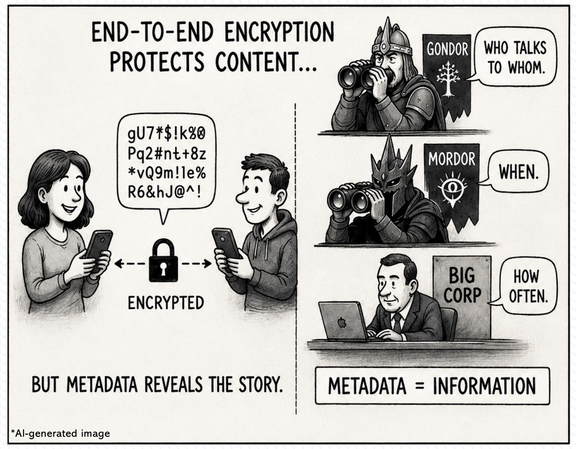
Oblivious Signaling

Mirza KB Shuhan — George Mason University

Foteini Baldimtsi — George Mason University & Mysten Labs

Giuseppe Ateniese — George Mason University

35TH USENIX Security Symposium — Artifact Evaluated: USENIX Available



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

Motivation

Can a single untrusted server deliver encrypted messages without learning their recipients?

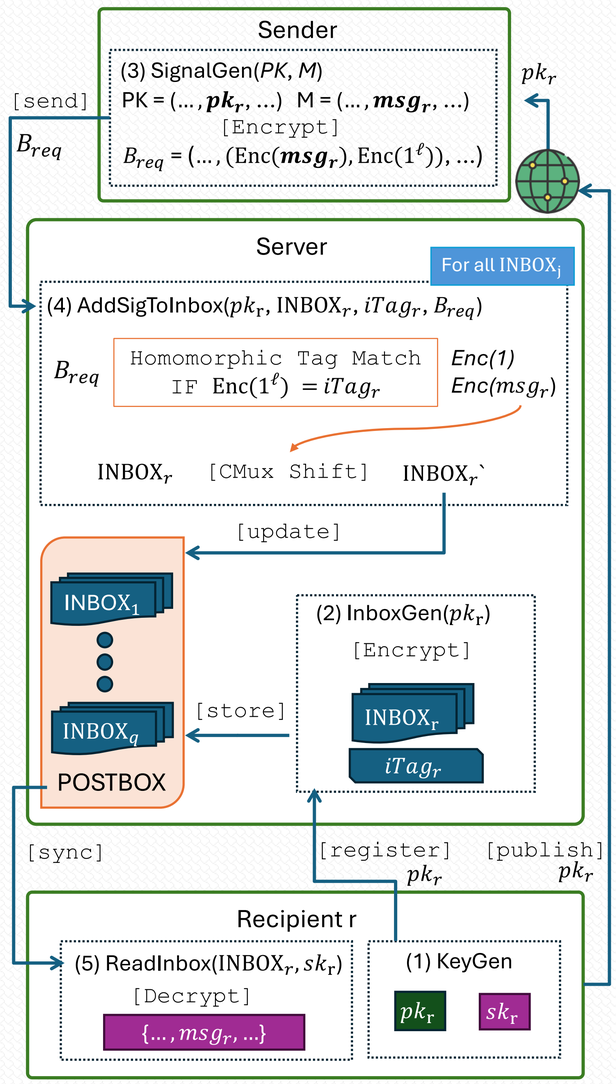
- Conventional inbox routing reveals communication patterns, even when message contents are end-to-end encrypted.
- Broadcasting hides message destinations but forces recipients to scan global traffic.
- Oblivious Message Retrieval (OMR) [CRYPTO'22, S&P'24, USENIX'24, USENIX'26] outsources this scan and preserves receiver privacy, but retrieval cost grows with global traffic, message-count bounds leak volume metadata, and cheap sending leaves spam undeterred.

Contributions

Do the privacy-preserving computation in delivery: update every encrypted inbox uniformly and make inbox checks independent of global traffic.

- Formalize OSig as a cryptographic primitive and define receiver privacy against a malicious server.
- An FHE-based protocol supporting uniform, batched inbox updates.
- Implement OSig in TFHE-rs and evaluate it against OMR.

Protocol Overview

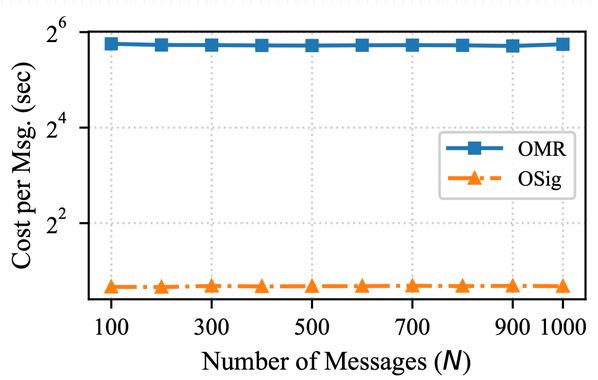


- Each recipient registers a public key; the server maintains a fixed-capacity encrypted inbox.
- Senders submit encrypted signal-tag pairs without revealing the intended recipient.
- The server homomorphically updates every inbox; only the matching recipient later gets the signal delivered to their inbox.

OMR vs OSig

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	$\tilde{O}(N\ell)$	$O((q/g)(\ell g + \nu))$

Cost Model Comparison



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

Paper: Artifact: Contact: