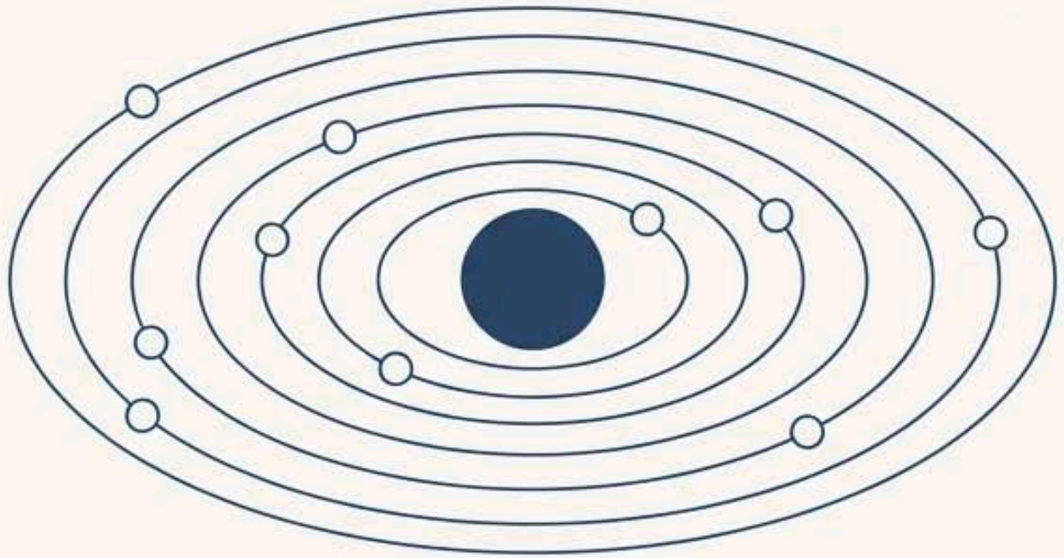
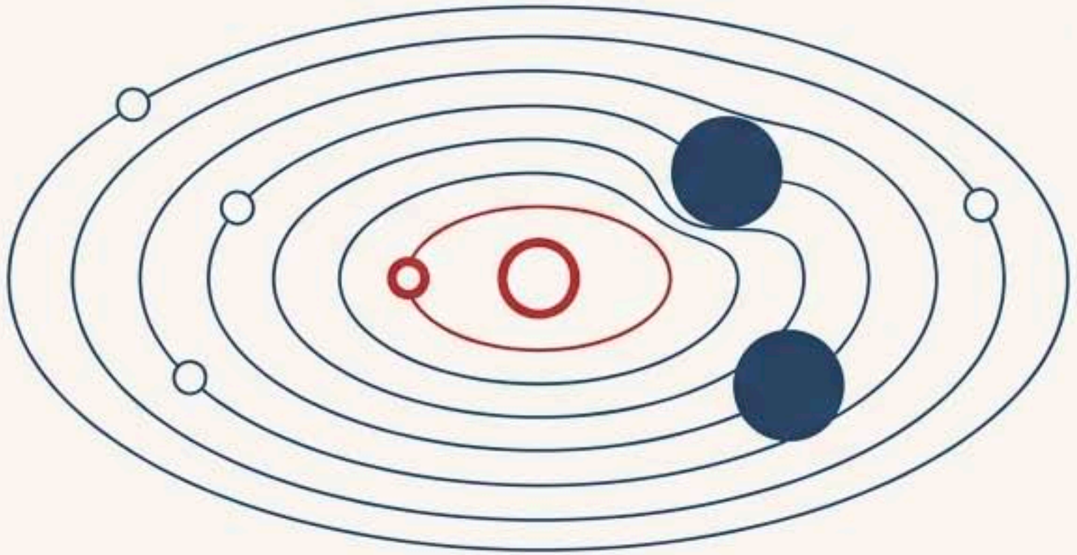
Human Proxies

A Copernican Turn for End-to-End Encryption

Establishing a new direction for private communication with the introduction of the "Inner Envelope' in the Echo Protocol.





Uni Nurf | ISBN: 978-3-7597-0504-4

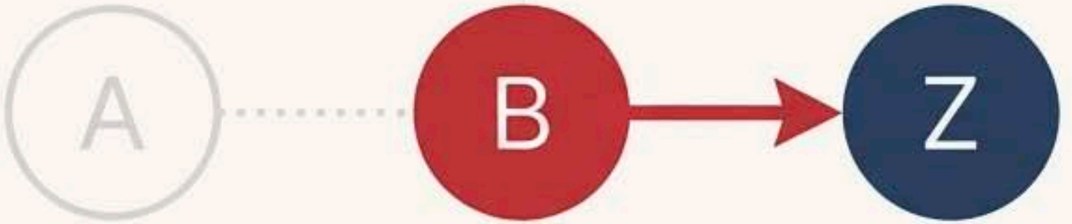
End-to-end encryption must be rethought.

