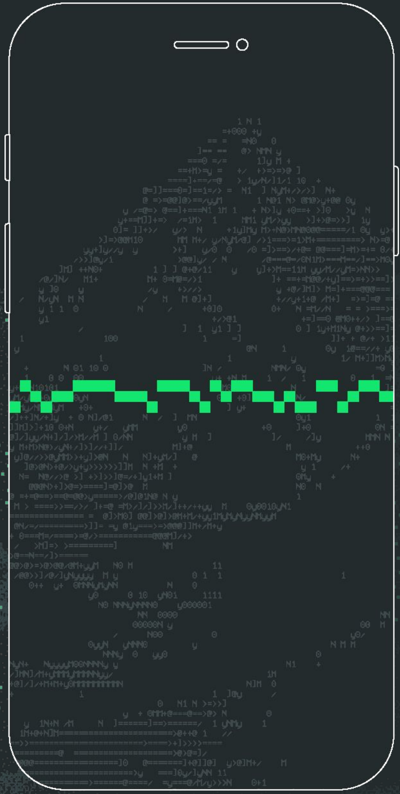
NymVPN

The first real-world decentralized mixnet for anonymity

FOSDEM - 2026



© 2025 Nym Technologies S.A. | nym.com

The Nym Team

Brought together in 2015 by PANORAMIX: the European Commission's largest R&D effort to build an anonymous networking system more powerful than Tor after Snowden revelations over NSA.

NEXTLEAP Panoramix UCL Inria EPFL KU LEUVEN

NYM
Future of Privacy on the Internet
With Edward Snowden
Harry Halpin (CEO, Nym)
Roxanne Varza (Director, Station F)
Edward Snowden

Co-founders

Harry Halpin, PhD
CEO and President of Board

ex-W3C/MIT, co-ordinated standards like the Web Cryptography API and Web Authentication (passkeys) amongst all major browsers,Ph.D. Informatics and philosophy

Alexis Roussel
COO and Board member.

ex-United Nations, early Swiss Bitcoin entrepreneur, first money transmitter license for Bitcoin (Bity), leads effort to put digital integrity in Swiss cantonal constitutions.

Prof. Claudia Diaz
Chief Scientist

Formerly tenured professor at KU Leuven, Europe's most widely-known professor in network privacy and mixnet pioneer. PhD. from KU Leuven.

Ania Piotrowska, PhD
Chief Scientific Officer

Original author of "Loopix" design paper that Nym is based on. Ph.D. in UCL.

© 2025 Nym Technologies S.A. | nym.com

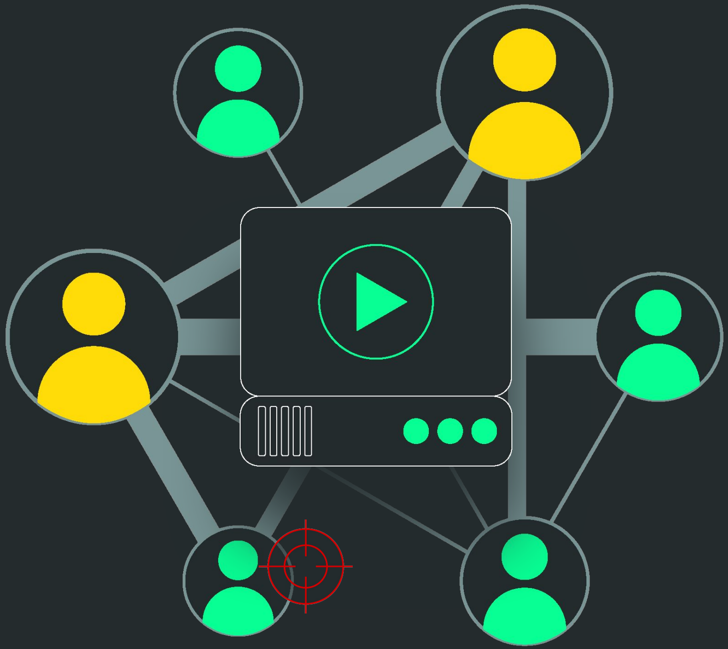
Every action online leaves a trace:
Metadata.

End-to-end encryption (TLS, Signal, WhatsApp) is **not enough. Metadata** is still easily observed.

Metadata: The timing and volume of data between end-points and other data (like IP address when using Internet).

Who you talk to is just as important as what you say.

