Cryptanalysis of Polynomial Authentication and Signature Scheme

Hongjun Wu, Feng Bao, Dingfeng Ye, and Robert H. Deng

Kent Ridge Digital Labs
21 Heng Mui Keng Terrace
Singpore 119613
{hongjun, baofeng, dfye, deng}@krdl.org.sg

Abstract. Polynomial Authentication and Signature Scheme (PASS) is a new public key authentication and signature scheme proposed by NTRU Cryptosystems Inc. It is based on the hard problems related to constrained polynomial evaluation. In this paper, we break PASS with the proposed parameters. We show how to forge valid authentication transcripts or digital signatures in PASS with knowledge of the public key only and without knowing any previous authentication transcripts or signatures.

1 Introduction

A group of highly efficient public key cryptosystems, including NTRU [1, 2] for asymmetrical encryption and PASS [3] for digital authentication and signature, were proposed recently by Hoffstein, Pipher, and Silverman from NTRU Cryptosystem, Inc. This group of cryptosystems is based on the hard problems of partial evaluation of constrained polynomial over polynomial rings. An outstanding feature of the proposed cryptosystems is that key generation, encryption/decryption, authentication and digital signature operations can be performed highly efficiently.

NTRU, after its first appearance at Crypto'96, has received a great deal of attentions in the cryptographic community. Odlyzko first pointed out the meet-in-the-middle attack on NTRU and this was followed by the lattice attacks on NTRU from Coppersmith and Shamir [4]. The reaction attack proposed recently by Hall, Goldberg and Schneier [5] also has effect on NTRU. The current suggested parameters for NTRU and corresponding security estimates take into account all the above attacks. For a discussion on security of NTRU with respect all these attacks, the reader is refereed to the NTRU Cryptosystem′s homepage (http://www.ntru.com/document center.htm).

The NTRU cryptosystem has also received a lot of attentions from industry. Sony Corporation of America has made an investment in NTRU, and Tao Group Ltd of Reading, England, signed an agreement with NTRU which will make the incorporation of encryption technologies into handheld and consumer devices (http://www.ntru.com/pressreleases/). The NTRU public key encryption scheme was submitted to IEEE P1363 group as a potential IEEE public key cryptosystem standard (http://grouper.ieee.org/ groups/1363/addendum.html).

E. Dawson, A. Clark, and C. Boyd (Eds.): ACISP 2000, LNCS 1841, 278-288, 2000.

More recently, Hoffstein, Pipher, and Silverman from NTRU Cryptosystem Inc proposed PASS, a public key cryptosystem for authentication and digital signature [3]. Like NTRU, PASS features extremely light computational requirements for both the prover and the verifier. The hard problem underlying the security of PASS is related to properties of short polynomials. Since short polynomials can be made to correspond to short vectors in a lattice, it is important to carefully consider the possibility of attack by lattice reduction methods in the design of PASS. The authors of PASS were well aware of lattice reduction methods such as the LLL [6] and the improved LLL lattice reduction methods [7, 8] and they designed PASS to be secure against these attacks.

In this paper, we present the cryptanalysis of PASS. We show that PASS with the proposed parameters is not sound, i. e., it is easy to forge one's authentication transcripts or signatures knowing only the public key and without any knowledge of the private key or any previous authentication transcripts or signatures. The amount of computation required to launch the attacks is small enough to be carried out very comfortably on a PC.

This paper is organized as follows. Section 2 presents the PASS authentication and signature scheme. Two attacks to PASS authentication and signature schemes are given in Section 3 and Section 4, respectively. Section 5 concludes the paper.

2 Description of PASS

Define a ring of truncated polynomials as

$$R = (Z/qZ)[x]/(x^N - 1) \tag{1}$$

where q is a prime number and N is a divisor of $q-1$. A typical element g of R is denoted as a polynomial or a vector

$$g = g_0 + g_1 x + g_2 x^2 + \cdots + g_{N-1} x^{N-1} = [g_0\ g_1\ g_2 \cdots g_{N-1}]$$

where $g_i \in Z/qZ$. The value of $g(\alpha)$ is computed as $g(\alpha) \bmod q$ for every $\alpha \in Z/qZ$. The norm of g is a real number given by

$$|g| = \sqrt{r_0^2 + r_1^2 + r_2^2 + \cdots + r_{N-1}^2}\ ,$$

where

$$r_i = \begin{cases} g_i & if\ g_i < q/2 \\ q - g_i & if\ g_i > q/2 \end{cases}.$$

A polynomial is called short if its norm is small. Since multiplication in R is mod $x^N - 1$, it is equivalent to a cyclic convolution product. For example, the product of f and g is given by

$$h = f \cdot g \text{ with } h_k = \sum_{i+j \equiv k \bmod N} f_i g_j\ .$$

Since the multiplication of $h = f \cdot g$ is $\bmod\, x^N - 1$, it follows that

$$h(\alpha) = f(\alpha) \cdot g(\alpha) \bmod q$$

for every α satisfying $\alpha^N \equiv 1 \bmod q$.

