Novel location permutation encryption based on exponential numbers

Weixuan Xie*[a], Ho-Hsuan Chang[a], Jianhui Li[b]
[a]Information Engineering College, Guangzhou City Construction College, Guangzhou, Guangdong, China; [b]Foshan Polytechnic, Foshan, Guangdong, China

ABSTRACT

The pattern of exponential number can achieve 99% ideal uniformity distribution level and is characterized with quasi-random nature. In this study exponential pattern is modified to possess an ideal uniform distribution property for operating location permutation. Cipher space of the proposed permutation scheme can achieve its factorial function upper bound. Brute-force restoration of permutation belongs to factorial complexity order which is more complex than exponential function. The proposed encryption scheme belongs to lightweight cryptographic function that is applicable to internet of things (IoT). This novel encryption technique can outperform the advanced encryption standard (AES) from the simplicity of algorithm, the availability, generation and distribution of long encryption key, and high confidentiality level points of view.

Keywords: Continued fraction, cryptography, cryptosystem, encryption, PGIS

1. INTRODUCTION

The fast development of technology and Internet contributes new applications to several emerging areas, which include internet of things (IoT), sensor networks, distributed control systems, and the smart grid. In these areas or environments resource-constrained devices are interconnected to accomplish some tasks, where the communication channel is typically wireless. Data transmission through unsecured wireless channel or public networks can be easily browsed, stolen, tampered, copied, and spread illegally. However, the majority of current cryptographic algorithms, i.e., the symmetric cryptosystems and the asymmetric systems, were designed for desktop or server platforms, which could not fit into resource-constrained devices.

Lightweight cryptographic functions are preferable where platform devices are characterized by limited memory, bandwidth and computing capability. National institute of standards and technology (NIST) initiated a project to solicit, evaluate, and standardize lightweight cryptographic algorithms in Lightweight Cryptography Workshop 2015, and 10 finalists were announced in March 2021[1]. A novel trapdoor one-way permutation function based on operating circular convolution over perfect Gaussian integer sequences (PGISs) was proposed in Reference[2]. With this property, a hybrid public/private key cryptography scheme based on PGIS can serve as the candidate of lightweight cryptographic function[2]. More properties, construction and applications of PGISs can refer to References[3-8].

In this study we propose a novel location permutation encryption based on a set of exponential numbers, which is considered the lightweight cryptographic algorithm. As defined and addressed in section 2, the pattern of exponential number can achieve 99% ideal uniformity distribution level and is characterized with quasi-random nature[9,10]. Possessing with these two merits, exponential pattern can be easily modified to become an ideal uniform distribution pattern which is adequate to serve as permutation algorithm for location permutation. Substitution and permutation techniques are still applied to some modern cryptography, i.e., DES and AES. The comparison between AES and the proposed scheme is analyzed in this paper.

2. PRELIMINARY

2.1 Pattern of exponential number

Let g^e be an exponential number, where g and e are positive integers. Let $g^e = d_m d_{m-1} \ldots d_0$ denotes the value of g^e from taking multiplication upon g with e-1 times, and it demonstrates that g^e has m+1 digits. In a base-10 numerical expression

* 450939142@qq.com

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 125061H
 · 0277-786X · doi: 10.1117/12.2662036

the value of the leftist digit is $d_m \times 10^m$, the second digit is $d_{m-1} \times 10^{m-1}$, etc., and $d_n \in \{0, 1, ..., 9\}$, $n = 0, 1, \ldots, m\text{-}1$.

Definition The pattern of an exponential number is denoted by (g^e), where $(g^e) \stackrel{\text{def}}{\cong} (d_m d_{m-1} \ldots d_0)$ is defined as the distribution of digits $\{d_n\}_0^m$ in an $(m + 1)$-tuple vector, where $d_m \neq 0$.

