NTRU Cryptosystems Technical Report

Report # 007, Version 2
Title: Plaintext Awareness and the NTRU PKCS
Author: Joseph H. Silverman
Release Date: v1 July 1998; v2 June, 2000

Abstract. RSA and Bell Labs [2, 3] have recently announced a potential attack on certain public key protocols, along with several suggested countermeasures. The most secure of these countermeasures uses the concept of plaintext aware, which means that it should be infeasible to construct a valid ciphertext without knowing the corresponding plaintext. Failure to be plaintext aware may open a cryptosystem to various sorts of attacks. In this note we describe some potential attacks on the NTRU Public Key Cryptosystem (PKC) analogous to the attack described in [2, 3] and suggest the use of an OAEP digital envelope to eliminate the threat of such attacks.

Note for Technical Report #007 Version 2. The material on OAEP in this report has been superceded by NTRU Technical Report #016, "Protecting NTRU Against Chosen Ciphertext and Reaction Attacks," available at `www.ntru.com`. The report #016 describes a padding technique of Fujisaki and Okamoto that protects against chosen ciphertext attacks (CCA) and other attacks described in this note, against the reaction attacks described in NTRU Technical Note #015, and against the CCA described in "A chosen-ciphertext attack against NTRU," E. Jaulmes and A. Joux, *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, Springer-Verlag.

A cryptosystem is said to be *plaintext aware* if it is infeasible for an attacker to construct a valid ciphertext without knowing the corresponding plaintext. (For a more precise definition of this concept, see [4].) Failure to be plaintext aware may open the door to various sorts of attacks, such as Bleichenbacher's Adaptive Chosen Ciphertext Attack [2, 3] on RSA's Public Key Cryptography Standard #1 (PKCS #1). In this note we will construct several attacks on the NTRU Public Key Cryptosystem, including an adaptive chosen ciphertext attack similar to [2].

A number of countermeasures to Bleichenbacher-type attacks are described in [3], including:

- Frequent changes of key pair.
- Check messages more rigorously for format after decryption.
- Require the sender to demonstrate knowledge of the data before indicating whether the decryption was successful.

- If a message is rejected for any reason, the timing and format of the error message sent back to the sender should be the same.
- Add structure to the data (e.g., by including a hash of the data) to decrease the probability of a message being accepted.

All of these sensible countermeasures apply to any public key cryptosystem, including NTRU, and many of them require few changes in currently implemented digital envelopes and protocols, such as RSA's PKCS#1. With regard to the first countermeasure, we want to stress that an important feature of the NTRU PKC is the ease and speed of key creation. This makes NTRU the only current commercially viable public key cryptosystem which supports single use public/private key pairs; that is, public/private key pairs which are used for a single transaction or a single session and then discarded. For this reason alone, the NTRU PKC is to be preferred in many situations.

However, the most effective countermeasure to all of the attacks described in this note, and indeed to any attack which depends on counterfeiting valid ciphertexts, is the use of Optimal Asymmetric Encryption Padding (OAEP) [4]. This method of creating plaintext aware digital envelopes uses a mixing process in which every bit of the message affects and is affected by every bit of a pseudorandom component. It has been proposed by RSA that OAEP be adopted as a standard formatting scheme for public key algorithms, and RSA plans to include it as part of their PKCS#1 v2.† We fully support this proposal. In Section 4 we will describe how OAEP may be implemented for the NTRU PKC.

Throughout this note we will use the notation and description of the NTRU PKC given in [1]. The contents of this note are as follows:

§1. An Adaptive Chosen Ciphertext Attack
§2. A Correlation Attack Via Induced Wrapping Failure
§3. A Multiple Transmission Attack
§4. Optimal Asymmetric Encryption Padding for the NTRU PKC
§5. An Insecure Digital Envelope

§1. An Adaptive Chosen Ciphertext Attack

Plaintext is generally placed into a digital envelope before being encrypted. This digital envelope might contain some random padding to prevent similarity between messages, and some features which allow identification of valid messages. For example, the RSA Public Key Cryptosystem Standard #1 v1.5 [3] uses the format

$$0 \quad 0 \quad \| \quad 0 \quad 2 \quad \| \quad \text{PS} \quad \| \quad 0 \quad 0 \quad \| \quad \text{D},$$

† "While attacks of this kind [adaptive chosen ciphertext] have not been shown to affect other algorithms [other than RSA], it is widely believed that OAEP could provide additional security to other public-key algorithms as an enveloping format. The cryptographic community is aware of the potential of adaptive chosen ciphertext attacks and is working to prevent them. For this reason, OAEP has been proposed as a formatting scheme for other public-key algorithms, such as elliptic curve cryptography." [5]

where D is a data string (often a key) and PS is a pseudo-random padding string. Thus the first four bytes are 0002, and the padding string PS is separated from the data string D by two null bytes 00.

