InPrime: Indonesian Journal of Pure and Applied Mathematics
Vol. 5, No. 2 (2023), pp. 136 – 143, doi: 10.15408/inprime.v5i2.32011
p-ISSN 2686-5335, e-ISSN: 2716-2478

Comparison Between Algebraic Cryptanalysis on DES and NTRU

Fadila Paradise* and Kiki Ariyanti Sugeng
Department of Mathematic, FMIPA Universitas Indonesia, Depok, Indonesia
Email: *fadila@sci.ui.ac.id, kiki@sci.ui.ac.id

Abstract

Algebraic cryptanalysis is a cryptanalysis method that aims to exploit the algebraic structure of an encryption algorithm to obtain the secret key. Algebraic cryptanalysis becomes interesting because it uses a small amount of known plaintext, which in real life very few known plaintexts are available. Algebraic cryptanalysis has previously been performed on several block cipher algorithms and public key lattice-based algorithms. In this study, DES and NTRU were chosen as the objects of algebraic cryptanalysis. This research aims to compare algebraic cryptanalysis on DES and NTRU in terms of their applicability, and to what extent algebraic cryptanalysis can be successful in obtaining keys.
Keywords: Algebraic Cryptanalysis; DES; NTRU; polynomial equation.

Abstrak

Algebraic cryptanalysis adalah metode kriptanalisis yang bertujuan untuk memanfaatkan struktur aljabar pada algoritma enkripsi untuk mendapatkan kunci. Algebraic cryptanalysis menarik karena hanya membutuhkan sedikit plaintext, di mana pada kehidupan nyata hanya sedikit plaintext yang bisa didapatkan. Algebraic cryptanalysis sebelumnya dilakukan pada algorima block cipher dan algoritma kunci publik berbasis latis. Pada penelitian ini, DES dan NTRU dipilih sebagai objek algebraic cryptanalysis. Penelitian ini bertujuan untuk membandingkan algebraic cryptanalysis pada DES dan NTRU, serta sejauh mana algebraic cryptanalysis bisa mendapatkan nilai kunci.
Kata Kunci: *Kriptanalisis aljabar; DES; NTRU; persamaan polinomial.*

2020MSC: 94A60.

1. INTRODUCTION

Cryptography is the study of the principles and techniques used to hide information in cipher form and then reveal it to an authorized user using a secret key [1]. Cryptanalysis is a study (and art) of methods and techniques to obtain information from encrypted texts or messages [2]. Cryptanalysis can also be said as the process of studying cryptographic systems to look for weaknesses or leaks of information [3].

There are so many methods for carrying out cryptanalysis, one of them is algebraic cryptanalysis. Algebraic cryptanalysis become very interesting because of several reasons. First, algebraic cryptanalysis aims to find the exact key value, while other cryptanalysis aims to find some possible keys and perform trial and error to find the right key. Second, algebraic cryptanalysis uses a small amount of known plaintext, which in real life very few known plaintexts are available. Lastly, the study of algebraic cryptanalysis is relatively new compared to others, such as linear and differential cryptanalysis [4].

Algebraic cryptanalysis has previously been performed on several block cipher algorithms, and public key lattice-based algorithms [5]. In this research, one block cipher and one lattice-based algorithm that have been standardized are taken to be the example objects of algebraic cryptanalysis,

* Corresponding author
Submitted April 18th, 2023, Revised November 12th, 2023,
Accepted for publication November 16th, 2023, Published Online November 30th, 2023

DES, and NTRU. DES was announced as a standard of the cryptographic algorithm for data security in FIPS 46-3 (1999) [6]. NTRU became the IEEE standard for public key cryptographic techniques based on hard problems over lattices in 2008 [7]. DES and NTRU certainly have very different structures. This research aims to see the difference in the application of algebraic cryptanalysis to symmetric and asymmetric algorithms, with DES and NTRU as example algorithms being the problem limitation of this research. Furthermore, this research also looks at the extent to which algebraic cryptanalysis can obtain the key value of the key.

2. THEORETICAL FRAMEWORK

2.1. Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric-key algorithm, specifically a block cipher cryptosystem developed by IBM in 1960-1971. DES is set as a standard by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standards Publications (FIPS PUBS) 46-3 [6]. DES was eventually replaced by the Advanced Encryption Standard (AES) after a public competition. On 19th May 2005, FIPS 46-3 was officially withdrawn [1].