Let's present two examples. The value 2^{47} = 140737488355328 has 15 digits, and the pattern of 79^{53}, denoted by (79^{53}), is expressed as follows:

$$(79^{53}) \stackrel{\text{def}}{\cong} (37517, 66821, 20996, 14616, 00811, 79563, 30183, 03244, 90427, 84683, 08857,$$
$$23191, 19977, 84629, 78352, 26593, 94219, 69109, 10161, 29703, 9) \quad (1)$$

Equation (1) indicates that the (79^{53}) pattern consists of 101 decimal digits, which is considered a vector or sequence with 101 elements. There exists neither the explicit relationship between $(g^e) \stackrel{\text{def}}{\cong} (d_m d_{m-1} \text{---} d_0)$ and $(g^{e+k}) \stackrel{\text{def}}{\cong} (c_n c_{n-1} \text{---} c_0)$ two patterns, nor the relationship between g^e and $(gh)^e$, where h is an arbitrary positive integer, $n > m$, and d_0 might not equal to c_0. The only method that can derive pattern $(C_n C_{n-1} \cdots C_0)$ from $(d_m d_{m-1} \cdots d_0)$ is through operating multiplication between $(d_m d_{m-1} \cdots d_0)$ and $g^k = (e_k e_{k-1} \cdots e_o)$, i.e., 2^{47} = 140737488355328 = 70368744177664 × 2, where 2^{46} = 70368744177664.

Though addition chain algorithm might be applied for fast calculating g^e and deriving the pattern of g^e, the multiplication of two integers is not a linear operation, where the product of two decimal digits can bring overflow to the adjacent next digit, and the overflow is data dependence which can only be analyzed case by case. In other words, there exists no general expression that can describe the relationship between two patterns obtained from two different exponential numbers. More specifically, it is especially challenging to find a set of functions $c_k = f_k(d_m, d_{m-1}, \cdots d_0)$, $k = 0, 1, \ldots, n$, which can be used to describe the relationship between $C_n C_{n-1} \cdots C_0$ and $d_m d_{m-1} \cdots d_0$ for arbitrary $\{c_i\}$ and $\{d_i\}$ two sets.

The pattern of g^e is unpredictable, which is characterized with quasi-random nature. In Reference[9] entropy was applied to evaluate the uniformity level of exponential decimal patterns. Regardless of whether the base element is a prime or a composite number, it showed that pattern with length larger than 90 can reach 99.9% uniformity level[9].

2.2 Complexity hierarchy

As described in Reference[10], those algorithms that can be performed in polynomial time are considered efficient algorithm, and those algorithms that can only be performed in exponential time are inefficient algorithms. We can present a hierarchy of increasing complexity orders as follows:

$$\log n, n, n^2, n^3, ..., 2^n, 3^n, ..., n!, n^n$$

Taking the execution time of solving factorial function with input size n = 30 as an example, it is still infeasible for the current computing system, which is 8.4×10^{14} centuries[10].

3. LOCATION PERMUTATION BASED ON EXPONENTIAL PATTERN

With the unpredictable quasi-random property, the pattern of exponential number can be applied to provide the desirable security to the resultant ciphertext, when plaintext is encrypted using a set of exponential numbers $\{g^e\}$[11]. This study presents a novel location permutation encryption scheme using patterns of $\{g_i^{e_i}\}_{i=1}^k$. However, we should modify these patterns to match the ideal uniform distribution requirement to enable permutation application, and the detailed analysis of this encryption scheme is addressed in the following subsections.

3.1 Construction of ideal uniform pattern

Let $N = 10n + m$ be the number of decimal digits of an exponential pattern, where $n > 0$ and $0 \leq m \leq 9$. The procedures of obtaining a pattern with the ideal uniform distribution based on arbitrary exponential pattern are summarized as follows:

(1) The first $10n$ digits of an exponential pattern are grouped into n blocks, where each block has ten digits, and we discard

the rest *m* digits from this pattern.

(2) We should check the existence of repeating decimal digits from the first digit till the last one in each block, and delete all repeating digits which are appeared at the later locations in this block. We make a record the number of digits that are deleted in each block.

(3) We should insert the same number of decimal digits which are deleted in Step (2), and these decimal digits are chosen in ascending order from the rest of other ten decimal digits that are not appeared in each block. In this step, ten decimal digits appear exactly one time in a 10-tuple block throughout the entire *n* blocks.

(4) We can index these *n* blocks sequentially with subscript number {0, 1, 2, …, *n*-1}, respectively, to identify the actual locations when the associated block is applied for operating permutation, where the block indexed by *k* indicates that ten decimal numbers of this block should add 10*k* to denote ten locations at the interval between 10*k* and 10*k* + 9.

From these four steps we can obtain a new pattern of length 10*n* with the same number of ten digits {0, 1, 2, …, 8, 9} within this pattern, and this implies that new pattern can match the ideal uniform distribution requirement, where $p(i) = \frac{1}{10}$, $\forall i \in \{0,1,2,...,8,9\}$.

