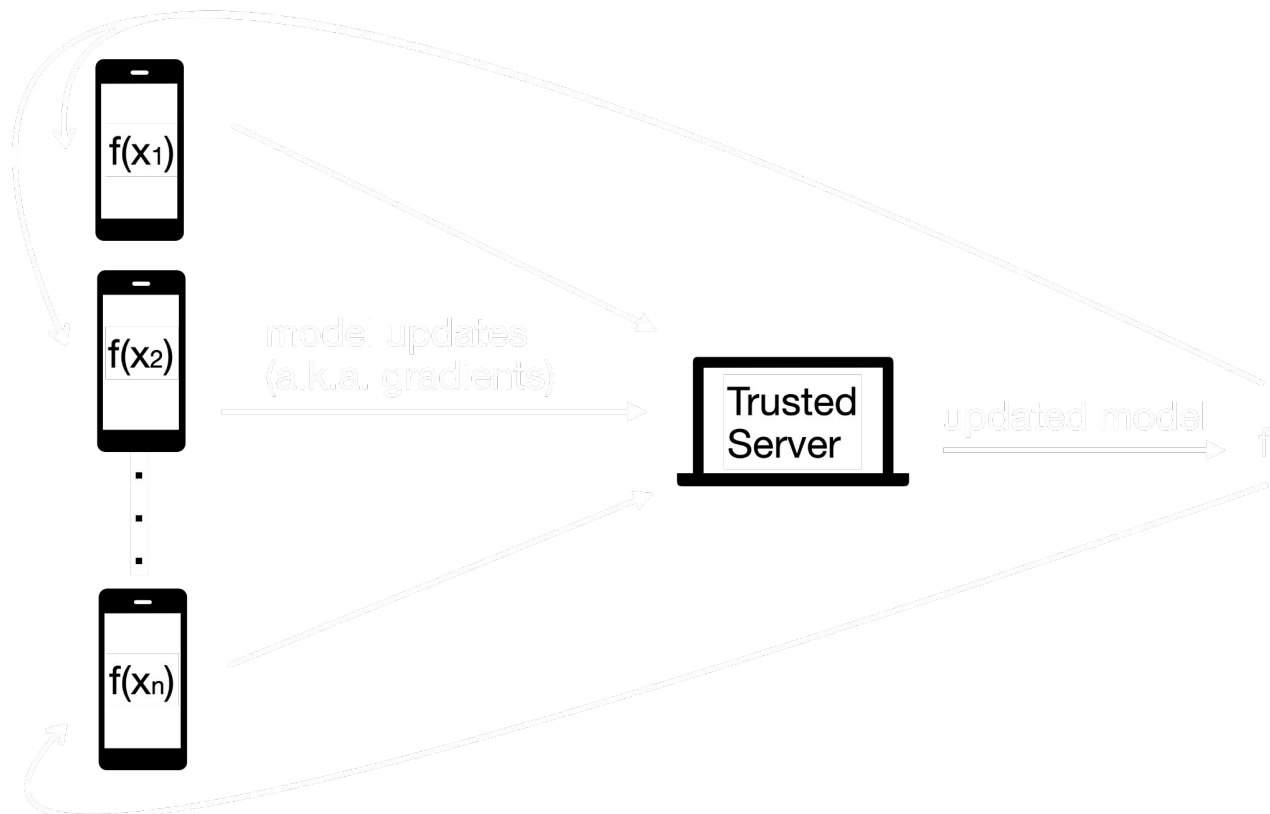


# Private Inexpensive Norm Enforcement, a new VDAF

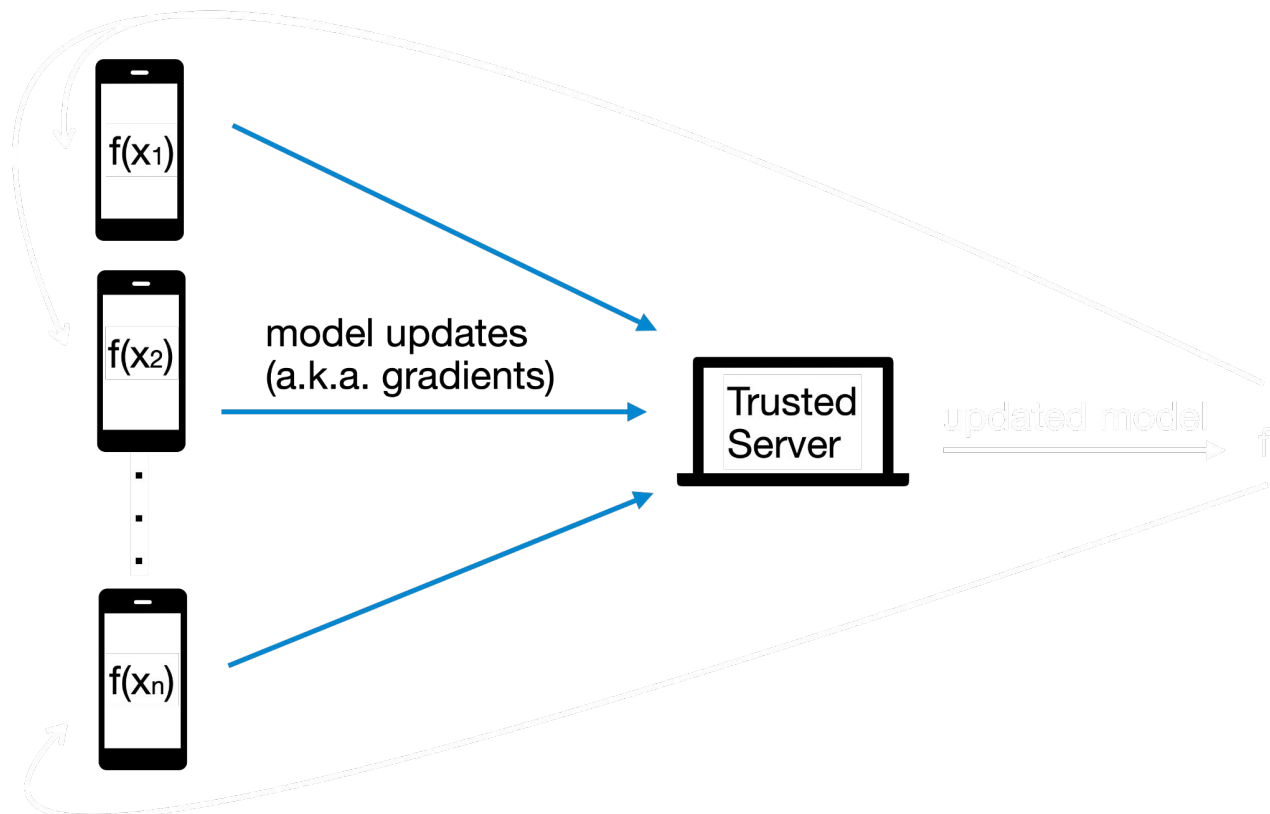
