УДК 519.7 DOI 10.17223/20710410/X/1

MATHEMATICAL PROBLEMS AND SOLUTIONS OF THE TENTH INTERNATIONAL OLYMPIAD IN CRYPTOGRAPHY NSUCRYPTO[1]

N. N. Tokareva[1], O. S. Zaikin[2], V. A. Idrisova[1], E. A. Ishchukova[3], K. V. Kalgin[1], N. A. Kolomeec[1], A. V. Kutsenko[1], S. N. Kyazhin[4], E. S. Malygina[5], I. A. Pankratova[6]

[1] *Novosibirsk State University, Novosibirsk, Russia*
[2] *Matrosov Institute for System Dynamics and Control Theory, Irkutsk, Russia*
[3] *Southern Federal University, Rostov-on-Don, Russia*
[4] *CryptoPro, Moscow, Russia*
[5] *Immanuel Kant Baltic Federal University, Kaliningrad, Russia*
[6] *Tomsk State University, Tomsk, Russia*

E-mail: crypto1127@mail.ru

International Olympiad in Cryptography Non-Stop University CRYPTO (NSUCRYPTO) is a big annual event in the world of cryptographic research. The olympiad offers mathematical problems for university and school students and, moreover, for professionals in the area of cryptography and computer science. It draws attention of young researchers to modern cryptography and raises awareness about open problems in the field. In this paper we propose problems of NSUCRYPTO'23 and consider their solutions. There were 14 problems related to combinatorial and algebraic methods of cryptography, to hash functions, cipher analysis and design, quantum encryption and signatures, SAT-solvers and finite-state machines. Problems vary from easy mathematical tasks that could be solved by school students to open problems that deserve separate study.

Keywords: *cryptography, ciphers, protocols, number theory, S-boxes, quantum circuits, matrices, hash functions, cryptocurrencies, postquantum cryptosystems, Olympiad, NSUCRYPTO.*

MATHEMATICAL PROBLEMS AND SOLUTIONS OF THE TENTH INTERNATIONAL OLYMPIAD IN CRYPTOGRAPHY NSUCRYPTO

Н. Н. Токарева[1], О. С. Заикин[2], В. А. Идрисова[1], Е. А. Ищукова[3], К. В. Калгин[1], Н. А. Коломеец[1], А. В. Куценко[1], С. Н. Кяжин[4], Е. С. Малыгина[5], И. А. Панкратова[6]

[1] *Новосибирский государственный университет, г. Новосибирск, Россия*
[2] *Институт динамики систем и теории управления имени В.М. Матросова СО РАН, г. Иркутск, Россия*
[3] *Южный федеральный университет, г. Ростов-на-Дону, Россия*
[4] *«КриптоПро», г. Москва, Россия*
[5] *Балтийский федеральный университет имени И. Канта, г. Калининград, Россия*
[6] *Томский государственный университет, г. Томск, Россия*

[1]The work of the first, fifth and sixth authors was supported by the Mathematical Center in Akademgorodok under the agreement No. 075-15-2022-282 with the Ministry of Science and Higher Education of the Russian Federation. The work of the ninth author was supported by the Kovalevskaya North-West Centre of Mathematical Research under the agreement No. 075-02-2023-934 with the Ministry of Science and Higher Education of the Russian Federation. The work is also supported by Novosibirsk State University, Southern Federal University, Kryptonite, Demlabs and Aktiv company.

Международная олимпиада по криптографии Non-Stop University CRYPTO (NSUCRYPTO) — крупное ежегодное событие в мире криптографических исследований. Олимпиада предлагает математические задачи для студентов университетов и школьников, а также для специалистов в области криптографии и компьютерных наук. Она привлекает внимание молодых исследователей к современной криптографии и повышает осведомленность об открытых проблемах в этой области. В данной работе мы предлагаем задачи NSUCRYPTO'23 и рассматриваем их решения. На олимпиаде было представлено 14 задач, связанных с комбинаторными и алгебраическими методами криптографии, хэш-функциями, анализом и проектированием шифров, квантовым шифрованием и подписями, SAT-решателями и конечными автоматами. Задачи варьируются от простых математических задач, которые могут решить школьники, до открытых проблем, которые заслуживают отдельного изучения.

Ключевые слова: *криптография, шифры, протоколы, теория чисел, S-блоки, квантовые схемы, матрицы, хэш-функции, криптовалюты, постквантовые криптосистемы, олимпиада, NSUCRYPTO.*

1. Introduction

Non-Stop University CRYPTO (**NSUCRYPTO**) is the unique international competition for professionals, school and university students, providing various problems on theoretical and practical aspects of modern cryptography, see [22]. The main goal of the olympiad is to draw attention of young researchers not only to competetive fascinating tasks, but also to sophisticated and tough scientific problems at the intersection of mathematics and cryptography. That is why each year there are several open problems in the list of tasks that require rigorous studying and deserve a separate publication in case of being solved. Since NSUCRYPTO holds via the Internet, everybody can easily take part in it. Rules of the Olympiad, the archive of problems, solutions and many more can be found at the official website [23].

The first Olympiad was held in 2014, since then several thousands students and specialists from more than 70 countries took part in it. The Program committee now is including 24 members from cryptographic groups all over the world. Main organizers and partners are Cryptographic Center (Novosibirsk), Novosibirsk State University, Mathematical Center in Akademgorodok, Kovalevskaya North-West Center of Mathematical Research, KU Leuven, Southern Federal University, Demlabs, Belarusian State University, Tomsk State University, Kryptonite and Aktiv company.

This year 24 in the first round and 38 teams in the second round from 15 countries became the winners (see the list [24]). This year we proposed 14 problems to participants and 3 of them were entirely open or included some open questions. Totally, there were 1100 participants from 44 countries.

Following the results of each Olympiad we also publish scientific articles with detailed solutions and some analysis of the solutions proposed by the participants, including advances on unsolved ones, see [6, 7, 12–17, 20].

