

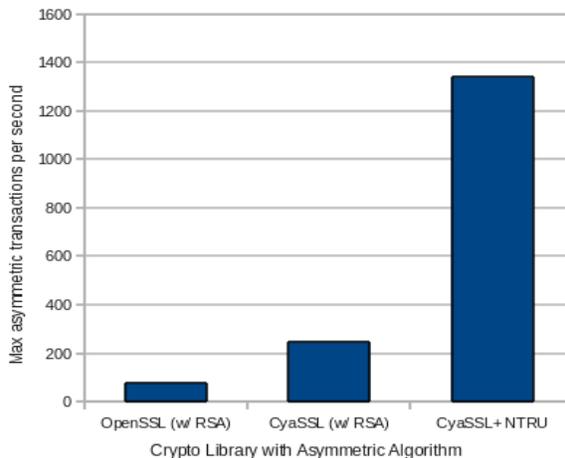
wolfSSL+NTRU – High-Performance SSL

Very fast, very small SSL

Ideal for Embedded and RTOS; OpenSSL-compatible

wolfSSL+NTRU: 20x-200x Faster

Performance initiating a new SSL connection
64 bit machine, 112bit security level (ie 2048bit RSA)



wolfSSL was built for embedded and RTOS environments and is also widely used in standard operating environments.

Because it is based on different math from RSA and ECC, the NTRU algorithm has different cryptographic properties. Most importantly, at comparable cryptographic strength, NTRU performs the costly private key operations much faster than RSA. In fact, **wolfSSL+NTRU runs 20x to 200x faster than OpenSSL RSA**. In addition, NTRU's comparative performance increases with the level of security required.

By moving to wolfSSL with the NTRU algorithm, organizations can gain 4x the CPU cycles and a corresponding saving in infrastructure costs, battery drain, or cost of goods sold.

Benefits

•Very Fast

wolfSSL+NTRU runs 20x to 200x faster than OpenSSL RSA, reduces server resource utilization for large-scale deployments, and significantly increase the number of concurrent connections.

•Very Small

wolfSSL+NTRU is smaller than any other public key crypto (8kB). In terms of crypto libraries, wolfSSL is up to 20x smaller than OpenSSL. wolfSSL is ideal for embedded systems and RTOS, but is applicable for any operating system requiring SSL.

•Standards Based

wolfSSL+NTRU fully supports the industry standards up to the current TLS 1.2 and DTLS 1.2 levels. NTRU Encrypt was standardized by IEEE as Standard IEEE 1363.1-200 and by the financial industry's ASCX9 as X9.98. NTRU Sign standardization is in process.

•Highly Portable

wolfSSL is built for maximum portability, and is very easy to compile on a variety of platforms. It supports the C programming language as its primary interface. Other host languages, including Java, PHP, Perl, and Python, are supported through a SWIG interface. Supported platforms include ARM, Intel, iOS, Linux, Motorola, Win32, Microchip, Freescale, STMicro, and more.

"Of the various lattice-based cryptographic schemes that have been developed, the NTRU family of cryptographic algorithms appears to be the most practical... There are viable alternatives for both public key encryption and signatures that are not vulnerable to Shor's Algorithm"

"Quantum Resistant Public Key
Cryptography: A Survey"

NIST 2009

**WOLFSSL+ WINS
MOBILE ENCRYPTION
AWARD**



**NEXT GENERATION
CRYPTO**

NTRU is an alternative asymmetric algorithm to RSA and ECC. It is based on a different mathematical problem, known as "lattice reduction", which makes it much faster and resistant to quantum computing attacks.

**QUANTUM-
RESISTANT**

When quantum computing attacks are realized, a product built with wolfSSL+NTRU will already be running a library with a future-proof algorithm.

**SUPPORTED
ALGORITHMS**

- Key exchange RSA, DSS, DH, EDH, NTRU
- Bulk encryption DES, 3D ES, AES, Camellia, ARC4, RABBIT, HC-128, ChaCha20
- MAC: MD2, MD5, SHA-1, SHA-512, RIPEMD, Poly1305



wolfSSL

Ntru

**Security
Innovation**
THE SOFTWARE SECURITY COMPANY

Phone +1.978.694.1008
www.securityinnovation.com
getsecure@securityinnovation.com