Analysis and Improvements of NTRU Encryption Paddings

Phong Q. Nguyễn   David Pointcheval

CNRS/École normale supérieure

France

Aug. 20th, 2002

Summary

- NTRU Encryption
- Security Notions
- Analysis of NTRU Paddings
- Improved Paddings

Truncated polynomial rings

- Let $\mathcal{P}$ be the ring $\mathbb{Z}[X]/(X^N - 1)$ where N is a "small" prime: 251, 347 or 503 (previously: 167, 263 or 503).
  $\mathcal{P}$ is identified with the set of integer polynomials of degree $< N$.
- The multiplication $*$ in $\mathcal{P}$ is called the convolution product.
  Convolutions can easily be computed thanks to $X^N - 1$.
- The function $\mathsf{r} \mapsto \mathsf{r}(1)$ is a ring homomorphism from $\mathcal{P}$ to $\mathbb{Z}$, because 1 is a root of $X^N - 1$.
- For a and b in $\mathcal{P}$, we write $\mathsf{a} \equiv \mathsf{b} \pmod{p}$
  when the coefficients are pairwise congruent modulo p.

The NTRU Primitive (1996)

- Let $\mathcal{S}$ be a subset of sparse polynomials with coeffs 0 and ± 1.
  q is a small power of 2, typically 128.
  p is a small odd number, typically 3.
- Private key := f and g in $\mathcal{S}$ such that $\mathsf{f}(1) = 1$ and $\mathsf{g}(1) = 0$.
  The number of 0 and ± 1 is known for both f and g.
  f is chosen to be invertible mod p and q:
  $\mathsf{f} * \mathsf{f}_p \equiv 1 \pmod{p}$ and $\mathsf{f} * \mathsf{f}_q \equiv 1 \pmod{q}$.
- Public key $\mathsf{h} := \mathsf{g} * \mathsf{f}_q \pmod{q}$. Note that $\mathsf{f} * \mathsf{h} \equiv \mathsf{g} \pmod{q}$.

Encryption and Decryption

- A message m is an element of $\mathcal{P}$ with coeffs 0 or ± 1.
  m is encrypted into $\mathsf{e} := \mathsf{m} + p\mathsf{r} * \mathsf{h} \pmod{q}$ where $\mathsf{r} \in_R \mathcal{S}$.
- To decrypt e, notice that $\mathsf{e} * \mathsf{f} \equiv \mathsf{m} * \mathsf{f} + p\mathsf{r} * \mathsf{g} \pmod{q}$.
  If the reduction is centered, this "should" be an equality over $\mathcal{P}$.
  By taking residues modulo p and dividing by f, one recovers m.
- For the recommended parameters, the decryption may fail,
  but the failure probability seems to be negligible.
- Encryption and decryption cost $O(N^2 \ln q)$.
  Keysize is $O(N \ln q)$.

Modifications to NTRU (2000)

- Replace $p = 3$ by a small polynomial $p = X + 2$.
  Ternary polynomials become binary polynomials.
- Special form for sparse polynomials: $\mathsf{f}, \mathsf{g}, \mathsf{r}$.
  For instance, $\mathsf{r} = \mathsf{r}_1 * \mathsf{r}_2 + \mathsf{r}_3$.
- These changes improve the efficiency.
  But they may affect the security.

Security of NTRU

- The best attack known is based on lattice reduction [CoSh97]. It tries to recover the private key from the public key.
- The authors of NTRU claim that the attack is exponential in N, and that $N = 263$ is "at least as secure" as RSA-1024.
- However, "textbook" NTRU, like "textbook" RSA/El Gamal, is not "secure".

Security notions

- Security goals:

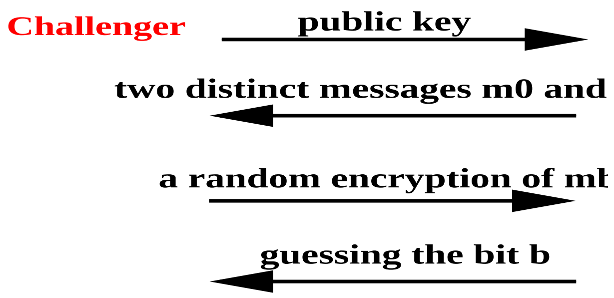
  One-wayness: intractability of decrypting a random ciphertext.

  Semantic security [GoMi84]: indistinguishability of ciphertexts.
- Security models:

  CPA: Chosen-plaintext attacks.

  CCA2 [RaSi91]: Adaptive chosen-ciphertext attacks.

IND-CPA


Challenger
public key
two distinct messages m0 and
a random encryption of mb
guessing the bit b

Security of the NTRU Primitive

- $\mathcal{E}(\mathsf{m};\mathsf{r}) := \mathsf{m} + p\mathsf{r} * \mathsf{h} \pmod q = \mathsf{e}$.
- No semantic security: $\mathsf{e}(1) \equiv \mathsf{m}(1) \pmod q$ because $\mathsf{r}(1) = 0$.
- Malleability: $X * \mathcal{E}(\mathsf{m};\mathsf{r}) = \mathcal{E}(X * \mathsf{m}; X * \mathsf{r})$.
- Though the primitive is probabilistic, there is a plaintext-checking oracle which can check whether e is an encryption of m, because h is "almost" invertible: one can compute $\mathsf{H} \in \mathcal{P}$ such that whenever $\mathsf{a}(1) \equiv 0 \pmod q$, $\mathsf{h} * \mathsf{H} * \mathsf{a} \equiv \mathsf{a} \pmod q$.
  Thus, $\mathsf{r} \equiv p^{-1}\mathsf{H} * (\mathsf{e} - \mathsf{m}) \pmod q$.