2. An overview of open problems

One of the main characteristic of the Olympiad is that unsolved scientific problems are proposed to the participants in addition to problems with known solutions. All 34 open problems that were offered since the first NSUCRYPTO can be found here [25]. Some of these problems are of great interest to cryptographers and mathematicians for many years.

These are such problems as "APN permutation" (2014), "Big Fermat numbers" (2016), "Boolean hidden shift and quantum computings" (2017), "Disjunct Matrices" (2018), and others.

Despite that it is marked that the problem is open and therefore it requires a lot of hard work to advance, some of the problems we suggested are solved or partially solved by our participants during the Olympiad. For example, problems "Algebraic immunity" (2015), "Sylvester matrices" (2018), "Miller — Rabin revisited" (2020) were solved completely. Also, partial solutions were suggested for problems "Curl27" (2019), "Bases" (2020), "Quantum error correction" (2021) and "s-Boolean sharing" (2021).

Moreover, some researchers continue to work on solutions even after the Olympiad was over. For example, authors of [19] proposed a complete solution for problem "Orthogonal arrays" (2018). Partial solutions for another open problem, "A secret sharing", (2014) were presented in [10], [11], and a recursive algorithm for finding the solution was proposed in [9].

3. Problem structure of the Olympiad

There were 14 problems stated during the Olympiad, some of them were included in both rounds (Tables 1, 2). Section A of the first round consisted of six problems, while Section B of the first round consisted of 8 problems. The second round was composed of 11 problems; 3 of them included unsolved questions (awarded special prizes).

Table 1
Problems of the first round

N	Problem title	Max score
1	Cubes and secrets	4
2	Agents' meeting	4
3	Affine cipher	4
4	Primes	2
5	0, 1, 2, 3	4
6	Algebraic cryptanalysis	4

Section A

N	Problem title	Max score
1	Cubes and secrets	4
2	AntCipher	6
3	Mixed hashes	6
4	Agents' meeting	4
5	0, 1, 2, 3	4
6	An aggregated signature	12, open problem
7	Algebraic cryptanalysis	4
8	Quantum encryption	8

Section B

Table 2
Problems of the second round

N	Problem title	Max score
1	Affine cipher	4
2	Simple ideas for primes	12, open problem
3	Mixed hashes	6
4	Column functions	8
5	Primes	2
6	An aggregated signature	12, open problem
7	A unique decoding	12, open problem
8	Algebraic cryptanalysis	4
9	Finite-state machines	8
10	Quantum encryption	8
11	AntCipher	6

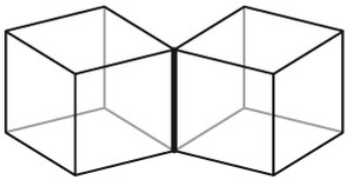
4. Problems and their solutions

In this section, we formulate all the problems of 2023 year Olympiad and present their detailed solutions, in some particular cases we also pay attention to solutions proposed by the participants.

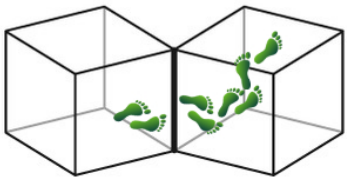
4.1. Problem "Cubes and secrets"

Formulation

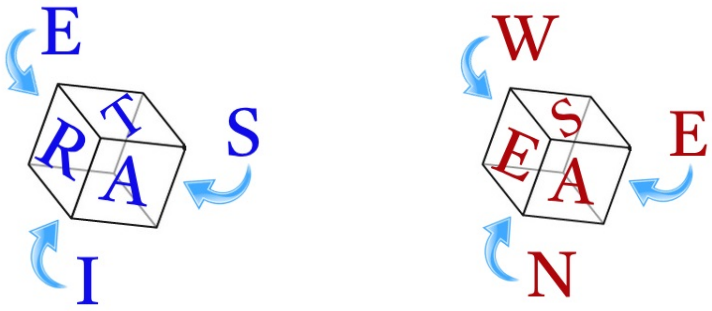
Alice is a beginner cryptographer. She was very impressed by the Scytale cipher, so she decided to invent her own simple cipher with the similar idea. Alice took two cubes with empty sides and joined them by an edge.



Then she wrote 12 letters of her secret message on empty sides of the cubes (one letter for one side). She did it in such a way that one can read the message just walking from side to side through edges. On every side it is possible to be only once.



She realized that the information about two joined edges and about the path on cubes form her secret key of encryption. At the same time letters on cubes form the resulting ciphertext. Could you read the secret message of Alice without the key? It is known also that the secret message is a meaningful text. Her cubes are



Solution

The participants gave many various answers to this task. One of the participants decoded his word combination as "ASIENSWEATER" and identified the organizers of the Olympiad as Asians. The condition of the task involved using all the letters on the second cube before returning to first cube, as we can only go through each cube face once. We get Alice's encrypted sentence "I see a new star".

The best graphic solution was given by the user 6383, because he illustrated on the cubes his way of decoding the cipher. The solution of Ilya Baranov (Russia) is also worth noting, as it is brief but correct, as well as the neatly organized solution of Shuaichu Pan (China).

4.2. Problem "Agents' meeting"

Formulation

Alice and Bob, two special agents, were invited on the big meeting where they should find each other and communicate. Alice knows who is Bob (she was given a photo of him), but Bob has never seen Alice. Before the meeting the Boss has send them the secret password for communication: it is the square root of the first six digits of the number π modulo n, where $n = 15\,102\,023$ is a public information (known for all). Alice should find Bob and convince him that she knows the password without an announcement of it. Propose how it is possible to do. In other words, propose the zero-knowledge protocol for this specific situation. By the way, what is the sense of the number n?

Solution

Let $x := \sqrt{314\,159} \pmod{15\,102\,023}$, so $x = 3\,627\,656$.

