THE ARITHMETIC OF THE TOPOLOGIST'S SINE CURVE IN CRYPTOGRAPHIC SYSTEMS DEDICATED TO IOT DEVICES

WIESŁAW MALESZEWSKI[1,2]

[1] *Polish-Japanese Academy of Information Technology*
Faculty of Information Technology
Koszykowa 86, 02-008 Warsaw, Poland

[2] *Łomża State University of Applied Sciences*
Faculty of Computer Science and Food Science
Department of Computer Science and Programming
Akademicka 14, 18-400 Łomża, Poland

(received: 25 October 2018; revised: 27 November 2018;
accepted: 7 December 2018; published online: 2 January 2019)

Abstract: When observing the modern world, we can see the dynamic development of new technologies, among which a special place, both owing to the potential and the threats is occupied by the Internet of Things which penetrates almost all areas of our life. It is assumed that the IoT technology makes our life easier, however, it poses many challenges concerning the protection of the security of information transmission and, therefore, our privacy.

One of the main goals of the paper is to present a new unconventional arithmetic based on the transcendental curve dedicated to the cryptographic systems that protect the transmission of short messages. The use of this arithmetic may develop the possibilities of protecting short sequences of data generated by devices with limited computational power. Examples of such devices include the ubiquitously used battery powered sensors, the task of which is to collect and transmit data which very often comprises concise information.

Another goal is to present the possibility of using the developed arithmetic in cryptographic algorithms.

Keywords: IoT cryptography, secure communication, topologist's sine curve, unconventional arithmetic

DOI: https://doi.org/10.17466/tq2019/23.1/c

1. Introduction

The concept of the "Internet of Things" was created by Kevin Ashton, a British entrepreneur and the founder of start-ups. The idea was formulated in 1999 to describe a system in which the material world communicates with

computers using ubiquitous sensors. Already at the turn of 2008 and 2009, the number of devices connected to the network exceeded the number of inhabitants of our globe. According to Cisco, that moment marked the real birth of the "Internet of Things", which is now understood as a network of connected devices, which has advanced capabilities of interaction with both people and other devices, and with the broadly understood surrounding physical world. These connections are to provide the continually developed infrastructure with the ability to perform various tasks [1], which according to many researchers will positively affect our lives [2, 3].

1.1. Infrastructure

Today, the network of the Internet of Things comprises billions of devices with limited computing capabilities, which often have only wireless communication interfaces [4]. Currently, the IoT development community distinguishes the following four classes of components of the structure of the Internet of Things.

- devices that generate data and allow their gathering, transmission, and processing;
- communication networks connecting devices (Internet);
- IT systems adapted for processing of the collected data;
- systemic data processing analytical solutions which, in situations that have arisen, can take relevant actions both programmed by man and being a product of artificial intelligence.

The traditional methods of data analysis well-developed today are not designed to efficiently process such huge amounts of information often transmitted in real time from IoT devices, which significantly limits the possibilities of using the potential of this infrastructure. The usefulness of the collected data depends on the real possibility of using it in order to trigger further actions, the accuracy of which will probably become a factor determining its functionality. Researchers predict that the greatest benefits will result from the simultaneous development of the Internet of Things and Artificial Intelligence, which will result in the so-called "Connected Intelligence" [5, 6].

The Internet of Things is made up of, inter alia, devices intended for consumers such as smart TVs, speakers, toys, body-wearable devices, smart meters, security systems, air-conditioning, thermostats, and lighting systems. Another important group are devices dedicated to manufacturing plants, such as modern assembly line machines, often equipped with many sensors and systems informing about the observed anomalies, announcing an upcoming failure, or informing about components, the status or quality of operation which informs about the imminent necessity of replacement. Properly compiled collected information can prevent unexpected downtimes and loss of productivity and, at the same time, profits of manufacturing enterprises [7].

1.2. Potential

The industries in which the greatest development of the Internet of Things can be observed and to which it can bring significant financial benefits include manufacturers of spare parts for devices monitored for material fatigue, health protection, areas related to the development of smart cities, energy systems and home security systems; moreover, according to forecasts, this infrastructure will bring numerous benefits to many other industries offering products and services that can develop using the Internet of Things, such as trade, automotive industry, sports, tourism or culture [8].

The benefits of using such solutions can be felt by companies operating in both the private and public sectors – they are related to better capital allocation, lower costs, and higher productivity. It is estimated that by 2026, the market of the Internet of Things will be worth between 4 and even 10 trillion dollars. From the point of view of a potential user, this infrastructure can increase safety in the sphere of health and finance, help to make better use of time and, at the same time, improve the quality of life.

1.3. Devices

IoT devices receive input data through sensors, which are often considerably miniaturized and send information via wireless interfaces to computers, mobile devices, and cloud applications. This makes it possible to place IoT devices in new locations, previously unavailable to computers [9]. Such sensors include machine, optical, light, acceleration, inclination (tilt), position, motion, velocity, humidity, temperature, leakage and level sensors, as well as electric and magnetic sensors. They attempt to imitate the organs of the senses of living beings in order to describe the surrounding environment as accurately as possible, thus becoming a part of our everyday life [10].

IoT device management systems help to integrate, organize, and monitor complex infrastructures built from multiple devices [11]. The offered functions very often play a key role in maintaining the efficiency, connectivity and security of IoT infrastructure components. They include device registration, authentication and authorization. They enable an automated configuration of devices, their sharing, monitoring, and diagnostics. In addition, they are also helpful in solving problems related to the functioning of the device. Examples of popular mobile device management protocols include the Open Mobile Alliance ([OMA DM) [12] and Lightweight Machine-to-Machine (OMA LwM2M) protocols [13].

IoT devices receive data via sensors, which are often considerably miniaturized owing to the MEMS technology [14], and send information via wired or wireless interfaces to mobile and cloud computers.

