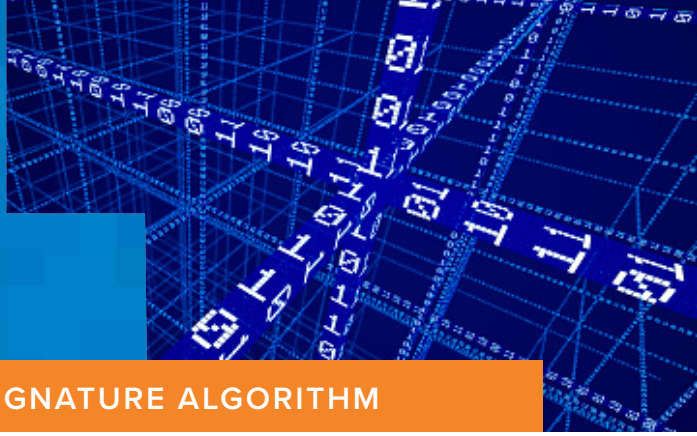
# pqNTRUsign



## THE MOST TRUSTED QUANTUM-RESISTANT SIGNATURE ALGORITHM

Digital signatures provide Integrity, Authentication and Non-Repudiation for online communications. Quantum Computers will soon break the most popular digital signature algorithms, including Elliptic Curve (ECDSA) and RSA-PSS, making online communications open and unsecured.

pqNTRUsign, the companion signature algorithm to NTRU, is resistant to all known quantum computer attacks, including Shor's and Grover's Algorithms.. By signing documents and code updates with pqNTRUsign today, users can rest easy that their identity won't be impersonated and their software won't be cracked once quantum computers arrive.

## KEY FEATURES

### pqNTRUsign SIGNATURE ALGORITHM

The most trusted, most mature post-quantum signing algorithm available

- Extensively vetted and challenged by the cryptographic community
- Developed by the NTRU research team through an iterative process starting in 2001
- Uses the same fundamental mathematics as NTRUEncrypt, the most scrutinized quantum-resistant algorithm
- Based on lattice cryptography, which offers superior performance, code size and key size versus other post-quantum alternatives
- Available in the quantum bit strengths the security community demands
- Open source version of the code is available for evaluation. Commercial licenses are required for revenue-generating applications.

### 128 Quantum Bit Strength

**pqNTRUsign-563**
Private Key = 540 b
Public Key = 1056 B
Signature size = 1056 B

### 192 Quantum Bit Strength

**pqNTRUsign-743**
Private Key = 560 b
Public Key = 1486 B
Signature size = 1486 B

### 256 Quantum Bit Strength

**pqNTRUsign-907**
Private Key = 640 b
Public Key = 1814 B
Signature size = 1814 B

1.978.905.6796 ■ onboardsecurity.com



onBoardSecurity