Bleichenbacher [2,3] has recently devised an adaptive chosen ciphertext attack on messages encrypted with the RSA PKC which use this, or any similar, digital envelope. In this section we will describe an attack on the NTRU PKC if messages are enclosed in an analogous digital envelope.

For simplicity, we will suppose that an NTRU plaintext block is formatted as

$$0 + 0 \cdot X + 0 \cdot X^2 + 2 \cdot X^3 + PS(X) + 0 \cdot X^k + 0 \cdot X^{k+1} + D(X),$$

where $PS(X)$ is a pseudo-random padding polynomial, and the polynomial $D(X)$ contains the data. This is similar to RSA PKCS#1 v1.5. As in Bleichenbacher's attack, we will further assume that a message is rejected if it does not have this form, and that an attacker is able to determine whether or not a message has been rejected.

Under these assumptions, an attacker takes an intercepted encrypted NTRU message e, chooses a random small polynomial ψ (i.e., with just a few coefficients equal to ± 1, and the rest 0), transmits the message

$$E = \psi * e \pmod q,$$

and observes whether or not it is accepted as valid. When E is decrypted, the underlying plaintext message will be $\psi * m \bmod p$, where m is the plaintext underlying e. Since a message is accepted if and only if six specific coefficients have specific values, the probability that E is accepted is p^{-6}. (For most implementations, $p = 3$.) Each time an E is accepted, the attacker gains 6 linear relations on the coefficients of the plaintext message m. Hence after some small multiple of p^6 transmissions, the attacker will be able to recover most or all of m.

Conclusion: It is inadvisable to accept or reject NTRU ciphertexts based solely on whether or not specific coefficients of the underlying plaintext have specific values. [However, for moderate security applications, it would be reasonable to accept/reject messages based on the value of K specific coefficients, especially if an attacker will not be allowed to send p^K encryptions.]

§2. A Correlation Attack Via Induced Wrapping Failure

A properly chosen set of NTRU parameters, such as those described in [1, §4.1], make it highly unlikely that decryption will ever fail due to the coefficients of $\phi * g + m * f$ spanning an interval of width larger than q. If this were ever to happen, we say that *wrapping failure* has occurred. In this section we describe an attack on the NTRU PKC based on wrapping failure if the attacker is able to determine (e.g., by timing methods) whether or not wrapping failure has occurred.

The attacker takes an intercepted encrypted NTRU message e, chooses a random polynomial ψ with small coefficients (say randomly chosen from $-1, 0, 1$ with a distribution similar to that of ϕ), transmits the message

$$E = e + \psi * h \pmod q,$$

and observes whether or not it is rejected due to wrapping failure. When E is being decrypted, the first step is to compute

$$a \equiv f * E \equiv p(\phi + \psi) * g + m * f \pmod q.$$

From this formula, we see that wrapping failure is much more likely if many of the 1 coefficients of ϕ match up with 1 coefficients of ψ, and similarly for the -1 coefficients. The attacker repeats this process a large number of times, and saves those values $\psi_1, \psi_2, \ldots, \psi_\nu$ which give wrapping failure. Then the average

$$\Psi = \frac{1}{\nu} \sum_{j=1}^{\nu} \psi_j$$

will be quite highly correlated with ϕ. More precisely, suppose that ϕ has d coefficients equal to each of 1 and -1, with the rest 0. Then the attacker forms a polynomial Φ by replacing the d largest coefficients of Ψ with 1's, the d smallest coefficients of Ψ with -1's, and setting the other coefficients equal to 0. Then ϕ and Φ will bear a close resemblance to one another, and the attacker can do a brute force search centered at Φ, possibly using the additional information that the larger (smaller) the coefficient of Ψ, the more likely it is that the corresponding coefficient of Φ is correct. Further, the attacker can make the process even more efficient by choosing the sample ψ's adaptively, based on which of the previous ψ's caused wrapping failure.

Note that it is easy for the attacker to determine if she has found the correct ϕ, since only the correct element of $\mathcal{L}_\phi$ will make the difference $e - \phi * h \bmod q$ into an element of $\mathcal{L}_m$. Finally, we remark that we have tested this method numerically and it works quite well, even in non-adaptive mode. For example, using the moderate security parameters in [1, §4.1], we found that 10,000 iterations produced several hundred wrapping failures, and from these we were generally able to correctly place at least 8 of the 10 non-zero coefficients of ϕ.

Conclusion: Messages should not be accepted/rejected based solely on wrapping failure; and those messages which are rejected due to wrapping failure should return the same error message in the same amount of time as messages rejected because they are incorrectly formatted.

§3. A Multiple Transmission Attack

If a single plaintext message is transmitted more than one time using the basic NTRU PKC scheme described in [1], then the message will be vulnerable to a

multiple transmission attack. (Other PKC's are also susceptible to such attacks, see for example [7].) We described such an attack in [6] and gave two simple solutions. Here we merely want to point out that the OAEP digital envelope described in the next section, and indeed any similar digital envelope with sufficient variability, will prevent such attacks.