A set S of t distinct non-zero elements $\alpha \in Z/qZ$ is chosen as a system wide parameter. Each element α of S is chosen such that $\alpha^N \equiv 1 \bmod q$ and $\alpha^{-1} \in S$. Also public are four subsets of R , denoted as L_f , L_g , L_c and L_h, respectively, and defined as follows. Fix a positive integer $d_f < N/2$. Define L_f to be the set of all polynomials f in R such that f has d_f coefficients equal to each of 1 and -1, with all other coefficients equal to 0. The norm of f is thus $\sqrt{2d_f}$. And L_g and L_c are defined similarly using d_g and d_c . L_h is defined as the set of polynomials h in R satisfying $|h| < \gamma_h q$ for a specified γ_h .

PASS is based on the fact that the product of two extremely short polynomials is still a short polynomial.

2.1 PASS Authentication Scheme

Alice, the prover, has a private key consisting of two polynomials f and f' that are chosen randomly from L_f . Her public key is the values of $f(\alpha)$ and $f'(\alpha)$ for all $\alpha \in S$, where S is the public system parameter given above. To prove to Bob, the verifier, that she possesses the secret key f , f' associated to her public key, Alice proceeds as follows:

- Alice randomly chooses *g, g´* from L_g and reveals the values of $g(\alpha)$ and $g'(\alpha)$ for all $\alpha \in S$. This is Alice's commitment.
- Bob randomly chooses a challenge c_0 and sends c_0 to Alice. c_0 is hashed with the commitment to produce polynomials: $c_1, c_2, c_3, c_4 \in L_c$.
- Alice reveals the polynomial $h = c_1 fg + c_2 fg' + c_3 f'g + c_4 f'g'$.
- Bob verifies that
  1) $h \in L_h$ $(i.e., |h| < \gamma_h q)$
  2) $h(\alpha) = c_1(\alpha) f(\alpha) g(\alpha) + c_2(\alpha) f(\alpha) g'(\alpha) +$
  $c_3(\alpha) f'(\alpha) g(\alpha) + c_4(\alpha) f'(\alpha) g'(\alpha)$

  for all the $\alpha \in S$.

2.2 PASS Signature Scheme

The private key and the public key in the signature scheme are the same as that in the authentication scheme. Alice, the signer, is to sign a message M with her private key. She proceeds as follows:

- Alice randomly chooses the polynomials g, g' from L_g and computes $g(S)$ (i. e., $\{ g(\alpha) \mid \alpha \in S \}$) and $g'(S)$.
- Alice hashes M with $g(S)$ and $g'(S)$ to construct polynomials: $c_1, c_2, c_3, c_4 \in L_c$.
- Alice computes h as

$$h = c_1 fg + c_2 fg' + c_3 f'g + c_4 f'g'$$

- The signature is $(g(S),\ g'(S),\ h)$.
- The verification process in the signature scheme is the same as that in the authentication scheme, except that $c_1, c_2, c_3, c_4 \in L_c$ are generated from $g(S)$, $g'(S)$, and M instead of the challenge.

2.3 A Specific Example of PASS

The following parameters are suggested for PASS in [3]:

$$q = 769,\ \ N = 768,\ \ t = N/2 = 384$$
$$d_f = 256,\ \ d_g = 256,\ \ d_c = 1,\ \ \gamma_h = 2.2$$

where N is simply chosen as $q-1$. It is estimated in [3] that PASS with such suggested parameters would be more secure than 1024 bit RSA since it takes longer time to recover the PASS private key. Unfortunately, as we will demonstrate in the remaining part of the paper that PASS with these parameters is extremely weak and can be broken with small amount of computations.

3 Cryptanalysis of the PASS Authentication Scheme

It was conjectured in [3] that for large N and t slightly larger than $N/2$, PASS would be sound. However, such conjecture is not true. We will present an attack in this section to forge the authentication transcript independent of the sizes of N and t.

