UDC 621.391.037 **doi: 10.20998/2522-9052.2019.3.14**

V. Pevnev, M. Tsuranov, H. Zemlianko, V. Kharchenko

National Aviation University "Kharkiv Aviation Institute", Kharkiv, Ukraine

USE OF A METHOD OF PASCAL OF CALCULATION OF CHECKSUMS IN NOISEPROOF CODING

Abstract. The **subject matter** of the article is opportunity use of a method of Pascal for finding of remainders of division of large numbers when using CRC. The **goal** is to analyze a possibility of use of a method of Pascal for definition of remainders of division in the CRC systems. Tasks: to analyze a possibility of use of CRC for noise-immune coding in different channels, to show a possibility of application of a method of Pascal for an image of noise-immune coding with use of checksums. **The used methods are** analytical method, methods of modal arithmetic's. **The received such results**. The technique of calculation of Checksum of the message which are used for the control of integrity and restoration distorted the message is developed. **Conclusions**. Use of a method of Pascal for definition of remainders of division allows accelerating considerably process of search of various options the message, which will be restored. Realization of the offered method allows creating parallel structures, which give the chance to solve a problem of recovery of the message on the scale of real time.

Keywords: noise-immune coding; a method of Pascal; CRC; integrity; a remainder of division; divisions behind a step.

Receipt. Statement of a problem

With development of mobile data transmission networks, emergence of the smart equipment and devices of the Internet of things the number of crimes in the information sphere considerably increased [1]. Increase in losses and orientation of incidents in the sphere of information security on the state resources forced legislators to develop and accept strategy to protection of a cyberspace of Ukraine [2]. Usually researchers of information security allocate a triad of properties of a system in terms of its security. In work [3] it is developed mathematical model of information security in which attention is evenly paid to each of components of a triad of information security.

It should be noted that in the majority of a research allocate only a component confidentiality, without paying attention to components integrity and availability. Sean Kanuk, the national officer of investigation concerning cyber security in National council of investigation in ODNR, emphasized recently that violation of integrity (data, processes, infrastructure, the software) is the largest threat in a cyberspace [4].

Proceeding from all aforesaid, the problem of integrity has to be considered as it is very important. The integrity has to be provided, but not be controlled. Using simple control of integrity, the error of signatures of messages can provide the message to a full deviation that will increase data processing time from IoT devices.

This delay can be rather critical for some systems (the life support system, the system of brakes of the car).

Presently in communication channel a large number of various noise-immune codes which significantly differ from each other, not only computing weight but also a possibility of correction of noises is used. In the majority of hardware devices for control and ensuring integrity checksums are used.

The purpose of the offered work: to analyse a possibility of use of a method of Pascal for definition of remainders of division in the CRC systems.

1. Review of references

At assessment of energy efficiency of use to the manager of noise-imunne coding in different communication channels biased to consider a set of factors different in the nature. It is necessary to understand driving force as a factor of any process (phenomenon) or a condition which affects on this or that process (phenomenon) [5].

Cyclic redundancy check (CRC) is the error detection code which is the most often used on the digital networks and storage devices for detection of random changes in the raw data. The data units entering these systems attached a short check number, on the basis of the rest from polynomial division of their contents. On extraction calculation repeats, and, eventually check numbers do not correspond, measures for mitigation of consequences can be taken against damage of data. CRCs can be used for error correction [6].

CRCs so are called because check (data validation) value is duplication (it develops the message, without adding information), and the algorithm is based on cyclic codes. CRCs are popular because they are simple to implement in the binary hardware easy to analyze mathematically, and especially good in detection of the widespread errors caused by noise in transmission channels. As the check number has fixed length, function which generates it is sometimes used in quality a hash function.

CRC was invented by W. Wesley Peterson in 1961; the 32-bit CRC function used in Ethernet and many other standards is work of several researchers and was published in 1975.

