ARTIFACT EVALUATED
USENIX
AVAILABLE

# Oblivious Signaling

single-server based metadata-hiding communication scheme


**Mirza KB Shuhan**
George Mason University

Foteini Baldimtsi
George Mason University
Mysten Labs

Giuseppe Ateniese
George Mason University



USENIX Security 2026, Baltimore, USA


GEORGE MASON UNIVERSITY

MystenLabs

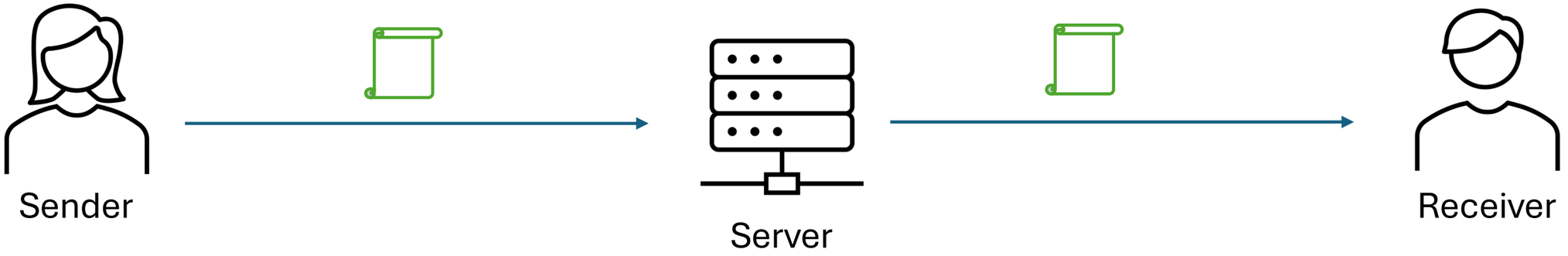
# Why Oblivious Signaling?

Your messages might be encrypted in end-to-end encrypted systems, but adversaries can **still trace communication links!**



Oblivious Signaling **hides *who talks to whom*.**

# Our Setting




- Senders send **signals** to the Receiver through the Server
- Server can not learn about the content of the signals
- Server can not learn which **signals** meant for which receivers
- Even if the Server colludes with the recipient, no additional information (other than network-level metadata) can be retrieved about the sender.

Receiver-Message Unlinkability

**Signals** are one-way fixed-sized messages. It can be the actual payload or the location of a larger message in the bulletin board.

# Our Holy Grail

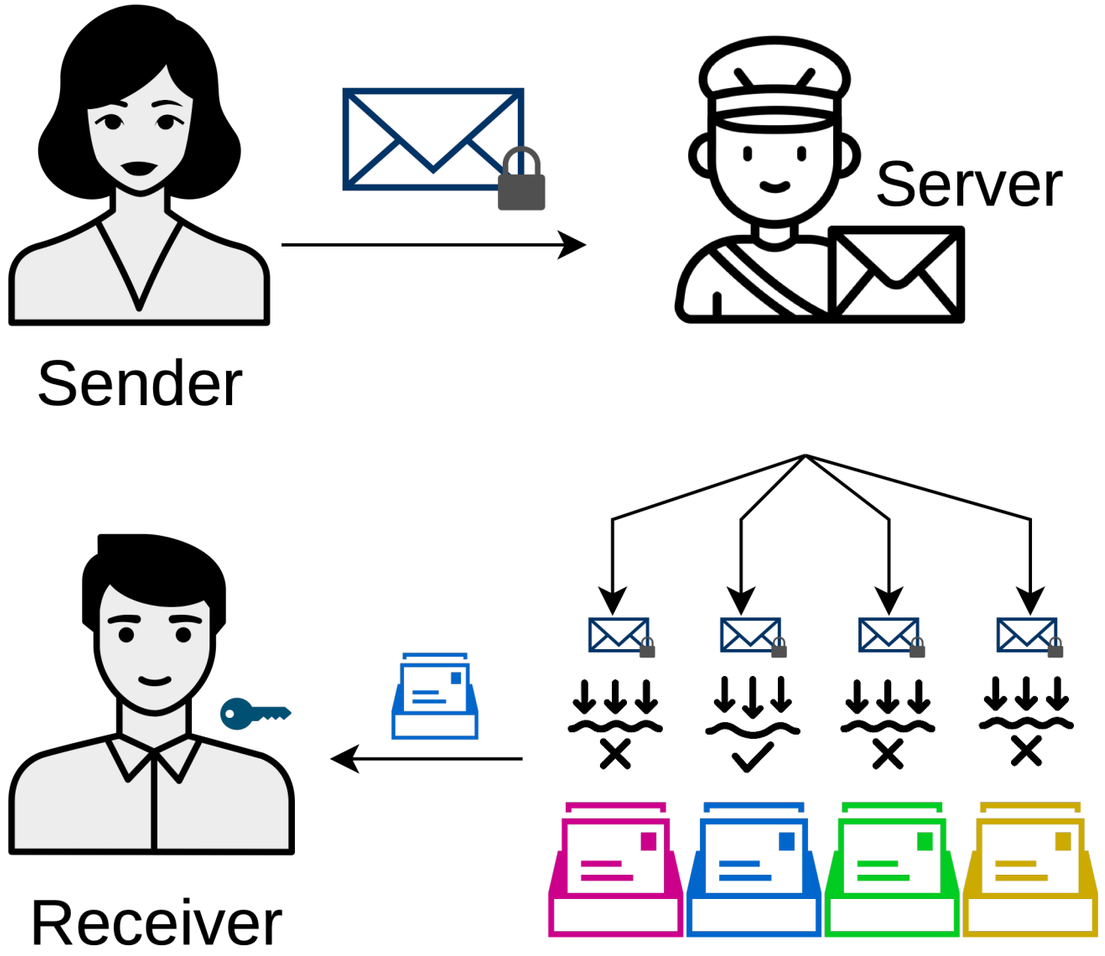
- Single Untrusted Server
  - Honest-but-Curious for execution
  - Malicious for privacy
- No Liveness Requirement
  - Async Communication




