CTRU, a polynomial analogue of NTRU

Philippe Gaborit, Julien Ohler, Patrick Solé

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

CTRU, a polynomial analogue of NTRU

Philippe Gaborit — Julien Ohler — Patrick Solé

N° 4621

November 2002

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4621--FR+ENG

INRIA
SOPHIA ANTIPOLIS

CTRU, a polynomial analogue of NTRU

Philippe Gaborit* , Julien Ohler† , Patrick Solé‡

Thème 2 — Génie logiciel
et calcul symbolique
Projet Café

Rapport de recherche n° 4621 — November 2002 — 12 pages

Abstract: CTRU, a new public-key cryptosystem is introduced. In this analogue of NTRU, the ring of integers is replaced by the ring of polynomials in one variable over a finite field. Attacks based on either the LLL algorithm or the Chinese Remainder Theorem are avoided. An important tool of cryptanalysis is the Popov normal form of matrices with polynomial entries. The speed of encryption/decryption of CTRU is the same as NTRU for the same value of N. An implementation in Aldor is described.

Key-words: Cryptography, NTRU, Popov normal form, Varshamov Gilbert bound

* LACO,Université de Limoges, 123 rue Albert Thomas, 87 000 Limoges, France gaborit@unilim.fr
† INRIA – Projet Café, 2004, Route des Lucioles B.P. 93 F-06902 Sophia Antipolis Cedex France
‡ CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France, ps@essi.fr

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : +33 4 92 38 77 77 —Télécopie : +33 4 92 38 77 65

CTRU, un analogue polynomial de NTRU

Résumé : Nous introduisons CTRU, un nouveau système de cryptographie à clé publique. Dans cet analogue à NTRU, l'anneau des entiers est remplacé par l'anneau des polynômes univariés à coefficients dans un corps fini. Nous évitons ainsi les attaques basées sur l'algorithme LLL ou bien le théor'eme du reste chinois. Un outil important de cryptanalyse de CTRU est la forme normale de Popov des matrices à coefficients polynomiaux. La vitesse d'encryption et de décryption de CTRU est la même que celle de NTRU pour les mêmes valeurs de N. Nous décrivons aussi une implémentation en ALDOR.

Mots-clés : Cryptographie, NTRU, forme normale de Popov, borne de Varshamov Gilbert

1 Introduction

Since 1996, a new Public Key Cryptosystem of industrial relevance has been developed [15]. Its name NTRU (pronounced "ain't true") indicates the use of number theory and rings.Its security is based on the hardness of the short vector problem for some special lattices. Its strong points are short key size, and speed of encryption and decryption, two assets of crucial importance in embarked applications like hand held devices and wireless systems. It has been assessed recently as the fastest Public Key Cryptosystem [8]. On the negative side we note a sensitivity to lattice reduction attacks [4] and Chinese Remainder Theorem (CRT) attacks [5]. There is no formal proof in print for the validity of decryption [6, §2.3]. In the present work we derive a polynomial analogue of NTRU hereby denoted by CTRU (pronounced "See true"). Roughly speaking the role played by $\mathbb{Z}$ in NTRU isplayed by the ring $\mathbb{F}_2[T]$ of polynomials in one variable T over the binary finite field $\mathbb{F}_2$. The role of the LLL algorithm is played by the Popov form from linear system theory [12]. CRT attacks are not to be feared in view of the non-simplicity of the roots of $X^N - 1$ over a finite field. The proof of validity of decryption is a simple and rigorous degree argument.

The correspondence is organized in the following way. The next section describes how the system operates: the relation between public and secret keys and the encryption and decryption procedures. Section III gives a brief tutorial on Popov normal form and describes two attacks: on the secret key and on an arbitrary message. A coding theoretic model is of some interest there. Section IV describe the parameters choice an user has to make. Section V is devoted to numerics. Section VI compares the complexity of implementation of $CTRU$ with that of $NTRU$.

2 Description of Operation

2.1 Notations

A CTRU cryptosystem depends on an integer N and on two irreducible polynomials P, Q of $A := \mathbb{F}_2[T]$. We shall assume that P and Q are polynomials of respective degrees s and m with $2 \leq s \leq m$, and, last but not least $GCD(m, s) = 1$. We work in the ring $R := A[X]/(X^N - 1)$, of "truncated polynomials with polynomial coefficients". The reader already familiar with NTRU might want to keep in mind the following dictionary.

