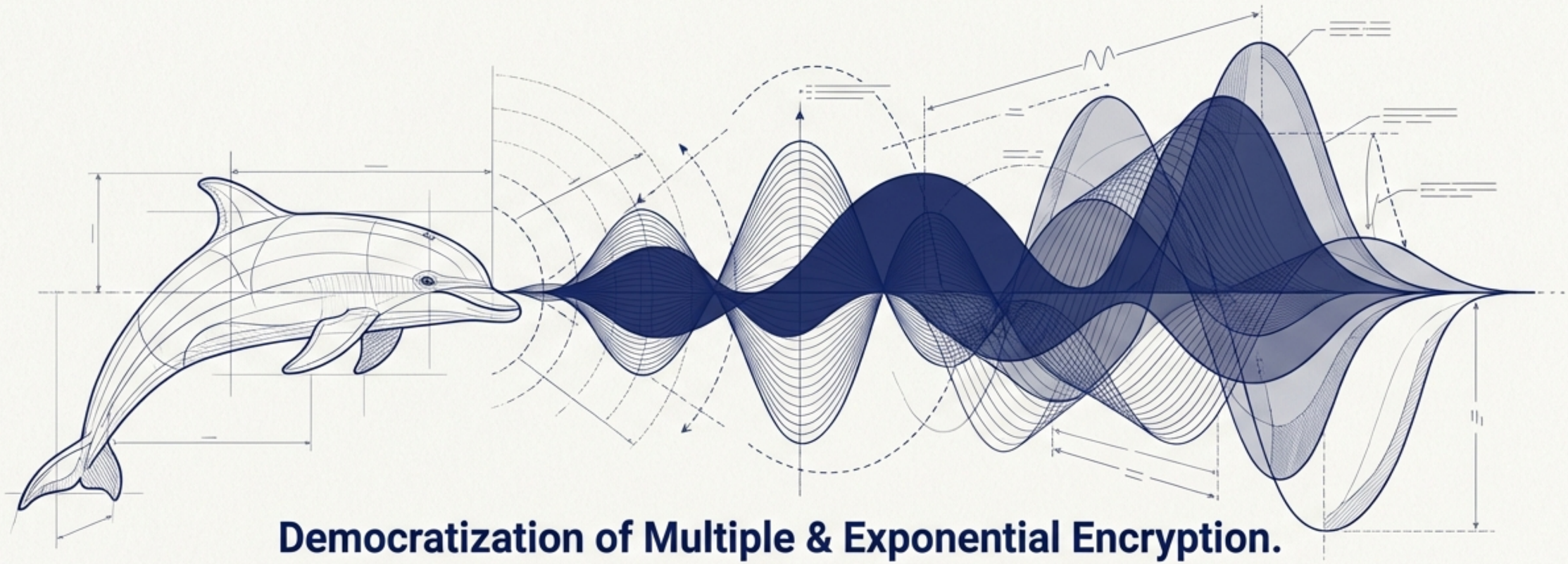
Communicating Like Dolphins with the Spot-On Encryption Suite



Democratization of Multiple & Exponential Encryption.

An open-source suite for secure chat, P2P e-mail, file transfer, and decentralized web search, built on the revolutionary Echo Protocol.

Freedom is the respect to the other’s cipher text!

A Comprehensive Suite for Your Digital Sovereignty

Spot-On integrates the three basic functions of an internet user into a single, comprehensively encrypted environment.

Searching

A decentralized, P2P web search engine with an encrypted, shareable URL database. No query hits are generated on other nodes.

Speaking (by text)

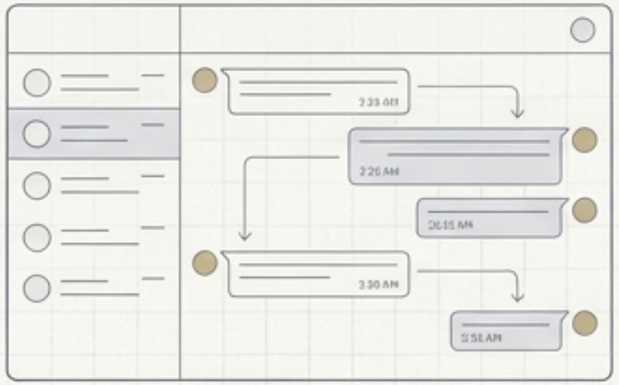
Secure 1:1 chat, group chat (e'IRC), and a fully functional P2P e-mail client.

Sending

Encrypted, peer-to-peer file transfer and sharing using the StarBeam protocol.

Secure & Versatile Communication: Chat and E-mail Reimagined

Private & Group Chat



- 1:1 private messaging with advanced security features.
- Decentralized, encrypted group chat in IRC style (e'IRC / 'Buzz').