*meme generated via imgflip

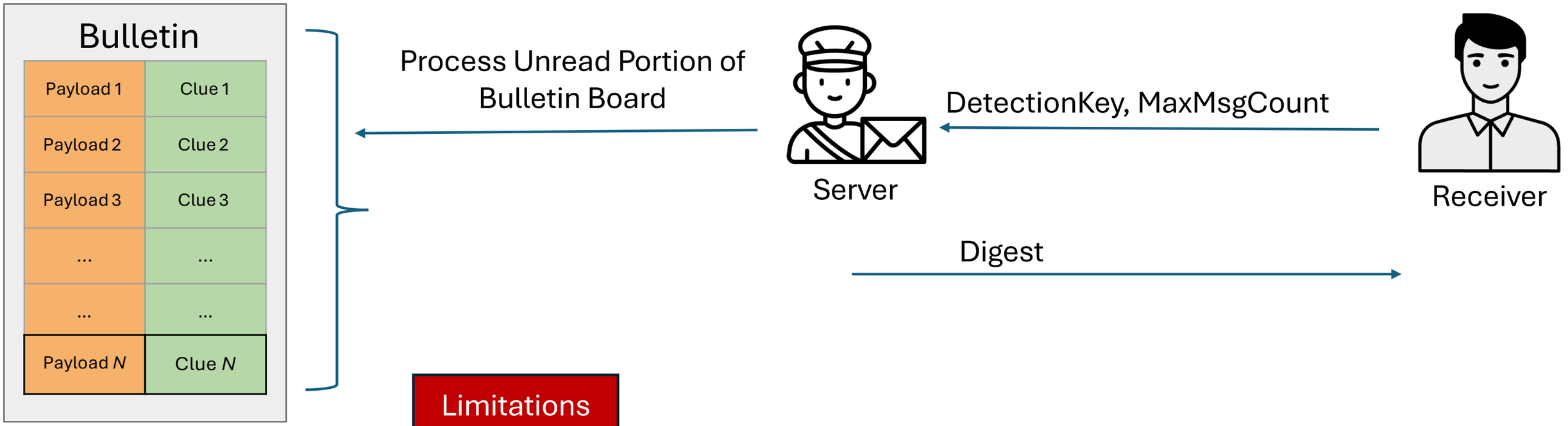
# Our Approach: Oblivious Signaling

- The server maintains a fixed-size **encrypted inbox** for each recipient
- When a sender submits a message, the server applies the **exact same homomorphic update** to every inbox in the system
- The target inbox absorbs the message; all other inboxes remain semantically unchanged
- Adopts **“Digital Postage”** Model; Sender pays the cost of computation



# Related Work: Oblivious Message Retrieval (OMR)

[CRYPTO'22, S&P'24, USENIX'24, USENIX'26]




**Limitations**

- The recipient bears the cost of computation, which is quasi-linear to the global traffic $(\tilde{O}(N\ell))$
- Sending is cheap; Spamming is effortless
- Requiring recipients to guess an #of incoming message leaks volume metadata

# OMR vs OSig Architecture

| Metric | Oblivious Message Retrieval (OMR) | Oblivious Signaling (OSig) |
|---|---|---|
| **Architecture Paradigm** | Pull-based | Push-based **("Digital Postage" model)** |

# OMR vs OSig Architecture

| Metric | Oblivious Message Retrieval (OMR) | Oblivious Signaling (OSig) |
|---|---|---|
| **Architecture Paradigm** | Pull-based | Push-based **("Digital Postage" model)** |
| **Computational Burden** | Borne by the recipient | Borne by the sender |