Your **social and spending activities** is revealed by your communication…**and is exposed even when blockchain is shielded.**



© 2025 Nym Technologies S.A. | nym.com

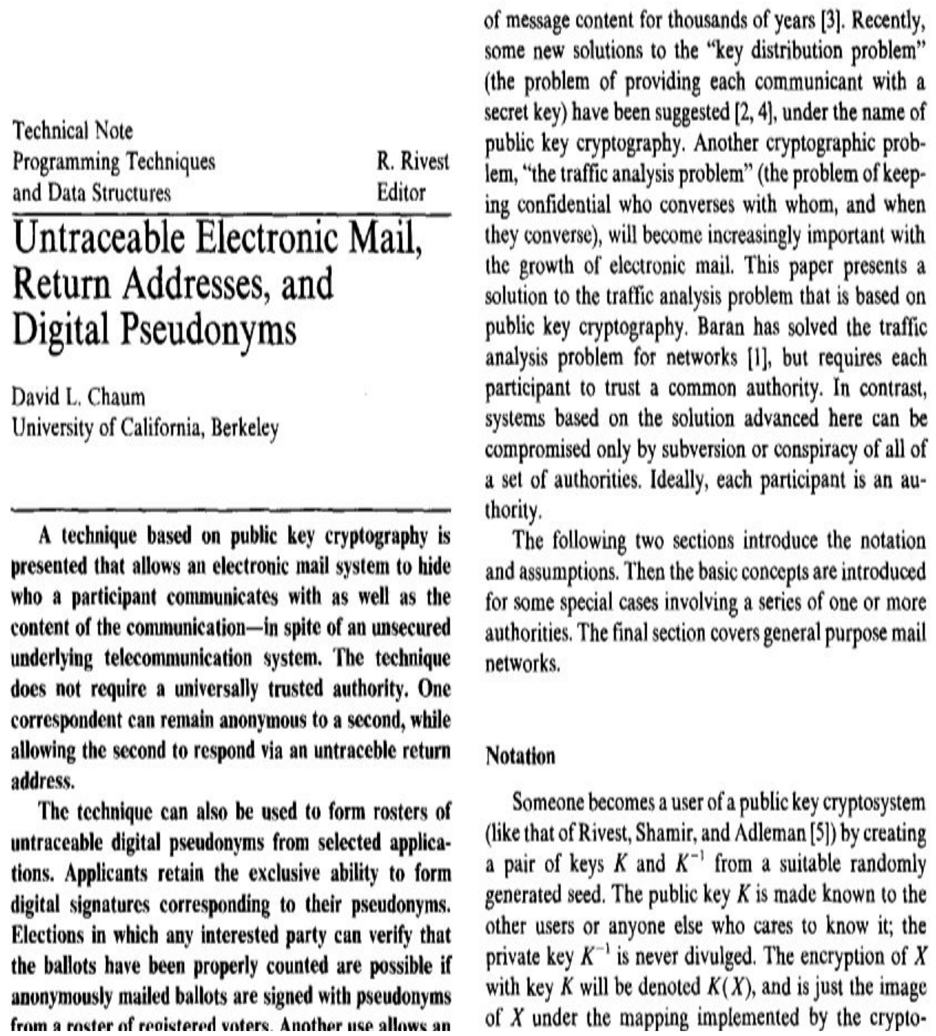
David Chaum
(1979/1981)

Invents mix-nets: An anonymous untraceable communication networks

Protect data & metadata

Yet … only works for e-mail.

© 2025 Nym Technologies S.A. | nym.com



Technical Note
Programming Techniques
and Data Structures

R. Rivest
Editor

Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms

David L. Chaum
University of California, Berkeley

A technique based on public key cryptography is presented that allows an electronic mail system to hide who a participant communicates with as well as the content of the communication—in spite of an unsecured underlying telecommunication system. The technique does not require a universally trusted authority. One correspondent can remain anonymous to a second, while allowing the second to respond via an untraceble return address.

The technique can also be used to form rosters of untraceable digital pseudonyms from selected applications. Applicants retain the exclusive ability to form digital signatures corresponding to their pseudonyms. Elections in which any interested party can verify that the ballots have been properly counted are possible if anonymously mailed ballots are signed with pseudonyms from a roster of registered voters. Another use allows an

of message content for thousands of years [3]. Recently, some new solutions to the "key distribution problem" (the problem of providing each communicant with a secret key) have been suggested [2, 4], under the name of public key cryptography. Another cryptographic problem, "the traffic analysis problem" (the problem of keeping confidential who converses with whom, and when they converse), will become increasingly important with the growth of electronic mail. This paper presents a solution to the traffic analysis problem that is based on public key cryptography. Baran has solved the traffic analysis problem for networks [1], but requires each participant to trust a common authority. In contrast, systems based on the solution advanced here can be compromised only by subversion or conspiracy of all of a set of authorities. Ideally, each participant is an authority.

The following two sections introduce the notation and assumptions. Then the basic concepts are introduced for some special cases involving a series of one or more authorities. The final section covers general purpose mail networks.

