

An Algebraic Approach to NTRU ($q = 2^n$) via Witt Vectors and Overdetermined Systems of Nonlinear Equations

J.H. Silverman, N.P. Smart, F. Vercauteren

December 2005

Introduction

Main results:

- ▶ Introduce the use of Witt vectors into cryptanalysis
 - ▶ May have other uses
 - ▶ Use of mod 2^m operation in various ciphers
- ▶ Develop very compact algebraic description of NTRU
 - ▶ Non-lattice description
- ▶ Investigate application of XL algorithm

Ring of Witt Vectors

A Witt vector of length m over \mathbb{F}_2 is an element of the set \mathbb{F}_2^m

- ▶ i.e. a binary vector of length m
- ▶ as a set $W_m(\mathbb{F}_2) = \mathbb{F}_2^m$.

However, on this set we define a ring structure such that there is an isomorphism

$$W_* : \begin{array}{ccc} W_m(\mathbb{F}_2) & \longrightarrow & \mathbb{Z}_2^m \\ [a_0, \dots, a_{m-1}] & \longmapsto & \sum_{i=0}^{m-1} a_i 2^i \pmod{2^m} \end{array}$$

Clearly, the operations in $W_m(\mathbb{F}_2)$ will be more complicated than componentwise addition and multiplication

- ▶ Since we need to take carry bits into account
- ▶ But: operations on a_i are still in \mathbb{F}_2

Ring of Witt Vectors

We thus have to find multivariate polynomials

$$S_0, \dots, S_{m-1}, P_0, \dots, P_{m-1} \in \mathbb{F}_2[X_0, \dots, X_{m-1}, Y_0, \dots, Y_{m-1}]$$

such that for all Witt vectors

$$\mathbf{a} = [a_0, \dots, a_{m-1}] \quad \text{and} \quad \mathbf{b} = [b_0, \dots, b_{m-1}]$$

we have

$$W_*([S_0(\mathbf{a}, \mathbf{b}), \dots, S_{m-1}(\mathbf{a}, \mathbf{b})]) \equiv W_*(\mathbf{a}) + W_*(\mathbf{b}) \pmod{2^m}$$

$$W_*([P_0(\mathbf{a}, \mathbf{b}), \dots, P_{m-1}(\mathbf{a}, \mathbf{b})]) \equiv W_*(\mathbf{a}) \cdot W_*(\mathbf{b}) \pmod{2^m}$$

Ring of Witt Vectors

As a simple example, when $m = 4$, we have the following polynomials over \mathbb{F}_2

$$S_0(\mathbf{a}, \mathbf{b}) = a_0 + b_0$$

$$S_1(\mathbf{a}, \mathbf{b}) = a_0 b_0 + a_1 + b_1$$

$$S_2(\mathbf{a}, \mathbf{b}) = a_0 b_0 a_1 + a_0 b_0 b_1 + a_1 b_1 + a_2 + b_2$$

$$S_3(\mathbf{a}, \mathbf{b}) = a_0 b_0 a_1 a_2 + a_0 b_0 a_1 b_2 + a_0 b_0 b_1 a_2 + a_0 b_0 b_1 b_2 \\ + a_1 b_1 a_2 + a_1 b_1 b_2 + a_2 b_2 + a_3 + b_3$$

$$P_0(\mathbf{a}, \mathbf{b}) = a_0 b_0$$

$$P_1(\mathbf{a}, \mathbf{b}) = a_0 b_1 + b_0 a_1$$

$$P_2(\mathbf{a}, \mathbf{b}) = a_0 b_0 a_1 b_1 + a_0 b_2 + b_0 a_2 + a_1 b_1$$

$$P_3(\mathbf{a}, \mathbf{b}) = a_0 b_0 a_1 b_1 a_2 + a_0 b_0 a_1 b_1 b_2 + a_0 b_0 a_1 b_1 + a_0 b_0 a_2 b_2 \\ + a_0 a_1 b_1 b_2 + a_0 b_3 + b_0 a_1 b_1 a_2 + b_0 a_3 + a_1 b_2 + b_1 a_2$$

Ring of Witt Vectors

How to compute the polynomials S_i and P_i ?