Fully Functional E-mail Client

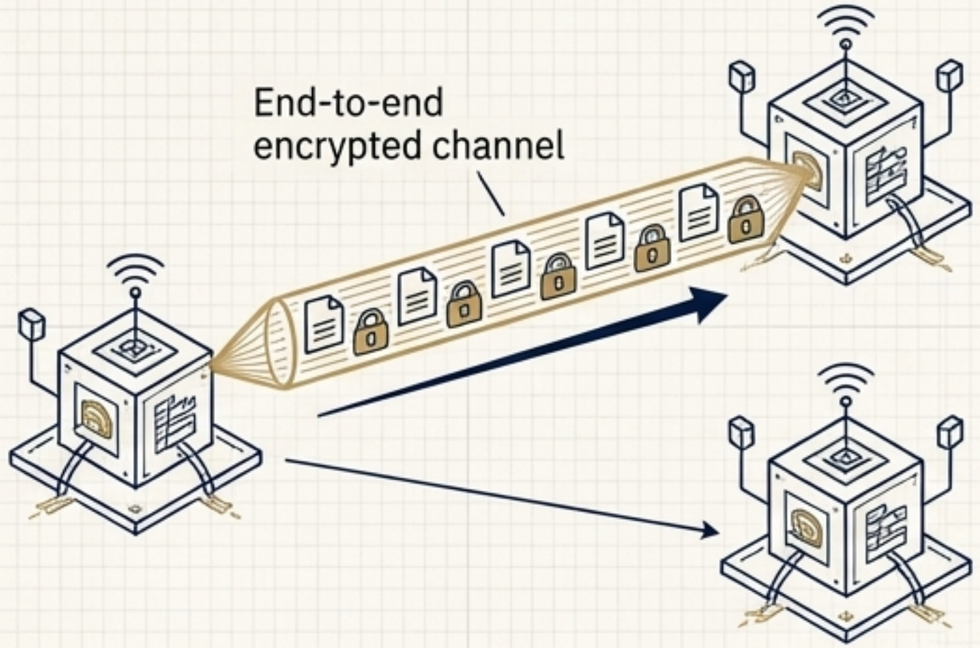
- Supports standard **IMAP & POP3.**
- **P2P E-Mail**: Store encrypted e-mails on a distributed network of friends using 'Care-Of (C/O)' or 'Virtual E-Mail Institution (VEMI)' methods.

POPTASTIC Protocol

An innovative protocol enabling encrypted chat and e-mail utilizing any standard POP3/IMAP server, effectively converting them into secure communication hubs.

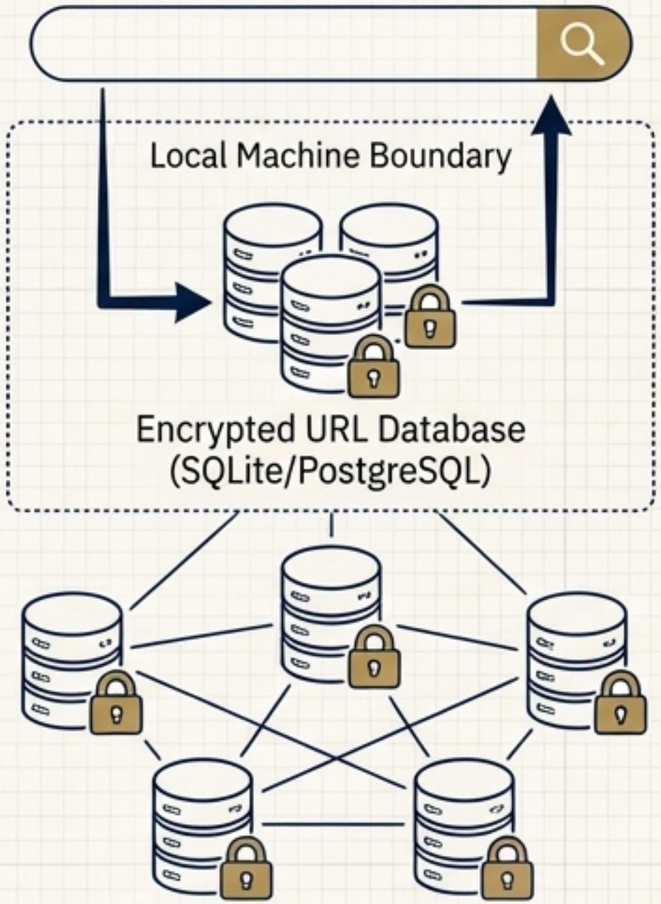
Decentralized Data: Encrypted File Sharing & Private Web Search

StarBeam File Sharing



- Transfers files of any size through end-to-end encrypted channels defined by cryptographic Magnet-URIs.
- Supports “One-Time Magnets” (OTM) that self-destruct after use.
- Optional NOVA password for an additional layer of symmetric file encryption.

