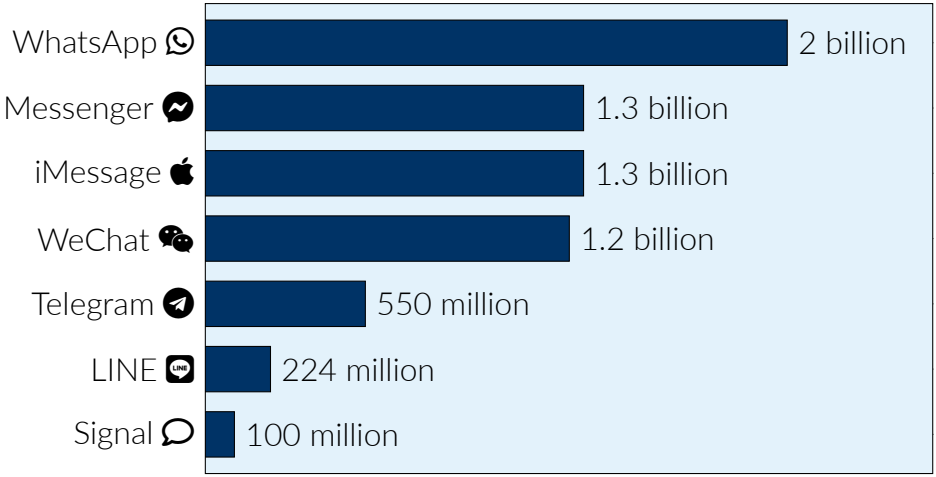
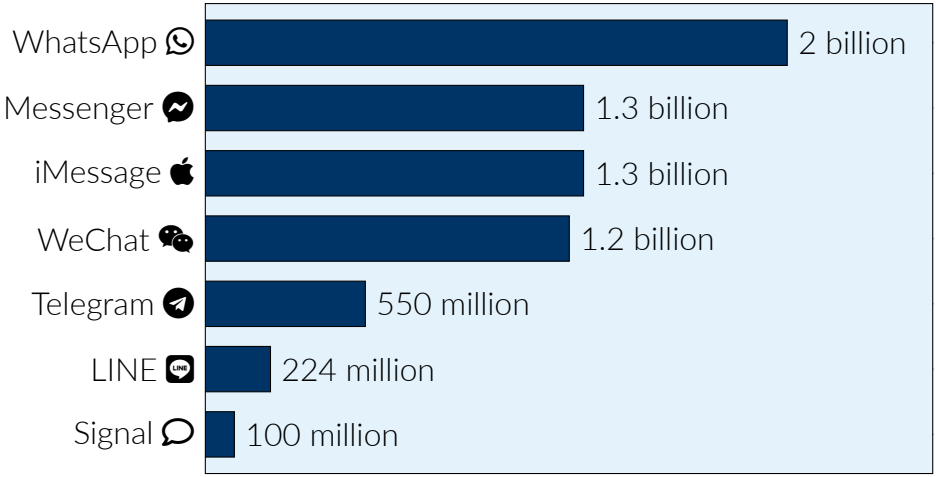
Secure Messaging in a Post-Quantum World

Most popular messaging apps



Most popular messaging apps



Most of these apps use specific protocols.

We focus on variations of the Signal protocol (,,).

Roadmap

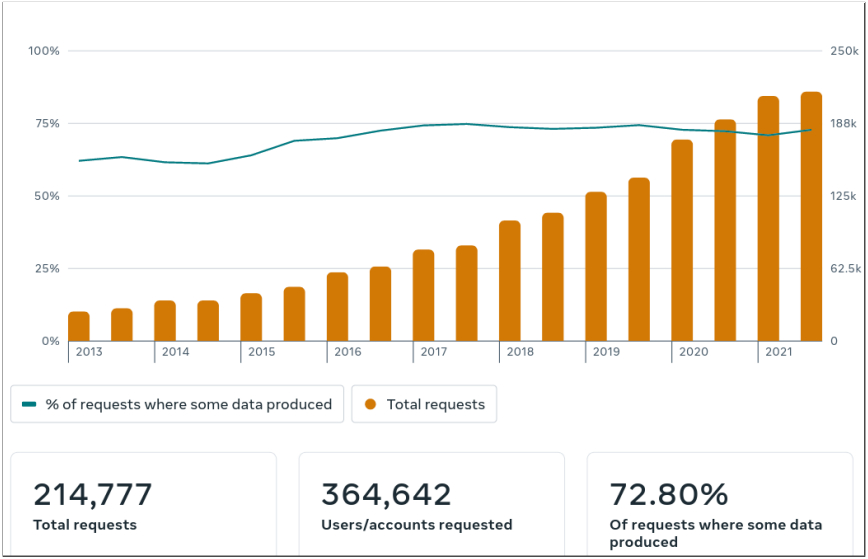
How do we obtain a secure messaging protocol that is simultaneously…

$$\underbrace{\text{post-quantum}}_{\text{Part I}} + \underbrace{\text{scalable}}_{\text{Part II}} + \underbrace{\text{metadata-hiding}}_{\text{Part III}} ?$$