CRCs are based on the theory of cyclic error correcting codes. Use of systematic cyclic codes which code messages by adding of a check number of fixed length for the purpose of error trapping in communication networks, at first was offered to W. Wesley Peterson in 1961 [7]. Cyclic codes not only are simple to implement, but also to have advantage of subcirculation especially well for detection of burst errors: the continuous sequences of garbage characters of data in mes-

sages. It is important because burst errors are the general transmission errors in many transmission channels, including magnetic and optical devices of storage. Usually n-bit CRC belonged to a data unit of arbitrary length, will find any only error burst not longer, than n of bit and a part of all longer error bursts which it will find, $(1 - 2^{-n})$.

The specification of the CRC code demands definition of a so-called polynomial of the generator. This polynomial becomes a divider in polynomial long division which takes the message as a dividend and in which it is discarded private, and the rest becomes result. The important protest consists that polynomial coefficients are calculated according to arithmetic of a final field, thus, addition operation can always be carried out a digit-by-digit parallel (is not present any, bear between digits).

In practice all most often used CRCs use the Galois field of two elements, GF (2). These two elements are usually called 0 and 1, conveniently corresponding to architecture of a computer.

CRC call n-bit CRC when its value of check is n in bits long. For this n of several CRCs are possible, everyone with a different polynomial. Such polynomial has the highest degree of n that means that it has n 1 conditions. In other words, the polynomial has n 1 length; its coding demands n 1 bit. Pay attention that the majority of polynomial specifications or discards MSB or LSB as it always 1 year. CRC and the connected polynomial usually have the name of the CRC-n-XXX form as in the table given below.

The simplest system of detection of errors, parity bit, is actually 1-bit CRC: it uses a polynomial of generator x 1 (two conditions) and has name CRC-1.

CRCs are specially intended for protection against the general types of errors on transmission channels where they can provide fast and reasonable ensuring integrity of the transferred messages. However they are not suitable for protection against intended change of data.

First, as there is no authentication, the hacker can edit the message and repeatedly calculate CRC without the found replacement. When it is saved together with data, CRCs and cryptographic hash functions by do not protect from intended data modification. Any application which demands protection against such attacks should use mechanisms of cryptographic authentication, such as message authentication codes or sign-code signatures (which are usually based on cryptographic hash functions).

Secondly, unlike cryptographic hash functions, CRC is easily reversible function which does it improper for use in sign-code signatures [8].

Thirdly, CRC is linear function with property it

$$crc(x \oplus y \oplus z) = crc(x) \oplus crc(y) \oplus crc(z)$$

as a result, even if CRC is ciphered with the stream cipher which uses XOR as its union operation (or the mode of the block cipher which effectively turns it into the stream cipher, such as OFB or CFB), both the message and the connected CRC can be managed without the knowledge of encrypting key; it was one of the known shortcomings of design of the protocol [6] of Wire equivalent private life (WEP).

CRC codes are used in different protocols for definition of errors, for example CRC-1 most hardware; also known as parity bit, CRC-4-ITU used in ITU-T G.704, CRC-5-ITU used in ITU-T G.704, CRC-5-USB - USB token packets, CRC-6-CDMA2000-A mobile networks.

2. Research problems

Main purposes of the paper to prove a possibility of application of a method of Pascal for calculation of checksum at noise-immune coding.

For achievement of a goal the following tasks were solved:

– to analyze a possibility of application of CRC for noise-immune coding in various communication channels;

– to show a possibility of application of a method of Pascal for the offered method in [9] a method of noise-immunecoding.

3. Use of checksums in noise-immunecoding

As it was already noted earlier, because of low-quality physical communication channels and influence of hindrances, in information that it is transferred can be brought distortion. On the reception party it is very difficult, and at times at all it is impossible to recognize the transferred message. Qualitatively to transfer information experts use such methods as transfer of the message several times or coding the message with adding to a large number of service information. This leads to the fact that the amount of information transmitted is several times greater than the information part, and the communication channel is engaged for a longer time.

Optimization of process of data transmission can be reached for use of checksums. The method of checksums is based on addition control bit to three information bits, determination of Checksum and information transfer with two to addition bytes of test information (is-a bit of parity or CRC 1).

This method assumes the possibility of detecting and restoring distorted bits of information by re-sorting distorted blocks of 4 bits.