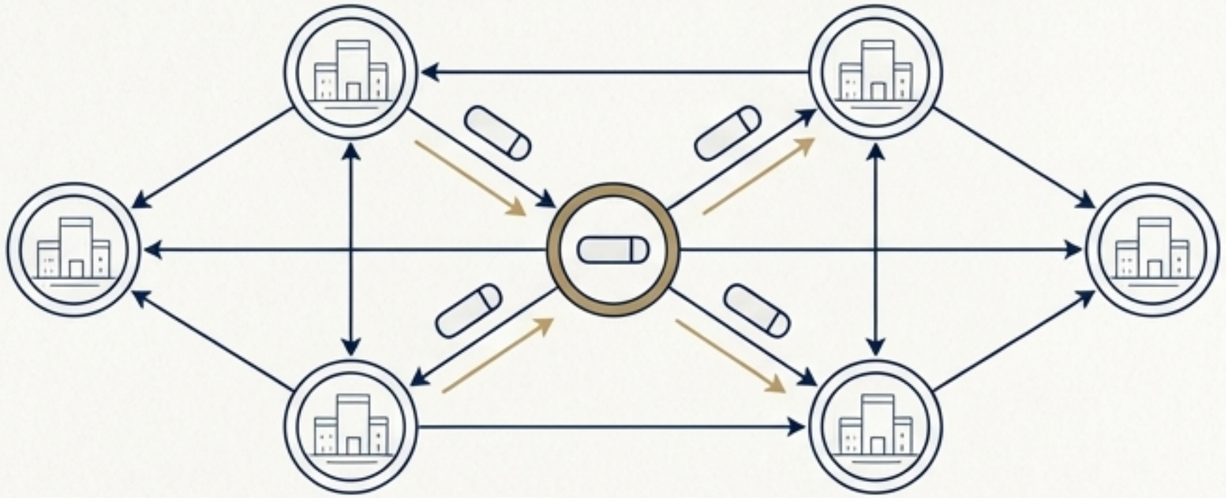
Open Source P2P Web Search



- Build and share an encrypted URL database (SQLite or PostgreSQL) with friends.
- Local search processing means no query hits are sent over the network, ensuring total search privacy.
- Import URLs via the Pandamonium web crawler or a built-in RSS reader.

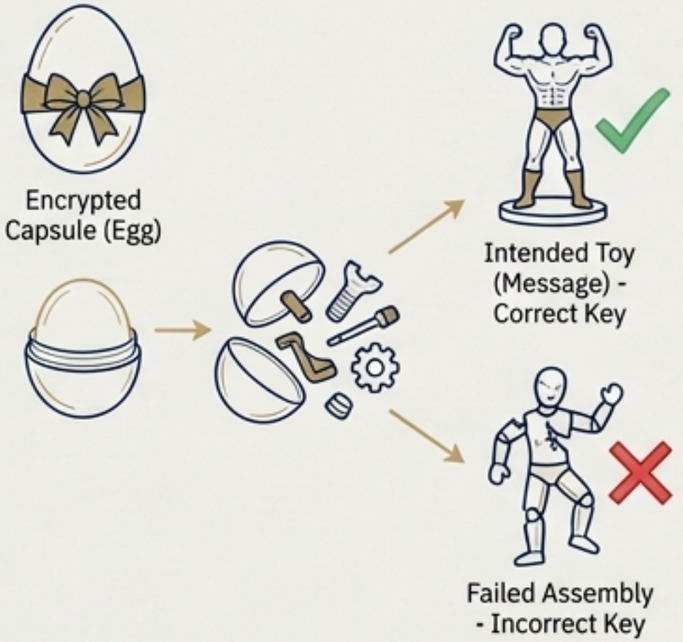
The Engine Below: An Introduction to the Echo Protocol

The Echo Protocol is a simple yet powerful network protocol that fundamentally changes how data travels.



- **Core Principle:** Each node sends every received message to every connected neighbor. There is no traditional routing information (sender/receiver IP) in the packets.
- **“Echo Match”:** A message is only decrypted and displayed if the hash of the decrypted content matches a hash of the original plaintext included in the packet. This is how a recipient identifies a message meant for them, trying every known key.
- **Metadata Resistance:** This “flooding” approach makes it extremely difficult to perform traffic analysis and determine who is communicating with whom.

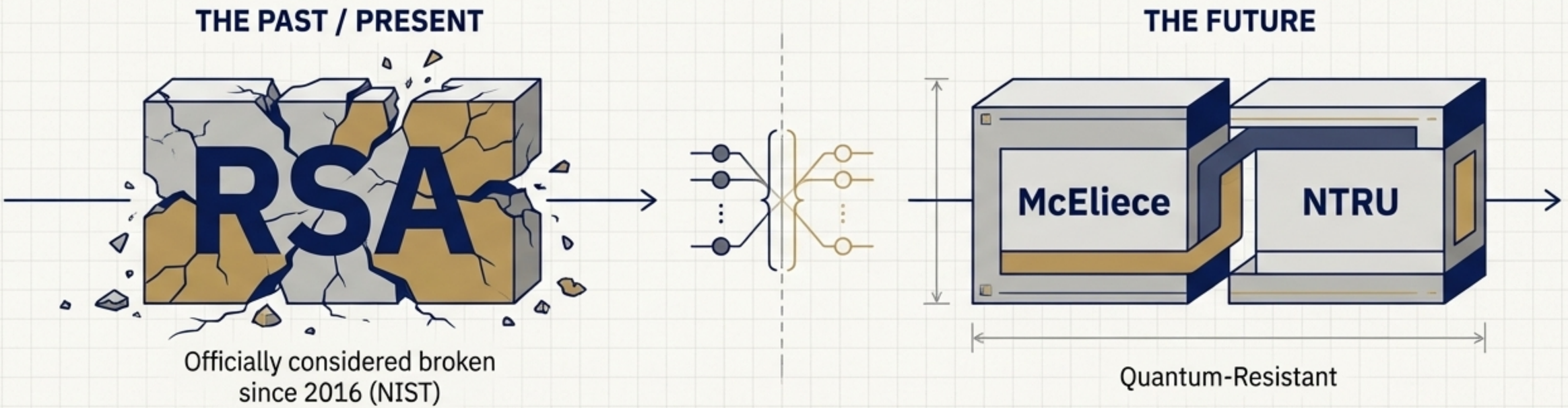
Analogy: The Surprise Egg



A node receives an encrypted capsule (the egg). It tries to ‘assemble’ the contents with every key it knows. Only the correct key will produce the intend’ (the message). All other attempts fail.