Let's take the (2^{312}) pattern as an example for demonstration the procedures of creating an ideal uniform distribution pattern. In equation (2), the (2^{312}) pattern consists of 94 digits, and we would discard the last four digits 2096, which are underlined, to form a new pattern with 90 digits. New pattern can be grouped into nine blocks, and we would use the first block for demonstration the above procedures. In the first block, 3 and 9 two digits appear three times 8343699359, where the latter two 3 and two 9 digits are underlined indicating that these four repeating digits should be deleted from this block. This results in 834$\underline{3}$699$\underline{35}\underline{9}$ → 834695. Among ten decimal digits only six digits {8, 3, 4, 6, 9, 5} appear in this block, thus we should insert the remaining four digits {0, 1, 2, 7}, which are arranged with ascending order, to the end of 834695 to form a new 10-tuple block. We use expression $834695 \to 8346950\overline{127}$ to present this operation, where these four digits are overlined for identification. The operation of other eight blocks is similar to the first one, from which we derive a new pattern of length 90, denoted by [2^{312}].

$$
\begin{aligned}
(2^{312}) &\stackrel{\text{def}}{\equiv} (8343699359, 0660550093, 5555353972, 4812947666, 8145404556,\\
&\quad 7488260563, 1280555545, 8038306271, 4852719565, 2096)\\
&\to (8343699359, 0660550093, 5555353972, 4812947666, 8145404556,\\
&\quad 7488260563, 1280555545, 8038306271, 4852719565)\\
&\to (834695, 06593, 53972, 4812976, 814506, 74826053, 128054, 8036271, 48527196)\\
&\to (834695\overline{0127}, 0659\overline{312478}, 5397\overline{201468}, 481297\overline{6035}, 814506\overline{2379},\\
&\quad 748260\overline{5319}, 128054\overline{3679}, 803469\overline{5459}, 485271\overline{9603})\\
&\to ([834695017]_0, [0659312478]_1, [5397201468]_2, [4812976035]_3, [8145062379]_4,\\
&\quad [7482605319]_5, [1280543679]_6, [8036271459]_7, [4852719603]_8)\\
&\to [8346950127, 0659312478, 5397201468, 4812976035, 8145062379,\\
&\quad 7482605319, 1280543679, 8036271459, 4852719603] \stackrel{\text{def}}{\equiv} [2^{312}].
\end{aligned}
\tag{2}
$$

To make a link between the 90 digits of an ideal uniform distribution pattern [2^{312}] and a set of ordered {0, 1, 2, …, 89} locations, here [2^{312}] is indexed by a set of subscript numbers $k \in \{0,1,2,...,8\}$ indicating that ten digits of each block should add the value 10*k*, respectively, to present the actual ten locations of the associated block, i.e.,

$$[8346950127]_0 \equiv \{8,3,4,6,9,5,0,1,2,7\},$$

and

$$[8036271459]_7 \equiv \{78,70,73,76,72,77,71,74,75,79\}.$$

However, we would omit the subscript number from the pattern to simplify the expression of formula and to operate adequately the location permutation, and the ideal uniform pattern based on exponential number 312^{312} is expressed as follows:

$$[2^{312}] \stackrel{\text{def}}{=} [8346950127, 0659312478, 5397201468,$$
$$4812976035, 8145062379, 7482605319,$$
$$1280543679, 8036271459, 4852719603].$$

Except the patterns of (2^{312}) and $[2^{312}]$, Table 1 presents also the patterns of (79^{53}), $[79^{53}]$, (79^{54}), and $[79^{54}]$ for comparison.