Then we find remainders of division on number 11, 13, 14, 15 and created four sequences of CRC-4. The choices of these numbers are not accidental.

They are mutually simple, that is having no common divisors. Also choosing these numbers, we choose a fairly large range of uniquely determined numbers. Transfer to decimal numbers I = 1..16 remains are applied in top the category the last symbol? Findings of the sum of finding of remainders of division on 11.13, 14.15 are applied 12 Sim - it was preferred from the massif by transfer to decimal number of finding of remainders of division on 11.13, 14.15:

$$11 \times 13 \times 14 \times 15 = 30030.$$

On host in the presence of twisting at the first check (check of bit of parity) it is possible to carry out the second inspection (to allocate only information part and, to find remainders of division on 11.13, 14.15 and

to compare to checksum). So the system is checked for existence of collisions. Thus, we will be able to localize a mistake and also in most cases to restore the message.

For simplification of the procedure of receiving remainders of division and acceleration of the developed method of noise-immune coding by means of checksums it is necessary to use the Pascal method.

4. Use of a method of Pascal concerning receiving a remainder of division

The criterion of divisibility [10, 11] was created by the French mathematician B. Pascal. By means of this method it is possible to receive a remainder of division [12]. Let's formulate the following statement:

Let

$$a = \overline{a_n \dots a_2 a_1},$$

where a – is number which remainder of division on d should be found, $a_i, i = 1,\dots n$ – number figures in a system with a basis, then

$$a = \left(\sum_{i=1}^{n} (r_i \times a_i) \rightleftarrows \bmod d\right) \bmod d, \qquad (1)$$

where $r_i = r_{i-1} \times m \rightleftarrows \bmod d, i > 1$, $r_1 = 1$.

In the offered method of noise-immune coding [9] the number is presented by means of a binary numeral system. For an example we will find a remainder of division $42_{10} = 101010_2$ on 3_{10} that's $a = \overline{101010}$, $m = 2$, $d = 3$.

Let's calculate r_i:

$r_1 = 1$ – by definition;

$$r_2 = r_1 \times m = 1 \times 2 = 2 \bmod 3;$$
$$r_3 = r_2 \times m = 2 \times 2 = 4 = 1 \bmod 3;$$
$$r_4 = r_3 \times m = 1 \times 2 = 2 \bmod 3.$$

As $r_2 = r_5$, $r_5 = r_3$, that is the sequence began to repeat.

It looks 1, 2, 1, 2, 1, 2, 1, … .

Now, it agrees (1), we will find the rest:

$$a = \left(\sum_{i=1}^{n} r_i \times a_i\right) \bmod 3 \rightleftarrows =$$
$$\left(r_1 \times 0 + r_2 \times 1 + r_3 \times 0 + r_4 \times 1 + r_5 \times 0 + r_6 \times 1\right) \bmod 3 =$$
$$\left(3 \times r_2\right) \bmod 3 = 0 \bmod 3.$$

It is obvious that r_i for any d will begin to repeat at most through d-1 steps. This fact allows to count only once in advance to a constant and to work with them that in turn does possible creation hardware and program realization of a method.

4.1 Determination of Checksum. Let's consider an algorithm of noise-immune coding which is based on search of options [13]. Let $a = \overline{a_{3n} \dots a_2 a_1}$ – be the message with a size multiple 3, $a_i, i = 1,\dots 3n$ – its figure in binary records. Let's consider it as a set of 3-bit groups. For each of them we will calculate its sum behind module 2 and we write down the received result in the message after the current group. That is we will receive a modified the message $\tilde{a} = \overline{a_{4n} \dots a_2 a_1}$, where $a_i = \left(a_{i+1} + a_{i+2} + a_{i+3}\right) \bmod 2$ for $i = 1,5,9,\dots,4n-3$.

It will allow to reveal one mistake in each of the fours. Now we will consider $\tilde{a}$ as Binary number and we will find its remainder of division on 11, 13, 14, 15. The choice of the specified numbers is caused by the size of Checksum which under existing conditions has the size which is equal two bytes. Further it is given r_i remainders of division for numbers 11, 13, 14, 15 (respectively):

1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, …;
1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, …;
1, 2, 4, 8, 2, …;
1, 2, 4, 8, 1, ….