Future-Proofed Cryptography: Beyond RSA

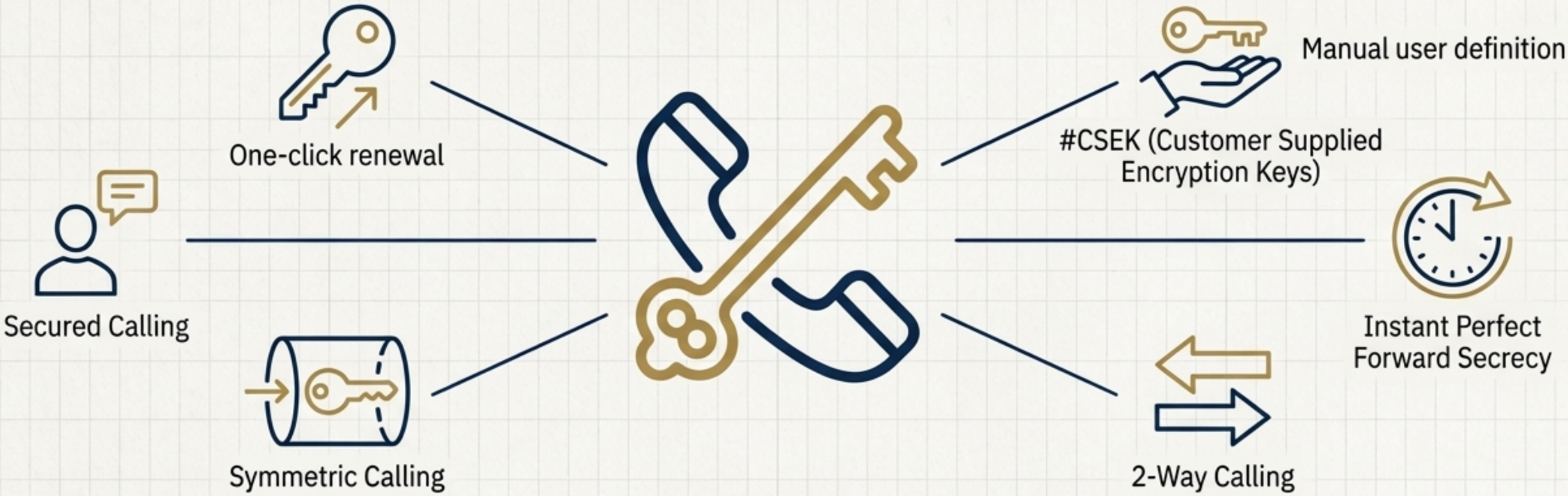
Spot-On was one of the first communication suites to implement post-quantum cryptographic algorithms as alternatives to RSA, which is vulnerable to quantum attacks using Shor's algorithm.



- **McEliece:** An asymmetric algorithm from 1978 based on coding theory. No known efficient method exists to break it, even with quantum computers.
- **NTRU:** An asymmetric technique from 1996 based on lattice problems, also considered resistant to quantum attacks.
- **User Sovereignty:** Users can choose their 'Cryptographic DNA,' selecting their preferred algorithm (RSA, Elgamal, NTRU, McEliece), key size, hash type, and more.

Inventing a New Paradigm: Cryptographic Calling

Cryptographic Calling, an invention of the Spot-On project, is the immediate transfer of new end-to-end encryption credentials through an existing secured channel. It makes managing E2E encryption as simple as making a phone call.



