International Journal of Theoretical & Applied Sciences, **1**(2)**:** 56-59(2009) **ISSN : 0975-1718**

On NTRU cryptosystem and L^3 algorithm : A problem

Sunder Lal, Santosh Kumar Yadav* and Kuldeep Bhardwaj**

Professor and Pro-Vice Chancellor, Dr. B.R. Ambedkar University Agra INDIA
**Dept. of Mathematics, Kalindi College University of Delhi, Delhi INDIA*
***Dr. B.R. Ambedkar University Agra INDIA*

ABSTRACT : The description of NTRU cryptosystem is entirely given in terms of quotient rings of integer polynomials. The L^3 algorithm guarantees that the first vector of the reduced basis is within a factor of the length of the shortest vector in the lattice. If one has a lattice where the second shortest vector is more then the first factor times as long as the shortest vector then the L^3 algorithm must return the shortest vector.

Keywords : NTRU Cryptosystem, L^3 Algorithm, Lattice, Circular Convolution, CGH challenges, Key Generation

INTRODUCTION

The first version of the NTRU cryptosystem was proposed by Hoffstein [7] in 1996. The basic collection of objects used by the NTRU Public Key Cryptosystem is the ring **R**. A full implementation of the NTRU Public Key Cryptosystem is specified by a number of parameters. However, for the purposes of this overview we'll concentrate on the three most important:

- N the polynomials in the truncated polynomial ring have degree N-1.
- q large modulus: usually, the coefficients of the truncated polynomials will be reduced mod q.
- p small modulus. As the final step in decryption, the coefficients of the message are reduced mod p.

To ensure security, it is essential that p and q have no common factors. The following table gives some possible values for NTRU parameters at various security levels.

	N	***q***	***p***
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

These values are provided to give us some idea of the quantities used in commercial applications.

All computations are performed in the Ring $R = Z_q[x]/(x^n - 1)$, where Z_q denotes the integers modulo q. This has the practical advantage that an element $a_0 + a_1x + ... + a_{n-1}x^{n-1}$ of R can be represented as an n-tuple of integers $[a_0, a_1, ..., a_{n-1}]$. Using this representation, addition in R is performed componentwise, and multiplication (which we will denote by $*$) is a circular convolution :

$$a*b = \sum_{k=0}^{n-1}\left(\sum_{\substack{i+j=k \\ \bmod n}} a_i b_j\right)$$

It is difficult to find a Minkowski reduced basis for a lattice. For small dimension this is tractable problem in NTRU. An approximation algorithm finds a reasonable reduced basis in polynomial time.

KEY GENERATION

Let $L(a,b) \overset{def}{=\!=} \{f \in R | f$ has a coeffs. equal to 1, b coeffs. equal to -1 and all other coeffs. equal to $0\}$

Let d_f be an integer less than $n/2$. Then the private key f is a random element of $L(d_f, d_f - 1)$. For reasons that will soon be clear, we also require that f be invertible in R, *i.e.*, $f \in R^*$, and that f be invertible when considered modulo $p \overset{def}{=\!=} 3$.

Similarly, let d_g be an integer less than $n/2$ and randomly choose $g \underline{R} L(d_g, d_g)$. The public key will be $h \overset{def}{=\!=} f^{-1} * g$. The security of the crypotosystem will rely on the assumption that it is infeasible, given $h = f^{-1} * g$, to find a $f' \in R^{\times}$ and $g' \in R$ satisfying $h = f'^{-1} g'$.

The following algorithm computes an L^3 reduced basis for $L = BZ^n$ within polynomially many iterations.

$L^3\left(\vec{b}_1, ..., \vec{b}_m\right)$

Compute the Gram-Schmidt orthogonal basis $\vec{b}_1^*, ..., \vec{b}_m^*$;

$B_i = \left\|\vec{b}_m^*\right\|^2$;

$k = 2$;

WHILE $k \leq m$ DO

IF $\left|\mu_{k,k-1}\right| > \frac{1}{2}$ THEN SIZEREDUCE (k);

IF $\left\|\overset{r}{b}^{*}_{k} + \mu_{k,k-1}\overset{r}{b}^{*}_{k-1}\right\|^2 < \frac{3}{4}\left\|\overset{r}{b}^{*}_{k-1}\right\|^2$ THEN

SWAP (k);

IF $k > 2$ THEN $k = k - 1$;

ELSE

$k = k + 1$;