In PASS, recovering the private key f and f' from the public key is expected to be difficult. Moreover, for polynomials f and f' chosen randomly from L_f, given

$f(\alpha)$ and $f'(\alpha)$ for all $\alpha \in S$, it is difficult to find short polynomials (with small norms) f_x and f'_x to satisfy $f_x(\alpha) = f(\alpha)$ and $f'_x(\alpha) = f'(\alpha)$ for all $\alpha \in S$. However, we notice that in order to satisfy

$$h(\alpha) = c_1(\alpha) f(\alpha) g(\alpha) + c_2(\alpha) f(\alpha) g'(\alpha) + c_3(\alpha) f'(\alpha) g(\alpha) + c_4(\alpha) f'(\alpha) g'(\alpha)$$

for all $\alpha \in S$ (i.e., the second condition verified by the verifier Bob), it is not necessary for f_x and f'_x to satisfy $f_x(\alpha) = f(\alpha)$ and $f'_x(\alpha) = f'(\alpha)$ for all $\alpha \in S$. *The reason is that if $g(\alpha) = g'(\alpha) = 0$ for a particular $\alpha \in S$, then $f_x(\alpha)$ and $f'_x(\alpha)$ can be set to any arbitrary values at that α.* If we can construct short polynomials g and g' such that $g(\alpha) = g'(\alpha) = 0$ for most of the $\alpha \in S$, then the short polynomials f_x and f'_x only need to satisfy $f_x(\alpha) = f(\alpha)$ and $f'_x(\alpha) = f'(\alpha)$ for a few $\alpha \in S$ and they can be constructed easily. In the following, we show how to generate the short polynomials g and g' with $g(\alpha) = g'(\alpha) = 0$ for most of the $\alpha \in S$.

Theorem 1. Let R be the ring defined in (1), q be a prime number, $N = q - 1$ and p be a divisor of N. If $g \in R$ and the coefficients of g are with period p, i.e., $g_i = g_{(i+kp) \bmod N}$ for any value of k, then there are at most p non-zero elements of Z/Zq satisfying $g(\alpha) \neq 0$.

Proof: The polynomial g with period p can be denoted as

$$g(x) = (g_0 + g_1 x + g_2 x^2 + \cdots + g_{p-1} x^{p-1})(1 + x^p + x^{2p} + \cdots + x^{N/p}).$$

For $(x^p - 1) \bmod p \neq 0$, $g(x)$ can be written as

$$g(x) = (g_0 + g_1 x + g_2 x^2 + \cdots + g_{p-1} x^{p-1}) \frac{x^N - 1}{x^p - 1}.$$

Note that $\alpha^N - 1 \equiv 0 \bmod q$, thus the necessary condition for $g(\alpha) \neq 0$ is that $\alpha^p - 1 \equiv 0 \bmod q$. Since there are at most p distinct solutions in Z/Zq for $\alpha^p - 1 \equiv 0 \bmod q$, there are at most p non-zero elements in Z/Zq satisfying $g(\alpha) \neq 0$.

According to theorem 1, the short polynomials g and g' with $g(\alpha) = g'(\alpha) = 0$ for most of the $\alpha \in S$ can be constructed easily if N has small factors. We simply choose their coefficients from the set $\{-1, 0, 1\}$ to generate short polynomials and with short period. Since the proposed value of N is $768 = 3 \times 2^8$, there are a number of small factors of N for g and g' to be constructed easily. For example, if we set the coefficients of short polynomials g and g' with period 6, then most likely there will be about $(768 - 6)/2 = 381$ values of $\alpha \in S$ with $g(\alpha) = g'(\alpha) = 0$ since the elements of S are chosen in [3] without being aware of this attack.

After obtaining the desired short polynomials g and g', we then proceed to construct the short polynomials f_x and f'_x. Denote S_1 as the subset of S containing all those $\alpha \in S$ with $g(\alpha) = g'(\alpha) = 0$ and denote $S_2 = S - S_1$. Now, short polynomials f_x and f'_x are only required to satisfy $f_x(\alpha) = f(\alpha)$ and $f'_x(\alpha) = f'(\alpha)$ for all $\alpha \in S_2$. The construction of f_x and f'_x becomes much easier especially when the number of elements in S_2 is sufficiently small. For example, if there are only 3 elements in S_2, even an exhaustive search (by randomly choosing the coefficients from the set $\{-1, 0, 1\}$) can be applied to determine the short polynomials f_x and f'_x since only about $769^3 = 2^{28.8}$ trials are needed in this scenario. It should be noted that such computations are done prior to the authentication process. With the four short polynomials g, g', f_x and f'_x, valid authentication transcripts can be produced. This attack is valid as long as *N* has many small factors, like 768, regardless of the size of the challenge.