Junye Chen, Christopher Patton

IETF 119 – CFRG

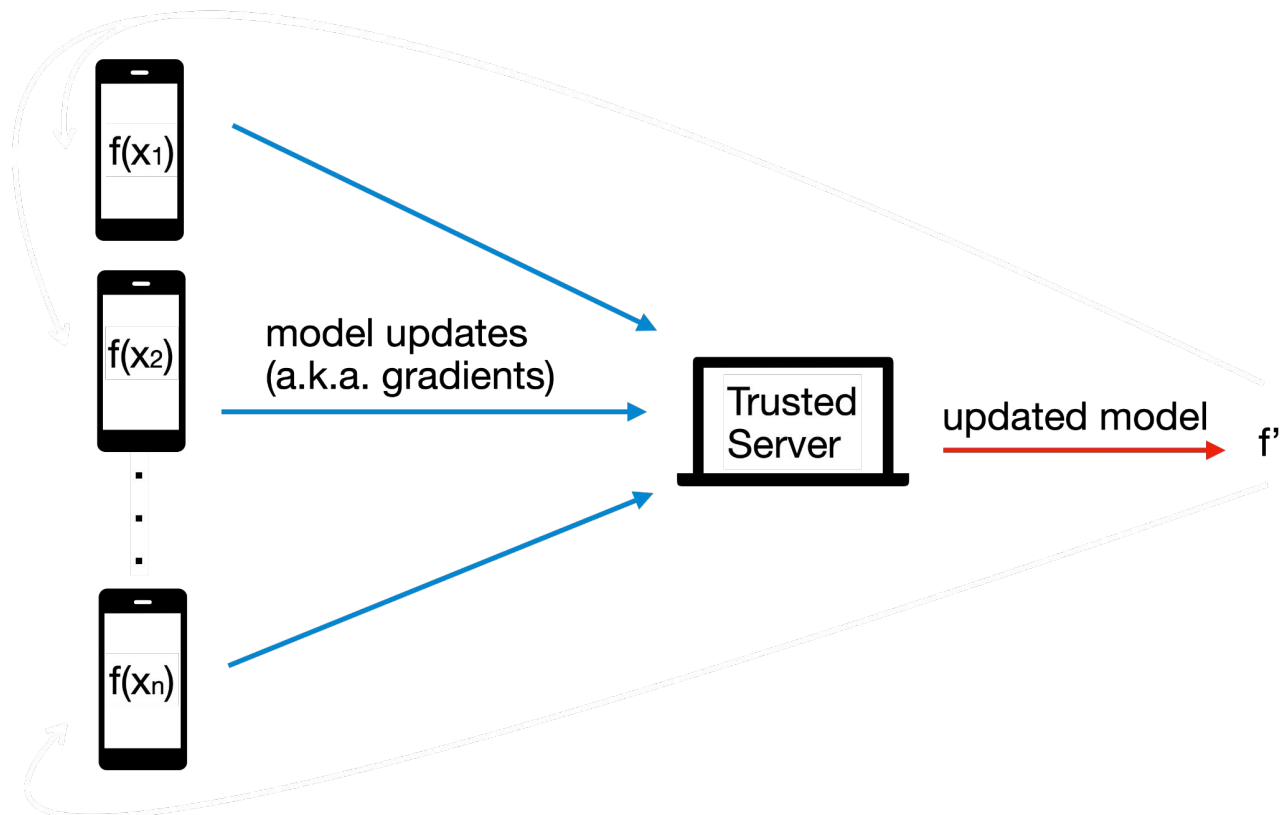
# Use Case: Federated Machine Learning



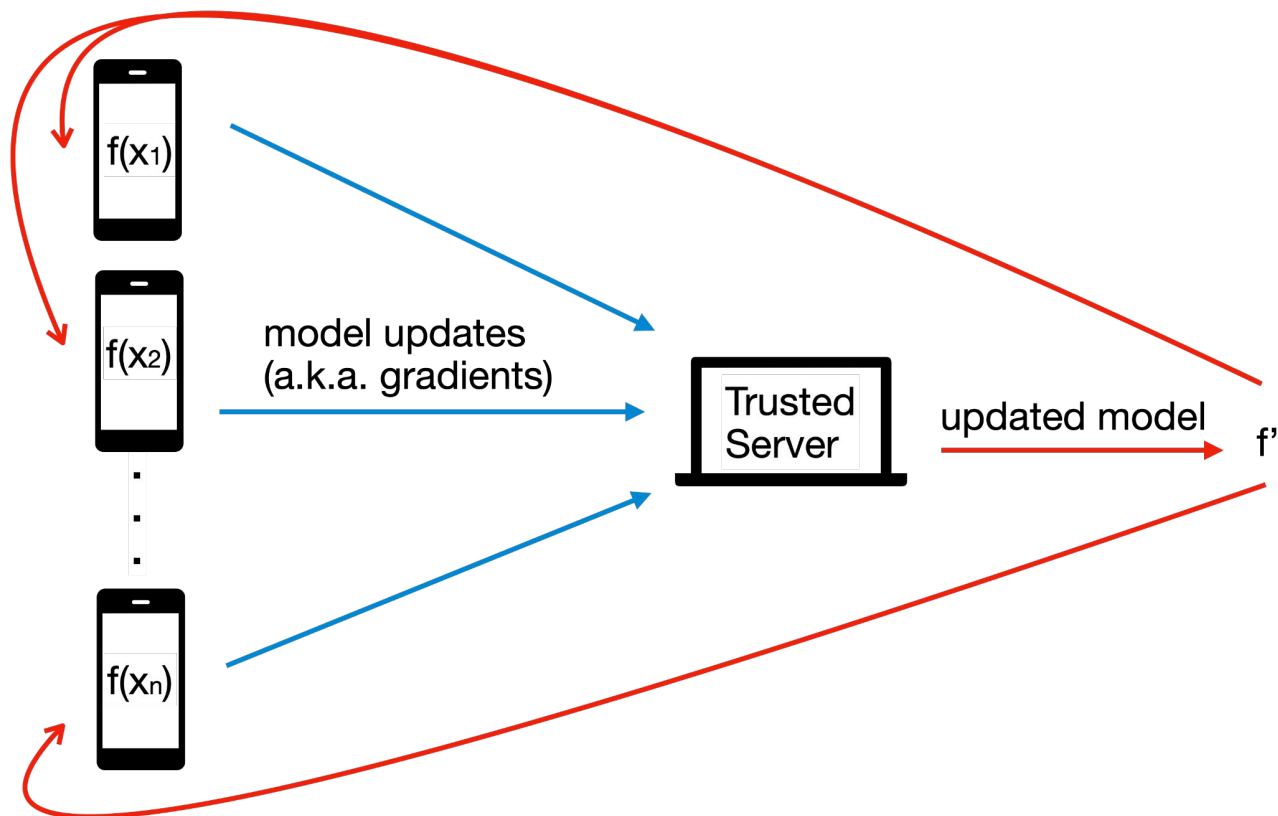