Despite its diversity, the IoT space is characterized by two overriding design problems. Firstly, due to their location, IoT devices are often limited to minimal physical dimensions; moreover, they are often deprived of easy access to power. This factor is the reason why low energy consumption is probably the most universal limitation on them. Secondly, since for economic reasons it is impossible

to create a personalized chip for each application, a highly modular approach is needed in which systems can be constructed by combining pre-existing integrated circuits [9, 15, 16].

1.4. IoT device safety

The new functions and used mechanisms raise a number of new problems that cannot be completely solved using classic protection methods related to security [17]. The interconnection of different devices manufactured according to different standards, often equipped with limited energy resources and low computing power, poses a number of new challenges [18].

The most limited IoT devices have only several kilobytes of RAM, and a few megahertz of the CPU [19, 20]. More powerful devices have tens, hundreds, and even thousands of more resources. In such a diverse environment, IoT devices must operate reliably and provide an adequate level of security. This is a serious challenge because security mechanisms should be designed to work efficiently in very limited devices, with the highest possible protection.

And the IoT technology very often develops much faster than the security mechanisms of devices and their users introducing new threats to security and privacy [21, 22]. Concerned about the dangers of the rapidly growing space of IoT attacks, in September 2015, FBI issued an announcement about the Emergency Call Number I-091015-PSA, which is a document describing the risks associated with the development of IoT, as well as including recommendations on safeguards and defense [23].

Another aspect related to IoT is personal data protection. Data sent through IoT can provide a lot of information about the owner of the device [15] which can be misused – information about the preferences, customs or habits of household members collected by the so-called ‘smart homes can be used for marketing or even criminal purposes. Some devices additionally require providing some information to fully use the functionalities offered by them. Such information is sent to the manufacturer, who in this way becomes its administrator, which imposes on him the obligation to protect it appropriately [24].

Also, the public should be aware of the fact that the appropriate configuration of devices is a prerequisite of any security (setting hard passwords and logins and the possible use of encryption keys if a device has such capabilities) because the awareness and caution of users is of fundamental importance.

1.5. Communication of IoT sensors

The wireless sensor nodes used are usually characterized by low power, small dimensions, and a low price. The nodes make data processing possible and also have wireless communication capabilities. The most often considered factors taken into account in the selection of sensors [10] include accuracy and the possibility of calibration, especially required for most measuring systems; the solutions used for communication between sensor nodes come from the cellular telephony family, including the global system for mobile communication (GSM), the general

packet radio system (GPRS), the universal mobile telecommunications system (UMTS)/3G, long-term evolution (LTE)/4G, satellite communications, licensed or unlicensed radio networks and power-line communication (PLC) [25, 26]. The trend of binding on electronic device constructors is to minimize energy consumption in order to maximize the operation time of a portable device after charging or replacing the battery.

Diversified conditions contribute to the construction of a connection network that uses several topologies in one system [27]. One of the most popular topologies is the mesh topology, which is a type of a network in which all nodes cooperate to distribute data within the network. This topology is usually used in areas such as home automation, intelligent HVAC control, and intelligent buildings [28].

Another type includes networks based on the mesh network topology, in particular using the ZigBee, Z-Wave and Thread protocols. A mesh network consists of several types of nodes, some of which need to be used as transmitters for other nodes in addition to capturing and disseminating the collected data.

Another type of topology is the star topology implemented in such a way that each host of the network is connected to the central hub by means of a point-to-point connection, with any computer indirectly connected to any other node using the hub. The network that should be classified as a star network does not necessarily have to resemble a star, but all nodes in the network must be connected to one central device. All the traffic passing through the network passes through a central hub. The advantage of the star topology is that the entire complexity of the network is routed to the central node, so all other nodes only need to communicate in their time or frequency range. The basic disadvantage of this topology is the fact that the radio links between the gate and end nodes can be very long, which affects the amount of energy that must be allocated for sending messages, however, in this topology, nodes can rest between transmissions of messages, helping to save the total amount of energy consumed by each node. It is different in the mesh topology, where nodes must be constantly "awakened" [29]. Another different type of network is the point-to-point network establishing a direct connection between two nodes only, which due to its specification is not a widely used topology of the Internet of Things [19].

It is assumed that one of the most cost-effective topologies is the star or extended star topology; in such a configuration more efficient devices act as access points to which less efficient devices are connected. The simple organization and maintenance of such a communication configuration is the reason why it is one of the most used configurations today.

2. Cryptography

Cryptography is a field of knowledge dealing with the protection of transmitted information against unauthorized access. In the classic division of modern

cryptography, we distinguish two main trends: symmetrical cryptography containing methods in which the sender and the recipient of the message use the same key serving both to encode and decode information, as well as asymmetric cryptography in which two mathematically related keys are used [30]. One of them is called a public key; it is used to encrypt messages and it is widely available, while the other is called a private key which is used to decrypt a ciphertext containing a message and is subject to the highest protection [31]. Asymmetric cryptography is a relatively new field and it is commonly believed that its beginnings are related to the discovery, by Whitfield Diffie and Martin Hellman in 1976, of asymmetric methods of information protection which eliminated the problem of key distribution and significantly simplified the organization of secret communication.

Cryptographic algorithms with a public key are based on computationally difficult problems. The very popular RSA algorithm bases its functioning on the problem of factorization. Other algorithms, such as *e.g.* the ElGamal encryption or algorithms based on elliptic curves, are based on the so-called discrete logarithm problem [32–34].

The use of asymmetric cryptography, on the one hand, bypasses the essential problem of key distribution and, on the other hand, generates higher computing costs of encryption and decryption of communication. While before the development of the Internet of Things these costs were often underestimated, they now take on special importance, as they effectively shorten the battery life.