1. Alice chooses α_1 such that $\mathrm{GCD}(\alpha, n)$ (for example, $\alpha_1 = 71$), then calculates

$$\alpha_2 = x \cdot \frac{1}{\alpha_1} \pmod{n} = 3\,627\,656 \cdot \frac{1}{71} \pmod{15\,102\,023} = 14\,089\,594.$$

After that Alice finds

$$x_1 = \alpha_1^2 \pmod{n} = 5\,041 \pmod{15\,102\,023}$$

and

$$x_2 = \alpha_2^2 \pmod{n} = 7\,974\,985 \pmod{15\,102\,023},$$

and sends both these values to Bob.

2. Bob checks that

$$x_1 \cdot x_2 = 5\,041 \cdot 7\,974\,985 \pmod{15\,102\,023} = 314\,159,$$

and asks Alice to send the value either $\sqrt{x_1}$ or $\sqrt{x_2}$ (i. e. α_1 or α_2, one of the divisors of x) to make sure that Alice really knows the value $x = \sqrt{314\,159} \pmod{15\,102\,023}$.

Best solutions were proposed independently by Kaniuar Bacho (Germany), Nilabha Saha (India), Thang Trinh Cao (Vietnam).

4.3. Problem "Affine cipher"

Formulation

Consider a 29-character alphabet {A,..., Z, α, β, γ}. Letters A,..., Z have numerical equivalents $0, \ldots, 25$, while numbers 26, 27 and 28 correspond to symbols α, β, γ.

We use a cryptosystem with plaintexts and ciphertexts being two-letter blocks, i. e. bigrams. For each bigram it is easy to find a numerical equivalent, it is an integer from 0 to $840 = 29^2 - 1$, determined by the rule $x \cdot 29 + y$, where x and y are the numerical equivalents of the letters of the bigram.

Encryption is implemented as an affine transformation $C = a \cdot P + b \mod 841$, where P is a plaintext, C is the corresponding ciphertext and the pair (a, b) is a secret key. Here a and b are integer numbers between 0 and 840. For example, if $a = 2$ and $b = 27$, then the bigram DP will be encrypted as $H\gamma$. In fact, for the bigram DP we put into the correspondence the number $3 \cdot 29 + 15 = 102$. After encrypting we get $2 \cdot 102 + 27 = 231$ that corresponds to the bigram $H\gamma$, since $231 = 7 \cdot 29 + 28$.

An analysis of the long ciphertext (for a fixed unknown key) showed that the bigrams "$\beta\ \gamma$", "UM" and "LC" are the most often found in this text. At the same time, we assume that the most frequent bigrams in English texts are "TH", "HE" and "IN".

Could you then decrypt the message "KEUDCR"? What about recovering of the key?

Solution

Let's compare the most common ciphertext bigrams in the text with their numerical equivalents:

$$\text{"23"} \leftrightarrow 29 \cdot 27 + 28 = 811,$$

$$\text{"UM"} \leftrightarrow 29 \cdot 20 + 12 = 592,$$

$$\text{"LC"} \leftrightarrow 29 \cdot 11 + 2 = 321.$$

Similarly, we compare the most frequent bigrams in English "TH", "HE" and "IN" with their numerical equivalents:

$$\text{"TH"} \leftrightarrow 29 \cdot 19 + 7 = 558,$$

$$\text{"HE"} \leftrightarrow 29 \cdot 7 + 4 = 207,$$

$$\text{"IN"} \leftrightarrow 29 \cdot 8 + 13 = 245.$$

From the encryption formula we get the decryption formula:

$$P = a^{-1}C - a^{-1}b := a'C + b',$$

where (a', b') is the decryption key. Let's compare the numerical equivalents of the bigrams "23", "UM" and "LC" using the decryption formula and numerical equivalents for "TH", "HE" and "IN":

$$\begin{cases} 811a' + b' = 558 (\mathrm{mod}\, 841) \\ 592a' + b' = 207 (\mathrm{mod}\, 841) \\ 321a' + b' = 245 (\mathrm{mod}\, 841) \end{cases}$$

So, we obtain $(a', b') = (785, 560)$.

Now we decrypt the ciphertext "KEUDCR":

$$\text{"KE"} \leftrightarrow 29 \cdot 10 + 4 = 294,$$

$$\text{“UD”} \leftrightarrow 29 \cdot 20 + 3 = 583,$$

$$\text{“CR”} \leftrightarrow 29 \cdot 2 + 17 = 75.$$

Finally, we have:

$$\text{“KE”} \mapsto 294 \cdot 785 + 560 (\mathrm{mod}\, 841) = 75 = 29 \cdot 2 + 17 \mapsto \text{“CR”},$$

$$\text{“UD”} \mapsto 583 \cdot 785 + 560 (\mathrm{mod}\, 841) = 711 = 29 \cdot 24 + 15 \mapsto \text{“YP”},$$

$$\text{“CR”} \mapsto 75 \cdot 785 + 560 (\mathrm{mod}\, 841) = 565 = 29 \cdot 19 + 14 \mapsto \text{“TO”}.$$

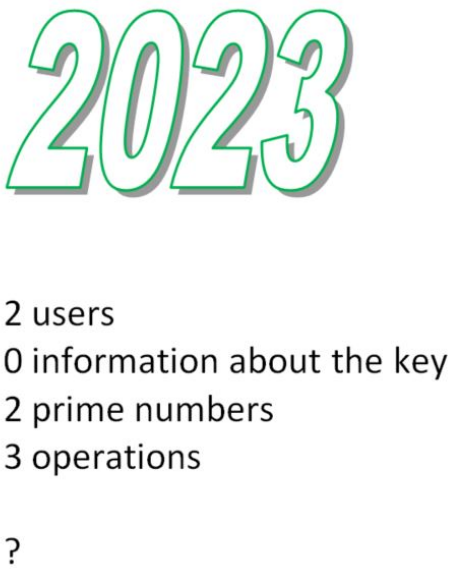
Many correct solutions for this problem have been presented, but the best solutions belong to the following authors: Xuefeng Xu, Jiafu Liu, Renzhang Liu (China); Ivan Ioganson, Vitaliy Cherkashin, Vladislav Izvekov (Russia); Abdul Qayyum, Haris Muhammad, Muhammad Qasim (Pakistan).