NTRU	CTRU
$\mathbb{Z}$	A
p	P
q	Q
$\log_2(p)$	s
$\log_2(q)$	m
$\mathbb{Z}[X]/(X^N - 1)$	$A[X]/(X^N - 1)$
$\|\ \|$	$deg(\ )$
$\|\ \|_\infty$	$\|\ \|$

The last two lines will be explained in the Encryption section, and the Popov form subsection, respectively. Observe that the quotients rings A_P and A_Q of A by the ideals (P) and (Q) respectively are the finite fields $\mathbb{F}_{2^s}$ and $\mathbb{F}_{2^m}$. We denote by R_P, R_Q the quotient rings of R by the ideals (P) and (Q) respectively. By the arithmetic constraint $GCD(m,s) = 1$ we see that $\mathbb{F}_{2^s} \bigcap \mathbb{F}_{2^m} = \mathbb{F}_2$. Like in NTRU independence of reduction mod (P) and (Q) is essential to avoid trivial attacks. By $\deg(F)$ we shall denote the degree of F *as a polynomial in* T Like for NTRU we need to define some auxiliary sets of polynomials.

Let

$$L(d) := \{F \in R |\ \deg(F) < d\}$$

be defined for any integers $d \leq m$. Its size is 2^{Nd}. First define the message space $\mathbf{M}$ as $L(N,s)$. Its size is 2^{Ns}. Next we define the sets where the secret key (f,g) and the randomizer ϕ are sampled from.

Let d_f, d_g, d_ϕ be integers $\leq m$. With these notations we define

$$L_f := L(d_f + 1),\ L_g := L(d_g + 1),\ L_\phi := L(d_{\phi+1})$$

2.2 Key Creation

To create a CTRU key two arbitrary polynomials f, g are picked in, respectively, L_f and L_g. Assume further that f is invertible in R_P and R_Q. This means that $f \pmod P$ (resp. $f \pmod Q$) does not belong to some small cyclic code over A_P (resp. A_Q), which is not too restrictive. Indeed, a simple computation, based on the CRT in the ring R_P shows that the proportion of invertible f in that ring is at least $(1 - \frac{1}{2^s})^N$. A similar result holds for R_Q.

The **secret key** is the pair (f,g). Thus the secret key is an element of $\mathbb{F}_{2^{d_f}}^N \times \mathbb{F}_{2^{d_g}}^N$ that is at most $(d_f + d_g)N$ bits. The **public key** is then

$$h := g/f \pmod{(X^N - 1, Q)}.$$

Thus the public key is an element of $\mathbb{F}_{2^m}^N$ that is an order of size of mN bits .

2.3 Encryption and Decryption

Like NTRU, the encryption in CTRU is probabilistic: given the same private key the same plaintext will be encrypted differently at different times. If Emma the encrypter wishes to send a plaintext $\mathcal{M} \in \mathbf{M}$ to Dennis the decrypter she transmits on a public channel the quantity

$$e := P\phi h + \mathcal{M} \pmod Q,$$

where h is Dennis' public key and ϕ random in L_ϕ. Upon reception Dennis computes

$$ef \equiv P\phi g + \mathcal{M}f \pmod Q.$$

Provided that $s + d_\phi + d_g < m$ and $s + d_f < m$ simultaneously hold Dennis can regard ef as a polynomial of R. Dennis can therefore legitimately reduce $ef \pmod P$ getting $\mathcal{M}f \pmod P$ and by inversion of $f \pmod P$ the plaintext $\mathcal{M}$.

For future use we decide to choose the values

$$d_f = m - s - 1,\ d_g = d_\phi = \lfloor \frac{m - s - 1}{2} \rfloor$$

which satisfy the above two requirements.

We emphasize the analogy with NTRU where the role of the degree in T of polynomials is played by the absolute value of integers. Since integers are more complicated objects than polynomials (which are carry-free!) the simple and *rigorous* argument above has to be replaced there by arguments based on the so-called quasi-multiplicativity of the euclidean norm, an *approximation* which can justified by the Khinchine inequality from probability theory [16] or the semi-empirical Coppersmith bound of [6].

3 Security Analysis

In [6] four different kinds of attacks are given. Given the similarity of structure of the two cryptosystems, the first three attacks are mainly identical and the fourth attack based on lattices is turned into an attack through the Popov normal form of a polynomial matrix.