Conclusion: Identical or similar messages should not be directly encrypted without some variability being introduced.

§4. Optimal Asymmetric Encryption Padding for the NTRU PKC

The material in this section has been superceded by NTRU Technical Report #016, "Protecting NTRU Against Chosen Ciphertext and Reaction Attacks," available at `www.ntru.com`, which describes a padding technique that protects against both adaptive chosen ciphertext attacks and reaction attacks.

§5. An Insecure Digital Envelope

In this section we show that even in its original formulation [1], an NTRU PKC message is automatically enclosed in a digital envelope, but we explain that use of this digital envelope as a means of message verification can lead to an easy attack on the message if the attacker is allowed to send a large number of messages and observe which ones are accepted as valid.

Briefly, Bob precomputes an inverse modulo q for the public key h, say,[†]

$$H_q * h \equiv 1 \pmod{q}.$$

Then to test if an encrypted message e and its decryption m are valid, he computes

$$H_q * (e - m) \pmod{q}. \tag{1}$$

If e is a valid ciphertext for the plaintext m, then the polynomial (1) will have small coefficients, and in fact, will lie in the sample space $\mathcal{L}_\phi$, since it will actually equal the ϕ used to perform the encryption. For example, using the sample spaces described in [1, §2.2], e and m are accepted if and only if the polynomial (1) has d coefficients equal to 1, d coefficients equal to -1, and the rest equal to 0. Thus the probability of a randomly chosen e being accepted as a valid message is $|\mathcal{L}_\phi|/q^N$. Even using the moderate security parameters $(N, p, q) = (107, 3, 64)$ and $\mathcal{L}_\phi = \mathcal{L}(5, 5)$ from [1], this probability is 2^{-589}.

However, this method of message verification opens the system to the following attack. The attacker takes an intercepted message e, chooses random values $0 \le j < k < N$, and sends the message

$$E = e + h * (X^j - X^k).$$

[†] The specific implementation of the NTRU PKC described in [1, §2.2] yields public keys h which are not invertible, but this is easily remedied by taking a slightly different sample space for g.

Notice that $E \equiv (\phi + X^j - X^k) * h + m \pmod q$. If we write (ϕ_j, ϕ_k) for the pair consisting of the j^{th} and k^{th} coefficients of ϕ, then there are nine possibilities for this pair as detailed in Table 2.

ϕ_j	-1	-1	-1	0	0	0	1	1	1
ϕ_k	-1	0	1	-1	0	1	-1	0	1
$\phi + X^j - X^k \in \mathcal{L}_\phi$?	NO	YES	NO	NO	NO	YES	NO	NO	NO

Table 2. Is $\phi + (X^j - X^k)$ in $\mathcal{L}_\phi = \mathcal{L}(d, d)$?

There is thus a $2/9$ probability that $e + h * (X^j - X^k)$ will be accepted as a valid ciphertext. We will assume that the attacker is able to find out which ciphertexts are accepted. Then by varying (j, k), she will rapidly uncover which pairs (ϕ_j, ϕ_k) equal one of $(-1, 0)$ or $(0, 1)$, which allows her to reconstruct much or all of ϕ. Finally, she recovers the encrypted message via $m \equiv e - \phi * h \pmod q$.

Conclusion: One should not use the digital envelope which tests if the quantity $H_q * (e - m) \bmod q$ is in the sample space $\mathcal{L}_\phi$.

References

[1] NTRU: A Ring-Based Public Key Cryptosystem, presented at ANTS 3 (Reed College,Portland, Oregon, June 21–25, 1998), to appear in Lecture Notes in Computer Science, Springer-Verlag.

[2] D. Bleichenbacher, Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1, *Advances in Cryptology — Crypto '98*, to appear

[3] D. Bleichenbacher, B. Kaliski, J. Staddon, Recent results on PKCS#1: RSA encryption standard, RSA Laboratories' Bulletin, Number 7, June 26, 1998.

[4] M. Bellare, P. Rogaway, Optimal asymmetric encryption, in *Advances in Cryptology — Eurocrypt '94,* A. de Santis (ed.), 92–111, Springer-Verlag, 1995.

[5] `www.rsa.com/rsalabs/`, RSA Laboritories, RSA Data Security, Inc.

[6] Jeffrey Hoffstein and Joseph H. Silverman, Implementation Notes for NTRU PKCS Multiple Transmissions, NTRU Cryptosystems Technical Report 006, May 26, 1998

[7] D. Coppersmith, M. Franklin, J. Patarin, M. Reiter, Low exponent RSA with related messages, in *Advances in Cryptology — Eurocrypt '96,* U. Maurer (ed.), 1–9, Springer-Verlag, 1996.

Comments and questions concerning this technical report should be addressed to

`techsupport@ntru.com`

Additional information concerning NTRU Cryptosystems and the NTRU Public Key Cryptosystem are available at

`www.ntru.com`