(Post-Quantum) Security

Your personal data is always under attack

Meta's transparency report for Jul-Dec 2021



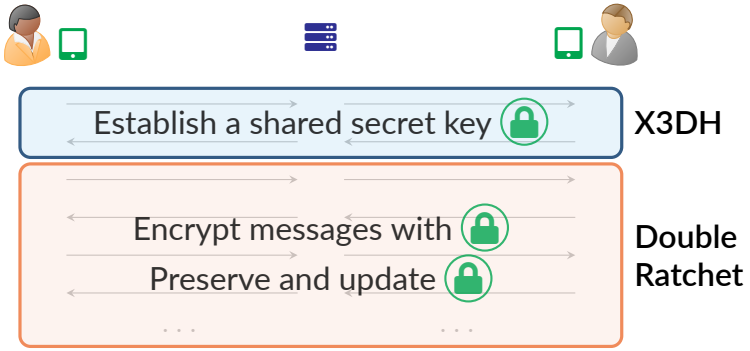
Legal means aren't the end of the story

Spyware sold off-the-shelf by companies and hackers

PEGASUS: THE NEW GLOBAL WEAPON FOR SILENCING JOURNALISTS

At least 180 journalists around the world have been selected as targets by clients of the cybersurveillance company NSO Group, according to a new Forbidden Stories investigation, published today.

The Signal protocol (two-users case)



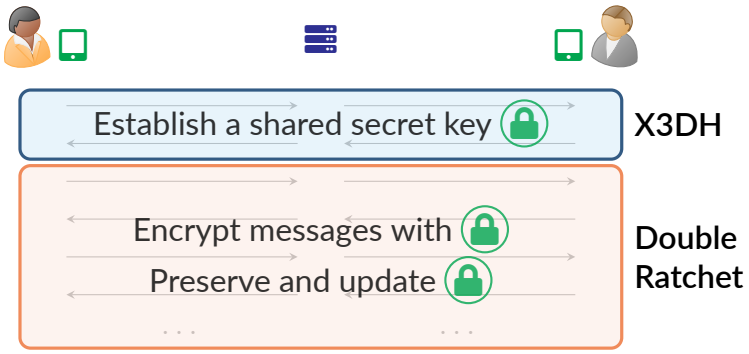
Two main threats

- State overreach
- Device compromise

Two main constraints

- Asynchrony
- Long sessions

The Signal protocol (two-users case)

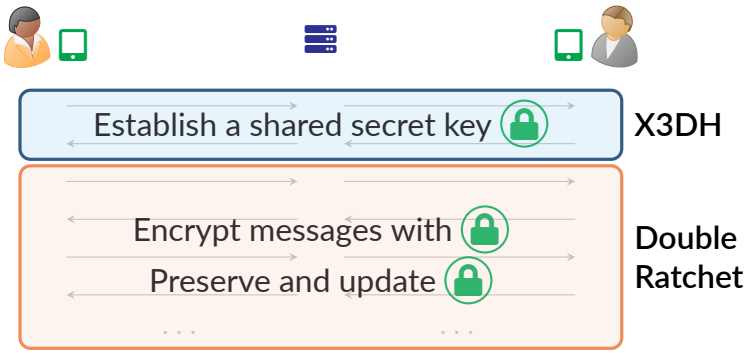


Pre-quantum world:

- **X3DH:**[1] Diffie-Hellman + XEdDSA + symmetric crypto (HKDF)
- **Double Ratchet:**[2] Diffie-Hellman + symmetric crypto (HKDF, HMAC, ...)