3.1 Brute force attack

In the case of a brute force attack an attacker may want to try all possible choices for f and try to find if fh has entries of small degree. By analogy the same attack can also be done against a given message by testing all possible ϕ and searching for $e - \phi h \pmod{Q}$ has coefficients of small degree. Therefore the key security is $\#L_g$ and the message security is $\#L_\phi$. Hence as for NTRU using the *meet-in-the-middle* attack one has to take the square root.

3.2 Meet-in-the-middle attack

A *meet-in-the-middle* attack was proposed by Odlyzko for NTRU and developped by Silverman in [19]. This attack can also be used against this cryptosystem using the same argument on the degree of the polynomials. This attack needs a lot of storage capacity and cut the search time by the usual square root. Hence it means that the set of possible g and ϕ has to contain at least 2^{160} elements in order to obtain a security of 2^{80}.

3.3 Multiple transmission attacks

If Amanda sends a single message m with different ϕ's but the same public key it is then possible to obtain information on the ϕ's. Suppose she sends different encrypted messages e_i, then computing $(e_i - e_1)h \pmod{Q}$, one obtains exactly the value of $\phi_1 - \phi_i$, repeating this operation with the different e_i leads to sufficient information for some coordinates of ϕ_1 to allow a brute force attack on the remaining coordinates.

3.4 Popov Normal form

Let F be a field and M an r by c matrix with entries in $F[T]$ where T is an undeterminate. We are interested in the $F[T]-$module L spanned by the rows of M. With every vector z of length c over $F[T]$ we attach its *sup norm* say $|z|$ defined as the largest degree in T of its entries. Formally

$$|z| = \max\{deg_T(z_i(T)) \mid i = 1, \cdots, c\}$$

There exists an effective algorithm of polynomial complexity to compute the minimum of the sup norm $|z|$ of $z \neq 0$ over $z \in L$. To describe this procedure we need the notion of (weak) **Popov form** for the matrix M. Define first the *pivot index* I_i attached to row i to be $= 0$ if the row i of M is zero and as the rightmost column index j such that $m_{i,j}$ has the largest degree in T for $j \leq c$. Next we say that M in weak Popov form if distinct rows are alloted distinct pivot indices. We can now quote [12, Lemma 8.1]

Lemma 3.1 *(Mulders & Storjohann) Let M be in weak Popov form and ρ the smallest sup norm of a row of M. All vectors in the $F[T]$-span of the rows of M have sup norm at least ρ.*

According to [12, Theorem 2.2] the complexity of computing the weak Popov form is $O(rcRd^2)$ field operations, with R being the $F-$rank of $M$and d a best upper bound of the degrees of the entries of M.

3.5 Attack on a public key

The private key (f, g) viewed here as a vector of length $2N$ over $\mathbb{F}_2[T]$ belongs to the lattice L_h of dimension and rank N given by

$$L_h := \{(f', g') \in \mathbb{F}_2[T]^{2N} \mid f'h \equiv g' \pmod{X^N - 1}\}$$

Let H denote the circulant matrix with first row the coefficients of the Taylor series in X of h. The lattice L_h is the $\mathbb{F}_2[T]$ span of the rows of the matrix M_h defined as

$$M_h = \begin{pmatrix} I_N & H \\ 0 & Q(T)I_N \end{pmatrix}.$$

Using the algorithm in [12] we can compute the minimum μ_h of L_h for the sup norm. If both $\mu_h \leq d_f$ and $\mu_h \leq d_g$ hold then the vector of sup norm μ_h will be a **spurious key** in the sense of [6]. Essentially, this means that such a key would allow an easvesdropper to read *any* message originated by a certain user. If, on the contrary,

$$d_g < \mu_h \leq d_f$$

then the Popov normal form will be unable to break the system.