The foundational model of **End-A-to-End-Z** encryption is built on a clear, identifiable sender.
But what if the message actually *originates* from **End-B**?

We introduce Human Proxies:
A new cryptographic primitive implemented in the Spot-On encryption suite that allows a friend from a messenger list to send a message on behalf of the original author.

The Foundational Model

The Human Proxy Model



The Foundation: A Network Built on the Echo Protocol

1. Network Flooding

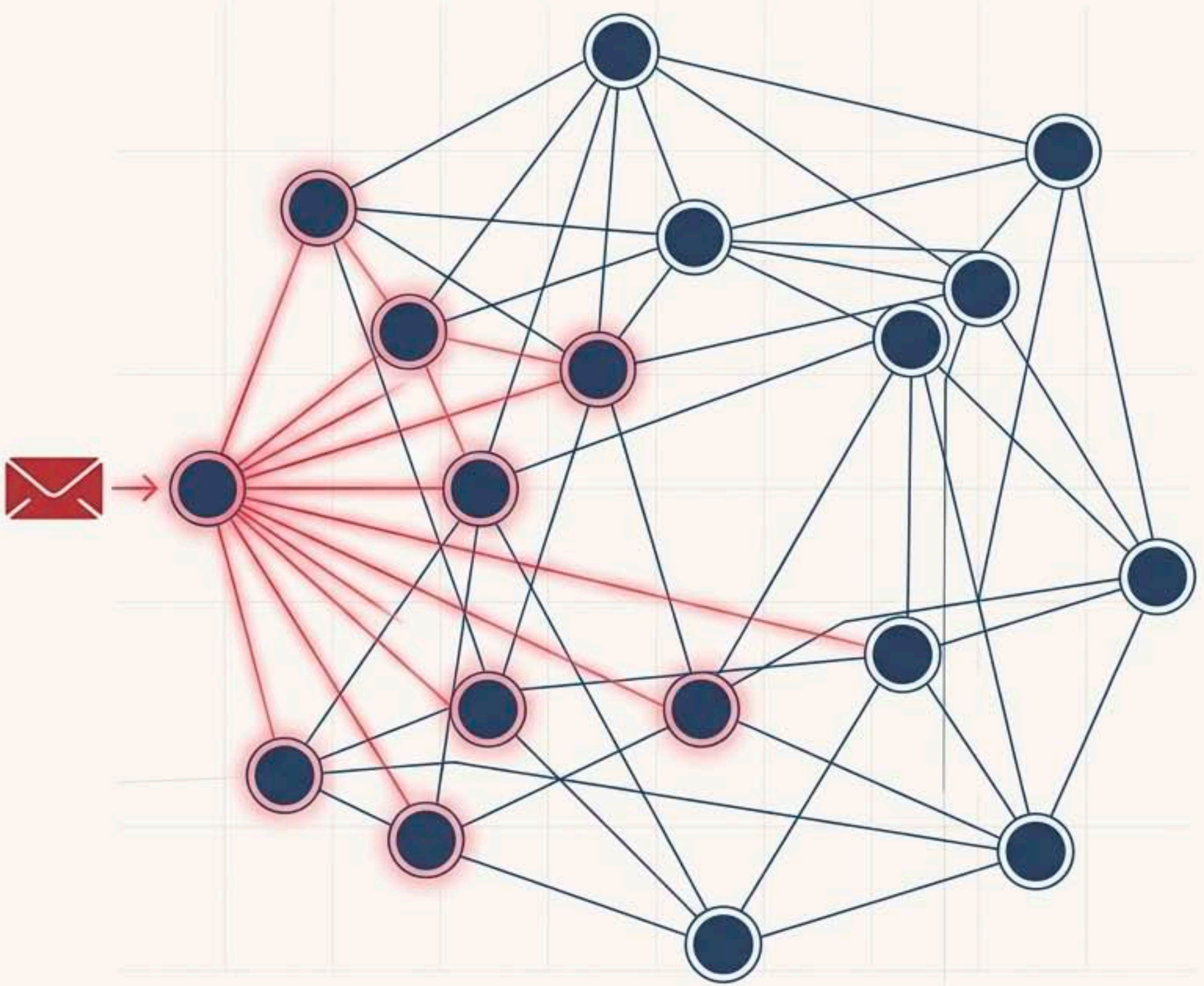
An encrypted packet is forwarded by a user to *all* connected nodes. Like an echo in a forest, the message resounds to everyone.