[1] https://signal.org/docs/specifications/x3dh/
[2] https://signal.org/docs/specifications/doubleratchet/

The Signal protocol (two-users case)

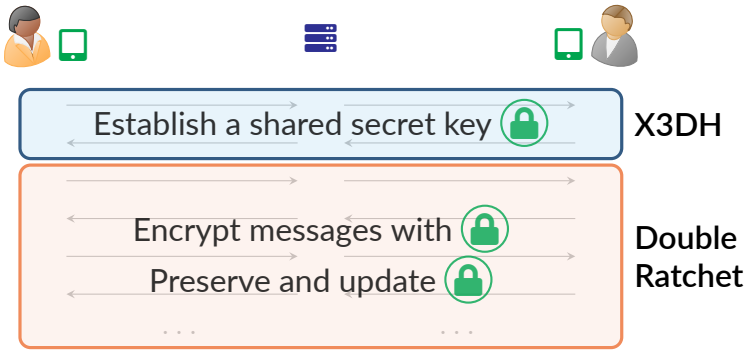


Post-quantum world:

→ **PQ X3DH:**[1] KEM + (ring) signatures + symmetric crypto

[1] Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest: *An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable*. PKC 2021 + Journal of Cryptology 2022.

The Signal protocol (two-users case)

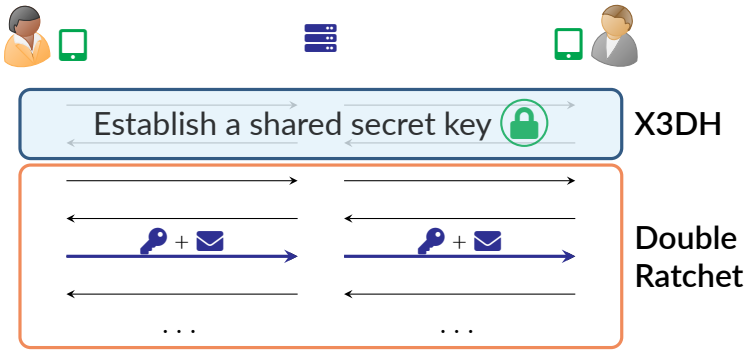


Post-quantum world:

- **PQ X3DH:** KEM + (ring) signatures + symmetric crypto
- **PQ Double Ratchet:**[1] KEM + symmetric crypto

[1] Joël Alwen, Sandro Coretti, and Yevgeniy Dodis: *The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol.* EUROCRYPT 2019

Inside the PQ Double Ratchet



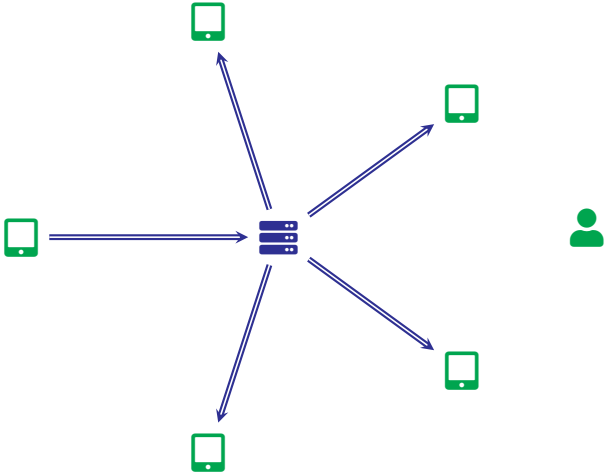
- Each user has a KEM keypair (only the encryption key is made public)
- Updating cryptographic material:
  - generates a new KEM keypair (including) and randomness
  - encrypts in a ciphertext using the encryption key of
  - incorporates into , and sends + to