Table 1. Exponentiations and the associated ideal uniform patterns.

g^r	Decimal exponential pattern (g^r) and uniform pattern [g^r]	Digits No.
(2^{312})	(8343699359, 0660550093, 5555353972, 4812947666, 8145404556, 7488260563, 1280555545, 8038306271, 4852719565, 2096)	94
$[2^{312}]$	(8346950127, 0659312478, 5397201468, 4812976035, 8145062379, 7482605319, 1280543679, 8036271459, 4852719603)	90
(79^{53})	(3751766821, 2099614616, 0081179563, 3018303244, 9042784683, 0885723191, 1997784629, 7835226593, 9421969109, 1016129703,9)	101
$[79^{53}]$	[3751682049, 2096143578, 0817956324, 3018245679, 9042786315, 0857231946, 1978462035, 7835269014, 9421603578, 1062973458]	100
(79^{54})	(2963895788, 7558695546, 6464131855, 0084459563, 4743799899, 6399721321, 0478249857, 5289829009, 2143355596, 1902742466, 081)	103
$[79^{54}]$	[2963857014, 7586940123, 6413850279, 0845963127, 4739801256, 6397210458, 0478295136, 5289013467, 2143596078, 1902746358]	100

3.2 Permutation based on idea exponential pattern

Let plaintext be English message with length $9k < N \le 10k$, where each one of English letters, comma, semicolon, period, blank space and special symbols occupies one location, and these N symbols are indexed by a set of ordered elements {0, 1, 2, …, N-1}. The first step of operating location permutation is inserting $10k$ - N numbers of "o" to the end of message for matching the same $10k$ length of an ideal uniform exponential pattern. Taking English sentence "The more you read, the more healthy and brave your spirit will be." with length 66 as an example, we can add four *oooo* to the end of this message to become 70 length, which is given by "The more you read, the more healthy and brave your spirit will be.*oooo*".

In the second step the contents of message are grouped into k blocks, which are indexed by {0, 1, 2, …, k-1}. Let f_k denotes the permutation function of processing the k-th message block by using the k-th block of an ideal uniform pattern. Two permutation functions taken from the first and the eight blocks of $[2^{312}]$ are shown for demonstration, which are

$$f_0 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 8\,3\,4\,6\,9\,5\,0\,1\,2\,7 \end{pmatrix} \tag{3}$$

and

$$f_8 = \begin{pmatrix} 80\,81\,82\,83\,84\,85\,86\,87\,88\,89 \\ 84\,88\,85\,82\,87\,81\,89\,86\,80\,83 \end{pmatrix} \tag{4}$$

In equation (4) all digit numbers belong eighties, we would like to delete the first digit 8 from f_8 to simplify the expression

and permutation operation, which derives the following mapping results

$$f_8 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 4\,8\,5\,2\,7\,1\,9\,6\,0\,3 \end{pmatrix} \tag{5}$$

The first step of operating location permutation is the partition of plaintext into a set of 10-digit blocks, that is, "The more y| ou read, t| he more he | althy and | brave your spirit will be.oooo". In this expression, we would use the "," symbol to indicate the partition instead of the semicolon symbol "," to avoid the confusion with message, because "," is considered the content of message. We may apply the first seventy digits of the ideal uniform pattern [79^{53}], which is given by "3751682049|2096143578|0817956324|3018245679|9042786315|0857231946|1978462035", to operate the location permutation.

The first block "Te more y" results in "e rT emhoy" by operating permutation based on the first ten digits 3751682049, and the second block "ou read, t" becomes "ueoda,r t" based on 2096143578, etc. By operating permutation based on [79^{53}], it derives "e rT emhoy| ueoda,r t | h h eremeo| ltya andh | ruvoarye b | triwpiis | olooeo. bl".

The more you read, the more healthy and brave your spirit will be. oooo

→ *e rT emhoyueoda, r t h h eremeoltya andh ruvoarye b triwpiis olooeo. bl (by*[79^{53}])

→ *rye b triwpiis olooeo. ble rT emhoyueoda,r t h h eremeoltya andh ruvoa* $(25 - shift)$

→ *rir w etbylooeoispi rb.eoTl eodehouamyh h , er ttloeyare mav oneadhr (by*[79^{54}]*)* (6)

3.3 Local to global permutation

The permutation function f_k is a 10-by-10 mapping scheme, where each set of 10 locations within the same block operates location permutation independently, from which the initial cyphertext is derived by combining all blocks collectively. This scheme can achieve only local permutation between a pair of 10 locations from two sets, where the computing load to attack each block by brute force is 10! = 3628800. When plaintext is with 10k length, the computing load can reach only to the amount of $O\big((10!)k\big)$.

Table 2. Comparison of $N^i\,(10!)^{(i+1)N/10}$, AESs and factorial function N!.