- ▶ i^{th} Witt polynomial $W_i \in \mathbb{Z}[X_0, \dots, X_i]$ is defined by

$$W_i(X_0, \dots, X_i) = X_0^{2^i} + 2X_1^{2^{i-1}} + \dots + 2^i X_i.$$

- ▶ Let $\Phi \in \mathbb{Z}[X, Y]$, then there exists unique sequence $(\varphi_0, \dots, \varphi_n)$ of elements $\mathbb{Z}[X_0, \dots, X_n; Y_0, \dots, Y_n]$ with

$$W_n(\varphi_0, \dots, \varphi_n) = \Phi(W_n(X_0, \dots, X_n), W_n(Y_0, \dots, Y_n))$$

- ▶ S_i reduction of Witt polynomials for $\Phi = X + Y$
- ▶ P_i reduction of Witt polynomials for $\Phi = X \cdot Y$

Ring of Witt Vectors

Conclusion: Witt Vectors provide a high-brow, but easy to compute, way of mapping

- ▶ Arithmetic modulo 2^m into
- ▶ Non-linear equations of binary variables

This mapping is provided by W_*^{-1}

NTRU Introduction

NTRU is a public key encryption scheme

- ▶ Not based on factoring/discrete logarithms, but on polynomial factorisation problem
- ▶ Appears “immune” to quantum computers
- ▶ Best known heuristic attack via lattice basis reduction
- ▶ Very compact and efficient

Various parameter choices

- ▶ $p, q, N, \mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_r$

We focus on q a power of 2 and only attack the public key

- ▶ Make no use of the encryption function used
- ▶ Hence, will not consider \mathcal{L}_r further

The NTRU Ring

- ▶ Let N denote a prime integer. Let $q = 2^n$ with $q \in [N/2, N]$.
- ▶ Integers modulo q we assume represented in

$$(-\lceil q/2 \rceil, \lfloor q/2 \rfloor]$$

- ▶ Identify the set \mathbb{Z}^N (respectively \mathbb{Z}_q^N) with the ring of polynomials

$$P(N) = \frac{\mathbb{Z}[X]}{(X^N - 1)}, \quad \text{respectively} \quad P_q(N) = \frac{\mathbb{Z}_q[X]}{(X^N - 1)},$$

via the natural association

$$f = (f_0, f_1, \dots, f_{N-1}) = \sum_{i=0}^{N-1} f_i X^i$$

The NTRU Ring

- ▶ Note that the modulus q is not necessarily prime, so \mathbb{Z}_q is not in general a field.
- ▶ If $f, g \in P(N)$ (resp. $P_q(N)$) then multiplication defined by

$$h = f \star g = f \cdot g \pmod{X^N - 1}$$

- ▶ For each $0 \leq k < N$, the k^{th} -coefficient h_k of h is given by

$$\begin{aligned} h_k &= (f \star g)_k \\ &= \sum_{i=0}^k f_i g_{k-i} + \sum_{i=k+1}^{N-1} f_i g_{n+k-i} \\ &= \sum_{i+j \equiv k \pmod{N}} f_i \cdot g_j. \end{aligned}$$

More NTRU Parameters

- ▶ Need a “small” element p of $P(N)$ that is relatively prime to q , i.e. p and q generate the unit ideal in $P(N)$.
- ▶ Typically $p = 2, 3$ or $2 + X$.
- ▶ This talk $p = 2 + X$, used in NTRU’s standard and is the choice of the NTRU challenges
- ▶ Method applies to any value of p

NTRU Keys

For integer d , $\mathcal{L}(d) \subset P_q(N)$ such that $f \in \mathcal{L}(d)$ has d coefficients equal to 1 and all other coefficients equal to zero.

Fix integers d_f, d_g and set (for our purposes)

- ▶ $\mathcal{L}_f = \{1 + p \star F : F \in \mathcal{L}(d_f)\}$ and $\mathcal{L}_g = \mathcal{L}(d_g)$

Define NTRU key by

- ▶ $f \in \mathcal{L}_f$
- ▶ $g \in \mathcal{L}_g$
- ▶ $h \equiv p \star f_q^{-1} \star g \pmod{q}$
- ▶ h is public key, f is private key

Recovering NTRU Keys

- ▶ NTRU problem: given h, p, d_f, d_g , find polynomial f or g
- ▶ Note: if restriction on f or g having small coefficients left out, get many solutions by choosing g and computing f

$$f \equiv p \star h^{-1} \star g \pmod{q}$$

- ▶ Difficulty: finding **small** g and f that satisfy the above!
- ▶ Leads quite naturally to lattice problem . . .

