



# **NXP & NTRU**

## **Cryptography for ARM MCUs**

Business Line Standard IC's  
Product Line Microcontrollers



# Customer Requirements

Some embedded designers desire sophisticated encryption for even low-cost applications that may be carrying or transmitting sensitive information. Key security benefits achieved via an implementation of software encryption schemes are:

- ▶ **Confidentiality** - allows the sender and receiver to be sure that the information being shared only in the way they intend
- ▶ **Authentication** - allows the receiver of the information to be certain where it came from
- ▶ **Integrity** – allows the receiver to verify that the message has not been altered in transit

# The NXP & NTRU solution

- ▶ The NTRU software security libraries for NXP ARM microcontrollers provide the user the tools to **achieve the benefits and features of cryptography** and include encryption and decryption of messages, authentication, digital signatures, and utility protocols like key negotiation in an inexpensive and flexible manner
- ▶ Encryption algorithms work on the smallest ARM7 LPC2000 through to our ARM926 LPC3000 microcontrollers
- ▶ Allows customers who need **short time-to-market** to leverage Ntru's encryption expertise on their products quickly and efficiently
- ▶ Customers can **update the software in the field** to keep ahead of hackers and protect their IP

The Ntru logo features the word "Ntru" in a stylized font. The "N" is a light green color, while the "tru" is a teal color. The letters are bold and have a slight shadow effect.

# Why Software?

- ▶ A software implementation of an encryption scheme provides the benefits of **flexibility, speed of implementation, and lower cost** over time.
- ▶ Having encryption in software provides the ability to **modify product design and/or product security** without the need to make expensive changes in hardware and the potential resulting changes to the manufacturing process.
- ▶ More importantly, the NXP ARM microcontrollers feature **In Application Programming (IAP)** and the popular LPC2300 and LPC2400 series also feature Ethernet, USB and CAN
  - IAP allows customers to change the security algorithm in the field without costly recall
  - Competitive hardware encryption cannot be updated without replacing the microcontroller, which is costly and complicated

# Why Software? (continued)

- ▶ The libraries enable the product developer to put strong security into their embedded products and leverage specific functionality like encryption, decryption, random number generation, digital signatures and other utilities protocols to achieve **benefits such as confidentiality, authentication, integrity and non-repudiation**
- ▶ Customers will be able to take advantage of the **leading encryption software and support from NTRU.**
- ▶ The encryption libraries can be **updated on “installed” units** with In Application Programming

# Software advantages vs Hardware

- ▶ **Cost-effective:** cryptographic software doesn't require additional circuitry. The use of software encryption shortens design cycles, improves reliability, and lowers deployment costs
- ▶ **Battery lifetime:** cryptographic software runs on the main processor, unlike a hardware coprocessor which draws additional power. Use of software encryption extends battery lifetime.
- ▶ **Performance and Flexibility:** cryptographic software can match the performance of hardware encryption on some other MCUs and gives customers the flexibility to make changes on installed applications
- ▶ **Regulatory:** Government export control rules do not apply until the MCU is programmed with the encryption software

**The NTRU software + NXP ARM MCUs offers customers the first general purpose ARM with encryption, Ethernet, USB and other communication peripherals**



# Encryption suite components

The components of the suite are made up of :

- ▶ Hash algorithms
- ▶ Symmetric (secret key) encryption/decryption
- ▶ Asymmetric (public key) encryption/decryption

**Customers can choose the encryption components  
that best fit their applications requirements**

# Hash Algorithms

- ▶ Hash algorithms provide a cryptographically secure “fingerprint” of a message which is used to ensure its authenticity
- ▶ SHA-1: Secure Hash Algorithm
- ▶ MD5: Message Digest

# Random Number Generation

- ▶ A random number generator is used to generate keys and other random data.
  - ▶ Good random number generators are very important – without them an attacker could simply guess a key.
  - ▶ Also used inside many cryptographic schemes
- 
- ▶ X9.82: Random Number Generator

# Symmetric encryption/decryption

- ▶ Symmetric, or secret-key, algorithms involve encrypting and/or authenticating a message using a single secret key. Both the sender and receiver must know this key.
- ▶ The two key benefits provided by symmetric encryption/decryption are confidentiality and/or authenticity. Certain “modes of operation” of symmetric algorithms provide both of these benefits simultaneously.
- ▶ Symmetric algorithms are the best choice for protecting bulk data from exposure and modification.
- ▶ Symmetric algorithms include:
  - **AES**: Advanced Encryption Standard
  - **Triple-DES**: Triple Data Encryption Standard

# Asymmetric algorithms

- ▶ **Key Benefits:** Confidentiality (key management); Authentication (Digital Signatures)
- ▶ Lets two parties communicate securely even if they've never communicated before
- ▶ **Asymmetric algorithms are best suited for Key Management and Digital Signatures**
  - Key management protocols make it easy to agree on a symmetric key for bulk data protection
  - Digital signature protocols let users prove their identity over a network, even to someone who's never met them before.