4.4. Problem “Primes”

Formulation

Marcus invented a new cryptosystem. To start to work with it one should choose two big prime numbers p and q, then calculate $n = p \cdot q$ and $m = p + q$. The number $n \cdot m$ will be used in the cryptosystem.

While testing the system Marcus has noticed that for the chosen numbers p and q the resulting number $n \cdot m$ ends with 2023. Is this possible?



Solution

To verify Marcus's cryptosystem, we have to look at the properties of prime numbers. Since there is no prime number 2 between p and q (remember, that p and q are big), then $m = p + q$ is even. That is why $n \cdot m$ is even too and hence it can not end with 3. So, the described situation is impossible. We suppose that this problem is the simplest one for the whole history of NSUCRYPTO. And, of course, we have got a great deal of correct solutions.

4.5. Problem "0, 1, 2, 3"

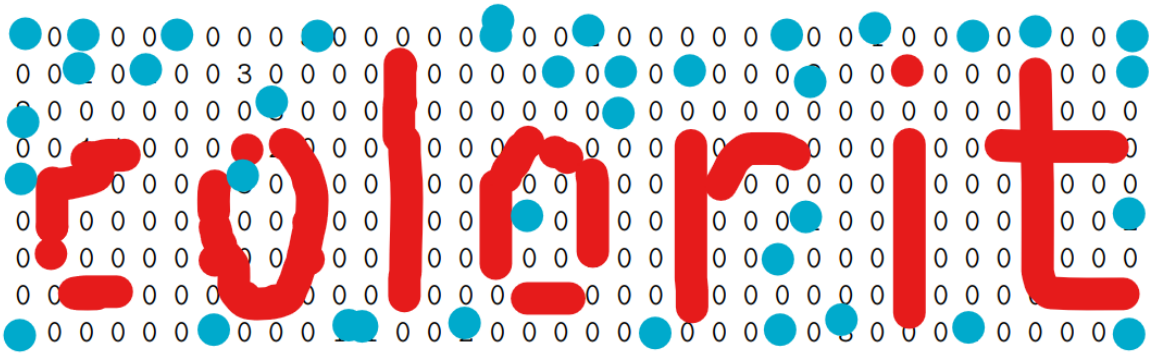
Formulation

Decrypt the meaningful message:

```
1 0 2 0 0 1 0 0 0 3 0 0 0 0 0 1 0 0 2 0 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1
0 0 1 0 2 0 0 3 0 0 0 0 3 0 0 0 0 2 0 3 0 1 0 0 0 2 0 0 3 0 0 0 2 0 0 3
2 0 0 0 0 0 0 0 3 0 0 0 3 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0
0 0 1 1 0 0 0 2 2 0 0 0 3 0 0 0 1 1 0 0 0 2 0 2 2 0 0 0 3 0 0 2 2 2 2 0
3 1 0 0 0 0 2 3 0 2 0 0 3 0 0 1 0 0 1 0 0 2 2 0 0 0 0 0 3 0 0 0 2 0 0 0
0 1 0 0 0 0 2 0 0 2 0 0 3 0 0 1 3 0 1 0 0 2 0 0 0 1 0 0 3 0 0 0 2 0 0 2
0 1 0 0 0 0 2 0 0 2 0 0 3 0 0 1 0 0 1 0 0 2 0 0 2 0 0 0 3 0 0 0 2 0 0 0
0 0 1 1 0 0 0 2 2 0 0 0 3 0 0 0 1 1 0 0 0 2 0 0 0 0 0 0 3 0 0 0 0 2 2 0
2 0 0 0 0 0 1 0 0 0 1 1 0 0 2 0 0 0 0 0 3 0 0 0 1 0 3 0 0 0 1 0 0 0 0 3
```

Solution

Let us look at the digits on the picture from a visual perspective. As you can notice, digits 1, 2, 3 are repeated in a certain way, and 0 forms a kind of a background. If we look closely at the mentioned digits, we can see the outlines of the letters. If we remove the 0 from the picture, we can see the right word. More important clues were the question marks in different colours. Digit 1 forms letters C and O, digit 2 – letters O, R and T, digit 3 – letters L and I. As a result, we get the phrase "COLOR IT". We choose the solution of the Xi Nan Shu (United Kingdom) as the best one, because he described his method in detail.



4.6. Problem "Algebraic cryptanalysis"

Formulation

Bob decided to construct a new stream cipher **BOB-0.1**.

He used the binary key of length 8, say $K = (k_1, \ldots, k_8)$. Then he generated the binary sequence β such that $\beta_n = k_n$ for all $n = 1, \ldots, 8$ and for $n > 8$ it is defined as $\beta_n = \beta_{n-1} \oplus \beta_{n-8}$. Then Bob constructed the secret sequence γ for XORing it with a binary plaintext. The sequence γ is generated by the following rule: $\gamma_n = \beta_n \cdot \beta_{n+2} \oplus \beta_{n+7}$ for $n \geqslant 1$.

Alice intercepted the eight secret bits of γ after the first 1200 missed bits. These bits are `00100001`. Is she able to recover the original key K?

Solution

The binary sequence β can be expressed algebraically as the xor of the original bits. Participants proposed different simple programs to cover these bits and then find the key. In right solutions participants realized that K could be either $(0,0,1,1,1,1,0,0)$ or $(0,1,1,0,1,1,0,0)$. The original K cannot be determined in the unique way.

4.7. Problem "AntCipher"

Formulation

Sam studies microelectronics, while his hobbies are biology and cryptography. He decided to unite all these areas in a research project aimed at constructing a tiny GPS tracker for an ant to monitor its movements.

The tracker consists of 3 modules: GPS, encryption, transmission. Once a minute, coordinates are determined, encrypted, and transmitted to a Sam's computer, where they are automatically decrypted. Due to the size limitation, the encryption module takes only a 2-bit plaintext and produces a 2-bit ciphertext, so the coordinates are divided into 2-bit blocks which are given to the encryption module. Sam has just developed a symmetric cipher called **AntCipher** for this purpose.