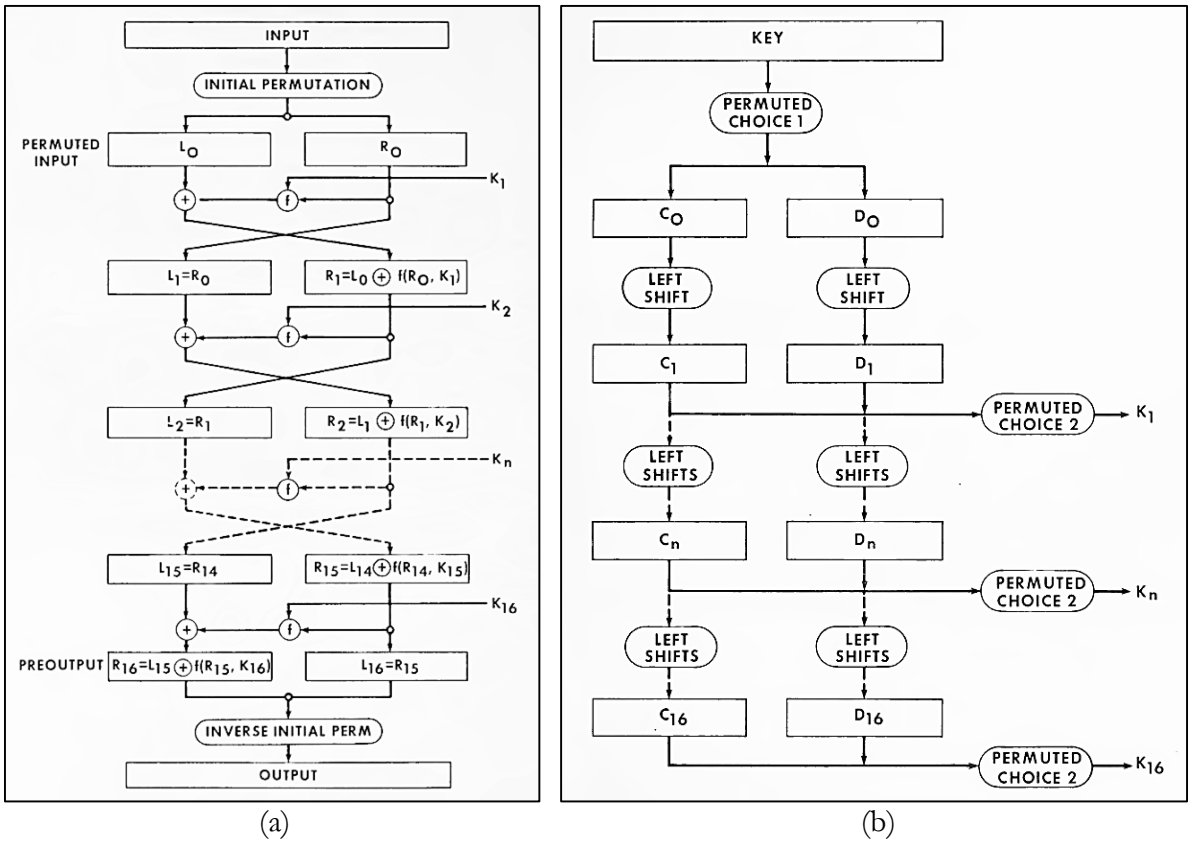

Figure 1. (a) DES Structure; **(b)** Key Scheduling Structure [6]

DES is designed to encrypt and decrypt blocks of data in 64 bits using a 56-bit key. The 64 bits of input block first goes through an initial permutation (IP) and then it is separated into 32-bit left (L_i) and 32-bit right (R_i). Each of these 32-bit blocks is processed through key-dependent

computation and swapped before going through the second key-dependent computation until the 16th iteration. The 32-bit right and 32-bit left of the last iteration finally go through a process that is the inverse of the initial permutation (IP^{-1}) and the output of IP^{-1} is retrieved as ciphertext [6].