2. Localized Decryption

Each node attempts to decrypt every packet it receives using all its local keys. Success is private and unattended.

3. No Defined Addresses

The protocol is "Beyond Cryptographic Routing." Packets have no destination or sender address; they are simply opened locally if the right key exists. This inherently complicates metadata analysis.



The Mechanism: The ‘Inner Envelope’

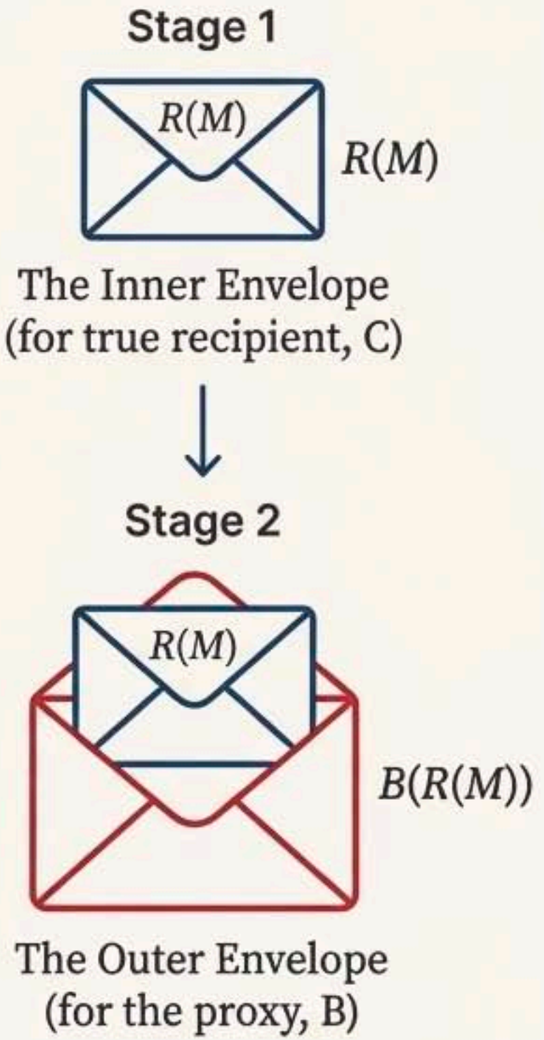
A Human Proxy works by nesting one encrypted message inside another.

The Inner Envelope (for the true recipient): Sender A creates the core encrypted message `$R(M)$` intended for Recipient C. This contains the actual message `$M$`.

The Outer Envelope (for the proxy): A wraps the Inner Envelope inside another **message,** $B(R(M))$, addressed to the chosen Human Proxy, B.

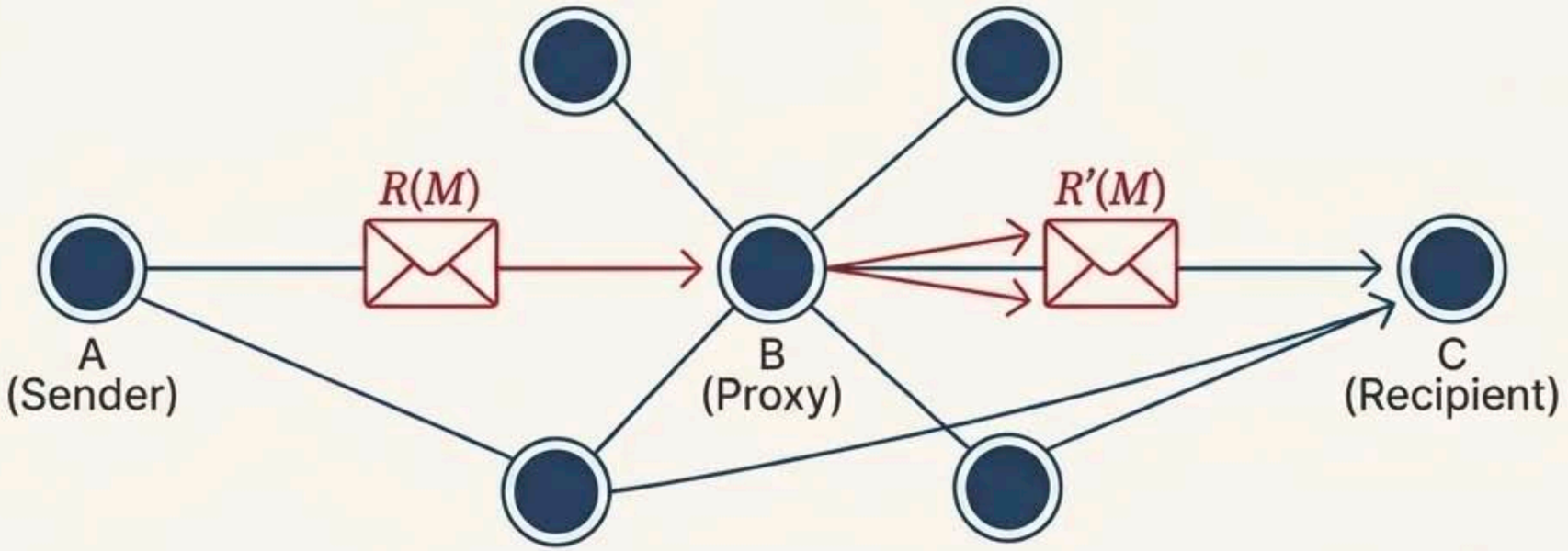
How the Proxy Handles It:

1. Proxy B receives and decrypts the *Outer Envelope* $B(R(M))$.
2. B extracts the *Inner Envelope* $R(M)$ and detects via a special keyed digest that it is a proxy task.
3. B cannot read $R(M)$. It does not know the final recipient.
4. B simply re-broadcasts a trimmed version, $R'(M)$, into the Echo network as if it were the original sender.



Analogy: It’s like placing a sealed letter inside another envelope. Your friend (the proxy) opens the outer one, sees the sealed letter inside isn’t for them, and drops it back into the mail system.

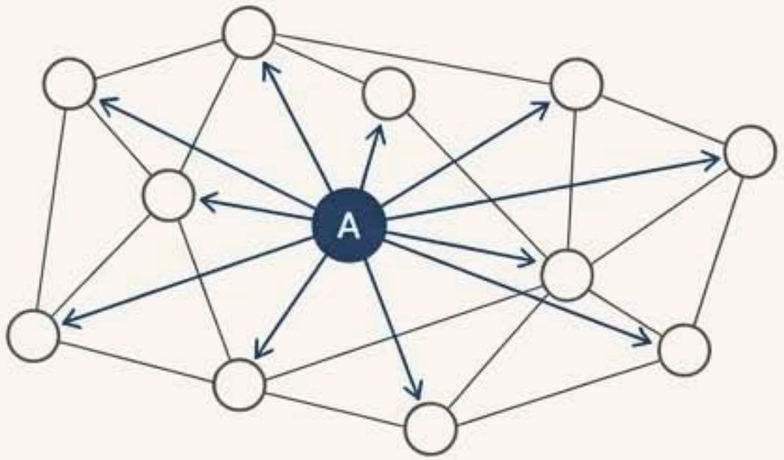
Visualizing the Human Proxy Message Flow



- `$R(M)$ is the message created by `A`.
- `$R'(M)$ is the message broadcast by `B`.
- `$R(M)$ and $R'(M)$ contain the identical encrypted message `M`.
- **Crucially, they have different, verifiable senders.** An observer sees a message originating from `$B$` and intended for `$C$`. The link between `$A$` and the message's content is broken.

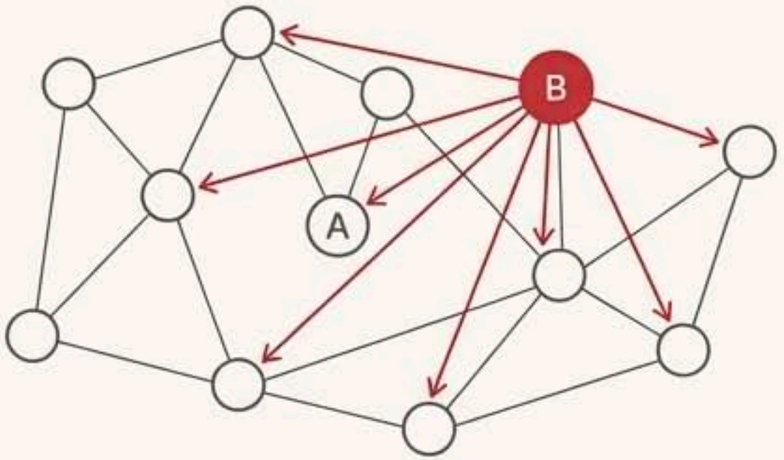
This is the Copernican Turn: The Sender Is No Longer the Center of the Communication Universe.

The Old Universe



In traditional E2EE, the sender ('A') is a fixed, analyzable starting point. Metadata analysis, timing analysis, and social graph analysis all radiate from this fixed center.

The New Universe



With Human Proxies, the starting point is fluid. The sender can be any node designated as a proxy. The original author ('A') becomes a "ghost" in the machine—the true cause of the message, but not its observable origin.

"The end-point of a graph in the network is no longer the end-point we are talking about. The sender can be any end- or starting-point in the network with Human Proxies."