These factors most certainly contribute to the increase in the popularity of hybrid cryptographic systems combining the advantages of symmetric and asymmetric solutions. In these systems, a message is encrypted using symmetric methods, while the key necessary to read a ciphertext created in such a way is encrypted using asymmetric methods. This solution makes it possible to simultaneously use computationally cheaper algorithms and solves the problem of key distribution.

2.1. IoT Cryptography

Such solutions become especially valuable, since a significant number of devices involved in IoT systems are not technologically sufficiently prepared cryptography which is efficient but generates high computational costs. Another important limitation is the lack of adequate computing power of the processor or sufficiently large memory; this factor also excludes effective encryption and data storage providing significant security guarantees against unauthorized users or devices.

The energy efficiency of IoT devices requires that the necessary tasks be carried out in the shortest possible time. Then the average supply current consumed by a device is small, which translates into its longer functioning time when battery-powered.

Researchers dealing with the issues of security of the Internet of Things recommend finding a number of cryptographic solutions useful for this infrastructure. The existing solutions include both symmetric algorithms such as the Ad-

vanced Encryption Standard [35] and asymmetric algorithms mainly based on elliptic curves [36].

2.1.1. Symmetric algorithms applicable to IoT – the AES algorithm

The AES (Advanced Encryption Standard) algorithm is a modern symmetric block cipher. It was published in 1997 by Vincent Rijmen and Joan Daemen, and then adopted as a federal standard in the USA in 2002 [37].

This algorithm uses a key with a length of 128, 192 or 256 bits for encrypting and decrypting data. Depending on the key length, a different number of encryption rounds is executed. In the first stage of the encryption process, a plain text is divided into 128-bit blocks, which are then written in the form of a 4×4 matrix, each field of which contains one-byte information. One initial key and keys for each scheduled encryption round are generated. In the initialization round, each byte in a data block is added to the byte of the initial key corresponding to it by means of XOR summation. The number of encryption rounds depends on the length of the key. The following operations are performed in each encryption round:

1. Each byte of data is replaced by a different byte, based on a predefined lookup table called Rijndael's S-Box. This is the so-called SB (Substitute Bytes) operation. (The structure of the table guarantees the non-linearity of the transformation that affects the non-linearity of the entire encryption).
2. Shifting bytes in the last three state matrices to the left. The bytes in the first row are not shifted. The bytes in the second row of the matrix are shifted by one position to the left, in the third row by two positions, and in the fourth row by three positions to the left. The leftmost bytes from each row move to the rightmost position in the same row. This operation is abbreviated as SR (Shift Rows).
3. The MC (Mix Columns) operation, or the multiplication of columns: all columns of the state matrix are multiplied by a fixed matrix of 4×4 size, each field of which contains one-byte information.
4. The AR (Add Round Key) operation: adding the XOR of all bytes of the data block to the bytes of the key proper for the given round. Subkeys, like data blocks, are 16 bytes long each.

In the next stage, the final round containing a similar structure to the previous rounds, however, with the column multiplication operation omitted, is executed. And the documentation of the algorithm contains a description of the key extension procedure. The 128-bit key is extended to 176 bytes, the 192-bit key to 208 bytes, and the 256-bit key to 240 bytes [37].

2.1.2. Asymmetric algorithms applicable to IoT

Most of the existing asymmetric algorithms dedicated to IoT devices are based on elliptic-curve cryptography. In the work [36] it is shown that elliptic curves are much more efficient than the RSA algorithm based on the factoring problem. Classical elliptic-curve cryptography algorithms base their functioning

on the arithmetic of adding curve points in the Weierstrass equation [34, 33]. Many researchers use other curve variants, such as the Edwards, Montgomery, and Hasse curves, which are characterized by even lower costs of addition [38–40].

2.1.3. Current problems of IoT cryptography

Although generating low computational costs of encryption and decryption, the information protection methods described above require a minimal message length. Many sensors of the Internet of Things collect and transmit data with a very simple structure, the writing of which takes only several or a dozen or so bits. The use of the methods described above requires the extension of the transmitted information using noise and then coding it. Such a procedure generates additional costs and its use adversely affects the functionality of devices with limited access to power which are required to ensure several years of maintenance-free operation by supplying energy from built-in batteries.

In the following part of the work, an original arithmetic based on the properties of the topologist's sine curve, sometimes referred to as the Warsaw sine curve, will be introduced.

3. Topologist's sine curve

Many popular cryptographic algorithms have been inspired by geometric structures. A good example are the elliptic curve cryptography algorithms, which are based on the algorithms of adding points that have both a concise algebraic description and a simple, yet elegant geometric description [41].

The algorithm proposed below is inspired by the high dynamics of the topologists sine curve in close proximity to zero, which can be seen in Figure 1.

Definition 1. (The topologist's sine curve)

The topologist's sine curve is a set of points:

$$T = \left\{ \left(x, \sin \frac{1}{x} \right) : \ x \in (0,1] \right\} \cup \{ x = 1 \wedge y \in [-1,1] \} \tag{1}$$

The graph of the sine curve is shown in Figure 1.

Definition 2. (Floor functions)