Let a' the received message. Let's check whether there are mistakes at each of the fours, having used the checksum of each of them, that is we will find all such of the sequence $1,5,9,\dots,4n-3$, that

$$a_i \neq \left(a_{i+1} + a_{i+2} + a_{i+3}\right) \bmod 2.$$

Let them m. It is possible to obtain compliance to checksum, to invert one bits in each of the fours. For finding of the initial message, we use full search. In total 4^m variants [14]. It is obvious that, for check of each option it is necessary to spend time for excess operations. We use the Pascal method. For this purpose we will calculate the remains for $\tilde{a}$ without invert. Now, changing one bit of the four, we can update the received remains. Thus the fours are not distorted are analyzed only once.

Let's review an example.

Let $a = 111011110_2$ (gaps 3 byte groups are allocated). Let's calculate for each of groups checksum. For example for the last $\left(1+1+0\right) \bmod 2$.

Thus $\tilde{a} = 111101101100_2$ (gaps 4 byte groups are allocated).

Let's find remainders of division on 11, 13, 14, 15:

$$\tilde{a} = 111101101100_2 = 3948;$$
$$\tilde{a} = 10 \bmod 11; \tilde{a} = 9 \bmod 13;$$
$$\tilde{a} = 0 \bmod 14; \tilde{a} = 3 \bmod 15;$$

Let the received message

$$a' = 111001101100_2.$$

Let's calculate control to the sum for each of the fours and we check with received. Thus, we reveal there are mistakes at the 3rd four (at the account on the right). Let's find remainders of division a':

$$a' = 3692; \; a' = 7 \bmod 11; \; a' = 0 \bmod 13;$$
$$a' = 10 \bmod 14; \; a' = 2 \bmod 15;$$

Possible options of the four that it is accepted with a mistake: 0110; 1010; 1100; 1111. Because only one four is distorted, rather separately to consider remainders of division of the distorted and not distorted part of the message. For not distorted part of the message for

various modules, they will equal 9 mod11, 4 mod13, 10 mod14, 3mod15.

For the distorted parts there are following options:

– first variant – 7 mod11; 2mod13; 10 mod14; 6 mod15;

– second variant – 8 mod11; 12mod13; 12 mod14; 10 mod15;

– third variant – 3 mod11; 4mod13; 6 mod14; 12 mod15;

– fourth variant – 1 mod11; 5mod13; 4 mod14; 0 mod15;

We calculate the remains for all message and we compare them to the received checksum:

– first variant – (9+7) mod11 = 5 mod 11 – does not coincide;

– second variant – (9+8) mod11= 6 mod11– does not coincide;

– third variant – (9+3) mod11= 1 mod11– does not coincide;

– fourth variant – (9+1)mod11= 10mod11; (4+5)mod13=9mod13; (10+4)mod14= 0 mod14; (3+0) mod15=3 mod15- all remains coincided - the solution is found.

When using a method of Pascal there is no need of division of numbers into value of modules. Let's make the table of correspondences of size of the rest from number of bit (tabl. 1).

Table 1 – **Compliance of size of the rest from number to bit**

	9	10	11	12
11	3	6	1	2
13	9	5	10	7
14	4	8	2	4
15	1	2	4	8

Let's consider the first option of the distorted four - 0110.

By use of Pascal method (1) define the remains from division:

(6 + 1) mod 11 = 7 mod 11;
(5 + 10) mod 13 = 2 mod 13;
(2 +8) mod 14 = 10 mod 14;
(2 + 4) mod 15 = 6 mod 15.

What corresponds to the remains which the sums of numbers 1024 and 512 received from division on 11, 13, 14.15 respectively. It is similarly possible to receive all other remains for all options of the distorted four. In case of distortion more than one four as it is told above, it is necessary to reconsider 2m variants.

As during calculation of the rest we consider the sum, it is possible to count only its part. Thus we can separately find influence of each figure of number on its remainder of division that allows creating parallel realization.