Attacks Against NTRU Keys

Best known **heuristic** attack is via lattice reduction

- ▶ Hence standard says select $N = 167, 251, 347$ or 503 .
- ▶ LLL in polynomial time, but vectors only short up to exponential factor!

Best known **deterministic** attack is meet-in-middle with complexity

$$\frac{1}{\sqrt{N}} \binom{N/2}{d_f/2}.$$

We present a new (compact) algebraic formulation of NTRU

- ▶ Reduce to $N + 2$ quadratic equations in N variables
- ▶ Correct result, but probably exponential time

Algebraic Formulation of NTRU

- ▶ Since $q = 2^n$ use W_* to map NTRU equation

$$f \star h \equiv p \star g \pmod{2^m} \quad (m \leq n)$$

- ▶ into N equations of Witt vectors of length m
- ▶ Corresponds to mN non-linear equations over \mathbb{F}_2
- ▶ Write $g = \sum_{i=0}^{N-1} g_i X^i$ with $g_i \in \{0, 1\}$ and
- ▶ $f = 1 + (2 + X) \star F$ with $F = \sum_{i=0}^{N-1} F_i X^i$ with $F_i \in \{0, 1\}$
- ▶ Have $2N$ **binary** unknowns g_i and F_i
- ▶ Need to take m at least 2
- ▶ Degree of non-linear equations is also m , can eliminate g_i using linear algebra by looking at equation mod 2

Algebraic Formulation of NTRU

- ▶ N quadratic equations in N unknowns F_i
- ▶ System of equations has very nice structure
- ▶ There exists two index sets S and T such that the k -th equation is given by

$$\sum_{\substack{i < j \\ i, j \in S_k}} F_i F_j + \sum_{i \in T_k} F_i + h_{k,0} \sum_{i \in S_k} F_i = h_{k+1,0} + h_{k,1},$$

with $h_{k,l}$ the l -th bit of the coefficient h_k and

$$S_k = \{i + k \pmod{N} \mid i \in S\}$$

$$T_k = \{i + k \pmod{N} \mid i \in T\}.$$

Algebraic Formulation of NTRU

- ▶ Derive two extra quadratic equations, using fact f has Hamming Weight d_f .
- ▶ Let F_i denote the coefficients of f , then

$$\sum F_i = d_f$$

over the integers.

- ▶ Using the map W_* with $m = 2$ we obtain extra equations

$$\sum_{i=0}^N F_i = d_f \pmod{2}$$
$$\sum_{i < j} F_i F_j = d_f \pmod{2}$$

Recap so far

From an NTRU public key (with $q = 2^n$) one can derive

- ▶ $N + 2$ quadratic equations over \mathbb{F}_2
- ▶ in N binary unknowns

Do not really need Witt vectors for this, but Witt vectors provide a nice and easy to work with formulation

This system from our experiments appears

- ▶ Almost always to have only one solution, the target private key
- ▶ If more than one solution, only one has correct Hamming weight

Use of XL

- ▶ Could use Gröbner basis techniques to solve system of non-linear equations
- ▶ XL algorithm: relinearisation and linear algebra

The XL algorithm has had a lot of interest in recent years

- ▶ Possible application to block and stream ciphers
- ▶ Systems produced from analysing cipher are very large (e.g. AES)

In our case we have a very small system

- ▶ But only just overdetermined

No one really knows the complexity of XL

- ▶ Conducted some experiments and analysis

Use of XL

In our situation:

Assuming XL works perfectly

- ▶ Algebraic approach to NTRU gives best deterministic attack asymptotically
- ▶ Only better when $N > 1000$, i.e. bigger N than current largest key size

But

- ▶ XL is unlikely to work perfectly
- ▶ Our experiments show this to be case
- ▶ Some structure in output of XL though needs further investigation

Conclusion

Have presented an algebraic formulation of NTRU

- ▶ Makes use of the notion of Witt vectors
- ▶ Witt vectors may have other uses in cryptography (e.g. RC5, RC6, IDEA)

Resulting system is overdetermined and reasonably small

- ▶ Unlike most other prior algebraic attacks on ciphers

If XL was perfect, would be best deterministic attack on NTRU asymptotically

No practical effect against recommended NTRU key sizes