QuxTech Quantum-Safe VoIP Security

QuxTech Quantum-Safe VoIP Security

Protecting Your Voice Communications for the Post-Quantum Era

---

The Challenge

Today's Encryption Won't Protect Tomorrow's Calls

Current voice communication systems rely on encryption methods developed decades ago. While secure against today's computers, these methods face an existential threat:

Quantum computers will break traditional encryption.

This isn't a distant future problem—it's happening now:

- Nation-states are stockpiling encrypted communications today
- When quantum computers mature, historical intercepts become readable
- Voice calls containing sensitive business, legal, or personal information are at risk
- The threat model has shifted from "break now" to "harvest now, decrypt later"

The Stakes

What's at Risk?

Sector	Vulnerable Communications
Financial Services	Trading instructions, M&A discussions, client advisory calls
Healthcare	Patient consultations, diagnostic discussions, treatment plans
	Attorney-client privileged communications, case

Legal	strategy
Government	Classified briefings, diplomatic communications
Enterprise	Board calls, strategic planning, intellectual property discussions
Defense	Tactical communications, intelligence briefings

The sensitive call you make today could be decrypted and exposed in 5-10 years.

The Solution

QuxTech Quantum-Safe VoIP Encryption

QuxTech has developed a next-generation voice encryption system that protects communications against both current and future threats—including attacks from quantum computers.

Built on NIST-Approved Standards

Our solution implements cryptographic algorithms selected and standardized by the U.S. National Institute of Standards and Technology (NIST) after an 8-year global competition:

- **FIPS 203** — Quantum-resistant key establishment
- **FIPS 204** — Quantum-resistant digital signatures

These standards represent the global consensus on post-quantum security.

How It Protects You

Defense in Depth

Before the Call Connects

Every call begins with a secure handshake that establishes encryption keys immune to quantum attack. Even if an adversary records this exchange, future quantum computers cannot recover the keys.

During the Call

Voice data is encrypted in real-time using military-grade symmetric encryption. Each audio frame receives individual protection with unique cryptographic material.

After the Call Ends

Encryption keys are securely destroyed. There is no “master key” that could later be compromised. Each call’s security is mathematically independent.

Key Capabilities

What QuxTech PQE VoIP Delivers

Quantum-Resistant Key Exchange

Establishes shared secrets that cannot be broken by quantum computers, ensuring long-term confidentiality of your communications.

Perfect Forward Secrecy

Each call uses unique, ephemeral keys. Compromise of one call does not affect any other—past or future.

Real-Time Frame Encryption

Sub-millisecond encryption latency ensures call quality is never compromised. Security doesn’t mean sacrificing clarity.

Cryptographic Authentication

Both parties are verified using quantum-safe signatures, preventing impersonation and man-in-the-middle attacks.

Tamper Detection

Any attempt to modify voice data in transit is immediately detected, ensuring integrity of communications.

Security Levels

Choose Your Protection Level

QuxTech PQE VoIP offers two security tiers to match your requirements:

Level	Protection Equivalent	Recommended For
Level 3	AES-192	Standard enterprise communications, general business use
Level 5	AES-256	Highly sensitive communications, regulated industries,

Both levels provide quantum resistance. Level 5 offers additional security margin for the most critical use cases.

Seamless Integration

Works With Your Existing Infrastructure

QuxTech PQE VoIP is designed to integrate with standard communication platforms:

Compatible Technologies

- WebRTC-based applications
- SIP/VoIP systems
- Custom communication platforms
- Mobile applications (iOS, Android)
- Desktop clients (Windows, macOS, Linux)

Standard Audio Codecs Supported

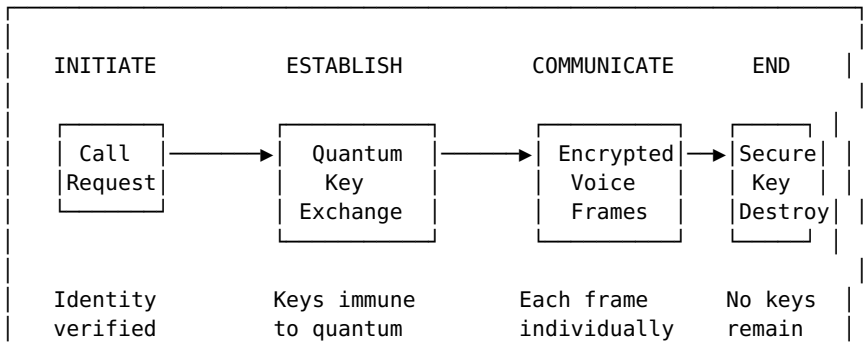
- Opus (recommended for quality)
- G.711 (legacy compatibility)
- G.722 (wideband)
- G.729 (bandwidth-efficient)

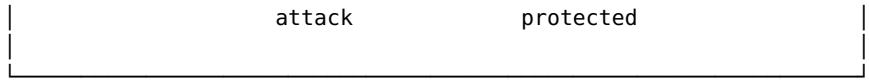
Deployment Options

- Cloud-hosted service
- On-premises installation
- Hybrid configurations
- Air-gapped environments

Call Security Lifecycle

From Connection to Completion





Every phase is protected. No weak links in the security chain.