The floor function:

$$\lfloor \cdot \rfloor : \ \mathbb{R} \to \mathbb{Z} \tag{2}$$

takes as input a real number x and gives as output the greatest integer less than or equal to x:

$$\lfloor x \rfloor = \max_{l \in \mathbb{Z}} \{ l \leq x \} \tag{3}$$

Let us consider the arithmetic sequence x_k, in the form:

$$x_k = x_1 + (k-1)r, \tag{4}$$

where x_1 and r are arbitrarily small positive real numbers and $k \in \{0,1,2,...\}$, then with any arbitrary, but fixed $n \in \mathbb{N}$, we can define the function:

$$f_n : \ \mathbb{R}_+ \cup \{0\} \to \mathbb{N}, \tag{5}$$

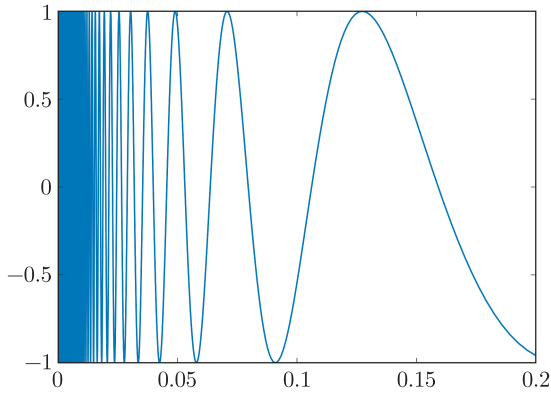

Figure 1. The topologist's sine curve,
from `commons.wikimedia.org/wiki/File:Topologist's_sine_curve.svg`

given by the formula:

$$f_n(x_k) := \begin{cases} \left\lfloor n \sin \frac{1}{x_k} \right\rfloor + n + 1 & \text{when } x \neq 0 \\ 0 & \text{when } x = 0 \end{cases} \tag{6}$$

the domain and the set of values comprising a discrete set of non-negative numbers. In the further parts of the work, we will be referring to the above function as the *discrete topologist's sine curve*. An example of this function can be found in Figure 2.

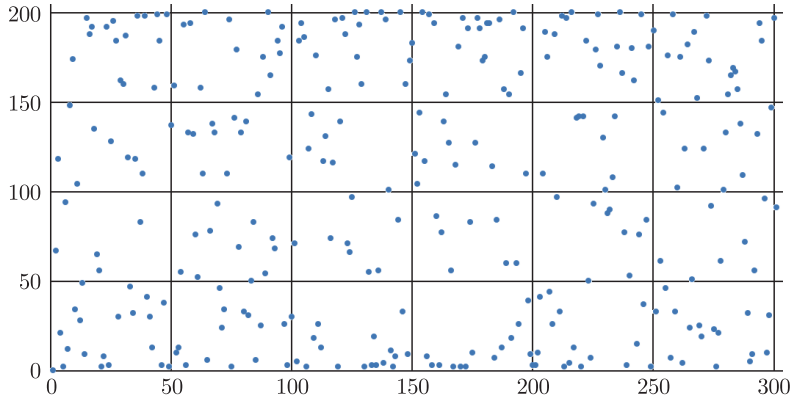

Figure 2. Discrete topologist's sine curve $f_{100}(x_k)$ in the domain
$x_k = k \cdot 10^{-6}$, $k = 1,2,3,...,300$

Then consider the collection:

$$G_{2n} = \bigcup_{i=1}^{2n} \{f_n(\tilde{x}_i)\} \tag{7}$$

where:

$$\tilde{x}_1 = x_1, \tag{8}$$

and

$$\tilde{x}_i := \min\left\{x_i: \bigvee_{j=1,2,\ldots,i-1} f_n(\tilde{x}_j) \neq f_n(x_i)\right\} \tag{9}$$

The set G_{2n} contains $2n$ of the initial different values of the function f_n defined on the sequence x_k.

Definition 3.

In the set $G = G_{2n} \cup \{0\}$ we define the mapping:

$$+_n^f:\ G \times G \to G, \tag{10}$$

specified using the formula:

$$f_n(\tilde{x}_i) +_n^f f_n(\tilde{x}_j) := f_n\Big((\tilde{x}_i + \tilde{x}_j)\,(\mathrm{mod}\, 2n+1)\Big) \tag{11}$$

Theorem 1.

The algebraic system $(G, +_n^f, 0)$ forms an abelian group.

The proof of this theorem is obvious.

Example 1.

Let us consider the function:

$$f_5(x) = \left\lfloor 5\sin\frac{1}{x}\right\rfloor + 6 \tag{12}$$

defined for the set of points $x_k = 10^{-6}k$, where $k = 1,2,3,\ldots$

Table 1. The table allows further points of the domain for which the implementation of the function $f_5(x_k) = \left\lfloor 5\sin\frac{1}{x_k}\right\rfloor + 6$ brings new elements to the set of values

x	0	1	2	3	5	7	8	9	12	14	17
$f_5(x)$	0	4	6	1	5	8	9	2	3	10	7

In order to simplify the calculations, let us replace, in Table 1, the individual values of the variable x with successive natural numbers. In this way, we will obtain a simplified table on which we will base our further considerations.

Table 2. New injective function $f_5^*(x)$ obtained after the above described modification $f_5(x)$ given by the Formula (11)

x	0	1	2	3	4	5	6	7	8	9	10
$f_5^*(x)$	0	4	6	1	5	8	9	2	3	10	7

The set of values of the above function together with the previously defined addition creates the abelian group $(G, +_n^f, 0)$. The table of operations in the group is presented in Table 3.

In the next steps, the obtained group will be used to build a cryptographic system in which subsequent stages of encryption/decryption will depend on the

Table 3. The table of addition in $(G, +_5^{f^*}, 0)$, generated by the sequence (4) with condition $a_0 = r = 10^{-6}$

$+_5^{f^*}$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	9	7	0	5	2	8	6	3	10	4
2	2	7	1	5	3	0	10	9	4	6	8
3	3	0	5	8	10	4	7	2	6	1	9
4	4	5	3	10	6	8	1	0	9	2	7
5	5	2	0	4	8	3	9	1	10	7	6
6	6	8	10	7	1	9	5	4	2	3	0
7	7	6	9	2	0	1	4	10	5	8	3
8	8	3	4	6	9	10	2	5	7	0	1
9	9	10	6	1	2	7	3	8	0	4	5
10	10	4	8	9	7	6	0	3	1	5	2

group arithmetic. It should be noted that the addition algorithm is strictly determined by the parameters defining the sequence x_k and the expected number of elements. Any small change to one of these parameters completely changes the properties of the group operations that are specified in Table 3. In order to reduce computational costs, trigonometric functions can be replaced by expansions of these functions into the Taylor series, while determining the level of precision of the approximations used. In this way, we will reduce our calculations to performing finite operations on polynomials well mastered by modern systems.