The cipher must be represented by the equation CNF=True, where CNF is a conjunction of disjunctions of literals, yet literal is a Boolean variable or its negation. In the Sam's CNF, x_1 and x_2 correspond to the plaintext, x_9 and x_{10} correspond to the ciphertext, while the remaining 6 variables are auxiliary. The equation is as follows:

$$(x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge$$
$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge$$
$$(\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_9 \vee x_{10} \vee \neg x_6) \wedge$$
$$(x_1 \vee x_2 \vee x_3 \vee x_4 \vee \neg x_7) \wedge (x_2 \vee x_3 \vee x_4 \vee \neg x_7 \vee \neg x_8) = True$$

The problem is that, due to the limitations, the CNF must consist of at most 20 literals and at most 16 variables, while the presented one consists of 46 literals and 10 variables. Please, help Sam to construct an equivalent CNF that fits the limits. By equivalent it is meant that for each pair of plaintext-variables' values, the same pair of ciphertext-variables' values is derived in the equation.

Solution

Hereinafter 1 is considered to be True and 0 is considered to be False.

The first way. Construct a minimal possible equivalent CNF.

Assume that $x_1 = 0$ and $x_2 = 0$. The CNF is modified as follows:

$$(x_9) \wedge (x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge$$
$$(x_9 \vee x_{10} \vee \neg x_6) \wedge (x_3 \vee x_4 \vee \neg x_7) \wedge (x_3 \vee x_4 \vee \neg x_7 \vee \neg x_8).$$

The first clause contains only a single literal x_9, while the second one contains only x_3. According to the unit clause rule [1], such literals are assigned to 1, so $x_9 = 1, x_3 = 1$ and the CNF is $(\neg x_{10}) \wedge (x_{10} \vee \neg x_4)$. The unit clause rule is applied one more time and x_{10} is assigned to 0. Thus, if x_1 and x_9 are assigned to $(0, 0)$, the values $(1, 0)$ of x_9 and x_{10} are derived, while values of the remaining variables do not matter. Similarly, if $(0, 1)$, $(1, 0)$, and $(1, 1)$ are assigned, $(1, 1)$, $(0, 0)$, and $(0, 1)$ are derived, respectively. Therefore this is a transposition cipher that operates with 2-bit words. Note that if x_1 is assigned to 0 (1), x_9 takes the value 1 (0), so x_9 is equal to $\neg x_1$. Yet x_{10} is equal to x_2. A key peculiarity here is that x_9 depends only on x_1, while x_{10} depends only on x_2. It means that the first dependency can be expressed as $(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) = 1$, while the second one is $(x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10}) = 1$. The formulae in both equations are canonical CNFs constructed via truth tables. Now these equations can be united into one:

$$(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10}) = 1.$$

The corresponding CNF consists of 4 variables and 8 literals that fits the limits.

The second way. Minimize the CNF.

According to the pure literal rule [1], if only one literal of a variable occurs in a CNF, then this variable is assigned in a way that the literal becomes 1. The rule is applied to variables x_7 and x_8 since only literals $\neg x_7$ and $\neg x_8$ occur in the CNF. By assigning $x_7 = 0$ and $x_8 = 0$ the last two clauses are removed, so the number of literals in the CNF is reduced from 46 to 36, while the number of variables is reduced from 10 to 8.

Following the resolution rule [1], the subformula $(a_1 \vee a_2 \vee \cdots \vee a_k \vee v) \wedge (b_1 \vee b_2 \vee \cdots \vee b_n \vee \neg v)$ is replaced by $(a_1 \vee a_2 \vee \cdots \vee a_k \vee b_1 \vee b_2 \vee \cdots \vee b_n)$. By applying this rule, the subformula $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3)$ is replaced by $(x_1 \vee x_2 \vee \neg x_9 \vee \neg x_{10})$. The same rule is applied to six clauses containing x_4, x_5, and x_6. As a result, variables x_3, x_4, x_5, and x_6 are removed, while the number of literals is reduced from 36 to 28:

$$\begin{aligned}(x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge \\ (x_1 \vee x_2 \vee \neg x_9 \vee \neg x_{10}) \wedge (x_1 \vee \neg x_2 \vee \neg x_9 \vee x_{10}) \wedge (\neg x_1 \vee x_2 \vee x_9 \vee \neg x_{10}) \wedge \\ (\neg x_1 \vee \neg x_2 \vee x_9 \vee x_{10}).\end{aligned}$$

By applying the resolution rule, $(x_1 \vee x_2 \vee x_9) \wedge (x_1 \vee \neg x_2 \vee x_9)$ is replaced by $(x_1 \vee x_9)$, while $(\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9)$ is replaced by $(\neg x_1 \vee \neg x_9)$. As a result, 4 variables and 20 literals remain in the CNF:

$$\begin{aligned}(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (x_1 \vee x_2 \vee \neg x_9 \vee \neg x_{10}) \wedge (x_1 \vee \neg x_2 \vee \neg x_9 \vee x_{10}) \wedge \\ (\neg x_1 \vee x_2 \vee x_9 \vee \neg x_{10}) \wedge (\neg x_1 \vee \neg x_2 \vee x_9 \vee x_{10}).\end{aligned}$$

The CNF fits the given limits, so the minimization can be stopped here. However, the number of literals can be further reduced. According to the first two clauses, $x_1 = \neg x_9$. In the last 4 clauses x_1 is replaced by $\neg x_9$:

$$\begin{aligned}(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (\neg x_9 \vee x_2 \vee \neg x_{10}) \wedge (\neg x_9 \vee \neg x_2 \vee x_{10}) \wedge \\ (x_9 \vee x_2 \vee \neg x_{10}) \wedge (x_9 \vee \neg x_2 \vee x_{10}).\end{aligned}$$