The Result: A New Level of Plausible Deniability

Definition

Plausible Deniability is the ability to deny involvement in an action, because the evidence is insufficient to prove responsibility.

How Human Proxies Achieve This

The true sender can plausibly deny having sent the message, as all network evidence points to the proxy as the originator. The proxy, in turn, can deny knowledge of the message's content or recipient, as they only forwarded an encrypted cipher-text.

Beyond File Encryption

Systems like VeraCrypt's 'hidden volumes' allow one to deny the *existence* of stored data. Human Proxies allow one to deny the *act of communication itself*.

Analogies

Political: A high-ranking official using informal command chains to shield themselves from the fallout of a covert operation.

Philanthropic: A 'Karma Yogi' or anonymous benefactor who acts through a delegate to ensure their good deeds remain unattached to their ego.

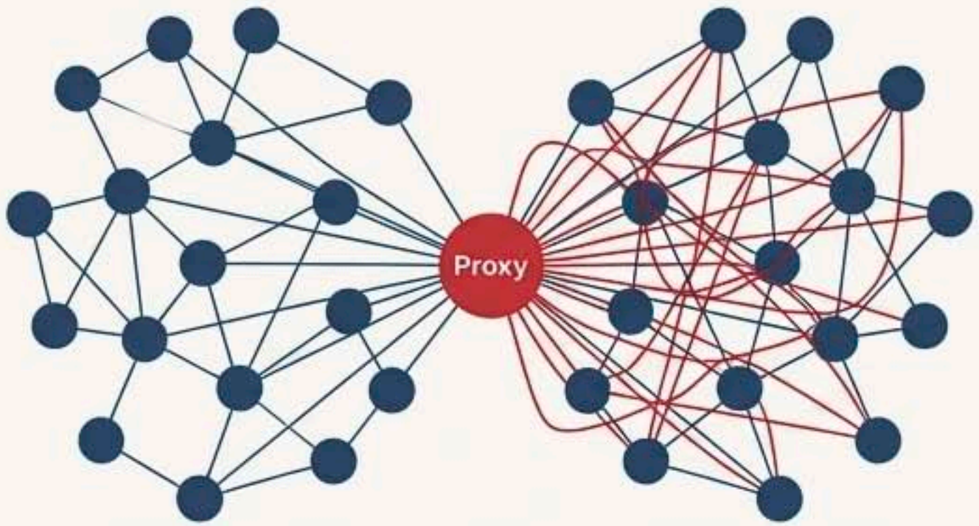
A Modern Remedy for the Global Indexing of Mankind

The Threat Landscape

Modern surveillance is not just about content; it's about indexing relationships and metadata on a global scale.

- **Data Retention:** Mandates storing "who-talked-to-whom" metadata (IP addresses, times).
- **Chat Control (Client-Side Scanning):** Bypasses E2EE by scanning content on the device *before* encryption.
- **The 'Permanent Record':** The assumption that all digital communication is recorded and archived forever.

The Human Proxy Defense



- **Against Data Retention:** The Echo Protocol's flooding and the proxy's role as the sender fundamentally distorts the 'who-talked-to-whom' graph.
- **Against Chat Control:** The proxy sends a message that was encrypted on a different machine. The proxy's device has no plaintext to scan.

From ‘Trepidation of Memory’ to ‘Trepidation of Relationship’

Background Concept: Trepidation of Memory

The difficulty in linking a public key to a private key if they were generated long ago and have been dormant. The memory of their connection “fades” over time.

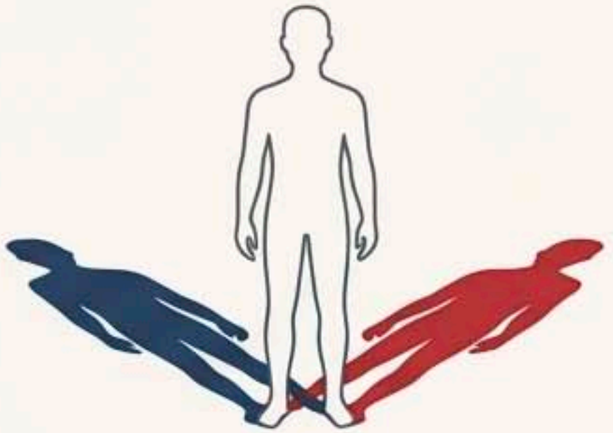
The New Paradigm: Trepidation of Relationship

1. A key exchange between two users (**A** and a future proxy, **B**) happens at some point in the distant past.
2. They do not communicate for a long time. Their connection does not appear in any recent metadata analysis. The relationship is forgotten by observers.
3. **B** is a **'sleeper'** in **A**'s friend list.
4. When **A** activates **B** as a Human Proxy, the action is completely unpredictable to a network analyst. The relationship itself was deniable.