The key-dependent computation is simply divided into two parts, cipher function and key schedule function. The cipher function consists of expansion, key mixing, substitution box (s-box), and permutation. The key schedule function is used to map a 56-bit key into 16 iteration keys ($\mathrm{K_n}$) of 48-bit length. Each of these iteration keys is used in key mixing in every iteration. Decryption on DES is the encryption process that uses reverse-order iteration keys. DES structure can be seen in Figure 1(a), and DES key scheduling structure can be seen in Figure 1(b) [6].

2.2. NTRU

NTRU is an asymmetric-key algorithm, specifically a lattice-based public key cryptosystem designed by Hoffstein, Pipher, and Silverman in 1996 [8]. NTRU was published at the Algorithmic Number Theory Symposium (ANTS) in 1998 and became the IEEE standard for public key cryptographic techniques based on hard problems over lattices in 2008 [7]. NTRU was redeveloped by NTRU Inc. [9] and became one of the finalists in round 3 of the post-quantum cryptography standardization process organized by NIST in 2020 [10].

The public key cryptosystem is an asymmetric cryptosystem in which the encryption key is different from the decryption key [11]. NTRU as a public key cryptosystem also has two different keys, the public key to encrypt messages and the private key to decrypt messages. The security of NTRU depends on 3 parameters (N, p, q) and 4 sets of polynomials $(\mathcal{L}_f, \mathcal{L}g, \mathcal{L}_r, \mathcal{L}_m)$. Below is a brief explanation of the symbols used in NTRU

- N, p, q are integers, p, and q must be relatively prime;
- $\mathcal{L}_f, \mathcal{L}g, \mathcal{L}_r, \mathcal{L}_m$ are sets of polynomials of degree $N-1$ with integer coefficients;
- f, g, r, m are polynomials with $f \in \mathcal{L}_f, g \in \mathcal{L}_g, r \in \mathcal{L}_r, m \in \mathcal{L}_m$;
- F_p is the inverse of f in modulo p;
- F_q is the inverse of f in modulo q;
- f is the private key;
- h is public key;
- r is randomizer;
- m is message or plaintext;
- e is ciphertext.

The NTRU algorithm is running on a ring of $R = \mathbb{Z}[X]/(X^N - 1)$. Private key f is a polynomial obtained from $\mathcal{L}_f$. The system counts

$$F_q \circledast f \equiv 1 \ (mod\ q), \tag{1}$$

and

$$F_p \circledast f \equiv 1 \ (mod\ p), \tag{2}$$

then calculates the public key

$$h \equiv F_q \circledast g \ (mod\ q). \tag{3}$$

The sender selects a message (m) from the set of plaintext $(\mathcal{L}_m)$. The system then chooses a

randomizer. The $r \in \mathcal{L}_r$ uses the recipient's public key to calculate ciphertext

$$e \equiv pr \circledast h + m \ (mod\ q). \tag{4}$$

The recipient then decrypts the ciphertext by using private key f to calculate

$$a \equiv f \circledast e \ (mod\ q), \tag{5}$$

and using private key F_p to calculate

$$m \equiv F_p \circledast a \ (mod\ p). \tag{6}$$

NTRU uses cyclic convolution product (denoted as $\circledast$) in carrying out multiplication between 2 polynomial equations. Let $H = F \cdot G$ with F, G, H are arbitrary polynomials of degree $N - 1$. Then for each $0 \leq k < N$, the kth-coefficient H_k of H is given by [12]:

$$H_k = \sum_{i+j \equiv k (\mathrm{mod}\ N)} F_i G_j. \tag{7}$$

2.3 Algebraic Cryptanalysis

Cryptanalysis is a study (and art) of methods and techniques to obtain information from encrypted texts or messages. Cryptanalysis can also be said to be an analysis of cryptographic methods using mathematical formulas to detect vulnerabilities and hidden components [2]. There are two different types of cryptanalysis based on the type of information the attacker has, statistical cryptanalysis and algebraic cryptanalysis. Statistical cryptanalysis exploits statistical weaknesses in the targeted algorithm. Algebraic cryptanalysis uses polynomials with multiple variables over a finite field. This cryptanalysis requires a very small number of known plaintexts [13].