Again the resolution rule is applied: $(\neg x_9 \vee x_2 \vee \neg x_{10}) \wedge (x_9 \vee x_2 \vee \neg x_{10})$ is replaced by $(x_2 \vee \neg x_{10})$; $(\neg x_9 \vee \neg x_2 \vee x_{10}) \wedge (x_9 \vee \neg x_2 \vee x_{10})$ is replaced by $(\neg x_2 \vee x_{10})$. The final CNF consists of 4 variables and 8 literals:

$$(x_1 \vee x_9) \wedge (\neg x_1 \vee \neg x_9) \wedge (x_2 \vee \neg x_{10}) \wedge (\neg x_2 \vee x_{10}).$$

There were 22 correct solutions in the first round and 35 ones in the second round. Most of them were variations of the two solutions discussed above. We would like to especially mention the following: (i) the only one complete second-way-like solution proposed by the team of Sergey Makogon, Semyon Kochetkov, and Kirill Tretyakov (Russia); (ii) a very detailed first-way-like solution by the team of Thang Trinh Cao, Nhat Dang, and Pham Minh (Vietnam); (iii) a pure experimental non-brute-force solution by Bach Pham Cong (Vietnam).

4.8. Problem "Mixed hashes"

Formulation

Alice and Bob are exchanging with encrypted messages. To encrypt data, they use the **Present** cipher with an 80-bit secret key in ECB format. They record the information in the form of graphic files in `*.ppm` format.

To be more secure, Alice and Bob decided that file headers should be removed before encryption. In order to be able to recover the file header, they agreed to transmit along with the encrypted file the hash value of the header itself, presented in **UTF-8** format. To do this, all header elements are written as a single line, using a space to separate the lines of the original header. The **sha-256** function is used as a hashing algorithm. So, for example, the following hash value will be generated for the header of `mikki.ppm`:

Heading `P6 360 537 255`
Sha-256 `999015795668c201db162926261ed979bc6e820aa1acfc385a0285685084d9f9`

Bob prepared eight files for Alice without headers, encrypted using the **Present** algorithm with the same secret key in ECB mode. He has sent the files themselves and hash values of the headers to Alice. While sending, the hash values were mixed up. So, Alice received eight files and eight hash values, but she does not know which hash value corresponds to which encrypted file. Could you help Alice to read the message from Bob? Hash values received are

```
602a4a8fff652291fdc0e049e3900dae608af64e5e4d2c5d4332603c9938171d
f40e838809ddaa770428a4b2adc1fff0c38a84abe496940d534af1232c2467d5
aa105295e25e11c8c42e4393c008428d965d42c6cb1b906e30be99f94f473bb5
70f87d0b880efcdbe159011126db397a1231966991ae9252b278623aeb9c0450
77a39d581d3d469084686c90ba08a5fb6ce621a552155730019f6c02cb4c0cb6
456ae6a020aa2d54c0c00a71d63033f6c7ca6cbc1424507668cf54b80325dc01
bd0fd461d87fba0d5e61bed6a399acdfc92b12769f9b3178f9752e30f1aeb81d
372df01b994c2b14969592fd2e78d27e7ee472a07c7ac3dfdf41d345b2f8e305
```

Solution

First, you need to determine which headers correspond to hash values passed by Bob.

UTF-8	Sha 256
P6 400 433 255	602a4a8fff652291fdc0e049e3900dae608af64e5e4d2c5d4332603c9938171d
P6 559 530 255	f40e838809ddaa770428a4b2adc1fff0c38a84abe496940d534af1232c2467d5
P6 512 512 255	aa105295e25e11c8c42e4393c008428d965d42c6cb1b906e30be99f94f473bb5
P6 525 489 255	70f87d0b880efcdbe159011126db397a1231966991ae9252b278623aeb9c0450
P6 585 577 255	77a39d581d3d469084686c90ba08a5fb6ce621a552155730019f6c02cb4c0cb6
P6 513 613 255	456ae6a020aa2d54c0c00a71d63033f6c7ca6cbc1424507668cf54b80325dc01
P6 598 605 255	bd0fd461d87fba0d5e61bed6a399acdfc92b12769f9b3178f9752e30f1aeb81d
P6 465 464 255	372df01b994c2b14969592fd2e78d27e7ee472a07c7ac3dfdf41d345b2f8e305

Next, you need to understand which file corresponds to which header. Matching file headers:

UTF-8	File
P6 512 512 255	File 1
P6 598 605 255	File 2
P6 585 577 255	File 3
P6 525 489 255	File 4
P6 400 433 255	File 5
P6 513 613 255	File 6
P6 465 464 255	File 7
P6 559 530 255	File 8

Since encryption is performed using a block cipher in ECB mode, we expect that the pattern will retain its outlines or some artifacts even after encryption. If this header does not belong to this file, then viewing such a file will either be completely impossible or display noise.

If the header is chosen correctly, then even without decrypting the files you will be able to see the message:

We received a large number of solutions to this problem. In the first round, 96 solutions were received and between them there are 26 solutions with maximum score. A lot of participants completed the first step of the task, i. e. determining the correct headers for the files. In the second round, 78 responses were received and 39 of them deserved the maximum score.

Solution 6086 used the ElectronicColoringBook tool which automatically selects file headers according to their size. After running it with -p3 (regular 24-bit coloring) option (and adjusting -x a bit, -1 to +3 to the automatic value), we get the following set of images:

While checking one of the works (team of Dominic-Eduard Roca and Blajut Cristin-Marian, Romania), we received the following message: «Doing that, we were able to open the images and get the message: *HEART* LOVEYOU where *HEART* is just the first image containing a heart symbol. We love NSUCrypto too».

4.9. Problem "An aggregated signature"

Formulation

Problem for a special prize!

Suppose that a big international organization, say **NSUCRYPTO association**, decided to organize its own news journal in the area of cryptography. The organization wants to publish only news that are verified by a large group of cryptographers. For this goal 10 000 leading experts in cryptography were invited to join the editorial board of the journal.