Compliance & Standards

Meeting Regulatory Requirements

QuxTech PQE VoIP helps organizations meet stringent compliance requirements:

Requirement	How PQE VoIP Helps
HIPAA	Encrypts protected health information in voice communications
PCI-DSS	Secures cardholder data discussed over calls
SOX	Protects financial communications with audit-grade security
GDPR	Implements state-of-the-art encryption for personal data
CMMC	Aligns with DoD cryptographic requirements
FedRAMP	Uses NIST-approved algorithms

Future-Proof Compliance

As regulations evolve to require quantum-resistant encryption, you'll already be compliant.

Performance

Security Without Compromise

Latency Impact

- Key establishment: < 100ms (one-time per call)
- Frame encryption: < 1ms (imperceptible)
- No degradation to voice quality

Bandwidth Overhead

- Minimal increase to packet size
- Compatible with bandwidth-constrained networks
- Optimized for mobile and satellite links

Scalability

- Supports thousands of concurrent calls
- Horizontal scaling for enterprise deployments
- No centralized bottlenecks

Why QuxTech?

Our Differentiators

Standards-Based

We implement NIST FIPS 203 and FIPS 204—not proprietary or experimental algorithms. Your security is built on the global standard.

Production-Ready

Battle-tested implementation with comprehensive security audits. Not a research project—a deployable solution.

Developer-Friendly

Clean APIs and comprehensive documentation enable rapid integration into your existing communication systems.

Transparent Security

Our cryptographic approach is based on published, peer-reviewed standards. Security through obscurity is not security.

Future-Proof

As quantum computing advances, your investment in quantum-safe encryption only becomes more valuable.

Deployment Timeline

Rapid Path to Quantum Safety

Phase	Activities	Duration
Assessment	Evaluate current infrastructure, identify integration points	1-2 weeks
Pilot	Deploy in test environment, validate functionality	2-4 weeks
Integration	Connect to production systems, configure	2-4 weeks

	policies	
Rollout	Phased deployment to user base	2-8 weeks
Optimization	Performance tuning, monitoring setup	Ongoing

Total time to production: **8-16 weeks** for most organizations.

Use Cases

Where PQE VoIP Makes the Difference

Executive Communications

Board calls and C-suite discussions often contain market-moving information. Protect against long-term exposure.

Legal Consultations

Attorney-client privilege requires the highest level of protection. Ensure privileged communications remain privileged.

Healthcare Telemedicine

Patient consultations involve sensitive health information. Meet HIPAA requirements with quantum-safe encryption.

Financial Advisory

Investment discussions, trading strategies, and client portfolios deserve protection that lasts decades.

Government & Defense

Classified and sensitive communications require encryption that will withstand future cryptanalytic advances.

Research & Development

Protect intellectual property discussions from industrial espionage—today and in the future.

The Bottom Line

Invest in Security That Lasts

Traditional Encryption	QuxTech PQE VoIP

Vulnerable to quantum attack	Quantum-resistant by design
“Harvest now, decrypt later” risk	Long-term confidentiality assured
Will require replacement	Future-proof investment
Unknown compliance future	Ahead of regulatory curve

The question isn’t whether to adopt quantum-safe encryption—it’s when.

Organizations that act now gain: - First-mover advantage in security posture - Protection for communications made today - Smooth transition before regulatory mandates - Competitive differentiation in security-conscious markets

---

Get Started

Next Steps

Request a Demo

See QuxTech PQE VoIP in action with a live demonstration of quantum-safe voice encryption.

Technical Evaluation

Our engineering team can assess your infrastructure and provide integration recommendations.

Pilot Program

Deploy PQE VoIP in a controlled environment to validate performance and compatibility.

Contact Us

QuxTech Security Solutions

- **Web**: www.quxtech.com
- **Email**: security@quxtech.com
- **Enterprise Sales**: enterprise@quxtech.com

Summary

QuxTech Quantum-Safe VoIP Encryption

- **Protects voice communications** against quantum computer attacks
- **Implements NIST standards** (FIPS 203, FIPS 204) for proven

security
- **Integrates seamlessly** with existing VoIP and WebRTC infrastructure
- **Delivers enterprise performance** with minimal latency impact
- **Meets compliance requirements** for regulated industries
- **Future-proofs your investment** in communication security

Secure today's calls against tomorrow's threats.

QuxTech PQE VoIP implements NIST FIPS 203 and FIPS 204 standards. "Quantum-safe" and "quantum-resistant" refer to cryptographic algorithms designed to resist attacks from both classical and quantum computers based on current cryptanalytic knowledge.