To summarize the result in this section, the PASS authentication scheme with the proposed parameters is not secure, i.e. it is not sound. A cheater, who knows only Alice's public key, can produce valid authentication transcripts on Alice's behalf easily without knowing Alice's private key. The amount of computation required is small and no previous authentication transcripts are needed in the attack.

4 Cryptanalysis of the PASS Signature Scheme

The attack described in Section 3 can be applied directly to break the PASS signature scheme.

The attack in Section 3 depends essentially on the fact that $N = 768$ has small factors. It is thus necessary to choose N as a prime number instead of $q-1$. In this section, another attack is applied to the PASS signature scheme even if N is chosen as a prime number. In this attack, the small space of L_c would enable signatures being forged easily.

We notice that the h can be written as

$$\begin{aligned} h &= c_1 fg + c_2 fg' + c_3 f'g + c_4 f'g' \\ &= c_1(f + r_1 f')g + c_2(f + r_2 f')g' \\ &= c_1 h_1 + c_2 h_2 \end{aligned}$$

where $c_3 = c_1 \cdot r_1$, $c_4 = c_2 \cdot r_2$, $h_1 = (f + r_1 f')g$ and $h_2 = (f + r_2 f')g'$. We could specify two polynomials r_1 and r_2 (the simplest way is to set $r_1 = r_2 = 1$). We then choose arbitrarily two short polynomials h_1 and h_2. Another two polynomials g and g' are computed to satisfy $h_1(\alpha) = (f(\alpha) + r_1(\alpha) f'(\alpha)) g(a)$ and $h_2(\alpha) = (f(\alpha) + r_2(\alpha) f'(\alpha)) g'(\alpha)$ for all the $\alpha \in S$. Here g and g' are not required to be short polynomials. After obtaining g and g', we compute c_1, c_2, c_3 and c_4. If

$c_3 = c_1 \cdot r_1$ and $c_4 = c_2 \cdot r_2$ with the pre-specified polynomials r_1 and r_2, we forged successfully a signature $(g(S),\ g'(S),\ h)$ in which

$$h = c_1 h_1 + c_2 h_2$$

The probability of success of one trial is about $1/|L_c|^2$. Repeat this attack by choosing different polynomials h_1 and h_2, the signature could finally be forged with about $0.5\times|L_c|^2$ trials, which is about $2^{-37.3}$ for $N = 768$ and $d_c = 1$.

The detailed attack is given in the rest of this section. Let f and f' be Alice's private key and $f(\alpha)$ and $f'(\alpha)$ be the corresponding public key for all $\alpha \in S$ = $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$. The attack is as follows.

1. Arbitrarily choose $r_1, r_2 \in R$ such that for any $c \in L_c$, $r \cdot c \in L_c$.
2. Compute $\beta_{1i} = f(\alpha_i) + r_1(\alpha_i) f'(\alpha_i)$ and $\beta_{2i} = f(\alpha_i) + r_2(\alpha_i) f'(\alpha_i)$ for $i = 1, 2, \ldots, t$. Assume that $\beta_{1i} \neq 0, \beta_{2i} \neq 0$ for all $i = 1, 2, \ldots, t$ (we will deal with the case when some of them are 0 later).
3. Let F_1, F_2 be two functions such that $F_1(\alpha_i) = \beta_{1i}, F_2(\alpha_i) = \beta_{2i}$ for $i = 1, 2, \ldots, t$. Choose two arbitrary short polynomials h_1, h_2. Compute the polynomials G_1, G_2 satisfying $h_1 = F_1 G_1, h_2 = F_2 G_2$ on S.
4. Hash message M with $G_1(S), G_2(S)$ to generate c_1, c_2, c_3 and c_4. If the generated c_1, c_2, c_3 and c_4 happen to satisfy $c_3 = r_1 c_1$ and $c_4 = r_2 c_2$, we set $h = c_1 h_1 + c_2 h_2$ and $g = G_1$, $g' = G_2$. Otherwise, go to step 3 and repeat the attack.
5. $(h, g(S), g'(S))$ is a valid signature of M.

