Thus, Example 2 shows that in spite of (48) holding, condition (28) for NTRU modulo p applicability does not hold, and applying modulo p operation to the ciphertext (49) after center-lifting in (48), we do not get back the plaintext (20) in (50).

5. NTRU Amendment to Fix NTRU Modulo p Flaw

NTRU constraints (4) guarantee correctness of decryption process (14), (15). But these constraints donot guarantee that at least one of the product (27) coefficients is exceeding the value of q in absolute value. To fix the NTRU modulo p flaw specified in the present paper, an amendment must be made so that in addition to (4), it is necessary that the following condition shall hold:

$$M = p.F_q = [M_0, ..., M_{N-1}]$$
$$for\ \exists i \in \{0, ..., N-1\},\ |M_i| > q. \quad (52)$$

Thus, the product, $p \cdot F_q$, shall have at least one coefficient exceeding q by the absolute value. If condition (51) holds, eliminating of the product, A, from equation (27) by modulo p operation is generally not possible because at least one term in the product maybe not a multiple of p. However, in spite of the condition of applicability of the modulo p flaw is violated if (51) holds, it is not excluded an opportunity that modulo p operation reveals a plaintext, and this question needs further investigation.

6. Conclusion

In this paper, we presented NTRU modulo p flaw by construction of an example of a plaintext decryption just applying modulo p operation to the ciphertext. We explained that the flaw happens when all coefficients of (27) are less than q in absolute value. In this case, A from (27) has coefficients that are multiples of p which can be eliminated by modulo p operation. We also presented statistics of probability of the determinant (39) absolute value getting equal to 1 that in many cases allows application of NTRU modulo p flaw. We considered dependence of the probability on N, the order of the polynomial (1). These statistics shows that the probability decreases with the growth of N .To fix the NTRU modulo p flaw, we proposed an amendment to NTRU by extending condition (4) by condition (51) guaranteeing that at least one coefficient of (27) is exceeding q in absolute value so that plaintext generally cannot be revealed using modulo p operation.

7. References

[1] Hoffstein, J., J. Pipher, and J.H. Silverman, NTRU: A ring-based public key cryptosystem, in Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA, June 21–25, 1998 Proceedings, J.P. Buhler, Editor. 1998, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 267-288.

[2]IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. IEEE Std 1363.1-2008, 2009: p. C1-69.

[3]Hermans, J., F. Vercauteren, and B. Preneel, Speed Records for NTRU, in Topics in Cryptology - CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings, J. Pieprzyk, Editor. 2010, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 73-88.

[4]Chefranov, A. and A. Ibrahim. NTRU Mod p Flaw. in World Congress on Internet Security (WorldCIS-2016). 2016. Infonomics Society. http://www.iicedu.org/WorldCIS-2016/WorldCIS-2016-Proceedings.pdf

[5]Hoffstein, J., J. Pipher, and J.H. Silverman, Lattices and Cryptography, in An Introduction to Mathematical Cryptography. 2014, Springer New York: New York, NY. p. 373-470.

[6]Strang, G., Cramer's Rule, Inverses, and Volumes, in Introduction to Linear Algebra. 2016, Wellesley-Cambridge Press.