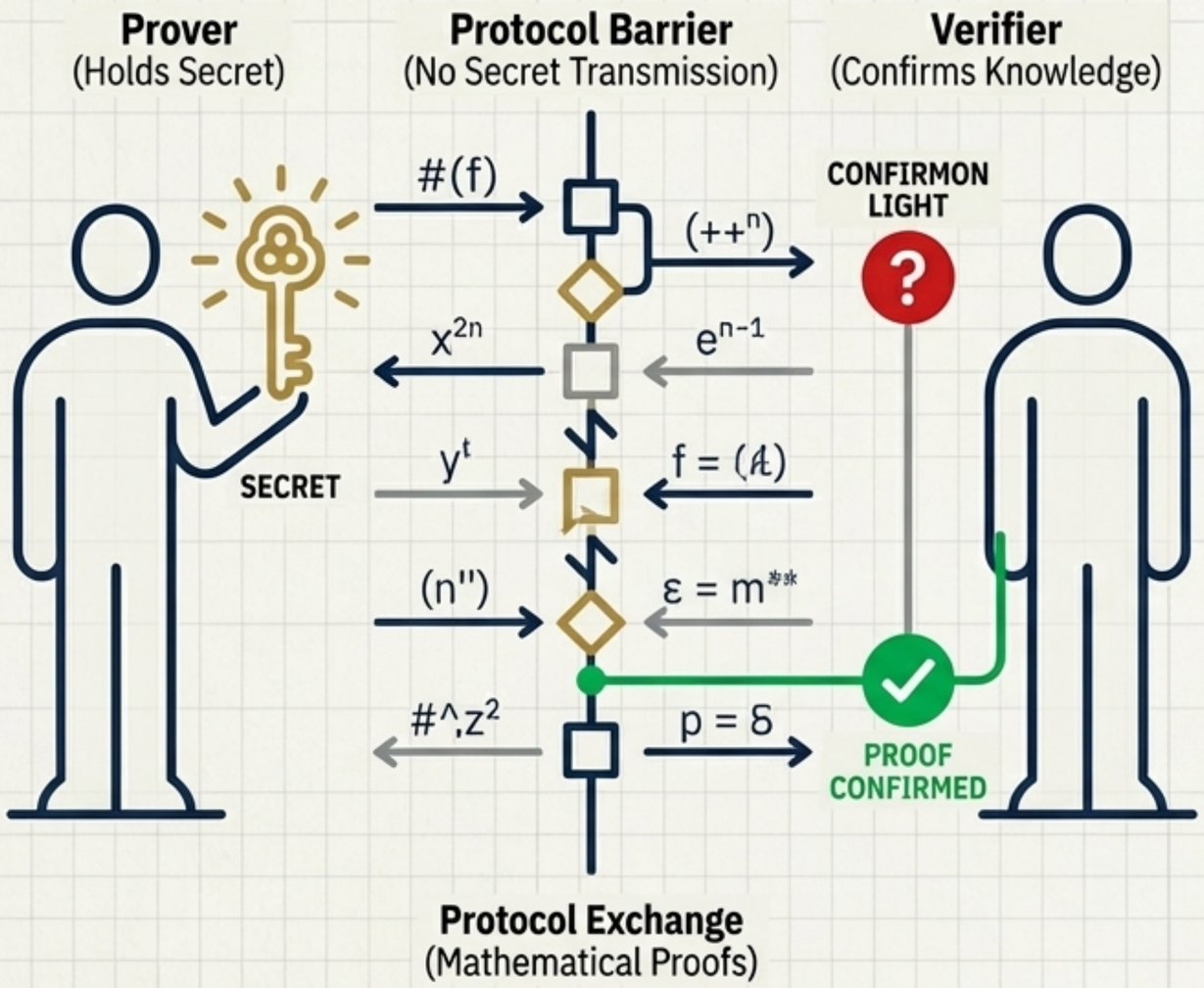
- **Core Idea**: With one click, a user can instantly renew the end-to-end symmetric passphrase (the ‘Gemini’) for messaging.
- **User Control**: Supports both automated key generation and manual user definition (**#CSEK**: Customer Supplied Encryption Keys).
- **Evolving Forward Secrecy**: This extends ‘Perfect Forward Secrecy’ (PFS) by making it immediate and user-controllable, leading to **‘Instant Perfect Forward Secrecy’ (IPFS).**

A Spectrum of Security: The Modes of Cryptographic Calling

Criteria	Asymmetric Calling	Forward Secrecy Calling	Symmetric Calling	SMP Calling	Secret Streams	Fiasco Forwarding	2-Way Calling
TLS/SSL-Connection	✓	YES	YES	YES	✓	NO	✓
Permanent asymmetric Chat/E-Mail Key	✓	✓	NO	NO	NO	NO	✓
Symmetric AES as Gemini	YES	✓	YES	YES	✓	NO	NO
Half AES + Half AES	NO	NO	YES	YES	✓	NO	NO
Secret SMP Password	NO	NO	NO	✓	✓	NO	NO
Ephemeral/temp. Chat/E-Mail PKI-Key	NO	NO	NO	YES	NO	NO	NO
Forward Secrecy as Pre-Condition	NO	NO	YES	YES	✓	NO	NO
Instant Perfect Forward Secrecy as result	✓	✓	✓	✓	✓	NO	✓
Several keys as a result	YES	YES	YES	YES	YES	NO	NO

Spot-On provides a granular toolkit of methods to establish and renew end-to-end encryption, from simple key transfers to advanced multi-key and zero-knowledge techniques.

Verifying Identity Without Revealing Secrets: The Socialist Millionaire Protocol



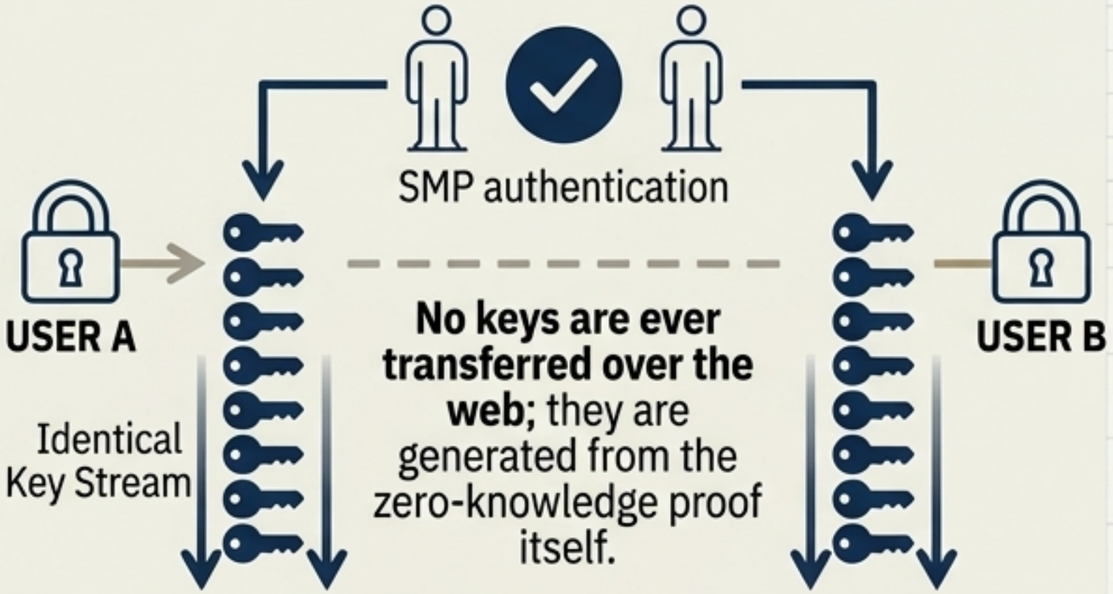
Beyond encryption, Spot-On provides robust authentication. SMP allows two parties to verify they share a secret (like a password or the answer to a question) without ever transmitting the secret itself.