In step 4, we note that the generated c_1, c_2, c_3 and c_4 satisfy $c_3 = r_1 c_1$ and $c_4 = r_2 c_2$ with probability $1/|L_c|^2$. That is the success rate for one trial.

In this attack, step 1 and step 4 can be carried out easily as shown in the Theorem 2 and 3 in the Appendix, respectively.

In step 2 we assume that $\beta_{1i} \neq 0, \beta_{2i} \neq 0$ for all $i = 1,2,\ldots,t$. Such assumption is, however, not always true. In the following, we improve the attack so that it works even if up to four elements of $\{\beta_{1i} \mid i = 1,2,\ldots,t\}$ and four elements of $\{\beta_{2i} \mid i = 1,2,\ldots,t\}$ are zero. We start with the following two facts.

Fact 1. Let $c_1, c_2 \in L_c$. If each of h_1, h_2 has $N-4$ small coefficients and four arbitrary coefficients, $h = c_1 h_1 + c_2 h_2$ is with norm $|h| < 2.2q$.

It is because that

1) h has $N-16$ small coefficients and 16 arbitrary coefficients;

2) For the small coefficients, the sum of h_i^2 is less than $0.8q^2$ if $h_i < 0.8\sqrt{q}$. This is fulfilled if each of the small coefficients of h_1, h_2 is smaller than $0.2\sqrt{q}$.
3) From the definition of norm in Section 2, $h_i^2 < q^2/4$ for any h_i.
4) Thus $\sum_{i=0}^{N-1} h_i^2 < 4q^2 + 0.8q^2$. It implies $|h| < 2.2q$;

Fact 2. Let $F \in R$ and $F(\alpha) = 0$ for up to 4 $\alpha \in S \subset Z/qZ - \{0\}$. Based on Theorem 4 in the Appendix, it is easy to construct a $G \in R$, such that H $(H = FG)$ has $N-4$ arbitrarily small coefficients.

With Fact 1 and Fact 2, our attack can be applied in the situation where up to four elements of $\{\beta_{1i} \mid i = 1,2,...,t\}$ and four elements of $\{\beta_{2i} \mid i = 1,2,...,t\}$ are zero. For $N = 768$ and $t = N/2$, the probability that more than four elements of $\{\beta_{1i} \mid i = 1,2,...,t\}$ or more than four elements of $\{\beta_{2i} \mid i = 1,2,...,t\}$ are 0 is only about 2^{-12}. So the improved attack would succeed without being significantly affected by the values of β_{1i} and β_{2i}.

Similar attack could be applied to the PASS authentication scheme. The valid authentication transcript can be generated with probability $1/|L_c|^2$. This value is about $2^{-38.3}$ for the proposed parameters. The PASS authentication scheme with the proposed parameters is thus not secure with respect to this attack.

5 Conclusion

PASS is a highly efficient public key authentication and signature scheme that was designed to resist LLL lattice reduction method and the improved LLL method. The authors of PASS estimated that the breaking time for the proposed parameter $N = 768$ is approximately 4.73×10^{18} MIP-years [3]. In this paper we showed that the above claim is false and that PASS with the proposed parameter is not sound. That is, one can forge authentication transcripts or signatures without recovering the private key and with small amount of computations.

We presented two attacks to PASS. Both attacks apply to the PASS authentication scheme and the PASS signature scheme, though we only demonstrated the first attack to the PASS authentication scheme in Section 3 and the second attack to the PASS signature scheme in Section 4. The first attack succeeded in forging authentication transcripts (or signatures) by exploiting the fact that the proposed parameter $N = 768$ has small factors. To resist this attack, we suggest choosing N as a prime number. However, a prime N can not resist the second attack presented in Section 4, which succeeded in breaking PASS using the fact that the space L_c is too small.

Enlarging q is not an effective counter measure against our second attack since q must be very large in order to give PASS a reasonable security. In that case, its computational efficiency will degrade significantly. Modifications may be applied to other parameters of PASS such as d_f, d_g, d_c, etc; however, their security implications must be considered very carefully since the corresponding γ_h must be changed in that case. And γ_h is a key factor for the security of PASS under other attacks such as LLL attack.

Generally, we believe that any further modification to PASS should take the attacks presented in this paper into consideration.