  Both and are able to derive the updated

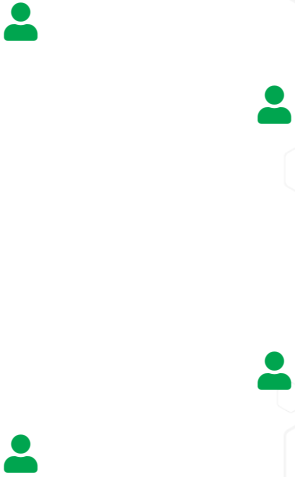
Scalable Group Messaging

Scaling Signal to groups – pairwise channels

Physical layer



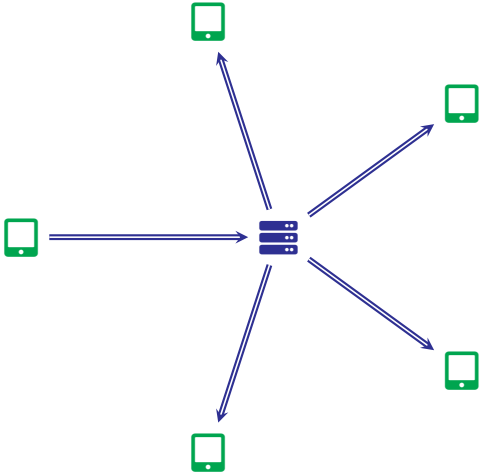
Insider view



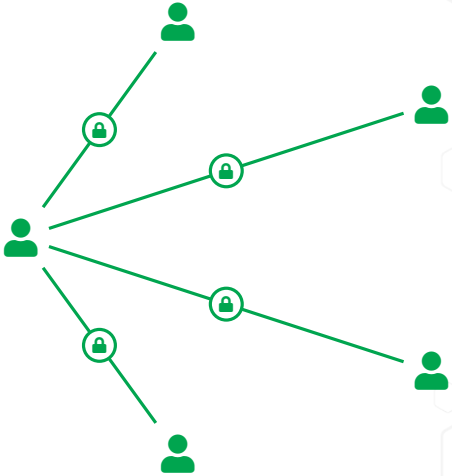
Scaling Signal to groups – pairwise channels

PQ SHIELD

Physical layer



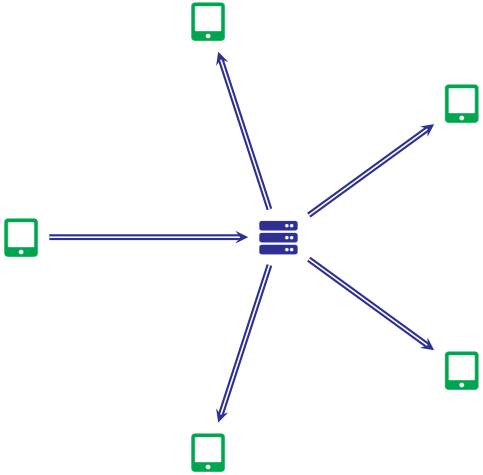
Insider view



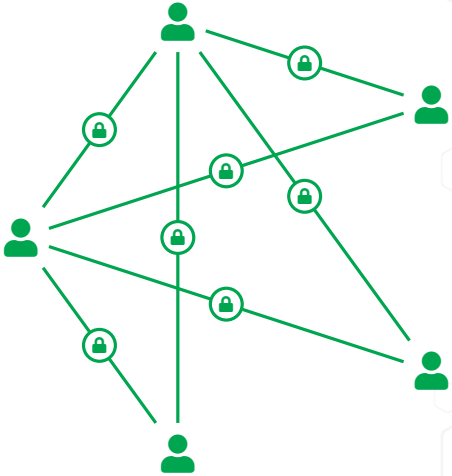
Scaling Signal to groups – pairwise channels