$N^i\,(10!)^{(i+1)N/10}$	$i = 1$	$i = 2$	$i = 3$	AES-128	AES-192	AES-256	N!
N = 20	2.63×10^{14}	(3.47×10^{27})					2.43×10^{18}
N = 30	1.43×10^{21}	$([6.85\times 10^{40}])$		3.4×10^{38}			2.65×10^{32}
N = 40	6.94×10^{27}	(1.20×10^{54})					8.16×10^{47}
N = 50	3.15×10^{34}	$([1.98 \times 10^{67}])$			6.28×10^{57}		3.04×10^{64}
N = 60	1.37×10^{41}	$[3.13 \times 10^{80}]$	(7.14×10^{119})	3.4×10^{38}	6.28×10^{57}	1.16×10^{77}	8.32×10^{81}
N = 70	5.80×10^{47}	$[4.81 \times 10^{93}]$	(3.98×10^{139})			1.16×10^{77}	1.20×10^{100}
N = 80	2.41×10^{54}	$[7.23 \times 10^{106}]$	(2.17×10^{159})			1.16×10^{77}	7.16×10^{118}
N = 120	$[6.26\times 10^{80}]$	3.26×10^{159}	(1.70×10^{238})			1.16×10^{77}	6.69×10^{198}

Note: The number marked by quotation mark (•) indicates the boundary where $N^i\,(10!)^{(i+1)N/10}$, and [•] mark indicates the proposed scheme outperforms other AES on the same row.

To enable global permutation through entire domain of message, which is to operate permutation across the whole set of locations $\{0,1,2,...,N-1\}$, first the initial cyphertext can be circularly shifted to the right by $m \in \{0,1,2,...,N-2\}$ steps, then the second location permutation is applied by another ideal uniform pattern. In other words, plaintext is subject to one circular shift and two rounds of location permutation. When $i \geq 1$ rounds of circular shift are applied, the cypher space will approach to the amount of $(N-1)(N-2)\cdots(N-i) \equiv O(N^i)$, and that of $i + 1$ rounds of permutation will be

proportional to $O\left(N^i \cdot (10!)^{(N/10)(i+1)}\right)$.

The proposed "*permutation + circularshift + permutation+...*" encryption scheme can achieve the complexity level of a factorial function, where $O\left(N^i \cdot (10!)^{(N/10)(i+1)}\right) \rightarrow N!$ for some small *i*. As shown in Table 2, $O\left(\mathrm{N} \cdot (10!)^{N/5}\right) > N!$ when $20 < N < 50$, and $O\left(N^2 \cdot (10!)^{3N/10}\right) > N!$ when $60 < N < 120$, where the number within the quotation mark (•) indicates the boundary where $N^i (10!)^{(i+1)N/10} > N!$ on the same row.

Equation (6) presents the results of operation two rounds of permutation based on [79^{53}] and [79^{54}] two ideal uniform patterns and one circular shift to the right by 25 steps. It is obvious that deriving "rir w etbylooeoispi rb.eoTl eodehouamyh h , er ttloeyare mav oneadhr" from plaintext "The more you read, the more healthy and brave your spirit will be.oooo" is straightforward. However, can one restore "The more you read, the more healthy and brave your spirit will be.oooo" from cyphertext "rir w etbylooeoispi rb.eoTl eodehouamyh h, er ttloeyare mav oneadhr"? when the permutation information of [79^{53}] and [79^{5}] are unavailable. It is extremely challenging!

4. COMPARISON BETWEEN AES AND THE PROPOSED SCHEME

The comparisons between AES and the proposed encryption scheme are summarized as follows:

(1) Confidentiality level of AES depends on long secret key, where key numbers of AES-128, AES-192, and AES-256 are 2^{128}, 2^{129} and 2^{256}, respectively; while cipher space of the proposed scheme is proportional to $N^i (10!)^{(i+1)N/10}$, where longer the length *N* of message contributes higher confidentiality level. Table 2 presents the comparison of complexity function of $N^i (10!)^{(i+1)N/10}$ and three AESs, which the number within the $[\bullet]$ mark indicates the boundary where the proposed scheme outperforms other three AESs on the same row. It shows that two rounds of circular shift and three rounds of location permutation can achieve higher confidentiality level than AES-128 when message length is $N = 30$, and it requires only one circular shift and two rounds of permutation when $N = 60$. To outperform AES-129 and AES-256, only two circular shifts and three rounds of permutation are required when $N = 50$. In case of one circular shift and two permutation rounds, the proposed scheme outperforms AES-256 when $N = 120$.