Example 2.

Let us consider the sequence $x_k = 10^{-6}k$, where $k = 1,2,3,...$ and the function:

$$f_2(x_k) = \left\lfloor 2\sin\frac{1}{x_k} \right\rfloor + 3. \tag{13}$$

Performing operations according to the scheme shown in the above example, we obtain Table 4 of group operations, the specific elements of which indicate the next stages of our proceeding.

Table 4. The laws of arithmetic in $(G, +_2^{f^*}, 0)$ for $a_0 = r = 10^{-6}$

$+_2^{f^*}$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	4	0	3
2	2	4	3	1	0
3	3	0	1	4	2
4	4	3	0	2	1

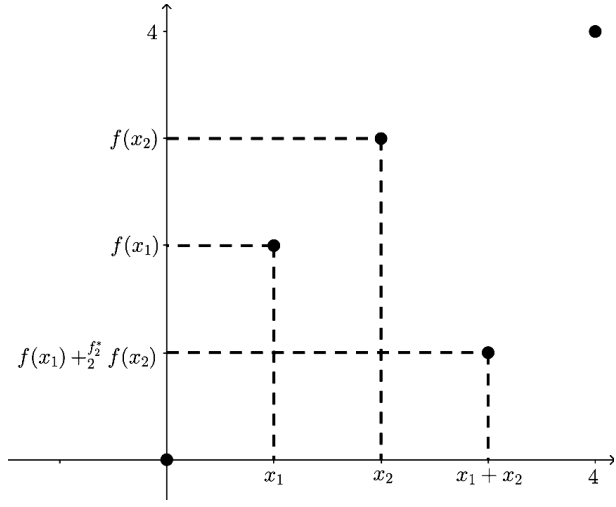

Figure 3. Graphical presentation of the proposed addition algorithm defined by the formula (11)

For the reception of the presented method, let us consider an elementary example in which the key is a randomly chosen character – we assume, for the purpose of this example, that the ASCII number of this character gives the remainder 3 of the division by 5.

Encryption

1. *The number* 3 *becomes the initial key* $K_i = 3$
2. *The initial key* K_i *specifies the row the elements of which will be the keys of subsequent rounds. In the presented example, the third row is a vector in the form* $[3,0,1,4,2]$. *Elements of this vector become the keys* k_i *of the subsequent five rounds of encryption.*
3. *Each of the rounds consists of two stages: in the first stage the operation of XOR addition using the round key is performed, while in the second one the permutation determined by the round key is performed.*

$k_1 = 3$	$\pi_1 = (3,0,1,4,2)$	$\pi_1^{-1} = (2,4,1,0,3)$
$k_2 = 0$	$\pi_2 = (0,1,2,3,4)$	$\pi_2^{-1} = (4,3,2,1,0)$
$k_3 = 1$	$\pi_3 = (1,2,4,0,3)$	$\pi_3^{-1} = (3,0,4,2,1)$
$k_4 = 4$	$\pi_4 = (4,3,0,2,1)$	$\pi_4^{-1} = (1,2,0,3,4)$
$k_5 = 2$	$\pi_5 = (2,4,3,1,0)$	$\pi_5^{-1} = (0,1,3,4,2)$

4. *In the encryption phase, subsequent characters of a message are replaced by the corresponding binary numbers according to the ASCII table. Then, each element of the* i^{th} *round key is written in an eight-character binary form. In this way, we obtain five blocks. In the next step, on the individual bits of a message and the key* k_i, *we perform the XOR addition, and then the blocks are permuted using the permutation* π_i.

5. *After completing all the rounds, the obtained result is added with the number assigned by the ASCII table to each character of the key k_1 and then the result is converted into characters (the purpose of the addition is to mitigate the risk of breaking the cipher based on the character frequency analysis)*

Decryption *is the process of reversing the order of the operations performed.*

The encryption and decryption processes are shown in Table 5 and Table 6.

Table 5. Next steps of encryption with the described algorithm

Input	h	e	l	l	o
Binary	0 1 1 0 1 0 0 0	0 1 1 0 0 1 0 1	0 1 1 0 1 1 0 0	0 1 1 0 1 1 0 0	0 1 1 0 1 1 1 1
k_1	0 0 0 0 0 0 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 1 0 0	0 0 0 0 0 0 1 0
XOR	0 1 1 0 1 0 1 1	0 1 1 0 0 1 0 1	0 1 1 0 1 1 0 1	0 1 1 0 1 0 0 0	0 1 1 0 1 1 0 1
π_1	0 1 1 0 1 0 0 0	0 1 1 0 1 0 1 1	0 1 1 0 1 1 0 1	0 1 1 0 1 1 0 1	0 1 1 0 0 1 0 1
k_2	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 1	0 0 0 0 0 1 0 0
XOR	0 1 1 0 1 0 0 0	0 1 1 0 1 0 1 0	0 1 1 0 1 1 1 1	0 1 1 0 1 1 0 0	0 1 1 0 0 0 0 1
π_2	0 1 1 0 0 0 0 1	0 1 1 0 1 0 0 0	0 1 1 0 1 0 1 0	0 1 1 0 1 1 1 1	0 1 1 0 1 1 1 0
k_3	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1
XOR	0 1 1 0 0 0 0 0	0 1 1 0 1 0 1 0	0 1 1 0 1 1 1 0	0 1 1 0 1 1 1 1	0 1 1 0 1 1 0 1
π_3	0 1 1 0 1 1 0 1	0 1 1 0 1 1 1 1	0 1 1 0 1 0 1 0	0 1 1 0 0 0 0 0	0 1 1 0 1 1 1 0
k_4	0 0 0 0 0 1 0 0	0 0 0 0 0 0 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	0 0 0 0 0 0 0 1
XOR	0 1 1 0 1 0 0 1	0 1 1 0 1 1 0 0	0 1 1 0 1 0 1 0	0 1 1 0 0 0 1 0	0 1 1 0 1 1 1 1
π_4	0 1 1 0 0 0 1 0	0 1 1 0 1 0 1 0	0 1 1 0 1 0 0 1	0 1 1 0 1 1 1 1	0 1 1 0 1 1 0 0
k_5	0 0 0 0 0 0 1 0	0 0 0 0 0 1 0 0	0 0 0 0 0 0 1 1	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0
XOR	0 1 1 0 0 0 0 0	0 1 1 0 1 1 1 0	0 1 1 0 1 0 1 0	0 1 1 0 1 1 1 0	0 1 1 0 1 1 0 0
π_5	0 1 1 0 1 1 1 0	0 1 1 0 1 1 1 0	0 1 1 0 0 0 0 0	0 1 1 0 1 1 0 0	0 1 1 0 1 0 1 0
Decimal	110	110	96	108	106
k_1	3	0	1	4	2
Add	113	110	97	112	108
cryptogram	q	n	a	p	l