PQ SHIELD

Physical layer

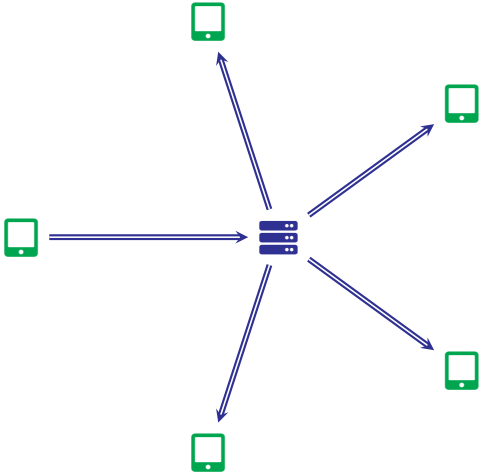


Insider view

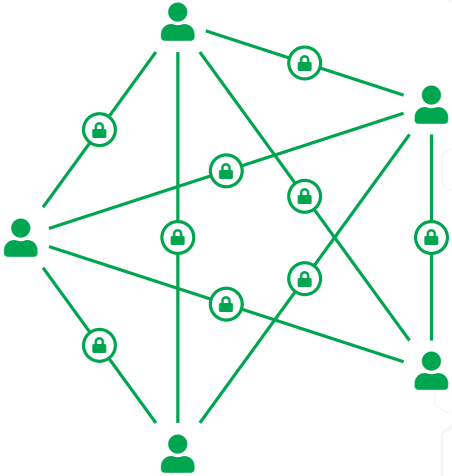


Scaling Signal to groups – pairwise channels

Physical layer



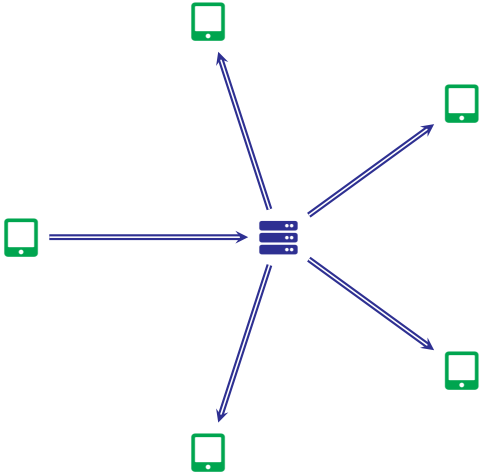
Insider view



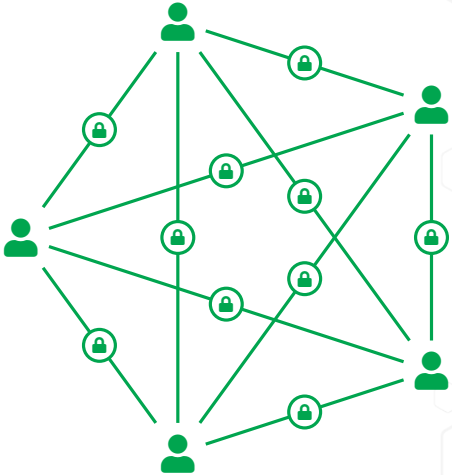
Scaling Signal to groups – pairwise channels

PQ SHIELD

Physical layer



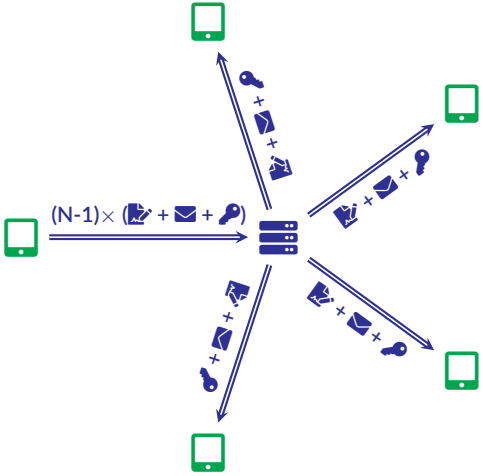
Insider view



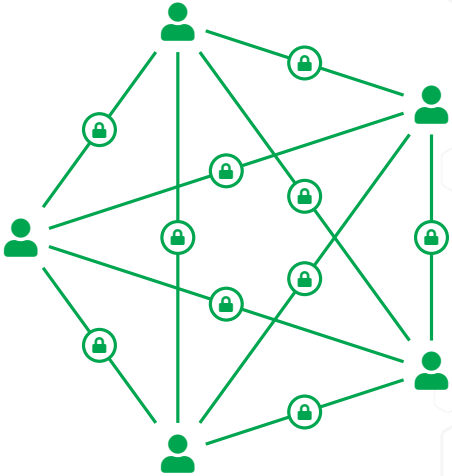
Scaling Signal to groups – pairwise channels

PQ SHIELD

Physical layer



Insider view

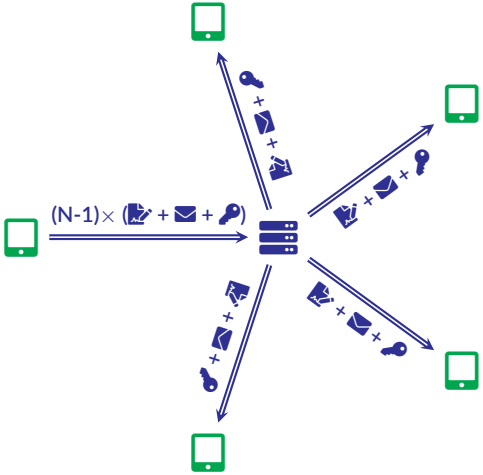


Cost of one update with $N = 256$, Kyber-512 and Dilithium-2:

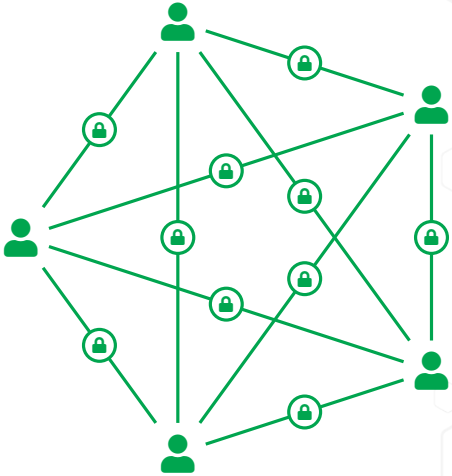
1.2 Megabytes for the sender

Scaling Signal to groups – pairwise channels

Physical layer



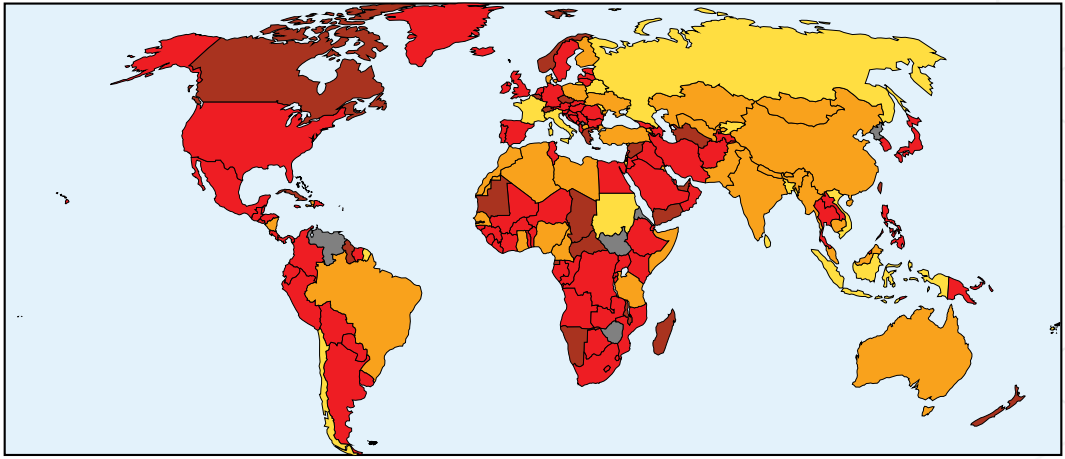
Insider view



Sending a single picture of 100 Kilobytes with $N = 256$:

25.5 Megabytes for the sender

How much does 1 GB of mobile data cost?[1]

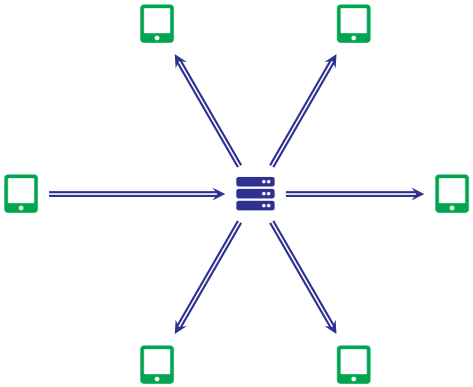


Median cost: ≤ $0.50 | ≤ $1.00 | ≤ $5.00 | ≥ $5.00

[1] https://www.cable.co.uk/mobiles/worldwide-data-pricing/

Our scalable protocol

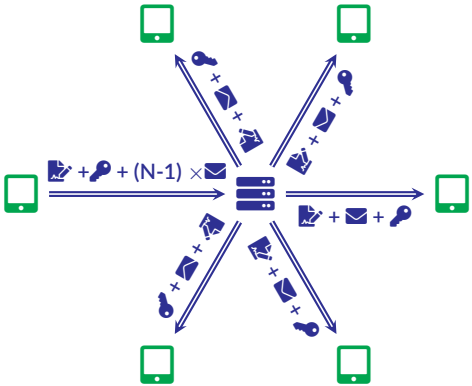
- **One channel:** a single shared secret for the whole group[2]
- **One signature and one encryption key:** a single signature authenticates the encryption key and all the ciphertexts



[2] First proposed by Karthikeyan Bhargavan, Benjamin Beurdouche, Prasad Naldurg: *Formal Models and Verified Protocols for Group Messaging: Attacks and Proofs for IETF MLS*

Our scalable protocol

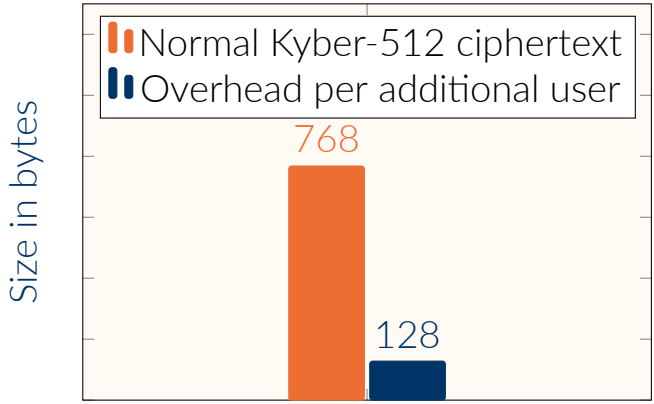
- **One channel:** a single shared secret for the whole group[2]
- **One signature and one encryption key:** a single signature authenticates the encryption key and all the ciphertexts