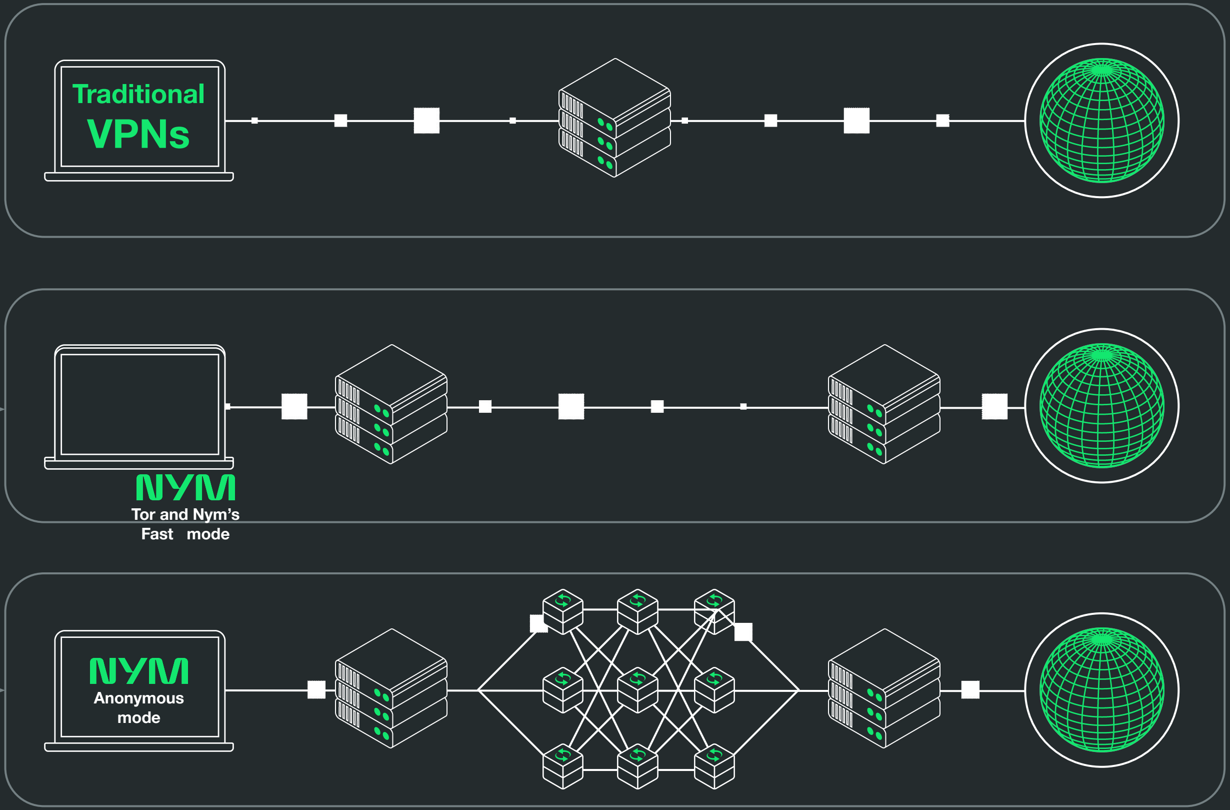
Notation

Someone becomes a user of a public key cryptosystem (like that of Rivest, Shamir, and Adleman [5]) by creating a pair of keys K and K^{-1} from a suitable randomly generated seed. The public key K is made known to the other users or anyone else who cares to know it; the private key K^{-1} is never divulged. The encryption of X with key K will be denoted $K(X)$, and is just the image of X under the mapping implemented by the crypto-

The Nym network in practice

The 2-server decentralized VPN (dVPN), more secure than any VPN, similar to **Tor.**

The 5-server **mixnet**, the strongest privacy available today



© 2025 Nym Technologies S.A. | nym.com

Nym

A quick and biased comparison!

	Nym	Tor/dVPNs	VPNs
Censorship-resistance via decentralization	✓	✓	✗
Independent operators	✓	✓	✗
Incentivized performance	✓	✗	✗
Unlinkable activity against nation-states	✓	✗	✗
Mixing packets	✓	✗	✗
Cover traffic	✓	✗	✗
Timing obfuscation	✓	✗	✗
Open source and free software	✓	✓	✗
Unlinkable payments	✓	–	✗