- **How it works:** Both users enter the same secret phrase. The protocol mathematically confirms the phrases match without sending the hash or the password over the connection.
- **Zero-Knowledge-Proof:** This is a method where one party (the prover) can prove to another (the verifier) that they know a value *x*, without conveying any information apart from the fact that they know *x*.
- **Use Case:** Authenticate your chat partner in real-time to ensure you are not talking to a compromised machine. A successful verification changes a '?' icon to a 'lock' symbol.

The Next Evolution: Zero-Knowledge Keys and Multi-Key Sessions

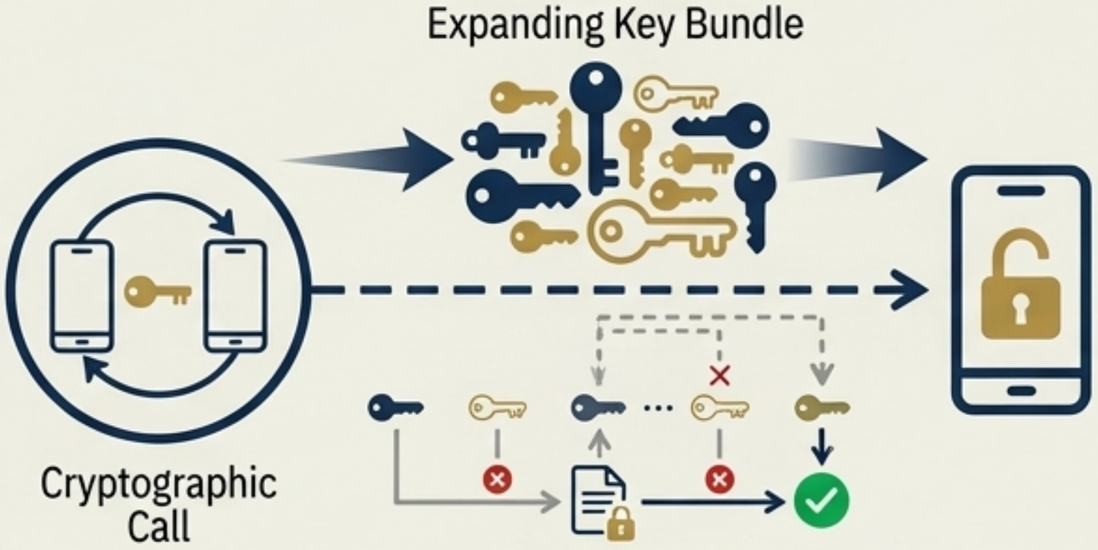
Spot-On combines its core primitives to create uniquely secure features that solve fundamental cryptographic challenges.

Secret Streams



A revolutionary method that uses a successful SMP authentication to derive a ***bunch*** of shared E2E passphrases on both ends. This solves the key sharing problem in a novel way.

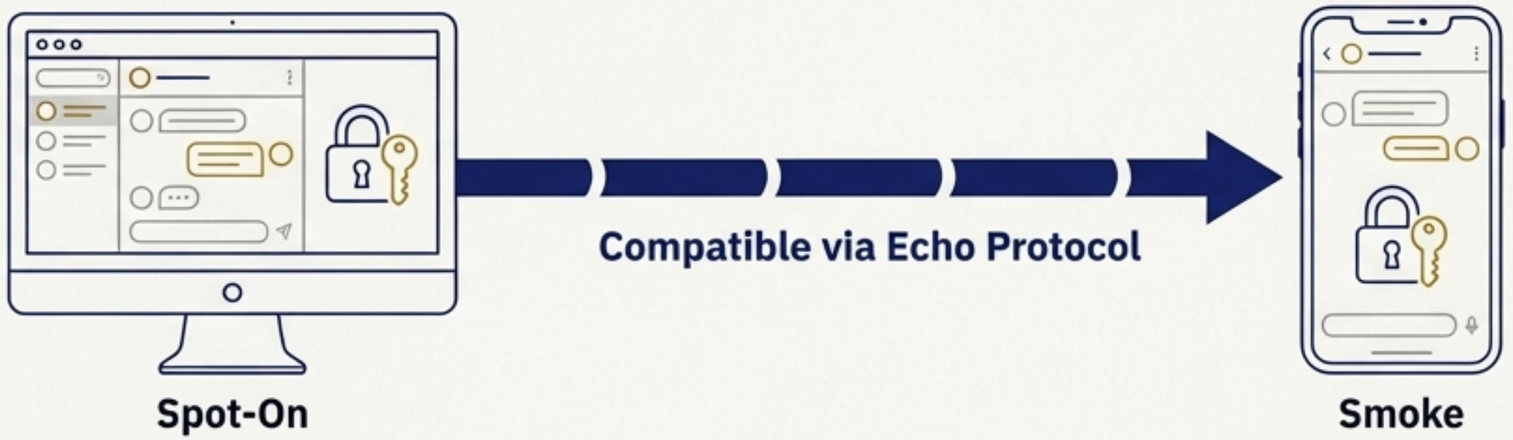
Fiasco Forwarding (in Smoke mobile client)



A development of Cryptographic Calling that sends a bundle of over a dozen potential keys in a single 'Call.' The recipient tries them in order, making analysis of any single message key extraordinarily difficult.