Example 2 illustrates a symmetric encryption algorithm basing its functioning on the proposed arithmetic of points of the discrete topologist's sine curve. In the trivial example, the idea of a cryptographic system is presented. The next steps of the algorithm result from the structure of a discrete subset of points of the rescaled transcendent curve. The presented algorithm could be used to protect very short information. In order to improve its safety, it would be necessary to introduce the procedure of changing the key and the procedure for changing the applied arithmetic resulting from the selected subset of the points of the transcendent curve. For sending messages, you can include a header along with information about the number of messages sent using a specific arithmetic. The encoded information should also contain the key to decode the next message. In addition, further research should consider a methodology allowing safe transmission of parameters defining the next applied arithmetic.

Table 6. Decryption procedure – execution of encryption steps in reverse order

cryptogram	q								n								a								p								l							
decimal	113								110								97								112								108							
k_1	3								0								1								4								2							
reduce	110								110								96								108								106							
binary	0	1	1	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	1	0
π_5^{-1}	0	1	1	0	0	0	0	0	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	0
k_5	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
XOR	0	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	0
π_4^{-1}	0	1	1	0	1	0	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	0	1	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	1
k_4	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
XOR	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	1	0	1	1	1	0
π_3^{-1}	0	1	1	0	0	0	0	0	0	1	1	0	1	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	1
k_3	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
XOR	0	1	1	0	0	0	0	1	0	1	1	0	1	0	0	0	0	1	1	0	1	0	1	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	0
π_2^{-1}	0	1	1	0	1	0	0	0	0	1	1	0	1	0	1	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	1	0	0	1	1	0	0	0	0	1
k_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0
XOR	0	1	1	0	1	0	0	0	0	1	1	0	1	0	1	1	0	1	1	0	1	1	0	1	0	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	1
π_1^{-1}	0	1	1	0	1	0	1	1	0	1	1	0	0	1	0	1	0	1	1	0	1	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	1	1	0	1
k_1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
XOR	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1
message	h								e								l								l								o							

An important rule for the security of cryptographic algorithms is the confusion rule – according to which each bit of the ciphertext should depend on different parts of the key and the principle of diffusion – changing the single bit of the message should affect the statistic change of half of the bits.

The presented system is designed to encrypt very short information, while the conducted research is focused on the development of a similar method allowing the encryption of messages of any length. An inspiration for the development of such a system can be the AES algorithm quoted in the work, which also belongs to the symmetric cipher family, its operation generates quite low computational costs, however, it cannot be used to encrypt very short information. Another goal of the conducted research is to develop a system in which points a_0, r and n determining the described arithmetic are part of the key initiating communication after connecting to the network and then, after a specified time interval, they are replaced by the measurement data read far below the accuracy of working sensors. Such a solution may generate a threat that the malicious side can gain control over the sensor and generate a known data sequence, or there may appear collinearity between the sensors in the form of correlated sequences generated by the sensors which are embedded in the same device. However, there are solutions in the literature which make it possible to bypass the above problem so that the data is random in nature [42].