Algebraic cryptanalysis consists of two steps. The first is converting the algorithm and some additional information into a system of polynomial equations over a field or ring. The second is solving the system of polynomial equations to obtain the key [14]. In the constraint satisfaction problem (CSP), there are several constraints in variables. Algebraic cryptanalysis is performed to determine enough constraints to reduce the number of possible keys to one, and enough constraints that make the system of equations solvable in a reasonable amount of time, with the expectation that the entire process should be faster than brute force by some margin [15].

Algebraic cryptanalysis aims to exploit the algebraic structure of an encryption algorithm to obtain the secret key. In other words, algebraic cryptanalysis in block cipher aims to find the single secret key while in the public key, it aims to find the private key [16]. This is done by transforming the encryption function into a large system of nonlinear equations on a finite field, then solving the system of equations using some methods such as Gröbner Basis or XL Algorithm.

The Gröbner basis was first introduced by Buchberger in 1965 as an algorithm for solving some basic problems in polynomial theory [17]. XL algorithm was introduced by Curtois, Klimov, Patarin, and Shamir in 2000. XL algorithm is a computational method to solve a system of equations [18]. There are more methods for solving the system of polynomial equations such as F4, SAT solvers, etc [19]. Algebraic cryptanalysis does not depend on any statistical properties. The complexity of algebraic cryptanalysis depends on the complexity of algebraic solution techniques used in solving the system [20].

3. RESULTS AND DISCUSSION

3.1 Difference Between DES and NTRU

Based on the explanation in point 2, the following is a table of differences between the DES algorithm and NTRU

Table 1. Differences Between DES and NTRU

Description	DES	NTRU
Type	Symmetric algorithm	Asymmetric algorithm
Operation	Permutation, substitution, XOR	Polynomial multiplication, polynomial summation
Non-linear function	S-box	-
Number of keys	1 secret key	1 public key and 1 private key
Key length	56 bits	642 bits public key and 340 bits private key for moderate security

The difference in the structure of the DES and NTRU algorithms then determines the difference in algebraic cryptanalysis in DES and NTRU.

3.2 Algebraic Cryptanalysis on DES

Algebraic cryptanalysis occurs in 2 steps, the first is forming a linear equation system, and the second is solving a linear equation system. In general, the first step of algebraic cryptanalysis on block cipher consists of 3 parts, analysis of linear operations such as multiplication and shifting operator, analysis of s-box, and linearization abridgment [21].

Analysis of linear operations aims to find the output form of linear operations. This process is relatively simple. Analysis of the s-box could be the more challenging step. S-box is a non-linear function. There are several ways in writing the input-output relation of an s-box as mentioned by Curtois (2019) [4]. One of the simplest methods in writing an s-box input-output relation is by finding the s-box input combinations representing an s-box output via a truth table.

DES has 6 s-boxes, and each s-box substitutes a 6-bit input into a 4-bit output. Therefore, in algebraic cryptanalysis on DES, 6 truth tables are needed which represent the relationship between the 6-bit s-box input and the 4-bit s-box output. The combination of s-box input then becomes the algebraic form of the s-box. DES has 6 equations representing each s-box.

After converting the s-box into algebraic equation form, the linearization abridgment can be replaced with a simulating encryption process using the unknown key. The encryption process is used in cryptanalysis on DES or block cipher cryptosystem because it contains a secret key in the calculation. The encryption simulation process can form a system of polynomial equations representing ciphertext. The unknown variables of this system of polynomial equations are the key bits. By solving the system of polynomial equations, the key value can be retrieved.

DES consists of 16 rounds so that the equations formed are complex. On the other hand, operation on DES uses a binary system means the values are in $\mathbb{Z}_2$. Some properties of binary operations make the calculation simpler, such as $a^2 = a$ or $a * b = 0$ with $a \neq b$. Therefore, several simple elimination algorithms such as ElimLin and XL Algorithm can be used as methods in solving

a system of polynomial equations on DES. The result of solving a system of polynomial equations on DES can refer to a single solution that could be retrieved as the key value.