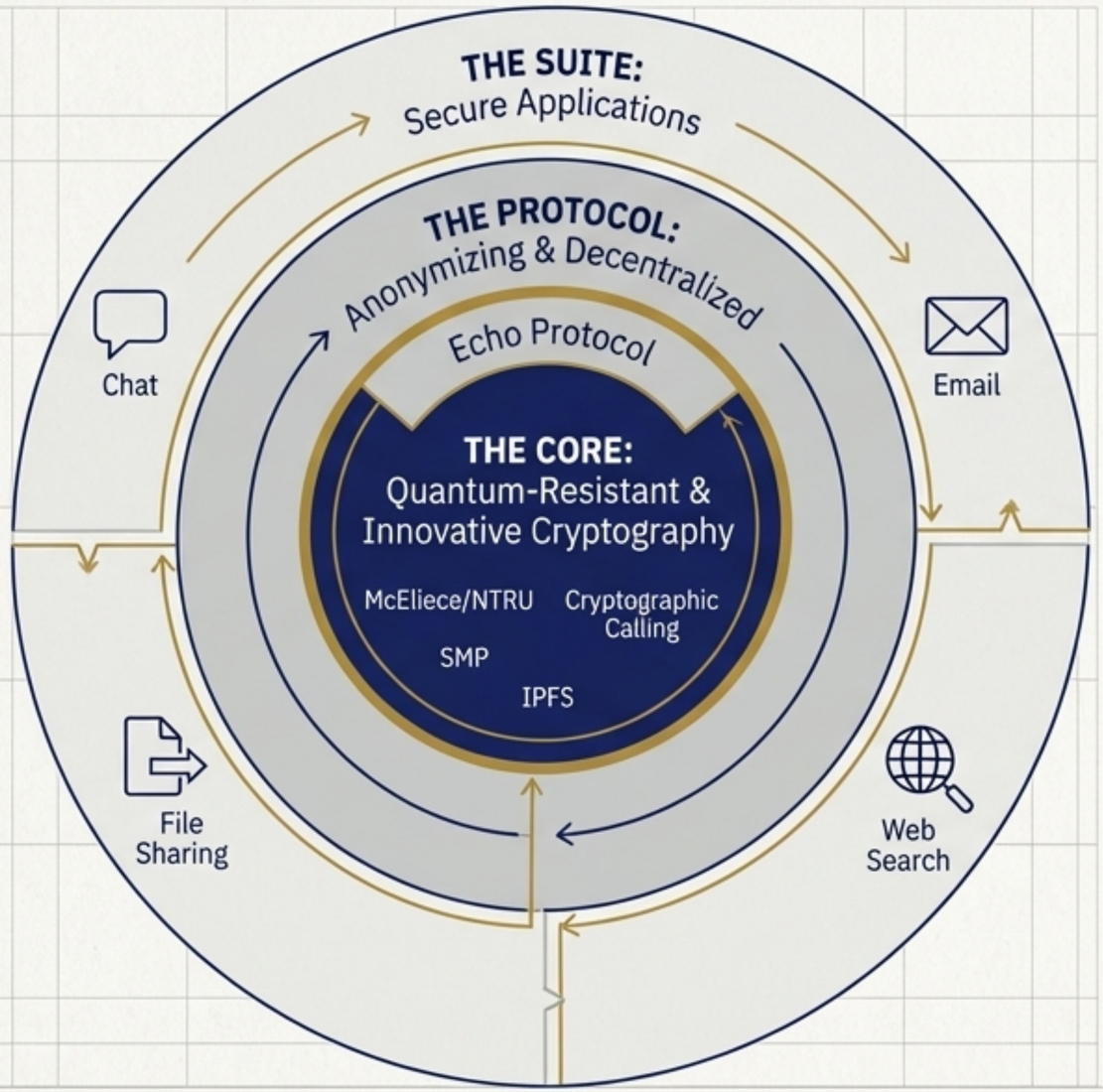
The Ecosystem Expands: Smoke Messenger for Mobile

The Spot-On ecosystem extends to mobile with Smoke, an Android-based crypto chat messenger built on the same core principles.



- **Compatibility:** The group chat (‘Buzz” in Spot-On, ‘Fire’ in Smoke) is fully compatible between the desktop and mobile clients.
- **No Phone Number Required:** Smoke uses a short string identifier (SIP hash), not a phone number, enhancing user privacy.
- **Post-Quantum on Mobile**: Smoke is recognized as the first mobile messenger worldwide to implement the quantum-resistant McEliece cryptosystem.
- **Own Your Server**: Can connect to a Spot-On server or use SmokeStack, a dedicated, easy-to-administer server app for Android.

A Multi-Layered Architecture for True Digital Security



Spot-On is architected in distinct, reinforcing layers:

1. A **versatile suite of applications** that provide comprehensive functionality.
2. Powered by the unique **Echo Protocol** that ensures privacy and resists metadata analysis.
3. Built on a **future-proof cryptographic core** with post-quantum algorithms and paradigm-shifting innovations.