# Use Case: Federated Machine Learning



# Use Case: Federated Machine Learning



# Use Case: Federated Machine Learning



# Verifiable Distributed Aggregation Function [VDAF]

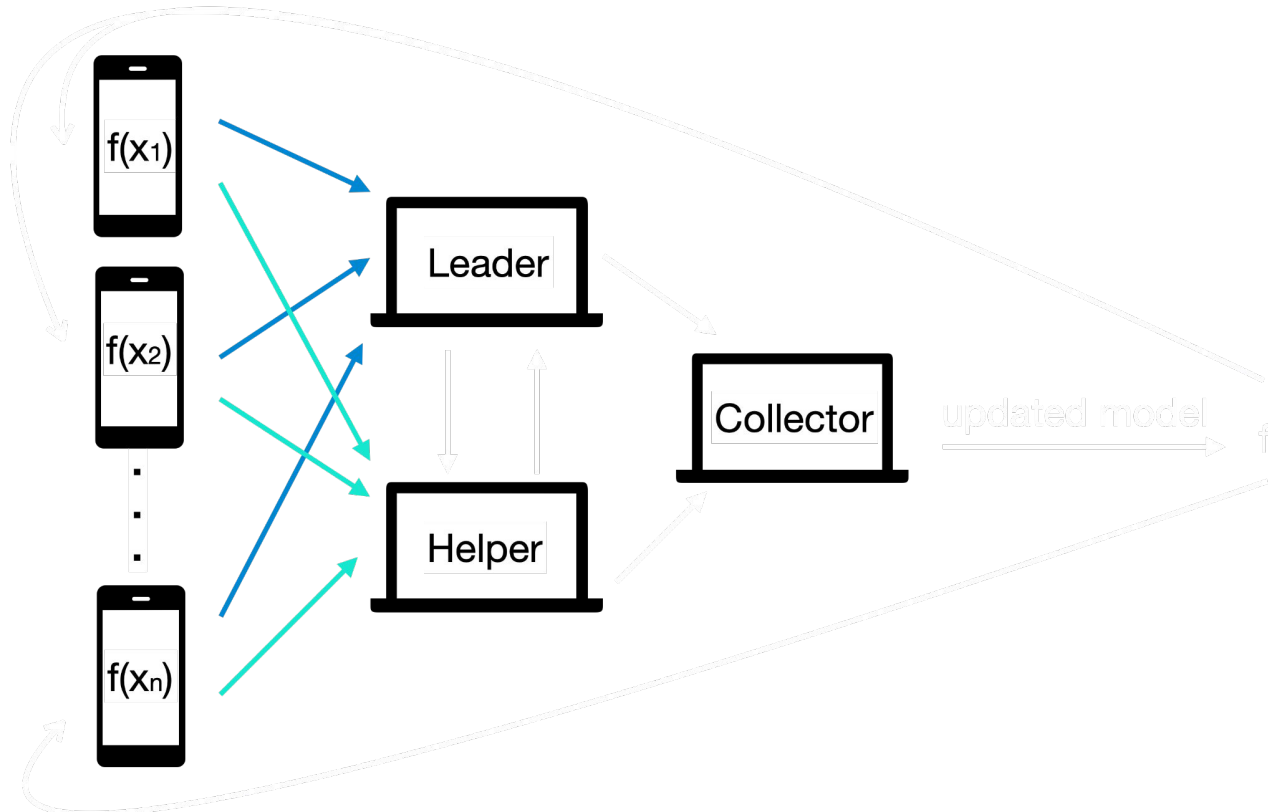
- Secure multi-party aggregation of client “measurements”.
- Prio3: Uses the idea of a Fully Linear Proof (FLP) [VDAF, Section 7], a distributed zero-knowledge proof system to verify properties of Client measurements.