The Proxy as Alter Ego and Sleeper Agent

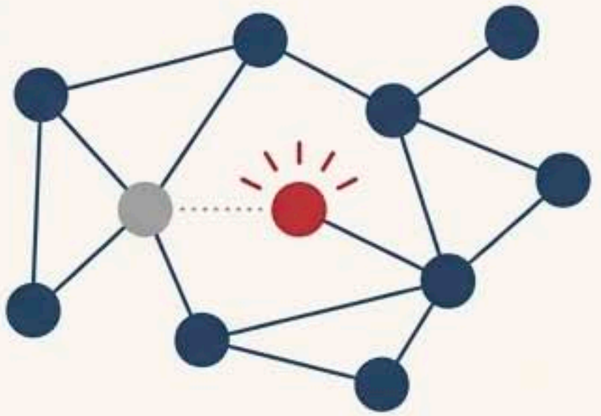
The Alter Ego

A Human Proxy is a true second self ("*alter idem*," Cicero). Unlike a simple avatar or nickname, it is a separate, functional identity on the network, with its own verifiable actions that can be plausibly denied by your primary identity.



The Sleeper Agent

A friend on your list can be unknown to network observers, becoming a sleeper cell that is only activated when used as a proxy. This is reminiscent of spycraft, where dormant assets are activated for critical operations, their prior connections to the handler being waterproof deniable.



"A mother whose child grows up with her current husband may never reveal that she knew the neighbor who is the child's real biological father."

Future Perspective: Proxifying the Proxied

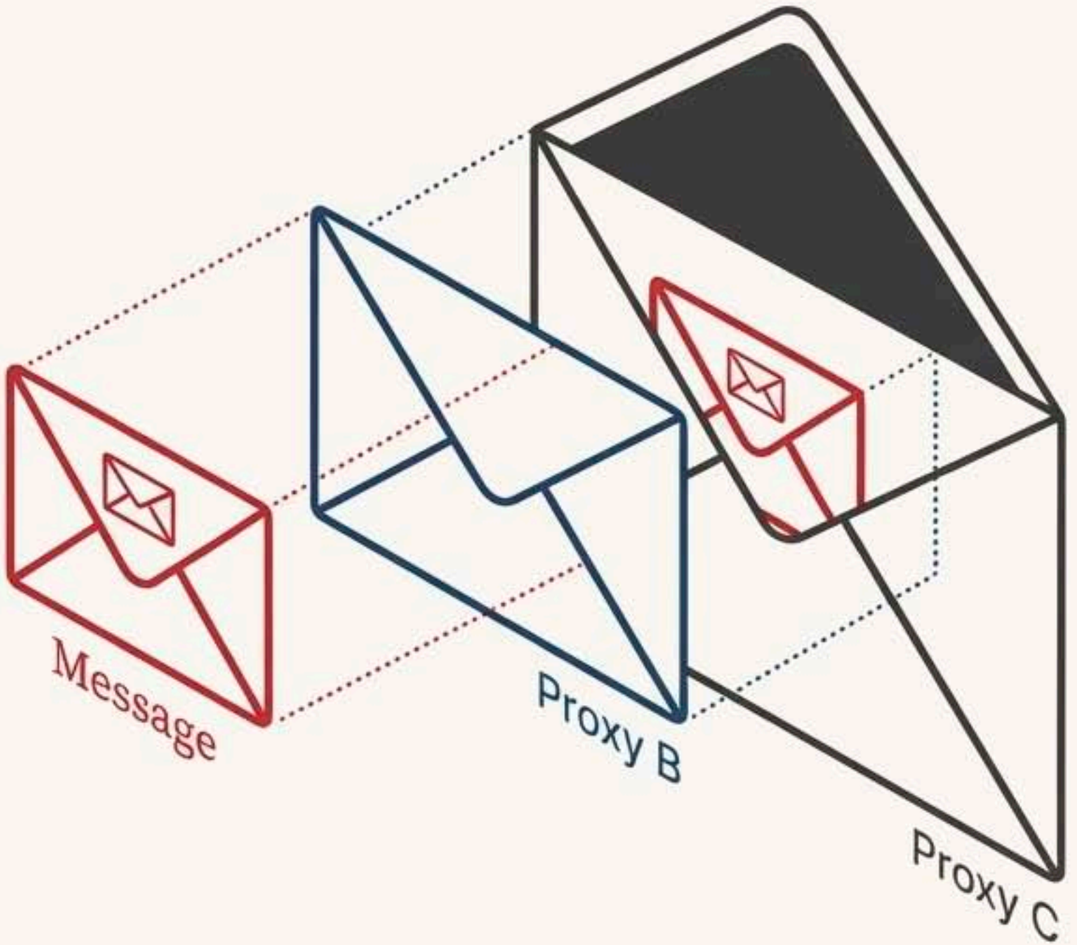
The Concept

A proxy can have its own proxy.