END IF

END WHILE

END L^3

ENCRYPTION/DECRYPTION

To encrypt a message $m \in \left\{-\frac{p-1}{2},...,\frac{p-1}{2}\right\}^n \subseteq R$, we randomly choose $\phi \underline{R} L(d_\phi, d_\phi)$, and compute the ciphertext :

$$c = p.(\phi * h) + m$$

To decrypt the ciphertext, we first compute

$$f * c = p.(\phi * g) + f * m$$

We have chosen the parameters d_f, d_g, d_f and d_m such that, with high probability, the coefficients of $p.(\phi * g) + f * m$ (*mod* $x^n - 1$) are between $-q/2$ and $q/2$ (before reducing modulo q). In this case, if we "center" $f * c = p.(\phi * g) + f * m$ (*mod* q), by choosing its coefficients between $-q/2$ and $q/2$, and then reduce modulo p we obtain $f * m$ (*mod* p), with only a small probability of error. We can recall that f was required to be invertible in $Z_p[x]/(x^n - 1)$, and call this inverse f_p^{-1}. Finally, if we apply f_p^{-1} and take the result modulo p, we obtain m (*mod* p), and since all coefficients of m are in $\left\{-\frac{p-1}{2},...,\frac{p-1}{2}\right\}$, this allows us to recover m.

In the above decryption procedure, we assumed that d_f, d_g and d_f were such that the coefficients of $p.(\phi * g) + fm$ (*mod* x^h-*1*) are between $-q/2$ and $q/2$ with high probability. While it is possible to find appropriate of d_f, d_g, d_f and d_m using elementary methods from probability theory.

CRYPTOGRAPHY

We consider $p \,.\, h$ as a linear map (*i.e.*, an $n \times n$ matrix over Z_q) acting on f considered as an n-dimensional vector in $\{-1, 0, 1\}^n \subseteq Z_q^n$, then the encryption process can be thought of as perturbing the "lattice point" ($p.h$) * ϕ by m. Thus, given a ciphertext c, the "closest" point to c of the form ($p.h$), is likely to be at a distance m from the ciphertext. However, the attacks we shall consider are to recover a decryption key f' given the public key h and consider a different, albeit related lattice construction [2].

Let $H \in Z_q^{n \times n}$ be the matrix corresponding to the linear map $a \mapsto h * a$ in R, and note that $H = F^{-1} G$ where F and G are the linear maps $a \mapsto f * a$, respectively. Now consider the $2n$-dimensinal Coppersmith-Shamir lattice, $\mathcal{L}^{CS}$, and $a \mapsto g * a$ generated by the columns of

$$\mathcal{L}^{CS} \overset{def}{=\!=} \begin{bmatrix} I & 0 \\ H & qI \end{bmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ \hline h_0 & h_{n-1} & \cdots & h_1 & q & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & h_2 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & h_{n-2} & \cdots & h_0 & 0 & 0 & \cdots & q \end{array}\right)$$

Let $\vec{u} = f' \,O\, g'$ be a shortest vector in $\mathcal{L}^{CS}$ and let $\sigma \in S_n$ be the cyclic permutation $[a_1, a_2, ..., a_n] \mapsto [a_n, a_1, ..., a_{n-1}]$. It is not hard to see, from the cyclic structure of $\mathcal{L}^{CS}$, that

$\sigma^k (f') \,O\, \sigma^k (g') \in \mathcal{L}^{CS}$ for all $0 \leq k < n$, and that all these vectors have the same norm. This is the situation we wish to avoid, however, since this means that $\frac{\lambda_2}{\lambda_1} = 1$. Therefore, we consider the lattice generated by the following variant of $\mathcal{L}^{CS}$

$$L'(\theta) \overset{def}{=\!=} \left(\begin{array}{ccc|ccccc} 1 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline \theta.h_0 & \cdots & \theta.h_1 & \theta.q & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ \theta.h_{-1} & \cdots & \theta.h_1 & 0 & \cdots & \theta.q & 0 & \cdots & 0 \\ h_1 & \cdots & h_{r+1} & 0 & \cdots & 0 & q & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ h_{n-1} & \cdots & h_0 & 0 & \cdots & 0 & 0 & \cdots & q \end{array}\right)$$

$L^r(\theta)$ is obtained by taking $\mathcal{L}^{CS}$ and then multiplying rows $n + 1$ though $n + r$ by $\theta \stackrel{def}{=\!=} q+1$. This has the effect of lengthening all vectors whose $n + 1$ through $n + r$ coefficients are not all zero. The hope is that g' will have a unique "run" of r zeros, *i.e.*, that there is exactly one index $i \in [1, 2,..., n]$ such that $g'_i = g'_{i+1} = ... = g'_{i+r-1} = 0$. If this is the case, then all of the rotations $\sigma^k(f')$o $\sigma^k(g')$ will be lengthened to have length at least

$\sqrt{2d_f - 1 + (q+1)^2 + 2d_g - r}$, except for one of them which will still have length $\sqrt{2d_f - 1 + 2d_g}$.