To estimate μ_h we shall use the following *coding theoretic model.* The ambient metric space will be then the vector space P_d of polynomials of $\mathbb{F}_2[T]$ of degree $< d$. For technical

reasons , we shall assume $d >> m$. The metric will be the sup norm and the code the lattice L_h, intersected with P_d. Then the ball of radius $r-1$ will be P_r^{2n}. An elementary counting argument shows that $|P_d^{2n}| = 2^{2dN}$, and that, similarly, $|P_d^{2n}| = 2^{2rN}$. By considering the special form of the matrix M_h we see that $|P_d^{2n} \bigcap L_h| = 2^{2Nd-mN}$. We can then use the general principle in coding theory that most codes are on the Gilbert Varshamov bound (A rigorous version for the Hamming metric is in [2, Lemma 3.3]). The approximate equality

$$|P_d^{2n}| \cong |P_r^{2n}||P_d^{2n} \bigcap L_h|,$$

leads then to the estimate

$$\mu_h \cong \frac{m}{2}.$$

Going back to the expression for d_f we see that the condition $\mu_h \leq d_f$ can be rewritten as $2s \leq m$. Numerical experiments in Aldor show that the attack is ineffective for given N in the range

$$s_0(N) \leq s \leq 0.4\, m,$$

with $s_0(N)$ small (≤ 3). For purpose of choice of parameters we will therefore choose $s \cong \frac{m}{4}$.

3.6 A decision problem

The security of NTRU relies on a special instance of the SVP problem for lattices. In this section we give an analogue decision problem for CTRU, which we call the shortest pair of vectors problem (SPVP).

Instance: Let A_1 and A_2 denote two matrices, of, respectively, $\mathbb{F}_2[T]^{r\times c1}$ and $\mathbb{F}_2[T]^{r\times c2}$, and d_1, d_2 two integers. Let D be a best upper bound on the degree in T of the entries of both matrices.

Question: Is there an $u \in \mathbb{F}_2[T]^r$ such that both $|u^t A_1| \leq d_1$ and $|u^t A_2| \leq d_2$ hold?

Note that, if $d_1 = d_2$ then the Popov normal reduction algorithm finds a solution in polynomial time.

If, on the other hand, $d_1 \neq d_2$ then we know of no algorithm to solve that problem.

So, we can say that the security of CTRU relies on a special instance of the SPVP problem.

4 Parameter selection

4.1 Choice of N

For NTRU the integer N had to be taken prime in view of Gentry's attack [5]. This attack relied on the factorization

$$X^N - 1 = G(X)(X^d - 1)$$

for some factor d of N, and on the Chinese Remainder Theorem (CRT) applied to the coprime and comaximal ideals (G) and $(X^d - 1)$. This attack does not extend trivially to

the finite field set-up in view of multiple roots of $X^N - 1$ (for even N) which yield common factors of G and $X^d - 1$. To give but an extreme example of this situation over $\mathbb{F}_2$ we have the factorization

$$X^{2^m} - 1 = (X-1)^{2^m}$$

for all $m \geq 1$.

4.2 Degree parameters

To adjust the degree parameters d_f, d_g, d_ϕ we compute from §2.3 the size in bits of several relevant quantities: secret and public key, plain and cipher text.

variable	size (bits)
(f, g)	$\frac{3}{2}(m-s)N$
h	Nm
$\mathcal{M}$	Ns
e	Nm

There is therefore a message expansion of m/s. This should not be a problem if the system is used in conjunction with a symmetric cipher, merely to exchange keys.

4.3 Recommended Parameters

We define three levels of security: moderate, high and very high corresponding to different parameters, we also give the supposed security which relies especially on the meet-in-the-middle attack of the previous section since the Popov normal form attack cannot be applied with the parameters we choose.

Moderate Security Parameters (CTRU-32): $N = 32$, $m = 32$, $s = 7$.
Private Key: 1200 bits, Public Key: 1024 bits
Key security : 2^{200}, Message security : 2^{200}.

High Security Parameters (CTRU-64): $N = 64$, $m = 32$, $s = 7$.
Private Key: 2400 bits, Public Key: 2048 bits
Key security : 2^{400}, Message security : 2^{400}.

Very High Security Parameters (CTRU-128): $N = 128$, $m = 32$, $s = 7$.
Private Key: 4800 bits, Public Key: 4096 bits
Key security : 2^{800}, Message security : 2^{800}.

