SECURITY INNOVATION

NTRU

QUANTUM-SAFE, STANDARDIZED CRYPTO

Quantum computing will immediately break the most commonly used asymmetric crypto solutions in the market today – RSA and ECC. Quantum-proof cryptography is relevant today.

NTRU CRYPTOGRAPHY & SIGNING

NTRU is a lattice-based public key cryptosystem, making it resistant to all known quantum computer attacks. First published in 1996, NTRU offers encryption, decryption, and signing. It has been adopted as an IEEE 1363.1 and X9 Standard. NTRU delivers substantial performance and size advantages, making it ideal for mobile and embedded applications. pqNTRUsign is the signature algorithm that accompanies NTRU.

It uses the same proven mathematics as NTRU. NTRU and pqNTRUsign are available in 128-, 192-, and 256- quantum bit strengths.

SMALLEST CODE FOOTPRINT & SYSTEM RESOURCE UTILIZATION

- Tiny compiled code (8 kb)
- Consumes minimal CPU and battery resources
- Ideal for all environments, but particularly well suited for embedded and mobile devices where code size is a major limitation
- Significantly reduces server utilization for large-scale deployments

HUGE PERFORMANCE INCREASES

- Highest performing public key cryptography
- Decryption is more than 92x faster than RSA decryption at an equivalent security level. NTRU is nearly 60% faster than RSA at encryption and TLS with a 370 times improvement in key generation time.
- Encryption and decryption are faster than the best-performing ECC algorithms at equivalent security levels.

NSA's Information Assurance Directorate:

"(Companies) will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer…"

https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtmlFeatures

LICENSING OPTIONS:

- Very reasonable commercial licensing terms are available for revenue producing applications using NTRU and/or pqNTRUsign.
- NTRU is free for all commercial client-side TLS applications.
- NTRU and pqNTRUsign are available under a free Open Source GNU General Public License (GPL) v2 with FOSS exceptions for other licenses. Source code is available at: GitHub.com/NTRUOpenSourceProject.

QUANTUM-SAFE HYBRID

- Accomplishes TLS authentication and key negotiation by combining today's classic cryptography with NTRU quantum-safe cryptography, ensuring the best of both worlds.
- Parallel implementation allows for benefits of NTRU on top of existing crypto infrastructure with a negligible performance penalty.

PREVENTS DATA HARVEST ATTACKS

- Protects information that needs to remain secret for many years by keeping encrypted traffic from being recorded and warehoused today and decrypted when quantum computers are available.
- Ideal for systems that have long lifecycles or can't be updated easily.

LIMITED TIME OFFER:

Until **October 1, 2016**, customers can obtain a perpetual, divisionwide license to use NTRU in server-side TLS applications for only **$50,000** - that's **67% off** the regular $150,000 license.

If you have a client-side TLS application, then there is **no charge** at all!

"Of the various lattice-based crypto schemes....NTRU appears to be the most practical...smallest key size... highest performance."

Quantum Resistant Public Key Cryptography
NIST