Lattice Basis Reduction Attack on Matrix NTRU

Thiago do R. Sousa
Tertuliano S. Neto

CEPESC

17 de setembro de 2024

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Sumário

Introduction - Timeline NTRU variants

1995

- NTRU'1996
- CTRU'2002

2005

- MaTRU'2005
- GNTRU'2006
- Matrix NTRU'2008
- GBNTRU'2008
- QTRU'2009
- NNTRU'2009

2010

- ETRU'2010
- OTRU'2010
- Modified NTRU'2011
- Scale-invariant NTRU'2013

2015

- ILTRU'2015
- GR-TRU'2015
- HXDTRU'2016
- SQTRU'2017
- Pairtru'2018
- NTRU-Prime'2018
- NTRU over Gaussian Field'2019

2020

- Flattening NTRU'2020

Introduction - Our contribution

- NTRU and its variants have security underpinned on hard lattice problems.
- Even more complicated versions for matrix variants such as the MaTRU'2005 system Coglianasse [2005].
- What about Matrix NTRU from Nayak [2008] ?
- Our contribution:
  - Present a sufficient condition for zero decryption failure
  - Present associated lattice that contains the private key
  - Show a serious vulnerability that allows one recover independently chunks of the keys.
  - Present a theoretical and practical attack that allows one to recover plaintext for parameter values that could be used in practice.

Introduction - Timeline Matrix NTRU

2008

- Nayak'2008 Introduces Matrix NTRU

2010

- Nayak'2010 Compares with classical NTRU
- Luo'2011 Improving key generation
-Nayak'2011 Reaction attack
- Nayak'2012 Compares performance with classical NTRU
- Kumar'2013 Framework for deploying Matrix NTRU in practice

2015

- Mandikar'2018 Practical application using Matrix NTRU

2020

- Nisa'2023 Meet in The Middle Attack on Matrix NTRU
- Wijayanti'2023 Extends Matrix NTRU to integers over integral domain
- Lattice-basis attack ?

- Parameters: $n > 1$, a prime p and $q >> p$ an integer such that $(p, q) = 1$.
- Modular arithmetic over matrices with integer coefficients, i.e., for

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \quad \in M_n(\mathbb{Z})$$

we define

$$A \mod p = \begin{pmatrix} a_{11} \mod p & \dots & a_{1n} \mod p \\ \vdots & \ddots & \vdots \\ a_{n1} \mod p & \dots & a_{nn} \mod p \end{pmatrix}.$$

Matrix NTRU - How to use it ?

KEY GENERATION:

- Choose a pair of matrices F, G
- Entries of F, G in $\{-1, 0, 1\}$
- F should be invertible: $F_p = F^{-1} \mod p$ and $F_q = F^{-1} \mod q$.
- Public key is

$$H = pF_qG \mod q$$

ENCRYPTION:

- Given a message $M \in M_n(\mathbb{F}_p)$, choose a ternary matrix $R \in M_n(\mathbb{Z})$ at random. Ciphertext is

$$E = HR + M \mod q.$$

DECRYPTION:

- Compute

$$A = FE \mod q \quad \text{and} \quad B = F_pA \mod p$$

- In Nayak [2012] a matrix NTRU with parameter n is comparable to a classical NTRU parameter $N = n^2$

NTRU - Private key polynomial:

$$
\begin{array}{rc}
f(x) = & f_1 + f_2 x + \cdots + f_n x^{n-1} \\
+ & f_{n+1} x^n + f_{n+2} x^{n+1} + \cdots + f_{2n} x^{2n-1} \\
+ & \cdots \\
+ & f_{n(n-1)+1} x^{n(n-1)} + f_{n(n-1)+2} x^{n(n-1)+1} + \cdots + f_{n^2} x^{n^2-1}
\end{array}
$$

Matrix NTRU - private key matrix:

$$
\begin{bmatrix}
f_1 & f_2 & \cdots & f_n \\
f_{n+1} & f_{n+2} & \cdots & f_{2n} \\
\vdots & \vdots & \vdots & \vdots \\
f_{n(n-1)+1} & f_{n(n-1)+2} & \cdots & f_{n^2}
\end{bmatrix}
$$

- Matrix NTRU is faster for comparable parameters (Nayak [2012]).
- Is it safer or has comparable security ?

Proposition

Consider the matrix NTRU system with parameters n, p, q where

1. F, G are the private key matrices
2. (f_k, g_k) is the k-th line of
$$\begin{pmatrix} F & G \end{pmatrix}_{n \times 2n}$$
3. H is the public key
4. p^{-1} be the inverse of p module q

Then, (f_k, g_k) belongs to the lattice generated by the lines of

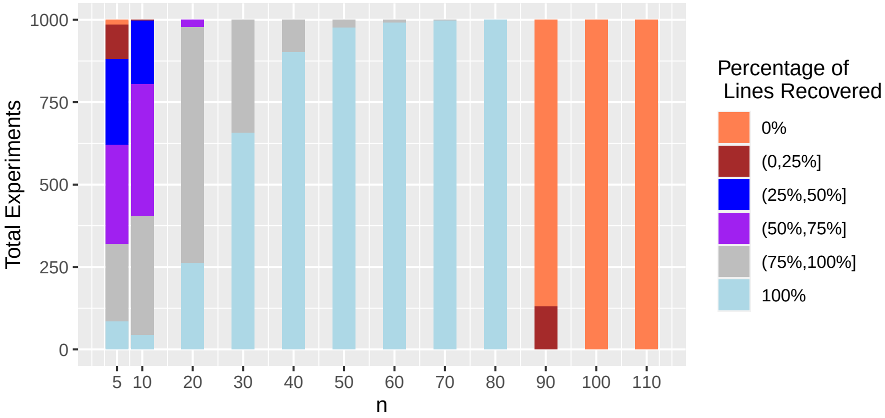
$$L = \begin{pmatrix} I_n & p^{-1}H \\ 0_n & qI_n \end{pmatrix}_{2n \times 2n} \tag{1}$$