© 2025 Nym Technologies S.A. | nym.com

Mixnets are built for a **global passive adversary**

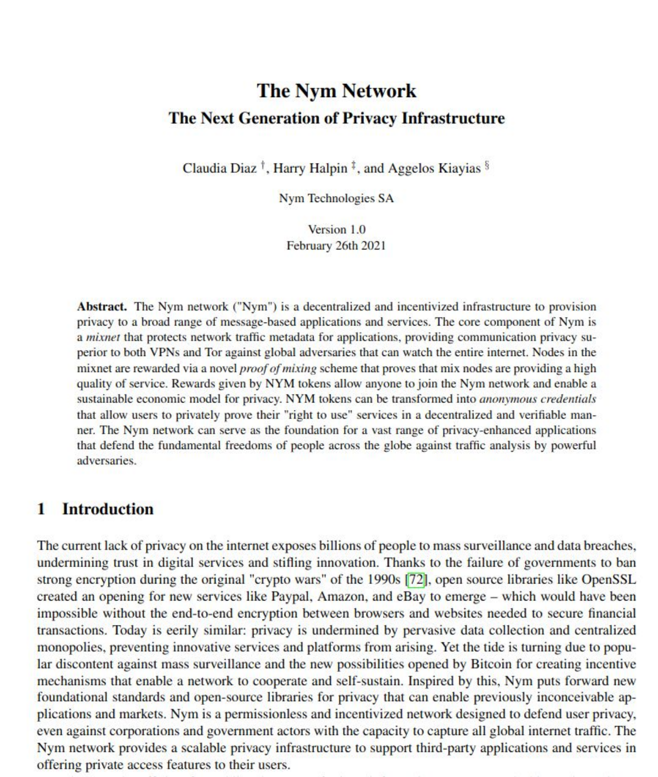
An adversary that can watch “every packet” from a God’s eye view such as Palantir/NSA on whole internet.

Tor is built for circuit-based synchronous traffic (web traffic) against local adversaries. Anonymity is hard to measure!

Mixnets are built for message-based asynchronous traffic against powerful adversaries. Anonymity (measured as entropy) grows with number of users.

Both have active attacks, but per-packet mix networks with independent routing are harder to attack as the adversary has to **control the whole route to de-anonymize a single packet**. Multiple packets are even harder to de-anonymize!

See **Nym whitepaper** for full design: https://nym.com/nym-whitepaper.pdf



The Nym Network

The Next Generation of Privacy Infrastructure

Claudia Diaz [†], Harry Halpin [‡], and Aggelos Kiayias [§]

Nym Technologies SA

Version 1.0
February 26th 2021

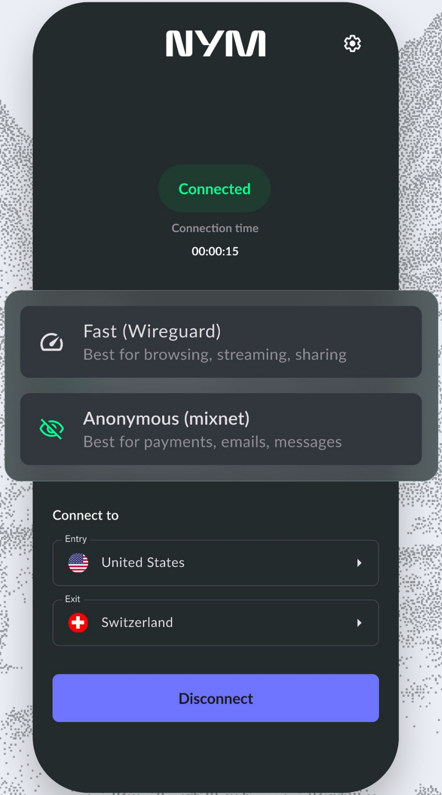
Abstract. The Nym network ("Nym") is a decentralized and incentivized infrastructure to provision privacy to a broad range of message-based applications and services. The core component of Nym is a *mixnet* that protects network traffic metadata for applications, providing communication privacy superior to both VPNs and Tor against global adversaries that can watch the entire internet. Nodes in the mixnet are rewarded via a novel *proof of mixing* scheme that proves that mix nodes are providing a high quality of service. Rewards given by NYM tokens allow anyone to join the Nym network and enable a sustainable economic model for privacy. NYM tokens can be transformed into *anonymous credentials* that allow users to privately prove their "right to use" services in a decentralized and verifiable manner. The Nym network can serve as the foundation for a vast range of privacy-enhanced applications that defend the fundamental freedoms of people across the globe against traffic analysis by powerful adversaries.

1 Introduction

The current lack of privacy on the internet exposes billions of people to mass surveillance and data breaches, undermining trust in digital services and stifling innovation. Thanks to the failure of governments to ban strong encryption during the original "crypto wars" of the 1990s [72], open source libraries like OpenSSL created an opening for new services like Paypal, Amazon, and eBay to emerge – which would have been impossible without the end-to-end encryption between browsers and websites needed to secure financial transactions. Today is eerily similar: privacy is undermined by pervasive data collection and centralized monopolies, preventing innovative services and platforms from arising. Yet the tide is turning due to popular discontent against mass surveillance and the new possibilities opened by Bitcoin for creating incentive mechanisms that enable a network to cooperate and self-sustain. Inspired by this, Nym puts forward new foundational standards and open-source libraries for privacy that can enable previously inconceivable applications and markets. Nym is a permissionless and incentivized network designed to defend user privacy, even against corporations and government actors with the capacity to capture all global internet traffic. The Nym network provides a scalable privacy infrastructure to support third-party applications and services in offering private access features to their users.