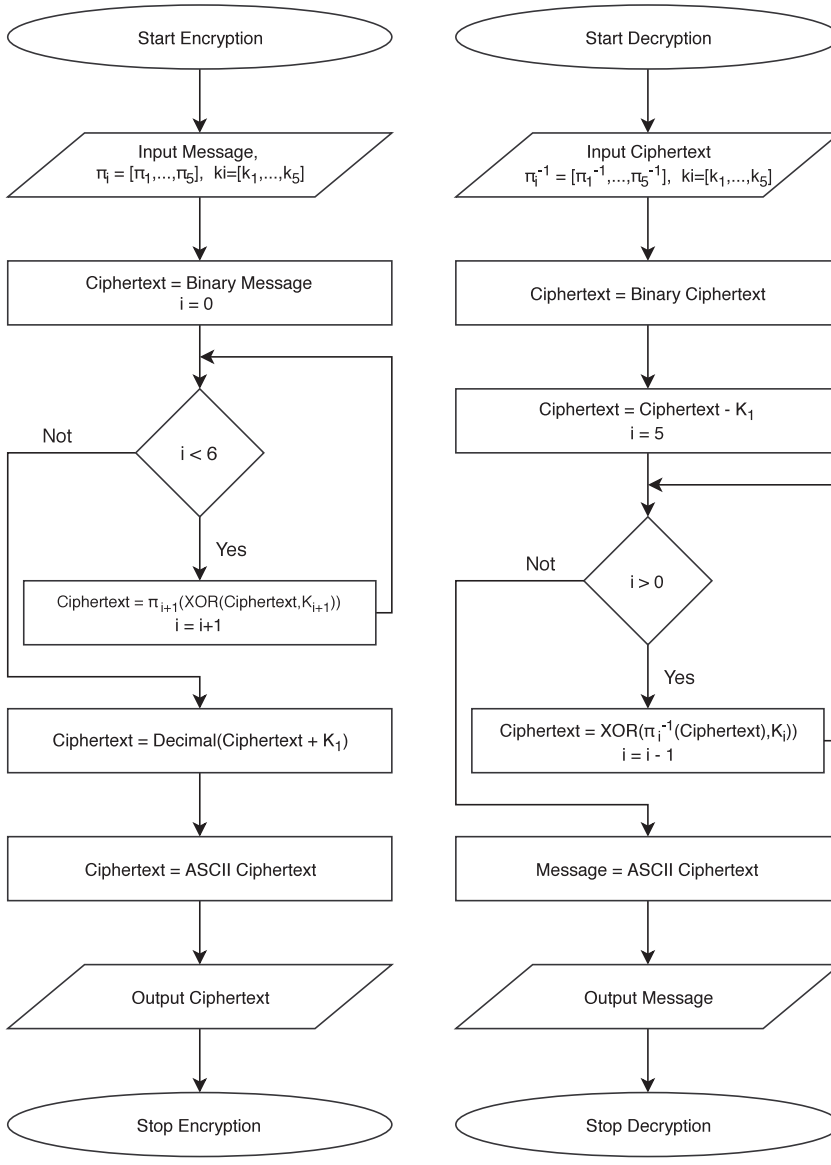

Figure 4. Block diagram of encoding and decoding information using the presented algorithm

Example 3.

In the next step, we are considering a system dedicated to IoT sensors. Let us assume that devices have the initial key needed to establish secure communication and the specified validity of this key. In addition, they are equipped with an implemented procedure for generating parameters at defined intervals which make it possible to define the Sequence (4), and thus also the groups and the arithmetic

defined therein. Let us also assume that there is a system developed especially for changing keys after their validity has expired. The algorithm described below already makes it possible to encrypt messages with different lengths.

1st Encryption Phase

1. *A message is written in the binary code and then divided into a series consisting of* $(2n+1)$ *blocks* (B_i)*, each containing* $(2n+1)$ *bits. The incomplete series are supplemented with pseudo-random numbers obtained, for example, as measurement results.*
2. *The original key is expanded in such a way that, as a result, a key with a length equal to the length of a single series is obtained. The key, like the series, is divided into* $(2n+1)$ *bit blocks.*
3. *As in the Example 3 in the addition table, we create permutations* $(\pi_i)_{i=1}^{2n+1}$.

2nd Encryption Phase

4. *Encrypting the jth block of the message, in the first coding step we act on the jth block of the code using the permutation* π_1 *and then combine it with the jth block of the modified message received through the first permutation of the blocks of the original message using the XOR function.*
5. *In each subsequent* $(i+1)^{th}$ *coding step, encoding the* j^{th} *block of a message we act on the jth block of the code using the permutation* π_{i+1} *and then combine it with the jth block of the message received through the permutation* π_{i+2} *of the blocks of the ciphertext obtained in the previous encryption step using the XOR function. If we exhaust the list of permutations, we return from the first permutation and continue the encryption procedure. Figure 5 illustrates the block diagram of the described method.*

The number of encryption steps depends on the computing power that we have, the energy resources, and the confusion and diffusion of the ciphertext that we want to achieve.

All operations performed during the encryption phase are reversible. Thus, the decoding process consists in performing operations reverse to the ones performed during the coding in a chronological sequence.

4. Summary

The paper describes the development of the Internet of Things technology. The IoT technology currently has great potential and is used in many areas of human functioning. Common features linking IoT infrastructure devices were discussed. Factors affecting the high degree of threats to the infrastructure of the Internet of Things, resulting, inter alia, from the numerous technical limitations imposed on applicable devices, were introduced. Next, communication protocols making the cooperation of IoT devices possible and types of the networks connecting these devices were described.

The main part of the article was to explore the currently used cryptographic algorithms and proposing solutions basing their functioning on the introduced

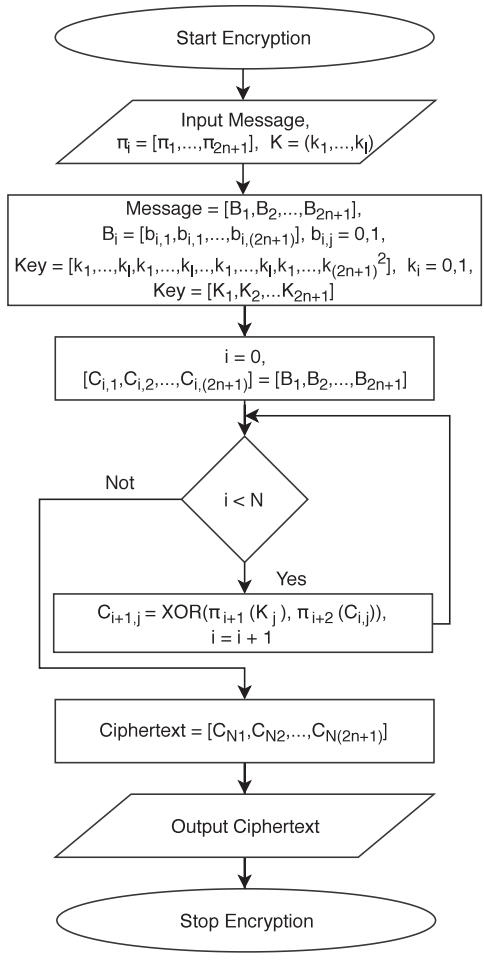

Figure 5. The block diagram shows the coding of information of any length by means of the transformation from the selection of parameters a_1 and r of the arithmetic Sequence (4) and Function (6). N is the number of coding cycles

arithmetics of points of the topologist's sine curves. These arithmetics are dependent on the selection of a series of points. Each minimal change in the output parameters defining the way of creating a group completely changes the arithmetic specified therein, which is a huge strength of this method. At the end of the paper, elementary examples of using the obtained solutions in cryptographic algorithms were provided and the directions for further work were outlined.