Asymmetric algorithms are:

- ▶ **RSA:** Key agreement and digital signatures
- ▶ **DSA:** Digital signatures only
- ▶ **Diffie-Hellman:** Key agreement only

# Secure Systems

- ▶ Designing secure communications means making at least the three following choices:
  - Which algorithm you will use
  - What protocol you will use
  - How you will establish keys
- ▶ The correct solution will depend on the setting
  - Easy to get security wrong in subtle ways – important to have experienced security professionals involved in reviewing your design

# Flash sizes for each Library

| Library             | Bytes |
|---------------------|-------|
| SHA-1               | 2164  |
| MD5                 | 2756  |
| PRNG                | 2888  |
| TDES Core           | 4176  |
| AES Core            | 3448  |
| DH                  | 5128  |
| DSA                 | 7776  |
| RSA Encrypt/Decrypt | 6092  |
| RSA Sign/Verify     | 3224  |

# Throughputs

| Hash Algorithm       |                          |
|----------------------|--------------------------|
| Name                 | Throughput (kbytes /sec) |
| SHA-1                | 1915                     |
| MD5                  | 3516                     |
| Symmetric algorithms |                          |
| Name                 | Throughput (kbytes /sec) |
| AES-CBC              | 825                      |
| AES-ECB              | 874                      |
| AES-CCM, CT only     | 373                      |
| AES-CCM, AD only     | 816                      |
| 3DES-CBC             | 326                      |
| 3DES-CTR             | 317                      |
| 3DES-ECB             | 333                      |

CT = CipherText (encrypt + authenticate)

AD = Associated Data (authenticate only)

# Throughputs (continued)

| Asymmetric, Encrypt/Decrypt |            |
|-----------------------------|------------|
| Name                        | Time (sec) |
| RSA-1024 encrypt            | 0.01       |
| RSA-1024 decrypt            | 0.27       |
| RSA-2048 encrypt            | 0.05       |
| RSA-2048 decrypt            | 2.13       |

| Asymmetric, Sign/Verify |            |
|-------------------------|------------|
| Name                    | Time (sec) |
| RSA-1024 sign           | 0.27       |
| RSA-1024 verify         | 0.01       |
| RSA-2048 sign           | 2.13       |
| RSA-2048 verify         | 0.05       |
| DSA-1024 sign           | 0.17       |
| DSA-1024 verify         | 0.33       |

| Diffie-Hellman      |                         |            |
|---------------------|-------------------------|------------|
| Modulus Size (bits) | Private Key size (bits) | Time (sec) |
| 1024                | 160                     | 0.17       |
| 1024                | 1024                    | 1.08       |
| 2048                | 224                     | 0.93       |
| 2048                | 2048                    | 8.48       |

# About NTRU

- ▶ NTRU is a market leader providing comprehensive security products and services to businesses that wish to leverage the power of trusted computing and embedded security technologies
- ▶ NTRU's trusted computing and embedded security product suites are preferred by industry leaders in technology, consumer goods and telecommunications markets.
- ▶ The continued development of Strategic partnerships with industry leading software and hardware companies, enables NTRU to provide innovative security solutions to the PC, wireless and anti-counterfeiting marketplace.
- ▶ Headquartered in Acton, Mass, USA
- ▶ Sheila Walker, VP Business Development, 978-844-5204, [swalker@ntru.com](mailto:swalker@ntru.com)
- ▶ <http://www.ntru.com/index.htm>



# Frequently Asked Questions

- ▶ How much do the software algorithms cost?
  - Pricing depends on the number of algorithms, the number of units it is being installed into and other factors, but in general, the cost of a single HASH algorithm is less than \$0.05 per unit and the entire library is less than \$0.20 per unit, plus licensing fees.
- ▶ Are there licensing fees? If so, how much are they?
  - There is an evaluation license fee that is paid to NTRU. If you decide to purchase a production license, which costs a few thousand dollars, then the evaluation license fee is applied toward that cost.
- ▶ Do I purchase the software from NXP or from NTRU?
  - The software and licensing fees are paid directly to NTRU.
- ▶ How do I purchase the software?
  - The software can be ordered through the NTRU website ([www.ntru.com](http://www.ntru.com))
- ▶ How do I get support on the encryption software?
  - Support will come from NTRU. There will be a support area on the website ([www.ntru.com](http://www.ntru.com)) and email support will also be available for licensed customers.



# Frequently Asked Questions (continued)

- ▶ Am I able to run my application code while the encryption software is running?
  - Yes, but the throughput will decrease. The table shows the throughput (in Kbytes/sec or seconds) if it is the only application running. If you are running user code at the same time, then the time to execute the encryption library will increase.
- ▶ May I use the NTRU software with microcontrollers other than NXP's?
  - No, the software is licensed only to be used with NXP's ARM microcontrollers.
- ▶ Is this encryption software “unbreakable”?
  - The goal of the encryption is to make compromising it too expensive or time consuming to justify the effort. Since this encryption is meant for low-cost, embedded applications, it should provide protection to meet most customers' needs and is at the same level as hardware encryption in standard microcontrollers.