Technical Specifications at a Glance

Platforms

Cross-platform (Windows, macOS, Linux, FreeBSD). Compiles on ARM, Alpha, PowerPC, Sparc64, x86_64. Portable application design.

Connection Protocols

TCP, UDP, SCTP, Bluetooth, DTLS. Full proxy support for running over networks like Tor.

Asymmetric Algorithms

RSA, Elgamal, NTRU, McEliece

Signature Algorithms

DSA, ECDSA, EdDSA, Elgamal, RSA

Symmetric Ciphers

AES, Camelia, Serpent, Threefish, Twofish

Hash Algorithms

SHA-512, Stribog, Whirlpool

License

Open Source (BSD License)

Server

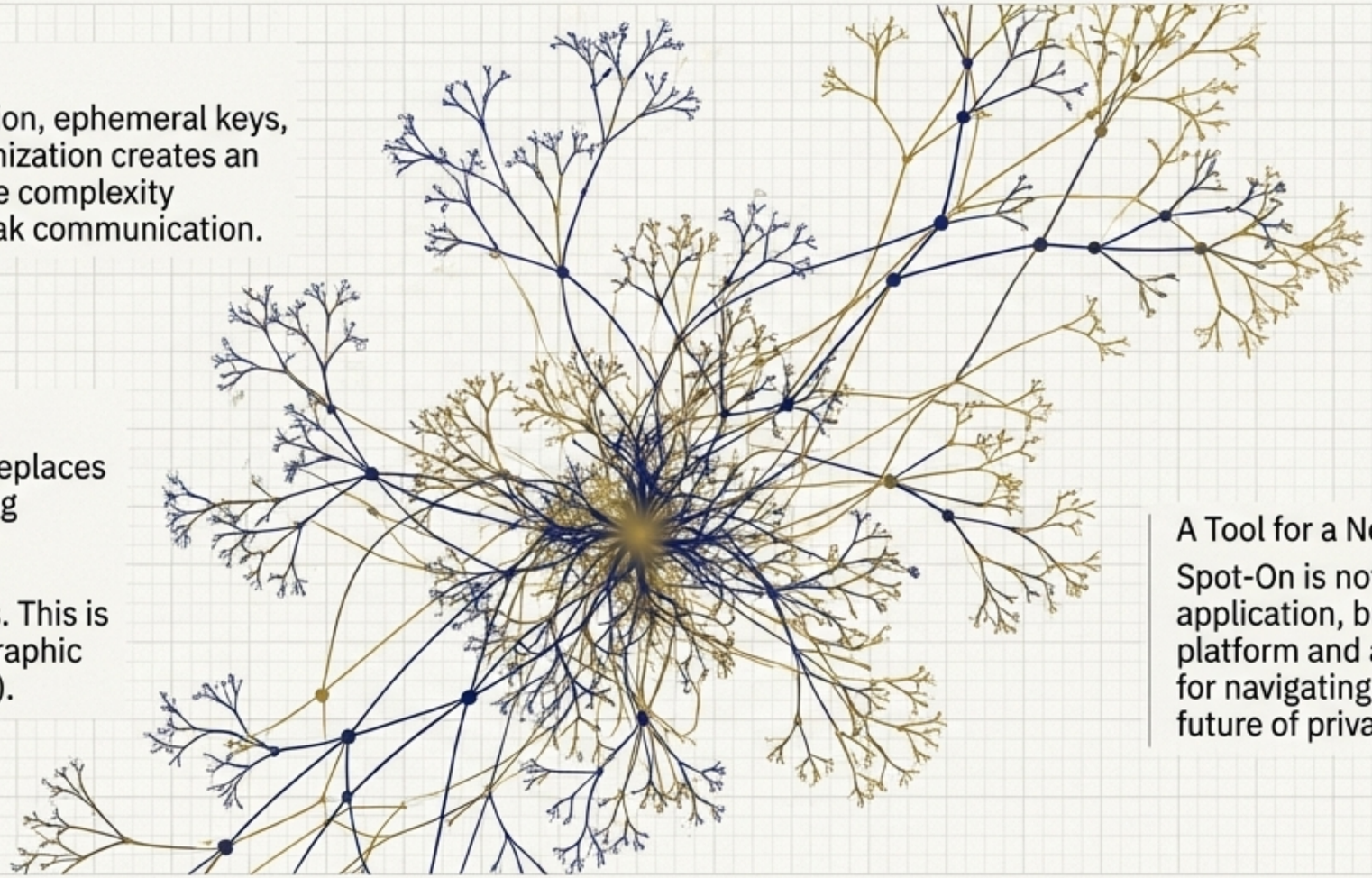
Integrated listener function for easy P2P/F2F server setup. Compatible with SmokeStack (Android). Serverless P2P connections also supported.

An Initial Welcome to the Era of Exponential Encryption

The combination of multi-encryption, metadata resistance, user-defined cryptographic diversity, and post-quantum algorithms marks a shift in what is possible. Spot-On's architecture is a practical implementation of this next generation of security.

Multiplication of Options:

Combining hybrid encryption, ephemeral keys, and protocol-level anonymization creates an exponential increase in the complexity required to analyze or break communication.



Beyond Routing:

Cryptographic Discovery replaces traditional routing, creating networks where access is based on cryptographic knowledge, not addresses. This is the foundation of Cryptographic Artificial Intelligence (CAI).

A Tool for a New Age:

Spot-On is not just an application, but a research platform and a functional tool for navigating and building the future of private communication.