3.3 Algebraic Cryptanalysis on NTRU

The NTRU algorithm is running on a ring of $R = \mathbb{Z}[X]/(X^N - 1)$ with a coefficient in $\mathbb{Z}_3$ for the private key, plaintext, ciphertext, and a coefficient in $\mathbb{Z}_q$ for the public key [12]. All operations in NTRU are calculated in algebraic form. NTRU does not have any s-box, but NTRU uses two modulus operations in encrypting and decrypting the text. So even though some operations on NTRU can be unified into an algebraic form, the final calculation must be done sequentially based on the modulus.

Algebraic cryptanalysis in DES utilizes the encryption process to form a system of polynomial equations because DES uses a secret key for encryption and decryption. Unlike DES, algebraic cryptanalysis in NTRU utilizes the decryption process to form a system of polynomial equations because the secret key in NTRU is the private key used in the decryption process [5]. Simulating the decryption process on NTRU by using unknown private key variables can produce a system of polynomial equations that represent plaintext. Based on the decryption process described in equations (5) and (6), and the cyclic convolution product in equation (7), the formula of polynomial equations that represent plaintext can be written as below.

$$m_z = \sum_{x+y \equiv z (\mathrm{mod}\ n)} \left(\sum_{i+j \equiv k (\mathrm{mod}\ n)} f_i \cdot e_j \ (mod\ p) \right) \cdot f_{p_y} \ (mod\ q). \tag{8}$$

The most challenging step in algebraic cryptanalysis on NTRU is solving the system of polynomial equations. As mentioned before, NTRU uses two modulus operations so the calculation must be done sequentially, which means the system of polynomial equations generated by equation (8) must be calculated in $\mathbb{Z}_q$ first. It is needed to find suitable methods to eliminate equations whose coefficients are in $\mathbb{Z}_q$. Let's say the system of polynomial equations can be eliminated. Each monomial in the equations is in modulus $\mathbb{Z}_q$ and consists of two variables of private key f and F_p. The monomials must be factorized to find the value of f and F_p. With q values that are not prime or multiples of prime, monomial factorization will produce many solutions.

4. CONCLUSIONS

Algebraic cryptanalysis on DES is different from algebraic cryptanalysis on NTRU. It is needed to transform s-box or any nonlinear function into algebraic form in analyzing DES or some other block cipher cryptosystem, while on NTRU any transformation is not needed. The encryption process can be used for cryptanalysis on DES, while NTRU or other public key cryptosystems must use the decryption process. Overall, the steps in forming a system of polynomial equations on NTRU are simpler than on DES.

Calculation on DES is on $\mathbb{Z}_2$ while NTRU is on $\mathbb{Z}_q$. This condition makes the system of polynomial equations in DES more feasible to solve. In addition, the polynomial equations on DES contain an unknown variable of a key, while polynomial equations on NTRU contain an unknown variable of two keys. This makes solving the system of polynomial equations on DES can refer to one solution while solving the system of polynomial equations on NTRU produces many solutions. It can be concluded that algebraic cryptanalysis on DES is more feasible to do than NTRU. As a result,

algebraic cryptanalysis is more likely to be implemented on DES than NTRU even though it consists of a complex system of polynomial equations

ACKNOWLEDGEMENTS

This research is funded by Dikti Research Grant No NKB-988/UN2.RST/HKP.05.00/2022.

REFERENCES

[1] G. Simmons, "Cryptology," Encyclopaedia Britannica, Inc., 2 August 2022. [Online]. Available: https://www.britannica.com/topic/cryptology. [Accessed 2 April 2023].

[2] A. Al-Sabaawi, "Cryptanalysis of Classic Ciphers: Methods Implementation Survey," *2021 International Conference on Intelligent Technologies (CONIT)*, pp. 1-6, Hubli, India, 2021, doi: 10.1109/CONIT51480.2021.9498530.

[3] T.W. Edgar, D.O. Manz, "Chapter 2 - Science and Cyber Security," *Research Methods for Cyber Security*, pp. 33-62, Syngress, 2017, doi: 10.1016/B978-0-12-805349-2.00002-9.

[4] N. Curtois and G. Bard, "Algebraic Attack of the Data Encryption Standard," *Proceedings of the 11th IMACC'07, Lecture Notes in Computer Science*, vol. 4887, pp. 152-169, Springer, Berlin, Heidelberg, 2008, doi: 10.1007/978-3-540-77272-9_10.