AN IMPORTANT THEOREM

Statement. *Let f o $g \in Z_q^{2n}$ denote the concatenation of f and g as vectors in Z_q^n. Then f o $g \in L^{CS} Z^n$.*

Proof. We consider f and g as a vectors in $\{0,..., q - 1\}^n$. Similarly, consider the linear map $H : R \to R$ defined by $a \mapsto h * a$. H can be thought of as a matrix in $Z_q^{n \times n}$, or equivalently as a matrix with entries in $\{0, ..., q - 1\}$. Then $Hf = g + q\vec{v}$, where $\vec{v} \in Z^n$. Therefore, we have that $C(f + (-\vec{u})) = f$ o g is in $\mathcal{L}^{CS} = L^{CS}Z^n$.

From the above theorem, the general method of attach should be clear.

Since f and g are small coefficients by construction, we expect f o g to be a short vector in the lattice L^{CS}. Indeed, this attack, introduced by Coppersmith and Shamir, was the first main attack against the earliest version of NTRU. In light of this attack, the security parameters (n, d_f, d_g, d_ϕ) were adjusted, a part of the justification of the security of the NTRU cryptosystem is that the parameters were chosen to make such an attack infeasible using contemporary lattice reduction techniques.

RESULTS

In NTRU cryptosystem the L^3 algorithm guarantees that the first vector of the reduced basis is within a factor of $2^{\frac{n-1}{2}}$ of the length of the shortest vector in the lattice. Therefore, if one has a lattice where the second shortest vector is more than $2^{\frac{n-1}{2}}$ times as long as the shortest vector, then the L^3 algorithm must return the shortest vector. This case is rather extreme since $2^{\frac{n-1}{2}}$ is very large, even for moderate values of n. However, a similar effect is noticeable for more reasonable lattices. If we denote by λ_1 the length of the shortest non-zero lattice vector, call it $\vec{v}$, then empirically, the quality of the basis returned by lattice reduction algorithms appears to improve as the quantity λ_2/λ_1 gets larger. Therefore, one might try to artificially augment the "gap" between the shortest vector and the second shortest vector is order to obtain shorter vector via lattice reduction.

CONCLUSION AND FUTURE TRENDS

More recently, NTRU cryptosystems have proposed a new variant where p is actually chosen to be a small polynomial that is relatively prime to $x^n - 1$ (instead of a small integer relatively prime to q). This requires several other modifications to the encryption and decryption procedures, but much of the structure is the same. The result shows that the shortest vector in a lattice cannot be approximated within the factor of v_2, whereas the L^3 algorithm only guarantees an exponentially large approximation factor. Some bounds leave open the question of whether a polynomial approximation to the shortest vector can achieved in polynomial time, and if so, how shall the degree of the approximation factor can be. The resilience of the current version of the NTRU cryptosystem and the theoretical significance of results such as the Ajtai-Dwork security proof and Micciancio's inapproximability result offer hope that the intractability of lattice reduction may ultimately provide alternative to the assumptions that integer factorization and the discrete logarithm problem are intractable.

REFERENCES

[1] Henri Cohen. *A Course in Computational Algebraic Number Theory. Springer*, (1993).

[2] B. Chor and R.L. Rivest. A knapsack-type public-key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, **5**(34)**:** 901-909(1988).

[3] . . . . . NTRU. In *Proceedings Eurocrypt' 97*, volume LNCS, pages 52-61. Springer-Verlag, (1997).

[4] Cynthia Dwork, Stanford university cs359: Lattices and their applications to cryptography and cryptanalysis (lecture notes: http:// theory.stanford.edu/csilvers/cs359/).

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT **30**(4)**:** 469-72July(1985).

[6] Oded Goldreich and Shafi Goldwasser. On the limits of non-approximability of lattice problems. *Electronic*

Colloquium on Computational Complexity (ECCC), **4**(031)**:** (1997).

[7] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory*, pages 267-288(1998).

[8] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. http://www.ntru.com.

[9] Antoine Joux and Jacques Stern. Lattice reduction: A toolbox for the cryptanalyst. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, **11**(3)**:** 161-185 Summer (1998).

[10] A. May. Cryptanalysis of NTRU, (1999).

[11] Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. In *IEEE Symposium on Foundations of Computer Science*, pages 92-98(1998).

[12] Alexander May and Joseph H. Silverman. Dimension reduction methods for convolution modular lattices. In *CALC*, pages 110-125(2001).

[13] Phong Nguyen and Jacques Stern. Cryptanalysis of the Ajtai-Dwork Cryptosystem. In *CRYPTO*, pages 223-242(1998).