(2) AES defines four transformations, which are the substitution of data using Rijndael S-box, the shifts of data rows, the mixes of columns using a predefined matrix, and the last transformation is performed using the encryption key. AES-256 operates 14 rounds of Add-Round-Key operation according to AES key schedule to ruin any symmetries that may have been introduced by the other steps in the algorithm, thus making it harder to crack. However, the proposed scheme operates *i* rounds circular shift and *i* + 1 rounds permutation with *i* can be as small as 2 or 3, and the encryption and decryption of AES are complicated compared with the proposed scheme.

(3) The security of AES depends on long secret encryption key, and long key requires more processing power and execution time. In addition, the cost and delay imposed by key distribution make the transfer of business communications to IoT or Internet challenging. Location permutation of the proposed scheme is governed by a set of ideal uniform patterns which are obtained from a set of exponential numbers. Thus, security of the proposed scheme relies on the secrecy of exponential numbers. The existence of unlimited exponential numbers contributes great advantage to operate the proposed scheme; however more complex algorithms for generating long encryption keys are required to operate AES. In addition, because each ideal uniform distribution pattern can be uniquely derived from one exponential number, the storage, management and distribution of a set of ideal uniform distribution patterns are equivalent to process and organize a set of exponential numbers $\left\{g_0^{r0}, g_1^{r1}, ..., g_n^{rn}\right\}$, and it is a less challenging work compared with the counterpart part of AES-256 cryptosystem where all long secret encryption keys are with 256 bits.

5. CONCLUSION

A novel location permutation based on a set of exponential numbers is proposed in this study. We show that the proposed permutation algorithm that can achieve the upper bound of operating permutation. The unlimited abundant exponential patterns can be applied to generate the ideal uniform distribution patterns for location permutation. With high confidentiality level and algorithm simplicity, the proposed encryption scheme is considered to be lightweight cryptographic function that is applicable to IoT platform. Finally, the proposed scheme can outperform AES from the

simplicity of algorithm, the availability, generation and distribution of long encryption key, and high confidentiality level points of view. The implementation of this novel scheme is our future work.

ACKNOWLEDGEMENTS

The research is supported by special projects (new generation of information technology) of ordinary universities in Guangdong Province under no. 2020ZDZX3104.

REFERENCES

[1] https://csrc.nist.gov/publications/detail/nistir/8369/final.
[2] Hsia, C. H., Lou, S. J., Chang, H. H. and Xuan, D., "Novel hybrid public/private key cryptography based on perfect Gaussian integer sequences," IEEE Access 9, 145045-145059 (2021).
[3] Chang, H. H., Chang, K. J. and Li, C. P., "Construction of period qp PGISs with degrees equal to or larger than four," IEEE Access 6(1), 64790-64800 (2018).
[4] Chang, H. H., Li, C. P., Lee, C. D., Wang, S. H. and Wu, T. C., "Perfect Gaussian integer sequences of arbitrary composite length," IEEE Trans. Inf. Theory 61(7), 4107-4115 (2015).
[5] Lee, C. D., Huang, Y. P., Chang, Y. and Chang, H. H., "Perfect Gaussian integer sequences of odd period $2^m - 1$," IEEE Signal Process. Letters 12(7), 881-885 (2015).
[6] Lee, C. D., Li, C. P., Chang, H. H. and Wang, S. H., "Further results on degree-2 Perfect Gaussian integer sequences," IET Communication 10(12), 1542-1552 (2016).
[7] Wang, S. H., Li, C. P., Chang, H. H. and Lee, C. D., "A systematic method for constructing sparse Gaussian integer sequences with ideal periodic autocorrelation functions," IEEE Trans. Communications 64(1), 365-376 (2016).
[8] Chang, K. J. and Chang, H. H., "Perfect Gaussian integer sequences of period p^q with degrees equal to or less than k + 1," IEEE Trans. Communications 65(9), 3723-3733 (2017).
[9] Chang, H. H., "Random sequences based on exponential numbers," ICNC-FSKD 2019, (2019).
[10] Yan, S. Y., [Number Theory for Computing], Springer, Berlin, (2002).
[11] Chang, H. H., "Data encryption based on exponential numbers," 8th Inter. Conf. on Mathematical Modeling in Physical Sciences, (2019).