- Sender `A` uses `B` as a proxy.
- Node `B` receives the Inner Envelope and, instead of broadcasting it directly, wraps it in a *new* Outer Envelope addressed to *its own** proxy, `C`.
- The message finally originates from `C`.

Analogy: The Matryoshka Doll

There may exist Inner Inner Inner... Envelopes, all with the same message, but sent from different start-points. Each layer of proxy adds another shell of obfuscation.

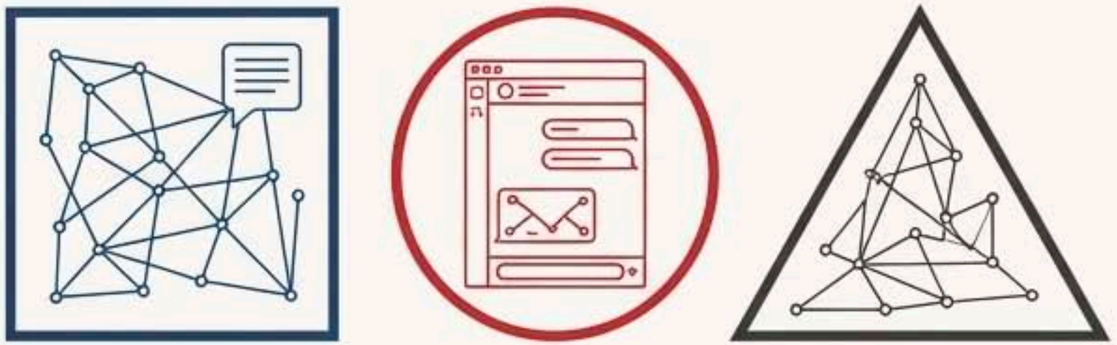


Status

This is noted in the source as a future research and development perspective, requiring `P × Q` messages (Participants x Proxies) versus the current `P` messages.

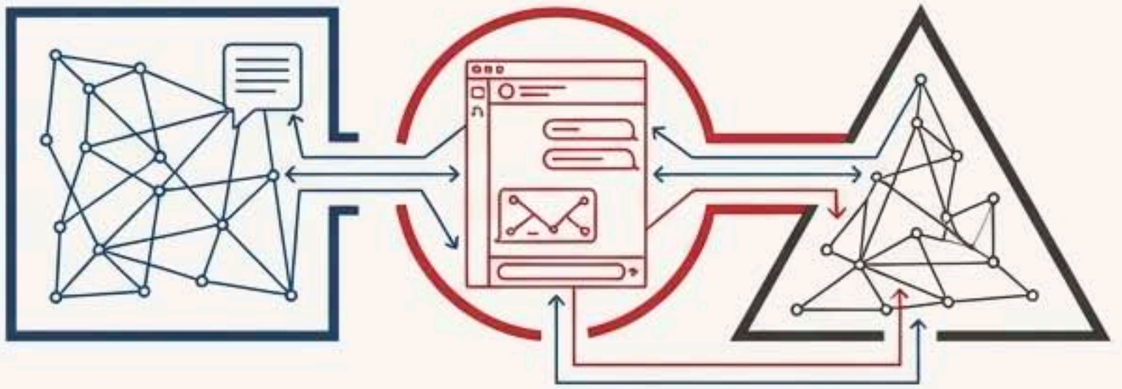
The Guiding Vision: True Interoperability of Endpoints

The Problem: A City of Babel



Most secure messengers (Signal, Telegram, etc.) are open only to themselves. They are self-contained systems with zero interoperability.