5 Performance Analysis

5.1 Complexity of Implementation

The first system CTRU should be compared to is NTRU. Keeping in mind the dictionary of §2.1 we see that the complexity of CTRU in terms of binary operations is the complexity

of NTRU in terms of *integer* operations. Namely the complexity of encryption is $O(N^2m^2)$ and the complexity of decryption is $O(N^2m^2)$. The question now boils down to comparing the complexity of additions and multiplications in $\mathbb{Z}_q$ (integers mod q) for NTRU and in the finite field $\mathbb{F}_q$ for CTRU. Assuming $m \leq 10$ and a Zech log implementation of the latter [14, p.91], it is well-known that the complexity of multiplication and multiplication in $\mathbb{F}_q$ is of the order of magnitude of the complexity of addition in $\mathbb{Z}_q$ that is $O(m)$. On the other hand the complexity of multiplication in $\mathbb{Z}_q$ is at best, for these values of m using Karatsuba algorithm [10] of order $O(m^c)$, with $c = \log(3)/\log(2) \approx 1.584962\cdots$

$\mathbb{Z}_q$	$\mathbb{F}_q$	operation
$\cong m$	$\cong m$	$+$
$\cong m^{1.59}$	$\cong m$	$\times$

So, for moderate m and the same values of N CTRU is certainly faster than NTRU. For large values of m the performance will depend on the chosen implementation.

5.2 Actual Implementation

We implemented the cryptosystem using the library *Algebra* of the computer language Aldor [1] on a bi-processor 2 x Pentium III operating at 935Mhz, with a gigaoctet of memory. Aldor is a high-level formal computation language written in C. We obtained the following results (speed scaled to 500 MhZ pentium), for the three different systems we propose. These results compare well with the results of [8] for other PKC. Note that our implementation was not optimized and could be improved by the use of the Fast Fourier Transform.

Operation	CTRU-32	CTRU-64	CTRU-128
Key generation (ms)	24	74	230
Encryption (ms)	2	5	28
Decryption (ms)	4	19	68

6 Conclusion

We presented here a polynomial analog of NTRU, called CTRU. This system enjoys a rigorous derivation of the decryption, and escapes LLL and CRT based attacks. The complexity of encryption and decryption is the same for the same N. The size of N which was prominent in NTRU seems to play here a lesser role in security analysis. As a consequence, shorter values of N might be employed, resulting in speed and key size improvements.

CTRU is patent pending.

Acknowledgement The three authors are indebted to Manuel Bronstein for basic education in Popov and Aldor. The second author is indebted to project CAFE from INRIA Sophia for a three months hospitality, and to a COLOR grant INRIA-I3S 2001-2002 for support.

References

[1] `http://www.aldor.org`

[2] A. Barg, Complexity issues in coding theory, Chapter 7 in *Handbook of Coding Theory*, V. S. Pless, W.C. Huffman, eds, North Holland (1998).

McEliece1514 in

[3] G.D. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, North-Holland (1997).

[4] D. Coppersmith, A. Shamir, Lattice attacks on NTRU, Eurocrypt 97, Springer LNCS 1233 (1997) 52–61.

[5] C. Gentry, Key recovery and message attacks on NTRU-composite, Eurocrypt 01, Springer LNCS 2045 (2001) 182–194.

[6] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267-288. (copyright 1998, Springer-Verlag)

[7] `http://grouper.ieee.org/groups/1363/StudyGroup/NewFam.html#HPS`

[8] P. Karu and J. Loikkanen, Practical comparison of fast public-key cryptosystems, Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology. `http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers.html`.

[9] N. Koblitz, Elliptic curves cryptosystems, Math of Comp. 48 (1987) 203–209.

[10] Knuth, D., *The Art of Computer Programming*, Vol 2, 2nd ed., Addison-Wesley, Reading, Mass, 1981.

[11] C. van Loan, *Computational Frameworks for the Fast Fourier Transform*, SIAM Frontiers in Applied Math (1992).

Theory, IT-34

[12] T. Mulders, A. Storjohann, On lattice reduction for polynomial matrices, (2000) Tech Report 356 ETH Zurich.

[13] R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory," JPL DSN Progress Report 42-44, 114-116 (1978).

[14] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland (1977).

[15] `www.ntru.com`

[16] J. Pipher, Course Notes for Fourier Institute summer school, Grenoble (2002).

[17] M.E. Pohst, M. Schoernig, On integral basis reduction in global function fields, Proceedings of ANTS-II, Springer Verlag. (1996) 273-282.

[18] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Comm. of The ACM, 21 (1978) 120-126.

[19] J.H. Silverman, A Meet-In-The-Middle on an NTRU Private Key, preprint available from `www.ntru.com`.

Contents

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399