Chosen-ciphertext attacks

- Because $X * \mathcal{E}(\mathsf{m};\mathsf{r}) = \mathcal{E}(X * \mathsf{m}; X * \mathsf{r})$, there are chosen-ciphertext attacks that can decrypt any message (like RSA/El Gamal).
- [JaJo00] presented more powerful chosen-ciphertext attacks which can recover the private key (not like RSA/El Gamal).
  It worked against an "OAEP-like" padding proposed by NTRU.
- NTRU therefore proposed new paddings in 2000: Π_1, Π_2 and Π_3.
  All were claimed to bring IND-CCA2 security (in the ROM), but no "security proof" was provided.
  Π_3 is the NTRU proposal for the CEES standard.

Analysis of Padding I

- $\mathcal{E}_1(m; r) := \mathcal{E}'(m||r; H(m||r))$
  where $\mathcal{E}'(m'; r') = \mathcal{M}(m') + p * \mathsf{h} * \mathcal{R}(r') \pmod q$
  and r represents 40 to 80 bits of randomness.
- Based on the [FuOk99] conversion technique.
  But [FuOk99] requires an IND-CPA primitive!
- Π_1 is not semantically secure: $\mathcal{E}_1(m; r)(1) = \mathcal{M}(m||r)(1)$.
  Depending on the encoding $\mathcal{M}$, r is likely to be sufficiently small
  to allow us to distinguish encryption of special messages,
  such as $m_0 = 0^k$ and $m_1 = 1^k$.

One-wayness of Padding I

- $\mathcal{E}_1(m; r) := \mathcal{E}'(m||r; H(m||r))$
  where $\mathcal{E}'(m'; r') = \mathcal{M}(m') + p * \mathsf{h} * \mathcal{R}(r') \pmod q$
  and r represents 40 to 80 bits of randomness.
- The one-wayness of Π_1 is a stronger assumption
  than the one-wayness of the NTRU primitive.
  We call the corresponding problem
  the NTRU Partial-Information Inversion problem.

Analysis of Padding II

- $\mathcal{E}_2(m;r) := \mathcal{E}'((m \oplus F(r))||r; H(m||r))$
  where $\mathcal{E}'(m';r') = \mathcal{M}(m') + p * \mathsf{h} * \mathcal{R}(r') \pmod q$
  and r represents 40 to 80 bits of randomness.
- The one-wayness is equivalent to that of the NTRU primitive.
  The reduction is very tight.
- But IND-CCA2 is related to the NTRU Partial-Information Inversion assumption.
  The reduction advantage is linear in the number of hash queries.

Analysis of Padding III

- $\mathcal{E}_3(m;r) := \mathcal{E}'(m_1||m_2; H(m||r))$
  where $\mathcal{E}'(m';r') = \mathcal{M}(m') + p * \mathsf{h} * \mathcal{R}(r') \pmod q$
  and r represents 40 to 80 bits of randomness.
- Based on an all-or-nothing transformation (OAEP).
  Halve $m = \overline{m}||\underline{m}$ and $r = \overline{r}||\underline{r}$.
  Let $m_1 = (\overline{m}||\overline{r}) \oplus F(\underline{m}||\underline{r})$ and $m_2 = (\underline{m}||\underline{r}) \oplus G(m_1)$.
- The one-wayness is equivalent to that of the NTRU primitive.
- But IND-CCA2 is related to the NTRU Partial-Information Inversion assumption with “bad” parameters.

An Improvement of Padding III

- $\mathcal{E}'_3(m; r) := \mathcal{E}'(s||t; H(m||r))$
  where $s = m \oplus G(r)$ and $t = r \oplus F(s)$.
- One can prove $\textsf{IND-CCA2}$ security under the basic NTRU assumption.
  - The OAEP construction provides semantic security,
  - The hash function $H()$ adds chosen-ciphertext security.
  - But the reduction is quadratic in the number of hash queries, because of the OAEP construction.

An Improvement of REACT [OkPo01]

- We use a symmetric encryption scheme (E, D).
- $\mathcal{E}_4(m; r) := \mathcal{E}'(r; H(r, b))||b$
  where $b = \mathsf{E}_K(m)$ and $K = G(r)$.
- It provides $\textsf{IND-CCA2}$ under the basic NTRU assumption.
  The reduction is linear in the number of hash queries.
  Reduces the amount of randomness of the generic REACT, by re-using the hash value.

Conclusion

- None of the NTRU paddings Π_1, Π_2 and Π_3 should be used:
  - Π_1 is not semantically secure.
  - Π_2 and Π_3 require a stronger assumption for IND-CCA2 than the basic NTRU assumption.
    The reduction is not tight.
- There exist efficient alternatives with
  a better security assumption and a tighter security proof.
- All NTRU paddings known use the random oracle model.