References

[1] Bari N, Mani G and Berkovich S 2013 *Fourth International Conference on Computing for Geospatial Research and Application*, IEEE, USA, 48

[2] Taylor A S, Harper R, Swan L, Izadi S, Sellen A and Perry M 2007 *Personal and Ubiquitous Computing* **11** (5) 383

[3] Niyato D, Hossain E and Camorlinga S 2009 *IEEE Journal on Selected Areas in Communications* **27** (4) 412
[4] Knud L L *State of the IoT 2018*, [online]: `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018` [accessed on 26 February 2019]
[5] Javaid N, Sher A, Nasir H and Guizani N 2018 *IEEE Communications Magazine* **56** (10) 94
[6] Tekinerdogan B 2017 *Engineering connected intelligence: a socio-technical perspective*, Wageningen University & Research
[7] Jalali M S, Kaiser J P, Siegel M and Madnick S 2017 *IEEE Security & Privacy* **17** (2) 39
[8] Lee I and Lee K 2015 *Business Horizons* **58** (4) 431
[9] Blaauw D, Sylvester D, Dutta P, Lee Y *et al.* 2014 *2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers* 1
[10] Lee Y-D and Chung W-Y 2009 *Journal of Business and Management* **20** (4) 55
[11] Perumal T, Datta S K and Bonnet C 2015 *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)* 54
[12] Open Mobile Alliance 2006 *Policy Evaluation, Enforcement and Management Callable Interface (PEM-1) Technical Specification* **1**
[13] Open Mobile Alliance 2017 *Lightweight machine to machine technical specification* **1** (1)
[14] Choudhary V and Iniewski K 2016 *Mems: fundamental technology and applications*, CRC Press
[15] Rykowski J 2017 *Napędy i Sterowanie* **19** 120
[16] Maj I 2015 *Bezpieczeństwo. Teoria i Praktyka* **1** (3) 51
[17] Riahi A, Challal Y, Natalizio E, Chtourou Z and Bouabdallah A 2013 *IEEE international conference on distributed computing in sensor systems* 351
[18] Choudhary D 2019 *Journal of Autonomous Intelligence* **1** (2) 16
[19] Marin L, Pawlowski M and Jara A 2015 *Sensors* **15** (9) 21478
[20] Bahrami M, Khan A and Singhal M 2016 *2016 IEEE International Conference on Mobile Services (MS)* 190
[21] Heer T, Garcia-Morchon O, Hummen R, Keoh S L, Kumar S S and Wehrle K 2011 *Wireless Personal Communications* **61** (3) 527
[22] Roman R, Zhou J and Lopez J 2013 *Computer Networks* **57** (10) 2266
[23] Ochaya W B 2018 *International Journal of Online Graduate Education* **1** (1) 1
[24] Preuveneers D, Joosen W and Ilie-Zudor E 2016 *12th International Conference on Intelligent Environments (IE)* 40
[25] Lee Y-Dong and Chung W-Young 2009 *Sensors and Actuators B: Chemical* **140** (2) 390
[26] Madhusudan S 2018 *EAI Endorsed Transactions on Internet of Things* **3** (10) 1 doi: 10.4108/eai.15-1-2018.153566
[27] Mayank S 2018 *Engineering Machine Learning, Blockchain, Robotics, IoT and more Programming for All*, [online]: `http://www.eetimes.com/electronics-news/4409928/Cisco-sees-14-trillion-opportunity-in-Internet-of-Things` [accessed: 26-February-2019]
[28] Ruano A, Silva S, Duarte H and Ferreira P M 2018 *Applied Sciences* **8** (3) 370
[29] Shang W, Yu Y, Droms R and Zhang L 2016 *NDN Project, NDN-0038 (Tech. Rep.)*
[30] Aumasson J-P 2017 *Serious Cryptography: A Practical Introduction to Modern Encryption*, No Starch Press
[31] Diffie W and Hellman M E 1976 *Proceedings of the national computer conference and exposition New York* 109 doi: 10.1145/1499799.1499815109
[32] Hellman M E 1979 *Scientific American* **241** (2) 146
[33] Koblitz N 1987 *Mathematics of computation* **48** (177) 203
[34] Miller V S 1985 *Conference on the theory and application of cryptographic techniques* **218** 417 doi: 10.1007/3-540-39799-X_31

[35] Yu W and Köse S 2017 *IEEE Transactions on Circuits and Systems I: Regular Papers* **64** (11) 2934
[36] Bafandehkar M, Yasin S Md, Mahmod R and Hanapi Z Mohd 2013 *International Conference on IT Convergence and Security (ICITCS)* doi: 10.1109/ICITCS.2013.6717816
[37] Dworkin M J, Barker E B, Nechvatal J R, Foti J, Bassham L E, Roback E and Dray J F 2001 *Federal Information Processing Standards (NIST FIPS)* **197**
[38] Bernstein D J and Lange T 2007 *International Conference on the Theory and Application of Cryptology and Information Security* 29
[39] Bernstein D J and Lange T 2017 *IACR Cryptology ePrint Archive* **2017** 293
[40] Bernstein D J, Chuengsatiansup C, Kohel D and Lange T 2015 *International Conference on Cryptology and Information Security in Latin America* 269
[41] Maleszewski W 2017 *Polish Journal of Applied Sciences* **3** (4) 141
[42] Hong S Lee and Liu C 2015 *IEEE Access* **3** 562