© 2025 Nym Technologies S.A. | nym.com

Nym Network:



NYM

Connected

Connection time

00:00:15

Fast (Wireguard)

Best for browsing, streaming, sharing

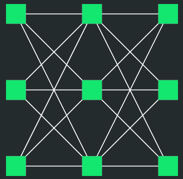
Anonymous (mixnet)

Best for payments, emails, messages

Connect to

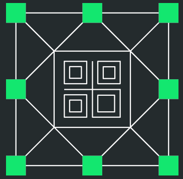
Entry: United States

Exit: Switzerland



NOISE GENERATING MIXNET (NGM)

The Nym mixnet prevents traffic analysis by an adversary capable of watching the entire network (Russia, China, etc.) or using AI tools. Can turn off mixing and use 2-hop (“fast”) mode for VPN-level speeds!



NYM CREDENTIALS (zk-nyms)

Allows access control to mixnet. Capable of proving purchasing of subscription. Can be used with zero-knowledge proofs to prove arbitrary facts.

Underlying Technologies

ZK-NYMS

Anonymous credential scheme available so that Nym nodes cannot link payment to usage. Decentralized Coconut signature scheme with Pedersen commits and private/public attributes, extensible.

KEY ROTATION, FORWARD SECRECY

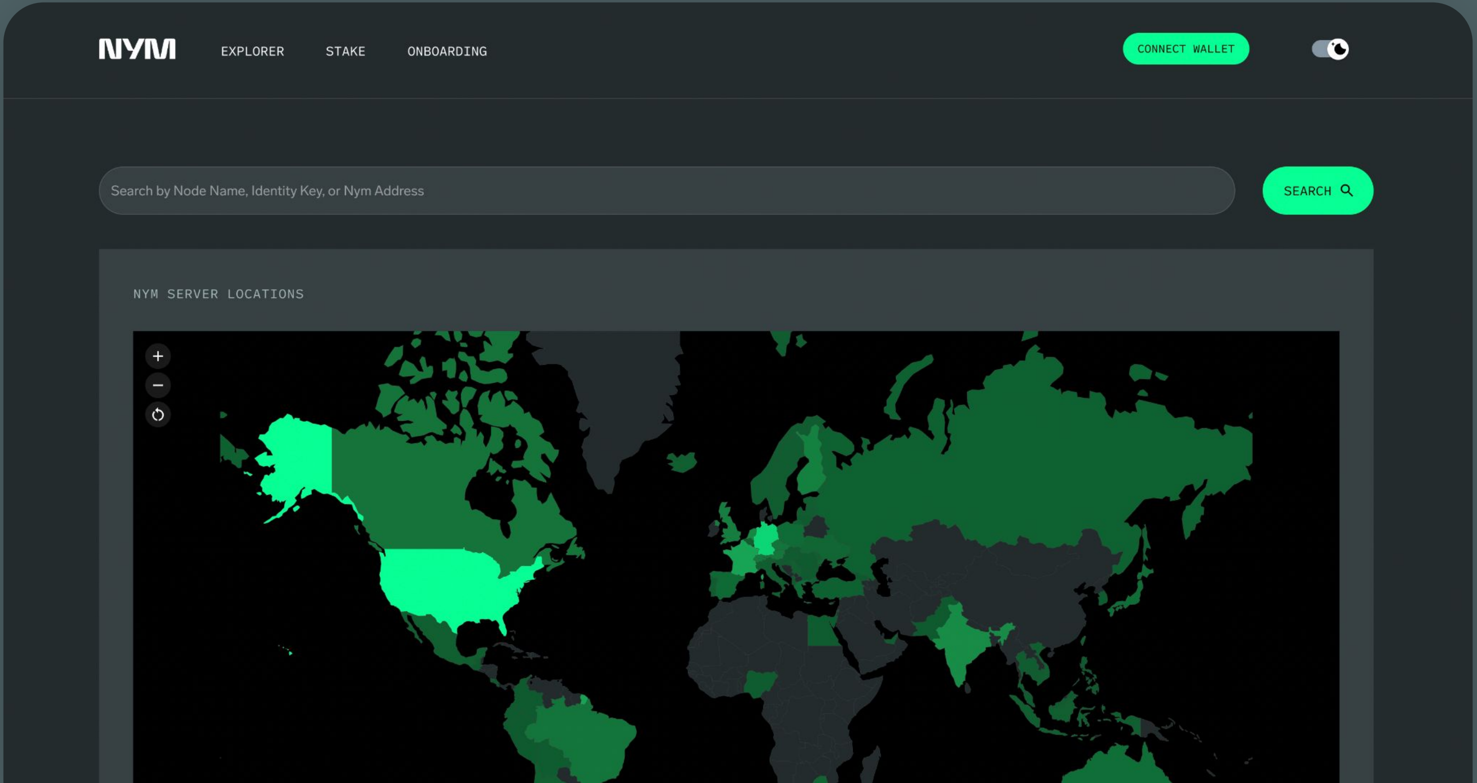
Randomly assigns nodes to layers to thwart adversarial nodes, provably better than “hop by hop” peer-routing. Keys rotated per epoch. PQ Noise between nodes.