The following publishing politics was accepted. The news can be published if and only if it is signed by all members of the editorial board. But cryptographers do not want to use 10 000 individual signatures. Since they are cryptographers, they think about the aggregated postquantum signature that can not be divided into separate individual signatures.

So, **NSUCRYPTO association** kindly asks you to propose such a signature scheme. There are several requirements for it:

* the size of the signature should be not big. It can be about several kilobytes;

* the size of the public key (for checking the signature) should be small. It is desired that the key size will be constant (or close to constant) even if the number of experts is increased, say up to 20 000;

* signature verification should not take more than 2 minutes;

* the signature should be resistant to attacks that use quantum computers.

Solution

Unfortunately, there were no significant advances in solving this problem among participants.

A number of proposed solutions are just references to the existing solutions. E. g.,

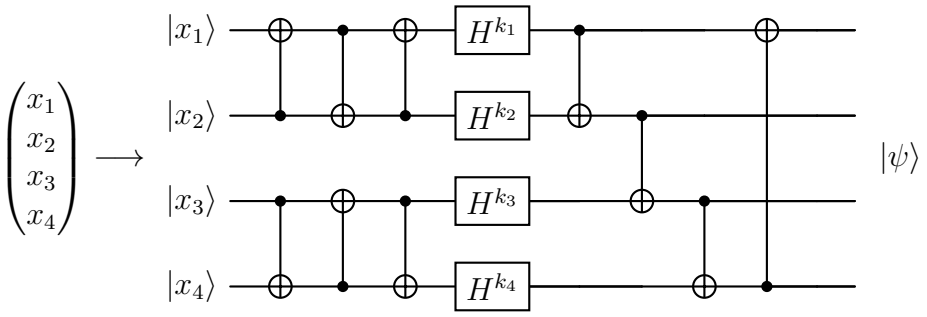
- an aggregated signature that is not postquantum-safe, but widely used and based on BLS signature [2];
- a postquantum-safe signature based on zero knowledge proofs [3], [4], but it takes more time to verify it than it is prescribed in the problem condition;
- another proposition is based on postquantum-safe Falcon, in which aggregated signature is a concatenation of single signatures and its size is more than it is prescribed in the problem condition [3].

The team of Victoria Vysotskaya, Kirill Tsaregorodtsev and Anastasiia Chichaeva proposed an original solution based on the scheme of postquantum signature Kryzhovnik [5], but this solution should be analyzed in more details in relation to correctness and effectiveness. We suppose that this problem will be investigated in the future by many authors since it has a certain theoretical and practical potential.

4.10. Problem "Quantum encryption"

Formulation

Bob works in a field of quantum mechanics and he has some ideas how it can be applied for the encryption of secret messages. He developed a toy cipher that encrypts 4-bit words by using 4-bit secret key (k_1, k_2, k_3, k_4) and the following quantum circuit:



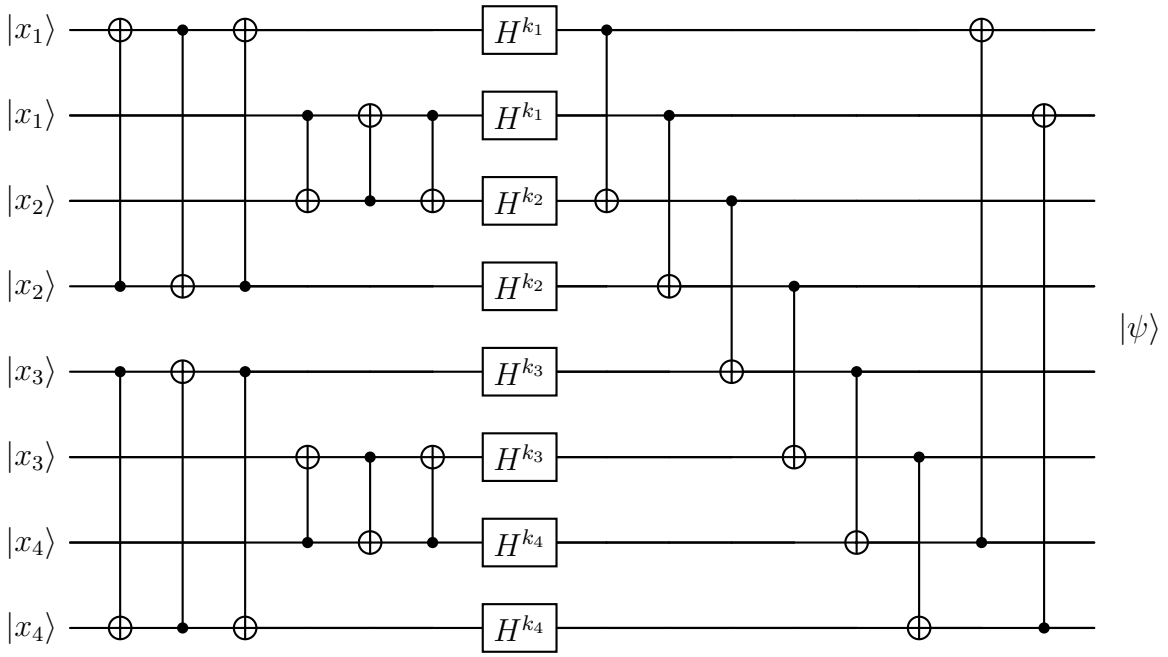
This cipher operates with 4-bit plaintext (x_1, x_2, x_3, x_4) that is initially encoded to the corresponding 4-qubit «plainstate» $|x_1, x_2, x_3, x_4\rangle$. This quantum state is an input of the circuit that consists of several single-qubit gates. Note that any quantum gate is a unitary operator that acts on the space of the states of the corresponding quantum system. The used gates are

Hadamard gate	$\|x\rangle$ — H — $\frac{\|0\rangle+(-1)^x\|1\rangle}{\sqrt{2}}$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
CNOT gate	$\|x\rangle$ — $\|x\rangle$ $\|y\rangle$ — $\|y \oplus x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0,1\}$

The notation H^b, where $b \in \{0,1\}$, means that if $b = 0$, the identity gate I is applied instead of H, while for $b = 1$ the gate H is considered.