[5] J. Ding, D. Schmidt, "Algebraic Attack on Lattice-Based Cryptosystems Via Solving Equations Over Real Numbers," *IACR Cryptology ePrint Archive 94*, 2012.

[6] National Institute of Standards and Technology (NIST), "Data Encryption Standard (DES)," Federal Information Processing Standards (FIPS) Publication 46-3, 1999. Available: https://csrc.nist.gov/CSRC/media/Publications/fips/46/3/archive/1999-10-25/documents/

[7] fips46-3.pdf.

[8] IEEE, "IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices," *IEEE Std 1363.1-2008*, pp. 1-81, 10 March 2009, doi: 10.1109/IEEESTD.2009.4800404.

[9] D. Micciancio and O. Regev, "Lattice-based Cryptography," In: D. J. Bernstein, J. Buchmann, E. Dahmen, (eds) *Post-Quantum Cryptography*, Springer, Berlin, Heidelberg, pp. 147-191, 2009, doi: 10.1007/978-3-540-88702-7_5.

[10] C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijnveld, J. M. Scanck and T. Saito, P. Schwabe, W. Whyte, K. Xagawa, T. Yamakawa, Z. Zhang, "NTRU: Algorithm Specifications and Supporting Documentation," NTRU Inc., 2020. [Online]. Available: https:// https://ntru.org/release/NIST-PQ-Submisssion-NTRU-20190330.tar.gz.

[11] NIST.IR.8309, "Status Report on The Second Round of NIST Post-Quantum Cryptography Standardization Process," NIST, Gaithersburg, 2020.

[12] D. Liestyowati, "Public Key Cryptography," *Journal of Physics: Conference Series*, vol. 1477, 2019, doi: 10.1088/1742-6596/1477/5/052062.

[13] J. Hoffstein, J. Pipher and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," *Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science*, vol. 1423, Springer, Berlin, Heidelberg, 1998, doi: 10.1007/BFb0054868.

[14] W.I. Alsobky, H. Saeed, "Different Types of Attacks on Blocks Ciphers," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 9, 2020, doi: 10.35940/ ijrte.C4214.099320.
[15] A. Hossein, B. Sadeghiyan, J. Pieprzyk, "S-boxes Representation and Efficiency of Algebraic Attack," *IET Information Security 13*, pp. 448-458, 2019, doi: 10.1049/iet-ifs.2018.5201.
[16] G.V. Bard, "Algebraic Cryptanalysis," Springer Dordrecht Heidelberg, New York, 2009, doi: 10.1007/978-0-387-88757-9.
[17] M. Bardet, M. Bertin, A. Couvreur, A. Otmani, "Practical Algebraic Attack on DAGS," In: Baldi, M., Persichetti, E., Santini, P. (eds) *Code-Based Cryptography*, *Lecture Notes in Computer Science*, vol 11666. Springer, Cham. 2019, doi: 10.1007/978-3-030-25922-8_5.
[18] H. Wang, L. Zhang, Q. Wang, S. Yan, "The Gröbner Bases Algorithm and its Application in Polynomial Ideal Theory,". *2019 Chinese Control and Decision Conference (CCDC)*, pp. 494-499, Nanchang, China, 2019, doi: 10.1109/CCDC.2019.8833013.
[19] C. Mascia, E. Piccione, M. Sala, "An algebraic attack on stream ciphers with application to nonlinear filter generators and WG-PRNG", 2021, doi: 10.48550/arXiv.2112.12268.
[20] A. Abdel-Hafez, R.A. Elbarkouky, W. Hafez, "Comparative Study of Algebraic Attacks," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 3, pp. 85-90, 2016, doi: 10.17148/IARJSET.2016.3519.
[21] S.L. Yeo, D.P. Le, K. Khoo, "Improved algebraic attacks on lightweight block ciphers,"
[22] *J Cryptogr Eng 11*, pp. 1–19, 2021. doi: 10.1007/s13389-020-00237-4.
[23] R. Biyashev, D. Dyusenbayev, K. Algazy, N. Kapalova, "Algebraic Cryptanalysis of Block Ciphers," *Proceedings of the 2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019)*, pp. 129-132, Atlantis Press, doi: 10.2991/wcnme-19.2019.30.