# OMR vs OSig Architecture

| Metric | Oblivious Message Retrieval (OMR) | Oblivious Signaling (OSig) |
|---|---|---|
| **Architecture Paradigm** | Pull-based | Push-based **("Digital Postage" model)** |
| **Computational Burden** | Borne by the recipient | Borne by the sender |
| **Spam Resistance** | **Effortless** (Sender pays nothing) | **Naturally Deterred** |

# OMR vs OSig Architecture

| Metric | Oblivious Message Retrieval (OMR) | Oblivious Signaling (OSig) |
|---|---|---|
| **Architecture Paradigm** | Pull-based | Push-based **("Digital Postage" model)** |
| **Computational Burden** | Borne by the recipient | Borne by the sender |
| **Spam Resistance** | **Effortless** (Sender pays nothing) | **Naturally Deterred** |
| **Volume Leakage** | **Leaks** via recipient guessing message bounds | **No such leakage** |

# OMR vs OSig Architecture

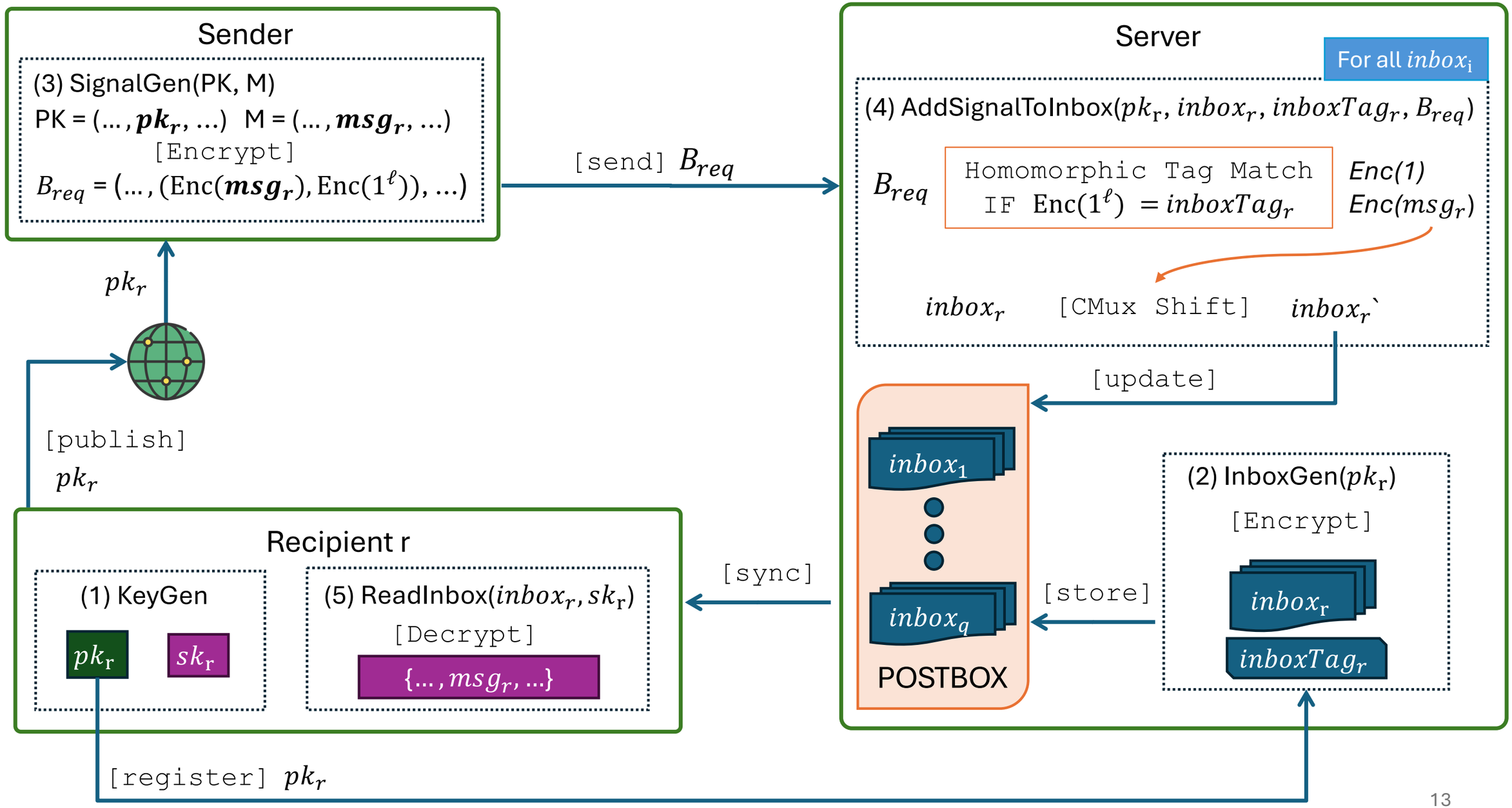
| Metric | Oblivious Message Retrieval (OMR) | Oblivious Signaling (OSig) |
|---|---|---|
| **Architecture Paradigm** | Pull-based | Push-based **("Digital Postage" model)** |
| **Computational Burden** | Borne by the recipient | Borne by the sender |
| **Spam Resistance** | **Effortless** (Sender pays nothing) | **Naturally Deterred** |
| **Volume Leakage** | **Leaks** via recipient guessing message bounds | **No such leakage** |
| **Scaling Dynamics** | Cost is quasi-linear to **global traffic** | Cost scales with **the anonymity set** |
| **Asymptotic Cost** | $\tilde{O}(N\ell)$ | $O((q/g)(\ell g + \nu))$ |