# PINE VDAF: [draft-chen-cfrg-vdaf-pine-00](#)

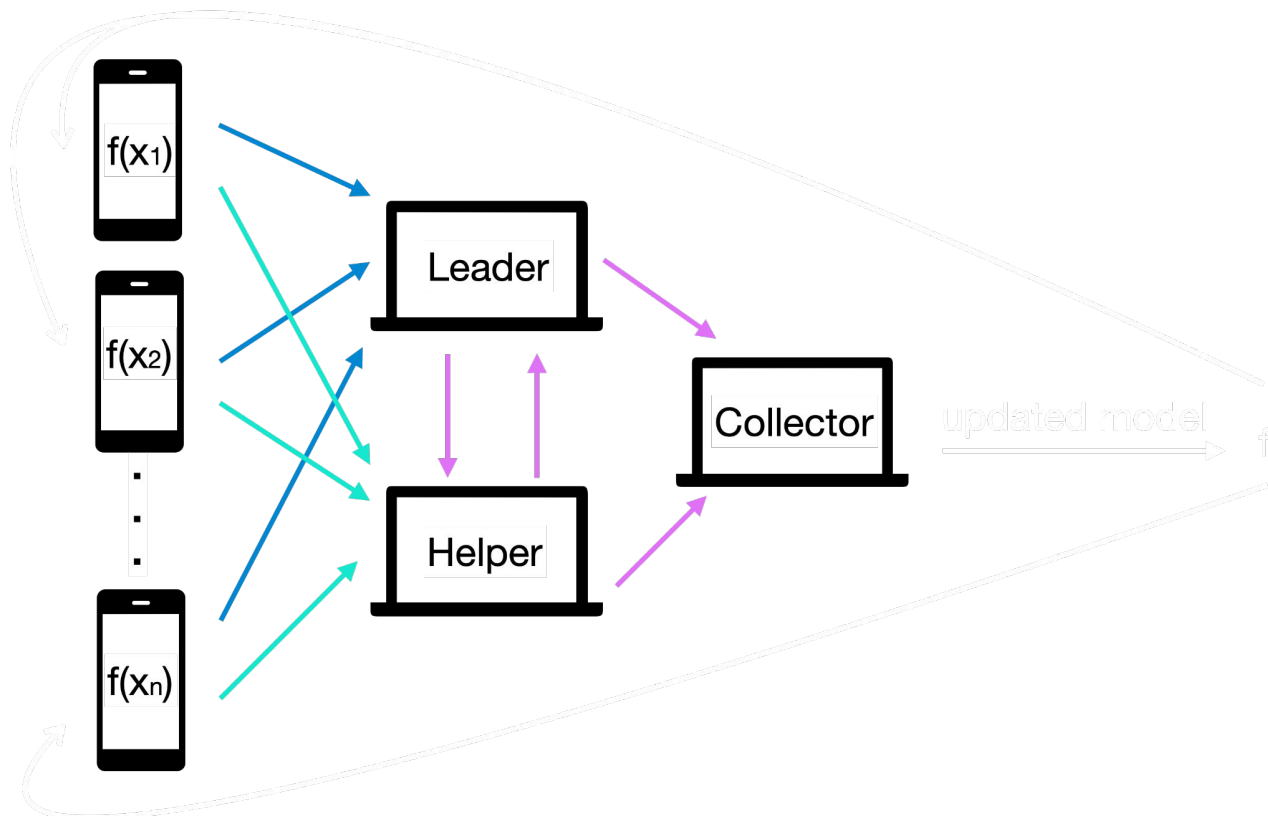
- The draft is based on a recent paper [ROCT'23].
- Goal: compute  $\sum_i x_i$ , where each  $x_i \in \mathbb{R}^d$  is a Client gradient.
- Requires: the “L2 norm”  $\|x_i\|_2 \leq l2\_norm\_bound$ . Note  $\|x_i\|_2 = (\sum_j x_{i,j}^2)^{0.5}$ .
- Uses the idea of a Fully Linear Proof (FLP) like Prio3.