CENSORSHIP RESISTANCE

Uses QUIC plus domain fronting currently and more features like postquantum obfs5 and delivery of rendezvous points to defeat the Great Firewall of China …

Nym Network

700+ servers ran today across world, plan to extend to residential IPs



Search by Node Name, Identity Key, or Nym Address

Try it out:

Putting a VPN interface on it that makes activating the mixnet easy to use!

- GET IT ON Google Play
- Download on the App Store
- Get it from Microsoft
- GET IT ON F-Droid
- GET IT ON Windows
- GET IT ON Linux
- GET IT ON Flathub

Download NymVPN below!

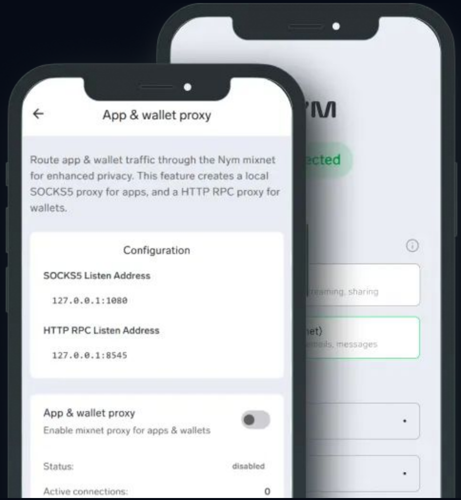
© 2025 Nym Technologies S.A. | nym.com

Using Nym Mixnet with your Apps

Just use **SOCKS** (Nym supports SOCKS4/SOCKS5) to route arbitrary data through the network with apps like Firefox.

OR

Compile a native integration with the programming language of your choice. Code is **GPLv3** for client code.



App & wallet proxy

Route app & wallet traffic through the Nym mixnet for enhanced privacy. This feature creates a local SOCKS5 proxy for apps, and a HTTP RPC proxy for wallets.

Configuration

SOCKS5 Listen Address

```
127.0.0.1:1080
```

HTTP RPC Listen Address

```
127.0.0.1:8545
```

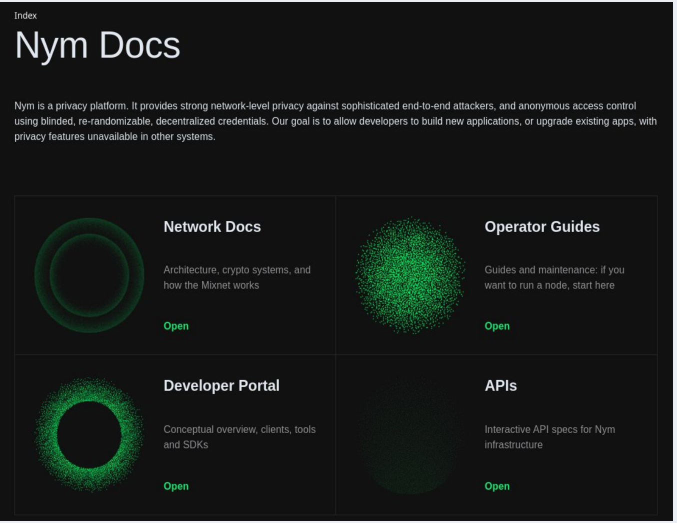
App & wallet proxy
Enable mixnet proxy for apps & wallets

Status: disabled

Active connections: 0

Mixnet APIs for most popular programming languages

nym.com/docs



Index

Nym Docs

Nym is a privacy platform. It provides strong network-level privacy against sophisticated end-to-end attackers, and anonymous access control using blinded, re-randomizable, decentralized credentials. Our goal is to allow developers to build new applications, or upgrade existing apps, with privacy features unavailable in other systems.

Network Docs

Architecture, crypto systems, and how the Mixnet works

Open

Operator Guides

Guides and maintenance: if you want to run a node, start here

Open

Developer Portal

Conceptual overview, clients, tools and SDKs

Open

APIs

Interactive API specs for Nym infrastructure

Open

Mixnet APIs and libraries are free to use and deploy

Nym Rust SDK:
https://crates.io/crates/nym-sdk

Nym Javascript SDK:
https://www.npmjs.com/package/@nymproject/sdk

FFI bindings for C and Go:
https://nym.com/docs/developers/rust/ffi

Nym SDKs

Integrate Mixnet functionality into existing apps / codebases in Rust or Typescript.

- Several solutions depending on environment (mobile and desktop, Web app vs native).

- Native & browser-based applications have very different restrictions (security, single- vs multi-threaded runtime, etc) so different approaches have had to be taken.

- We have a ***real-world testnet*** to integrate against for testing new software! Just reach out for an account.

The Nym mixnet is **free to use** with SDKs and via SOCKS**. No anonymous credential (zk-nym) required for access for developers**.

Nym SDKs: Rust SDK

Powerful native Rust SDK for commandline and desktop applications.