# Building Blocks

- Fully Homomorphic Encryption

  It must satisfy the following properties:
  - IK-IND-CPA Security
    - Indistinguishability of Keys and Messages
  - Circular Security
    - Encrypted secret does not compromise confidentiality
  - Wrong Key Decryption
    - Decryption with wrong secret key yields uniformly random plaintext

# Oblivious Signaling

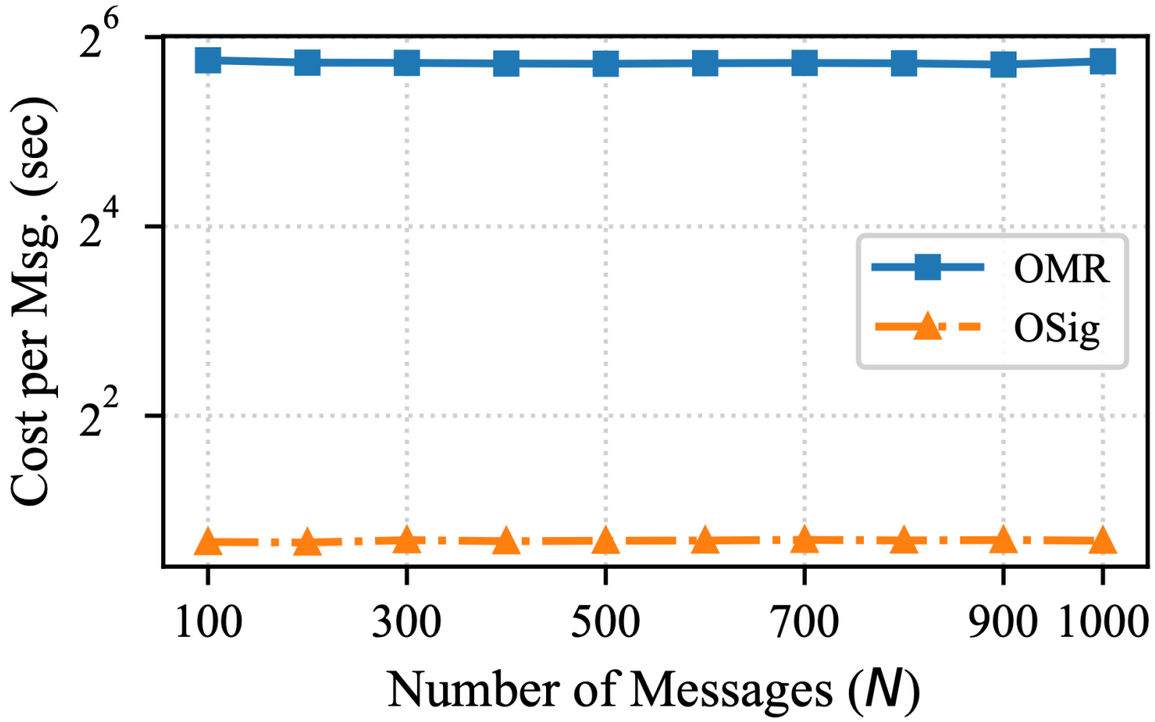


# Prototype Evaluation

- We chose TFHE scheme for prototype
- Prototype in Rust Using TFHE-rs library
- Simulation was run on GCP Compute (112 vCPUs, 224 GB RAM)

- A receiver public key occupies ~32.9 KB
- A receiver secret key ~23.5 KB
- A sender-generated ciphertext (signal, pTag) ~16.6 KB
- A recipients server evaluation key occupies ~127.8 MB

# Experiments | Cost Model Comparison




- Cost metric is the mean server processing time per recovered pertinent message.
- OSig takes around ~1.60s per successful delivery
- OMR takes around ~53s per successful retrieval
- The frequency of pertinent messages is fixed at k = N/q across q = 100 recipients

# Let's make tracking us mathematically exhausting!



Find me at

**Email:** mshuhan@gmu.edu
**LinkedIn:** @shuhanmirza