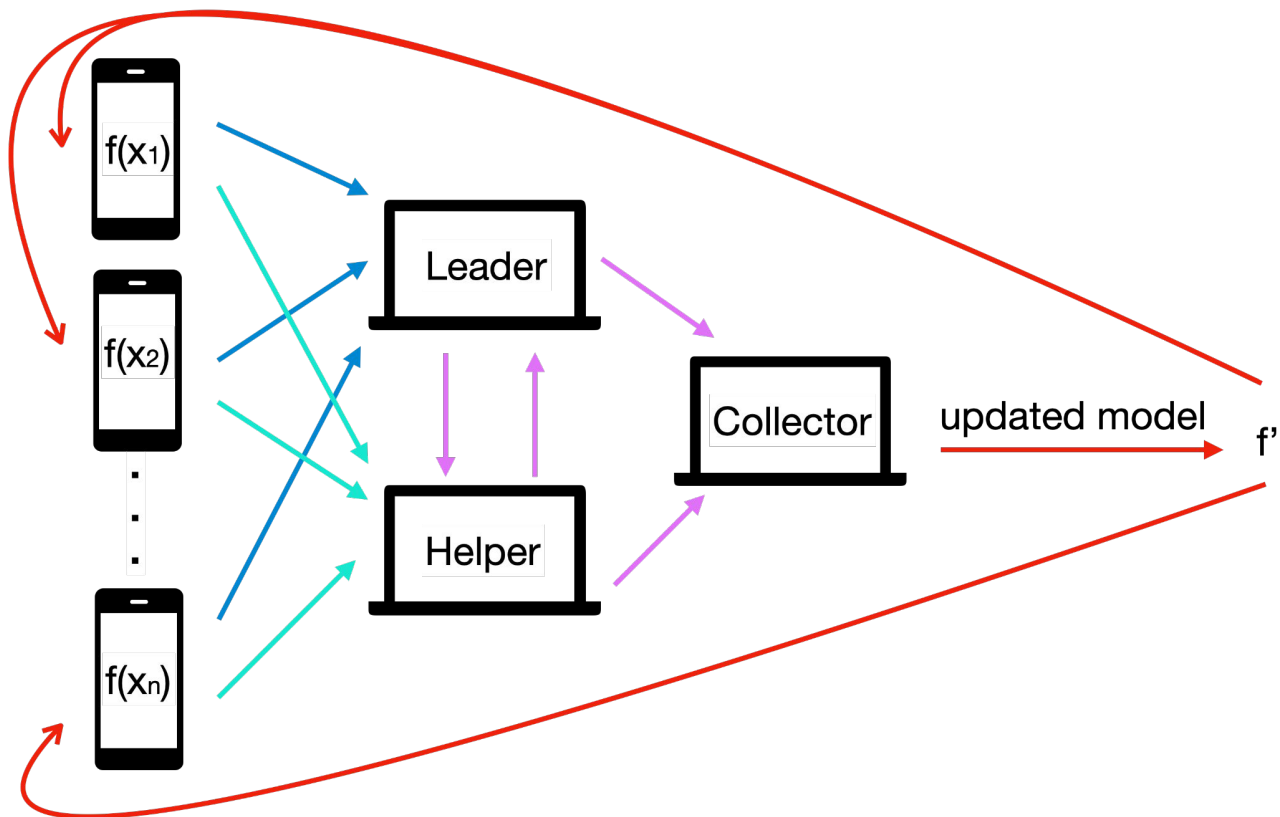
# Use Case: Federated Machine Learning with PINE VDAF



# Use Case: Federated Machine Learning with PINE VDAF



# Use Case: Federated Machine Learning with PINE VDAF



# Why Not Prio3?

- Computing squared L2-norm (the sum of squares of all entries in the encoded gradient) can overflow the field modulus.
  - Example: Suppose L2 norm bound is 10, field modulus  $q = 23$ , client gradient = [99, 0, 7].  
Taking the squared L2-norm of this gradient modulo  $q$  is only 6.
- Challenge: prevent “wraparound” effect.
- One could ensure each entry of the gradient is sufficiently small, but the communication cost would be too high,  $\sim O(\text{dimension} * \text{num\_frac\_bits})$ .

# PINE Wraparound Check

- A random vector is sampled, each entry is a -1, 1, or 0.
- Compute a dot product of the random vector with the encoded gradient.
- If the squared L2-norm of the gradient wraps around field modulus, this dot product is likely to be large. [ROCT'23] proves this check correctly detects wraparound with probability  $\frac{1}{2}$ .
- Repeat this check to reach the desired soundness error.
- Incompatible with Prio3.

# Performance Comparison

- $l2\_norm\_bound = 1.0$ ,  $num\_frac\_bits = 15$ ,  $dimension = 10^5$
- PINE's communication cost is 15x less compared to Prio3's.

# Next steps for draft-chen-cfrg-vdaf-pine-00

- **Current status of the draft**

- Core design work is complete
  - Reference code and test vectors
  - Core component is supported by [security proofs](#)
- Remaining work:
  - Complete the draft text
  - Finalize parameters (minimize communication cost)
  - Incorporate feedback from implementers

- **Is CFRG interested in this adopting this work?**

- Enables federated learning in the VDAF framework ⇒ improves privacy for training machine learning models
- Opens up new use cases for [PPM](#)

- **Ready for an adoption call?**

- More security analysis would be helpful
- Further optimization is possible