For example, everyone process can transfer the part and a position of the first figure of her in all number that allows to find its influence on a remainder of division of numbers. Having collected all results, we can receive the rest.

Conclusions

Use of a method of Pascal for definition of remainders of division allows to accelerate considerably process of search of various options the message which will be restored. Realization of the offered method allows to create parallel structures which give the chance to solve a problem of recovery of the message on the scale of real time.

REFERENCES

1. ISTR Internet Security Threat Report (2019), Vol. 23, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
2. Law No. 2163 - VIII "On Basic Principles of Cyber Security in Ukraine (2019), available at: https://ips.ligazakon.net/document/view/T172163?an=1
3. Pevnev, V.Ya. and Tsuranov, M.V. (2010), "Mathematical model of information security", *Systemy obrobky informatsiyi*, Vol. 3, KhUPS, Kharkiv, pp. 62–64. (in Russian)
4. Robert K. Ackerman (2019), *Blog: Data Integrity Is the Biggest Threat in Cyberspace*, available at: http://www.afcea.org/content/?q=node/11438
5. Utkina, V.F. and Krjuchkova, Ju.V. (1988), *Efficiency of technical systems*, Mashinostroenie, Moscow, 328 p.
6. *An Algorithm for Error Correcting Cyclic Redundancy Checks* (2019), available at: https://web.archive.org/web/20170720165847/http://www.drdobbs.com/an-algorithm-for-error-correcting-cyclic/184401662
7. Peterson, W.W. and Brown, D.T. (1961), "Cyclic Codes for Error Detection", *Proceedings of the IRE*, Vol. 49 (1). pp. 228–235, DOI: https://doi.org/10.1109/JRPROC.1961.287814
8. Stigge, Martin; Plötz, Henryk; Müller, Wolf; Redlich, Jens-Peter (2006), "Reversing CRC – Theory and Practice" (PDF), Humboldt University Berlin, Berlin, 17, Archived from the original (PDF) on 19 July 2011, Retrieved 4 February 2011.
9. Pevnev, V.Ya. and Tsuranov, M.V. (2013), "Theoretical justification of the method of recovery messages received with errors", *Systemy obrobky informatsiyi*, .Vol. 2(109), KhUPS, Kharkiv, pp.194–196.
10. Leonard Eugene Dickson (2012), *History of the Theory of Numbers: Divisibility and Primality*, Vol. 1. Dover Publications, Inc. Mieola, New York, 512 p.
11. Mozhaev, O., Kuchuk H., Kuchuk, N., Mozhaev, M. and Lohvynenko M. (2017), "Multiservise network security metric", *IEEE Advanced information and communication technologies-2017*, Proc. of the 2th Int. Conf., 2017, Lviv, pp. 133–136.
12. Des cerecteres de divisibilite des nombres deduits de la somme de leurs chiffres [On the divisibility properties of numbers deduced from the sum of their digits] (1665), Oeuvres completes, Paris: Ed.du Seuil, 1963, pp. 84-86, available at: http://books.google.com.ua/books?id=B1c0s3ffN_0C&pg=PA243&dq=criteria+of+divisibility&hl=uk&ei=L1SLTvD0AsPm4QTxk5SMBA&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q=criteria%20of%20divisibility&f=false

13. Pevnev, V.Ya. and Tsuranov, M.V. (2012), “Comparative analysis of the speed of error-correcting codes”, *Theoretical and applied problems of information security*, proc. Intern. scientific.-practical. Conf., MVD, Minsk, pp. 153–156.
14. Pevnev, V.Ya. and Tsuranov, M.V. (2012), “The construction of the optimal code tables”, *Systemy obrobky informatsiyi*, Vol. 3(108), KhUPS, Kharkiv, pp. 27–30.