SBSeg24 São José dos Campos

CEPESC

Lattice basis Attack

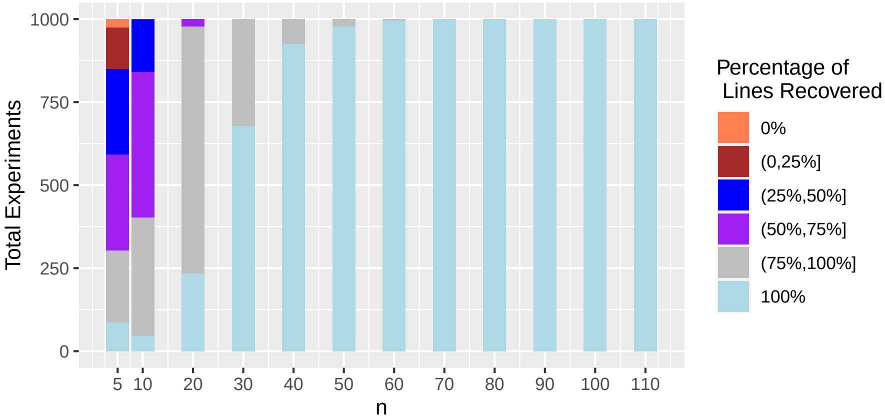
Figure: Attack for recovering lines of the matrix F with $p = 3$ and $q = 256$.



- Decryption failure after $n >= 90$.

Lattice basis Attack

Figure: Same settings as before but with $q = 4096$.



- Finding a private key in the matrix NTRU system is associated with the SVP problem in a lattice of dimension $2n$, and not $(2n^2)$ as one would expect since it is comparable to an NTRU with polynomials of degree n^2.
- This is a serious vulnerability as one can recover INDEPENDENTLY each line of the private key in just a one go Lattice reduction attack.
- Can we use this attack in practice ?

Lattice basis Attack - How to use it in practice ?

- **PROBLEM:** We can recover F up to a permutation, but how can we recover F ?
- **IDEA:** Look at the decryption equation for matrix NTRU. What happens if we try to decrypt with a permutation of F^* ?

$$F^* = DF, \quad \text{where} \quad U \quad \text{is unimodular}$$

Proposition

Consider a Matrix NTRU system where:

1. M is a message encrypted with F
2. E is the ciphertext which decrypts correct to M
3. F^* is any permutation of lines of F

Then, decryption of E with F^* gives M

Lattice basis Attack - How to use it in practice ?

- **PROBLEM:** We can recover F up to a permutation, but how can we recover F ?
- **IDEA:** Look at the decryption equation for matrix NTRU. What happens if we try to decrypt with a permutation of F^* ?

$$F^* = DF, \quad \text{where} \quad U \quad \text{is unimodular}$$

Proposition

Consider a Matrix NTRU system where:

1. M is a message encrypted with F
2. E is the ciphertext which decrypts correct to M
3. F^* is any permutation of lines of F

Then, decryption of E with F^* gives M

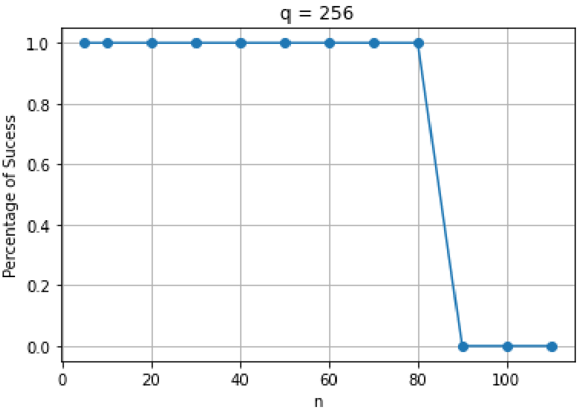
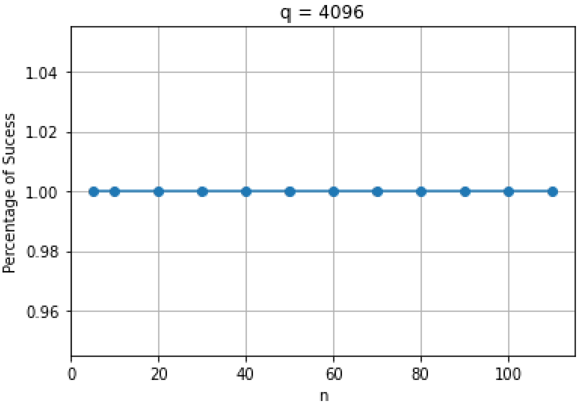


Figure: Message recovery attack for matrix NTRU $p = 3$ and $q = 256$

Message recovery attack - Results

Figure: Message recovery attack for matrix NTRU $p = 3$ and $q = 4096$



Conclusion

- Introducing a matrix introduces the possibility of recovering the private key line by line
- The matrix approach diffuses less the key bits
- Matrix NTRU is seriously vulnerable and should not be used.
- A matrix NTRU with n^2 entries in the private key allows an attack with complexity proportional to n and not n^2 (as it is the case the NTRU 'equivalent').
- NTRU submission with $n = 509$ has already some moderate security but a matrix NTRU with parameter $\sqrt{n} \approx 23$ is completely vulnerable.

Muito obrigado!

thiagodoregosousa@gmail.com
tsouzaneto@gmail.com