References

1. J. Hoffstein, J. Pipher and J.H. Silverman, „NTRU: A New High Speed Public Key Cryptosystem“, preprint; presented at the rump session of *Crypto'96*.
2. J. Hoffstein, J. Pipher and J.H. Silverman, „NTRU: A Ring Based Public Key System“, *Proceedings of ANTS III*, Porland (1998), Springer-Verlag.
3. J. Hoffstein, D. Lieman and J.H. Silverman, „Polynomial Rings and Efficient Public Key Authentication“, *Proceedings of International Workshop on Cryptographic Techniques and E-Commerce*, pp 7-19, Ed M. Blum and C. H. Lee, July 5-8, 1999, Hong Kong. Also available at http://www.ntru.com/ documentcenter.htm.
4. D. Coppersmith and A. Shamir, „Lattice Attacks on NTRU, Preprint, April 5, 1997“; presented at *Eurocrypt'97*.
5. C. Hall, I. Goldberg and B. Schneier, „Reaction Attacks Against Several Public-Key Cryptosystems“, preprint April 1999, available at http://www.counterpane. com.
6. A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovsz, „Factoring Polynomials with Rational Coefficients,“ *Mathematische Ann.*, 261 (1982), pp. 513-634.
7. C. P. Schnorr, „A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms,“ *Proceedings* of *Theoretical Computer Science*, 53 (1987), pp. 201-224.
8. C. P. Schnorr, „A More Efficient Algorithm for Lattice Basis Reduction“, *J. Algorithms*, 9 (1988), pp. 47-62.

Appendix

Theorem 2. There exists a polynomial $r \in R = (Z / qZ)[x]/(x^N - 1)$ such that for any $c \in L_c$, the product $r \cdot c \in L_c$.

Proof: The validity of this theorem is trivial by noting that x^i fulfills the requirement for any *i*.

Theorem 3. Let $F \in R$ and $F(\alpha) \neq 0$ for $\alpha \in S \subset Z / qZ - \{0\}$. For any $H \in R$, it is easy to construct a $G \in R$, such that $F(\alpha)G(\alpha) = H(\alpha)$ for all $\alpha \in S$.

Proof: Given H , the values of $H(\alpha)$ for all non-zero $\alpha \in S$ can be computed. Define $G(\alpha) = H(\alpha)/F(\alpha)$ for $\alpha \in S$ and arbitrarily set $G(\alpha)$ for $\alpha \in Z/qZ - \{0\} - S$. The coefficients of G can be computed directly since

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{N-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_N & \cdots & \alpha_N^{N-1} \end{pmatrix}$$

is a non-singular matrix for different $\alpha_1, \alpha_2, ..., \alpha_N$.

Denote $F = a_0 + a_1 x + \cdots + a_{N-1} x^{N-1}$ and matrix **F** as

$$\mathbf{F} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

Lemma 1.The rank of **F** equals to the amount of $\alpha \in Z/qZ - \{0\}$ satisfying $F(\alpha) \neq 0$.

Proof. Let $E = b_0 + b_1 x + \cdots + b_{N-1} x^{N-1}$ and $FE = c_0 + c_1 x + \cdots + c_{N-1} x^{N-1}$, we must have

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \begin{pmatrix} b_{N-1} \\ b_{N-2} \\ b_{N-3} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} c_{N-1} \\ c_{N-2} \\ c_{N-3} \\ \vdots \\ c_0 \end{pmatrix}$$

Consider all the E satisfying $FE = 0$. All these E (their coefficient vectors) consist of a linear space. It is the null space of **F**. Every such E must satisfy $E(\alpha)=0$ for those α such that $F(\alpha)\neq 0$. By counting the number of such E we reach Lemma 1.

Theorem 4. Let $F \in R$ and $F(\alpha) = 0$ for exactly k $\alpha \in Z/qZ - \{0\}$. It is easy to construct a $G \in R$ so that the polynomial $H = FG$ is with $N - k$ arbitrarily small coefficients.

Proof. From Lemma 1 the rank of **F** is $N-k$. There are k linear independent rows in **F**. Without loss of generality, assume that the first $N-k$ rows are linear independent. Arbitrarily set the last $N-k$ coefficients of H as small numbers $h_{N-1}, h_{N-2}, \ldots, h_k$. Solve G from

$$\begin{pmatrix} \\ \textit{the first } N-k \\ \textit{rows of } \mathbf{F} \\ \\ \end{pmatrix} \begin{pmatrix} g_{N-1} \\ g_{N-2} \\ g_{N-3} \\ \vdots \\ g_0 \end{pmatrix} = \begin{pmatrix} h_{N-1} \\ h_{N-2} \\ \vdots \\ h_k \end{pmatrix}$$