Received (Надійшла) 15.07.2019
Accepted for publication (Прийнята до друку) 21.08.2019

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Пєвнєв Володимир Якович – кандидат технічних наук, доцент, доцент кафедри комп’ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна;
Volodymyr Pevnev – Candidate of Technical Sciences, Associate Professor, Associate Professor of Computer Systems, Networks and Cyber security Department, National Aviation University “Kharkiv Aviation Institute”, Kharkiv, Ukraine;
e-mail: v.pevnev@csn.khai.edu; ORCID ID: http://orcid.org/0000-0002-3949-3514

Цуранов Михайло Віталійових – старший викладач кафедри комп’ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна;
Mikhail Tsuranov – Senior Lecturer of Computer Systems, Networks and Cyber security Department, National Aviation University “Kharkiv Aviation Institute”, Kharkiv, Ukraine;
e-mail: m.tsuranov@csn.khai.edu; ORCID ID: http://orcid.org/0000-0002-2115-7029

Землянко Георгій Андрійович – магістрант кафедри комп’ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна;
Heorhii Zemlianko – Master Student of Computer Systems, Networks and Cyber security Department, National Aviation University “Kharkiv Aviation Institute”, Kharkiv, Ukraine;
e-mail: g.zemlynko@student.csn.khai.edu; ORCID ID: http://orcid.org/0000-0003-4153-7608

Харченко В’ячеслав Сергійович – доктор технічних наук, професор, завідувач кафедри комп’ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна;
Vyacheslav Kharchenko – Doctor of Technical Sciences, Professor, Head of Computer Systems, Networks and Cyber security Department, National Aviation University “Kharkiv Aviation Institute”, Kharkiv, Ukraine;
e-mail: v.kharchenko@csn.khai.edu; ORCID ID: http://orcid.org/0000-0001-5352-077X

Використання методу Паскаля для підрахунку контрольних сум у завадостійкому кодуванні

В. Я. Пєвнєв, М. В. Цуранов, Г. А. Землянко, В. С. Харченко

Анотація. Предметом вивчення в статті є можливість використання методу Паскаля для знаходження залишків від ділення великих чисел при використанні CRC. **Метою** є проаналізувати можливість використання методу Паскаля для визначення залишків від ділення у системах CRC. **Завдання:** проаналізувати можливість використання CRC для завадостійкого кодування у різних каналах зв’язку, показати можливість застосування методу Паскаля для способу завадостійкого кодування з використанням контрольних сум. Використовуваними **методами** є: аналітичний метод, методи модальної арифметики. Отримані такі **результати.** Розроблена методика підрахунку контрольної суми повідомлення, які використовуються для контролю цілісності та відновлення спотвореного повідомлення. **Висновки.** Використання методу Паскаля для визначення залишків від ділення дозволяє значно прискорити процес перебору різних варіантів повідомлення яке буде відновлено. Реалізація запропонованого методу дозволяє створити паралельні структури, які дають можливість вирішити задачу відновлення повідомлення в масштабі реального часу.

Ключові слова: завадостійке кодування; метод Паскаля; цілісність; ділення за модулем; контрольні суми; залишки від ділення.

Использование метода паскаля для подсчета контрольных сумм в помехоустойчивом кодировании

В. Я. Певнев, М. В. Цуранов, Г. А. Землянко, В. С. Харченко

Аннотация. Предметом изучения в статье является возможность использования метода Паскаля для нахождения остатков от деления больших чисел при использовании CRC. **Целью** является проанализировать возможность использования метода Паскаля для определения остатков от деления в системах CRC. **Задачи:** проанализировать возможность использования CRC для помехоустойчивого кодирования в различных каналах связи, показать возможность использования метода Паскаля для способа помехоустойчивого кодирования с использованием контрольных сумм. Используемыми **методами** являются**:** аналитический метод, методы модальной арифметики. Получены следующие **результаты.** Разработана методика подсчета контрольной суммы сообщения, которые используются для контроля целостности и восстановления искаженного сообщения. **Выводы.** Использование метода Паскаля для определения остатков от деления позволяет значительно ускорить процесс перебора различных вариантов восстанавливаемого сообщения. Реализация предложенного метода позволяет создать параллельные структуры, которые дают возможность решить задачу восстановления сообщения в реальном времени.

Ключевые слова: помехоустойчивое кодирование; метод Паскаля; целостность; деление по модулю; контрольные суммы; остатки от деления.