[2] First proposed by Karthikeyan Bhargavan, Benjamin Beurdouche, Prasad Naldurg: *Formal Models and Verified Protocols for Group Messaging: Attacks and Proofs for IETF MLS*

Multi-recipient public-key encryption

We can compress ciphertexts when encrypting the same message to *N* parties.
We exploit this when encrypting to the whole group.



Efficiency summary

Bandwidth costs in a group of N members

Scheme	**Message**	Update (upload)	Update (download)	**Update (total)**
Pairwise channels (Signal)	**O(N)**	O(N)	O(1)	**O(N)**
TreeKEM (MLS)	**O(1)**	O(log N)*	O(log N)*	**O(N log N)***
Our protocol§	**O(1)**	O(N)	O(1)	**O(N)**

*Best-case complexity

§Keitaro Hashimoto, Shuichi Katsumata, Eamonn Postlethwaite, Thomas Prest, and Bas Westerbaan: *A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs*. CCS 2021.

Protecting your Metadata

Metadata collection is systemic

PQ SHIELD

> “ Metadata, however, showing how a WhatsApp account was used and which numbers were contacting one another and when, can be tracked with a surveillance technology known as a pen-register. PenLink provides that tool as a service. ”

Forbes

CYBERSECURITY • EDITORS' PICK

Meet The Secretive Surveillance Wizards Helping The FBI And ICE Wiretap Facebook And Google Users

Thomas Brewster Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

Feb 23, 2022, 01:53pm EST

2

A small Nebraska company is helping law enforcement around the world spy on users of Google, Facebook and other tech giants. A secretly recorded presentation to police reveals how deeply embedded in the U.S. surveillance machine PenLink has become.

Metadata collection, in more details

RollingStone

GOT A TIP? | LOG IN | SUBSCRIBE

POLITICS

FBI Document Says the Feds Can Get Your WhatsApp Data – in Real Time

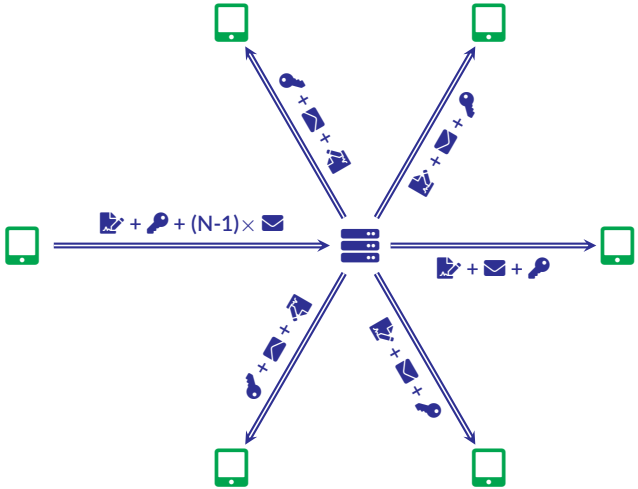
A previously unreported FBI document obtained by *Rolling Stone* reveals that "private" messaging apps WhatsApp and iMessage are deeply vulnerable to law-enforcement searches

BY ANDY KROLL

NOVEMBER 29, 2021

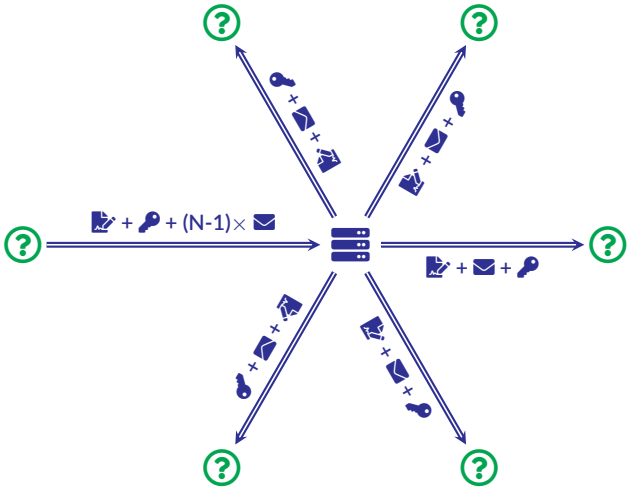
	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp
Subscriber data	☠	☠			☠	☠	☠	☠
Message sender, receiver data	☠	☠					☠	
IP address						☠	☠	
Date/time information	☠	☠	☠		☠	☠		☠
User contacts	☠	☠			☠	☠	☠	☠