- Now on crates.io:
- Made up of several modules, each with different uses:
    - *TcpProxy* Module, exposes localhost socket. Currently the most ‘plug-and-play’ module with one design drawback: inability to perform TLS due to reliance on localhost socket. This will be superceded by the more generic *MixSocket/MixStream* module (see below) which fixes the TLS issue in the near future.
    - *Mixnet* Module, exposes raw Mixnet Client. The basis of the other modules, not aimed at direct use by developers when integrating existing apps, but useful if custom logic is required.
    - *MixSocket/MixStream*, TCP socket like interface which allows for either direct Nym Client - Nym Client communication, or use of the Nym Network Exit Gateways to proxy IP packets to the wider internet.
        - *Mixtcp* was built with this module, and is a fork of the *smoltpc* TCP/IP stack that runs its traffic entirely through the Mixnet.
            - Includes example of performing TLS handshake and creating of HTTPS client through the Mixnet communicating with a clearnet remote host.

Nym SDKs: Typescript SDK

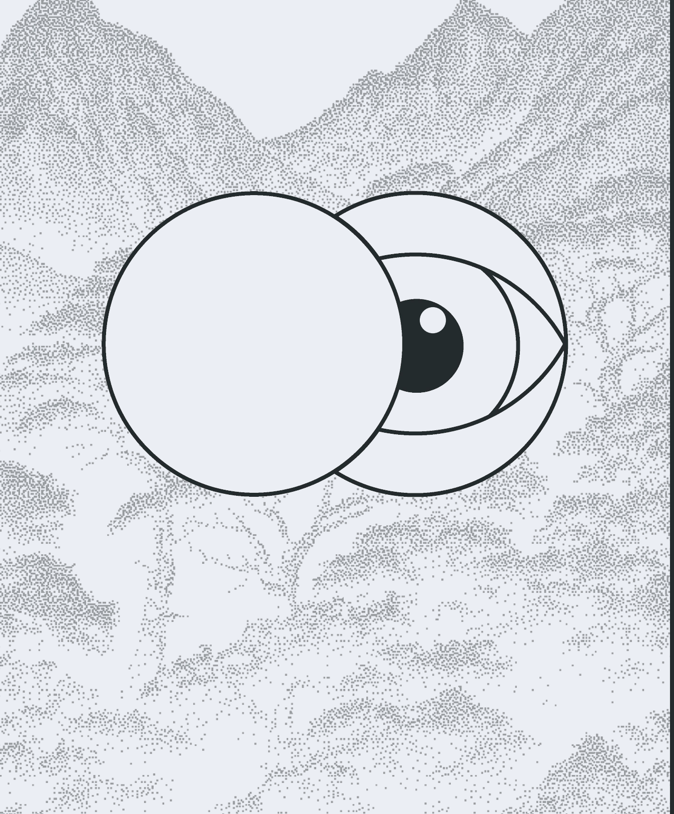
Bundled Web Assembly (WASM) Client for use in the browser.

- The problem space: Browsers are a very restricted environment to work in:
  - limited options for external communications (WebSockets, Web Transport API, WebRTC)
  - mixed content restrictions (HTTPS-only)
  - no access to the file system or any syscalls
  - lack of access to browser TLS negotiation from JS or the CA certificate store when proxying

- We have two packages for developers right now:
  - *MixnetClient*: ‘raw’ per packet WASM Nym Client for direct Nym Client - Nym Client communication (message-based).
  - *MixFetch*: easy-to-use replacement for browser’s *Fetch* API - perform HTTP requests through the Mixnet
    - CA store is bundled at compile time
    - Concurrent requests supported very soon by removing NextJS dependencies.

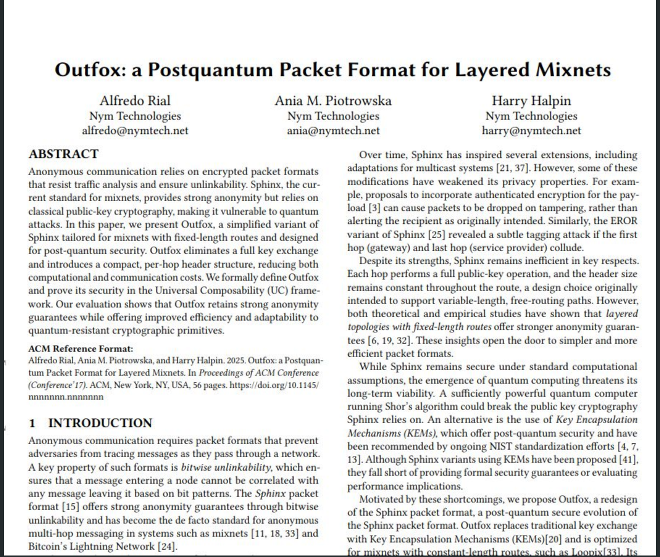
- Both packages run in a WebWorker, so can be embedded directly into browser page **without** the need for extra user config or installation of extra software (e.g. a browser extension).
- Opens up very use-cases for anonymous publishing and censorship resistance.

