HoodVPN

HoodVPN Litepaper

Version 1.0 — The Next Generation of VPN Security

Secure Today. Ready for Tomorrow.

CONFIDENTIAL — FOR DISTRIBUTION ONLY

EXECUTIVE SUMMARY

The Next Generation of VPN Security

The security landscape is changing. Advances in quantum computing threaten to undermine many of the cryptographic algorithms that protect today's internet. While large-scale cryptographically relevant quantum computers are not yet available, organizations are already preparing for the transition to post-quantum cryptography.

HoodVPN is designed with this transition in mind. Built around modern VPN technologies and a security architecture intended to support post-quantum cryptographic standards, HoodVPN aims to provide encrypters communication that remains resilient as cryptographic best practices evolve.

Rather than waiting for the threat to become immediate, we are ready today.

Quantum Threat

Cryptographic algorithms protecting today's internet are at risk.

Forward-Looking

Designed for the post-quantum era — before the threat arrives.

Resilient by Design

Encrypted communication built to evolve.

THREAT LANDSCAPE

Why Post-Quantum Matters

Decades of Trust

Today's VPNs generally rely on RSA and elliptic-curve cryptography (ECC) for authentication and key exchange. These algorithms have protected internet communications for decades.

The Quantum Threat

Sufficiently capable quantum computers are expected to efficiently solve mathematical problems that underpin many current public-key systems using algorithms such as Shor's algorithm.

Transition Underway

Organizations worldwide are adopting post-quantum standards to withstand future attacks. HoodVPN is built to support this evolution.

"The question is no longer if — it's when."

THREAT VECTOR

The Harvest Now, Decrypt Later Problem

Capture Now

Encrypted traffic captured today may remain valuable for years. Attackers can store it and attempt to decrypt it later.

At-Risk Data

Sensitive intellectual property, financial information, healthcare records and long-lived communications require future cryptographic resilience.

Long-Term Protection

HoodVPN is designed with long-term protection as a guiding principle.

ARCHITECTURE

Built for the Post-Quantum Era

HoodVPN is engineered to integrate post-quantum cryptographic mechanisms into its secure communication architecture.

Key design goals include:

Post-Quantum Key Establishment
Support for standardized post-quantum key establishment.

Encrypted VPN Tunnels
Strong encrypted VPN tunnels.

Modern Authentication
Modern authentication mechanisms.

Secure Session Establishment
Secure session establishment.

Privacy-Focused Networking
Privacy-focused networking.

Cryptographic Agility
Forward-looking cryptographic agility.

Rather than locking the platform to a single algorithm, HoodVPN is designed so that cryptographic components can evolve alongside emerging standards and best practices.

PHILOSOPHY

Security Philosophy

Traditional VPNs were designed primarily around today's threats.
HoodVPN is designed for both today's and tomorrow's.

Its architecture emphasizes:

- Defense in Depth
- Cryptographic Agility
- Secure Session Management
- Leak Prevention
- DNS Protection
- Privacy by Default
- Continuous Security Evolution