • When computation is made cheap, what matters is the “waiting time”

![Diagram showing a round trip in the protocol](image)
Evaluation results

• Feasibility of training a neural network on CIFAR100
• Simulation using a multi-agent messaging system ABIDES

![Graph showing elapsed time vs. training rounds for different methods: BBGLR, Flamingo, Baseline. The graph indicates 6 RTTs with all clients, 3 RTTs with only 1 RTT, and 1 RTT with all clients.](ABIDES)
Summary

• This work: A secure aggregation system that handles real-world federated training tasks

• Many interesting future directions
  • Validation of client inputs
  • Stronger security, e.g., adaptive adversary

Thanks!
Backup Slides
Malicious security

Alice

Bob

$v_1 \rightarrow \overline{v_1}$

$v_2 \rightarrow \overline{v_2}$

Enc(PK, $s_{12}$)

Enc(PK, $s_{13}$)

Enc(PK, $s_{13}$)

Enc(PK, $s_{23}$)

Bob

Charlie

Alice

$x_1 \rightarrow \overline{x_1}$

$x_2 \rightarrow \overline{x_2}$

$x_3 \rightarrow \overline{x_3}$

$s_{12}$

$s_{13}$

$s_{23}$

Decryptors

$SK_1$

$SK_2$

$SK_3$
Malicious security

Alice

Bob

Charlie

Decryptors

\(\text{Enc}(PK, s_{12})\)
\(\text{Enc}(PK, s_{13})\)
\(\text{Enc}(PK, s_{23})\)
A cross-check round

Key idea:
Honest decryptors agree on what to decrypt
A fault-tolerant sum with malicious security

\[
\begin{align*}
&\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \\
&\mathbf{v}_1^t, \mathbf{v}_2^t, \mathbf{v}_3^t \\
&\mathbf{s}^{t}_{12}, \mathbf{s}^{t}_{13}, \mathbf{s}^{t}_{23}
\end{align*}
\]

Waiting… Process… \(\overrightarrow{v}_1 + \overrightarrow{v}_2\)

Enc(\(PK, s_{12}^t\)) Enc(\(PK, s_{13}^t\))

Waiting… Process… Waiting…

\[
\begin{align*}
&\mathbf{SK}_1, \mathbf{SK}_2, \mathbf{SK}_3 \\
\text{Partial decryptions} &\mathbf{SK}_1, \mathbf{SK}_2, \mathbf{SK}_3 \\
\text{Process…} &\overrightarrow{v}_1 + \overrightarrow{v}_2 \\
&\text{–PRG}(s_{12}^t) \\
&\text{–PRG}(s_{13}^t) \\
&\mathbf{x}_1^t + \mathbf{x}_2^t
\end{align*}
\]