Postquantum Next Steps



1) Post-quantum Noise protocol variant for registration and network security, support for rotating ML-KEM keys and long-term McEliece
2) Outfox: A post-quantum mixnet packet format

R&D design with security proofs by Nym show it can be done! Presented at WPES 2025 at ACM CCS (October 13 2025): https://arxiv.org/pdf/2412.19937v2



Outfox: a Postquantum Packet Format for Layered Mixnets

Alfredo Rial
Nym Technologies
alfredo@nymtech.net

Ania M. Piotrowska
Nym Technologies
ania@nymtech.net

Harry Halpin
Nym Technologies
harry@nymtech.net

ABSTRACT

Anonymous communication relies on encrypted packet formats that resist traffic analysis and ensure unlinkability. Sphinx, the current standard for mixnets, provides strong anonymity but relies on classical public-key cryptography, making it vulnerable to quantum attacks. In this paper, we present Outfox, a simplified variant of Sphinx tailored for mixnets with fixed-length routes and designed for post-quantum security. Outfox eliminates a full key exchange and introduces a compact, per-hop header structure, reducing both computational and communication costs. We formally define Outfox and prove its security in the Universal Composability (UC) framework. Our evaluation shows that Outfox retains strong anonymity guarantees while offering improved efficiency and adaptability to quantum-resistant cryptographic primitives.

ACM Reference Format:
Alfredo Rial, Ania M. Piotrowska, and Harry Halpin. 2025. Outfox: a Postquantum Packet Format for Layered Mixnets. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 56 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Anonymous communication requires packet formats that prevent adversaries from tracing messages as they pass through a network. A key property of such formats is *bitwise unlinkability*, which ensures that a message entering a node cannot be correlated with any message leaving it based on bit patterns. The *Sphinx* packet format [15] offers strong anonymity guarantees through bitwise unlinkability and has become the de facto standard for anonymous multi-hop messaging in systems such as mixnets [11, 18, 33] and Bitcoin's Lightning Network [24].

Over time, Sphinx has inspired several extensions, including adaptations for multicast systems [21, 37]. However, some of these modifications have weakened its privacy properties. For example, proposals to incorporate authenticated encryption for the payload [3] can cause packets to be dropped on tampering, rather than alerting the recipient as originally intended. Similarly, the EROR variant of Sphinx [25] revealed a subtle tagging attack if the first hop (gateway) and last hop (service provider) collude.

Despite its strengths, Sphinx remains inefficient in key respects. Each hop performs a full public-key operation, and the header size remains constant throughout the route, a design choice originally intended to support variable-length, free-routing paths. However, both theoretical and empirical studies have shown that *layered topologies with fixed-length routes* offer stronger anonymity guarantees [6, 19, 32]. These insights open the door to simpler and more efficient packet formats.

While Sphinx remains secure under standard computational assumptions, the emergence of quantum computing threatens its long-term viability. A sufficiently powerful quantum computer running Shor's algorithm could break the public key cryptography Sphinx relies on. An alternative is the use of *Key Encapsulation Mechanisms (KEMs)*, which offer post-quantum security and have been recommended by ongoing NIST standardization efforts [4, 7, 13]. Although Sphinx variants using KEMs have been proposed [41], they fall short of providing formal security guarantees or evaluating performance implications.

Motivated by these shortcomings, we propose Outfox, a redesign of the Sphinx packet format, a post-quantum secure evolution of the Sphinx packet format. Outfox replaces traditional key exchange with Key Encapsulation Mechanisms (KEMs)[20] and is optimized for mixnets with constant-length routes, such as Loopix[33]. Its

Anonymize the Internet: Build AnonApps!

- The problem space: Browsers are a very restricted environment to work in:
  - limited options for external communications (WebSockets, Web Transport API, WebRTC)
  - mixed content restrictions (HTTPS-only)
  - no access to the file system or any syscalls
  - lack of access to browser TLS negotiation from JS or the CA certificate store when proxying

- We have two packages for developers right now:
  - *MixnetClient*: 'raw' per packet WASM Nym Client for direct Nym Client - Nym Client communication (message-based).
  - *MixFetch*: easy-to-use replacement for browser's *Fetch* API - perform HTTP requests through the Mixnet
    - CA store is bundled at compile time
    - Concurrent requests supported very soon by removing NextJS dependencies.

- Both packages run in a WebWorker, so can be embedded directly into browser page **without** the need for extra user config or installation of extra software (e.g. a browser extension).
- Opens up very use-cases for anonymous publishing and censorship resistance.

NYM

Web
nym.com

Twitter
@nymproject

Email
harry@nymtech.net
alexis@nymtech.net

Github
@nymtech

Universal
Privacy Alliance

🟩 © 2025 Nym Technologies S.A. | nym.com

Download NymVPN

nym.com/download