The Spot-On Vision: Zero-Specifics

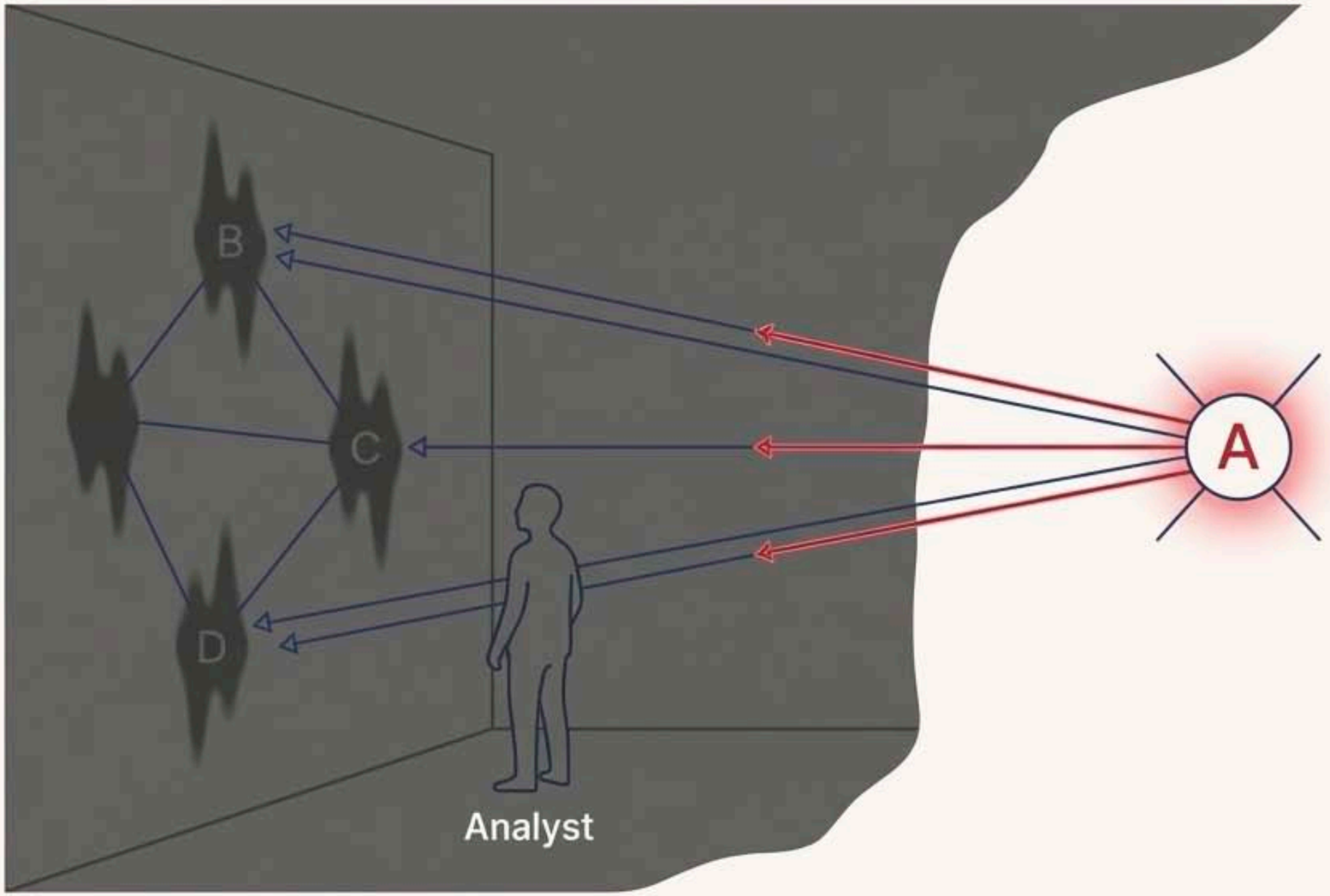


Communication should be possible even if the recipient doesn't have the same application installed. The endpoint is what matters, not the specific software.

Example: "Share it from multiple devices with and without Spot-On installed at one end. [...] Send a file from an Echo application just to a SSH end of a machine."

Conclusion: Human Proxies are one powerful expression of a deeper design principle: making endpoints fluid, interchangeable, and interoperable.

When Machines Steer Machines, What is Real?



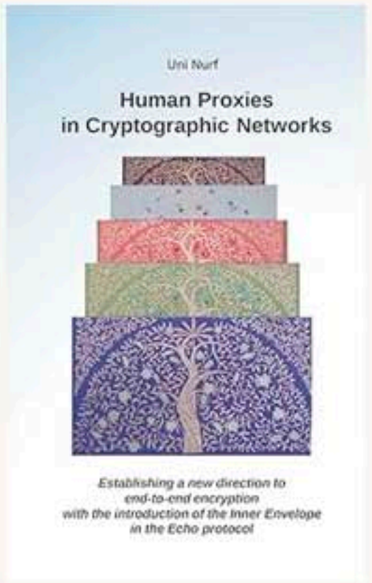
The Analyst's Dilemma

With the existence of Human Proxies, an external observer must assume that *any* node could be a proxy. Every perceived sender could be a "shadow on the cave wall," with the true originator remaining unseen.

"Nobody - not even an external network analyst that has only a part of the network in view - can assume that a certain mailbox in the network [...] has been thrown in the message-letter - there could be other mailboxes."

The New Assumption

Every node must be assessed as a potential originator, and every originator as a potential proxy. The ground truth of the network becomes fundamentally ambiguous.



“Everyone’s a Proxy, baby — that’s the truth!”

— Hot Chocolate, adapted.