Initial protocol
(🔑 = encryption key, ✉ = ciphertext, ✍ = signature)



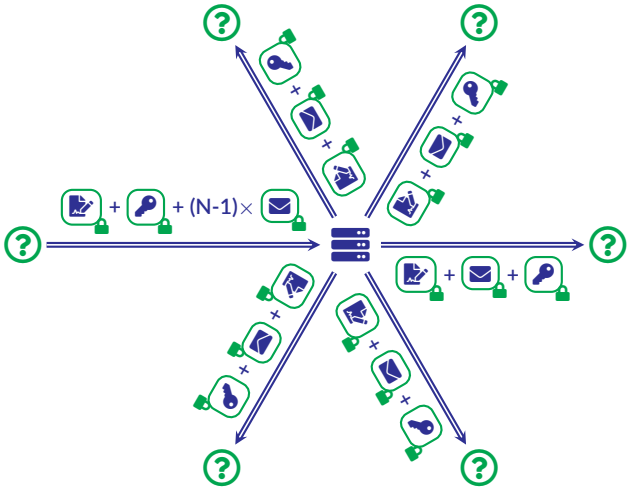
⚠ Messages are confidential, but not metadata (🖵)

Use client-anonymous authenticated channels



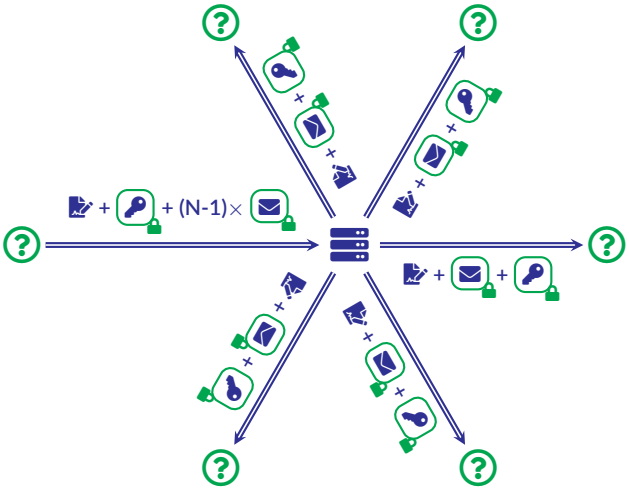
The packages , , leak the identities

OK, then let's also encrypt all the packages with



Now anyone can upload garbage messages to the group!

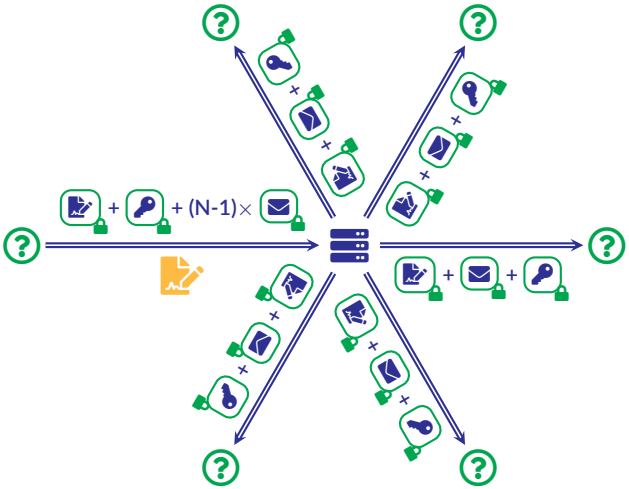
Let's encrypt all packages *except the signature*



But each signature is linked to its sender

Solution: derive a signature keypair (✎, 🔍) from 🔒‡

- The verification key 🔍 is public, but only users 👤 know the signing key ✎
- Group members can authenticate themselves anonymously



‡Keitaro Hashimoto, Shuichi Katsumata and Thomas Prest: *How to Hide MetaData in MLS-Like Secure Group Messaging: Simple, Modular, and Post-Quantum.* CCS 2022.

Conclusion

We show how to make secure messaging:

- Post-quantum
- Scalable
- Metadata-hiding

More information in our whitepaper

- https://pqshield.com/whitepapers/
- Also references the extensive body of work we build upon

Questions?