The result of the encryption is the «cipherstate» $|\psi\rangle$ that is further transmitted via the quantum channel. The decryption procedure takes the state $|\psi\rangle$ and applies the inverse circuit.

Bob was advised to increase the number of qubits in order to reduce the effect of possible errors in quantum computation and quantum channel, so he decided to modify the circuit and make copies of qubits of the plainstate. The resulting circuit is the following:



Alice looked at the cipher and claimed that she would be able to reveal the secret key $\left(k_1, k_2, k_3, k_4\right)$ if she knew some number N of certain amplitudes of the state $|\psi\rangle$. The state $|\psi\rangle$ is characterized by 256 amplitudes, so essentially we have $N \leqslant 256$.

Could you check the assumption of Alice and find the least possible value of N if the claim is correct?

Remark. Let us briefly formulate the key points of quantum circuits. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis quantum states $|0\rangle$ and $|1\rangle$. The superposition is written as $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, where α_0 and α_1 are complex numbers, called amplitudes, that possess $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit which has the state $|\psi\rangle$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$.

In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \to |x\rangle \otimes |y\rangle$ on $x, y \in \{0, 1\}$ which is defined on pairs $|x\rangle, |y\rangle$, and by bilinearity is expanded on the space of all linear combinations of $|0\rangle$ and $|1\rangle$. When we have two qubits in states $|\psi\rangle$ and $|\varphi\rangle$ correspondingly, the state of the whole system of these two qubits is $|\psi\rangle \otimes |\varphi\rangle$. In general, for two qubits we have $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01} |0\rangle \otimes |1\rangle + \alpha_{10} |1\rangle \otimes |0\rangle + \alpha_{11} |1\rangle \otimes |1\rangle$. The physical meaning of complex numbers α_{ij} is the same as for one qubit, so we have the essential restriction $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. By induction, this process is expanded on the case of three qubits and more. Thus, the general form of the state of n qubits is

$$|\psi\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x |x\rangle,$$

where amplitudes $\alpha_{00\ldots0}, \alpha_{00\ldots01}, \ldots, \alpha_{11\ldots1}$ have the same physical meaning as discussed before. Here we use more brief notation $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle \equiv |x_1, x_2, \ldots, x_n\rangle \equiv |x_1 x_2 \ldots x_n\rangle$.

Solution

One can notice that CNOT-gates, applied in total after the row of Hadamard gates, define a particular permutation of amplitudes of the computational basis states in the «cipherstate» that is the spectrum is preserved. The gates applied before Hadamard gates define just swapping of corresponding qubits from the «plainstate».

Thus, after applying appropriate permutations to basis states of both «plainstate» and «cipherstate», the problem is reduced to the analysis of the action of the row of Hadamard gates only. Consider it in more details: for $x, k \in \mathbb{F}_2$ we have

$$|x\rangle \text{ —— } \boxed{H^k} \text{ —— } a\,|0\rangle + b\,|1\rangle,$$

where

$$a = a(x,k) = \frac{k}{\sqrt{2}} + (1-x)(1-k),$$
$$b = b(x,k) = \frac{(-1)^x k}{\sqrt{2}} + x(1-k).$$

Then for a group of 2 qubits in identical basis states we have

$$\begin{array}{l} |x\rangle \text{ —— } \boxed{H^k} \text{ ——} \\ \\ |x\rangle \text{ —— } \boxed{H^k} \text{ ——} \end{array} \quad a^2\,|00\rangle + ab(|01\rangle + |10\rangle) + b^2\,|11\rangle$$

with

$$a^2 = \frac{k^2}{2} + (1-x)^2(1-k)^2,$$
$$b^2 = \frac{k^2}{2} + x^2(1-k)^2,$$

from which it is clear that $k = 1$ if and only if $a^2 = b^2 = 1/2$.

After 4 blocks of Hadamard gates (within every block the value of k_i is common) have been applied to the state $|y_1, y_1, y_2, y_2, y_3, y_3, y_4, y_4\rangle$, it is enough to reveal 16 amplitudes of the form $X_1X_2X_3X_4$ with $X_i \in \{a_i^2, b_i^2\}$, $i = 1, 2, 3, 4$, only. It follows from the observation mentioned above and the property $a_i^2 + b_i^2 = 1$ that the key will be defined exactly.

There was a number of correct solutions with different approaches to analysis with at most 16 revealed amplitudes, in particular, of team of Aloysius Ng Yangyi, Xu Chen Tan, David Toh (USA); team of Xuefeng Xu, Jiafu Liu, Renzhang Liu (China); team of Thang Trinh Cao, Nhat Dang, Pham Minh (Vietnam) and Himanshu Sheoran (India).

4.11. Problem "Simple ideas for primes"

Formulation

Problem for a special prize!

It is well known that prime numbers form a very special and mysterious class. They have too many applications in public-key cryptography (and not only there).

During many years (to be precise, hundreds of years) mathematicians think about simple constructions for prime numbers. Let us consider particular examples in this area.

- *Fermat numbers*, $F_k = 2^{2^k} + 1$, where integer k starts from 0, give us five prime numbers: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. However, the next number, $F_5 = 4\,284\,967\,297 = 641 \cdot 6\,700\,417$, is composite as was proven latter. So far no more prime Fermat numbers were found.
- Several *Mersenne numbers*, $M_k = 2^k - 1$, are prime. For example, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, while M_{11} is already composite. Here we consider Mersenne numbers

with k being prime, since it is a necessary condition for M_k to be prime. Up to now there are known 51 prime Mersenne numbers. The last one found prime Mersenne number is $M_{82\,589\,933}$; it was obtained in 2018 and up to now it is the biggest known prime number.

• From time to time, some original ideas appear. For instance, seven consecutive (by construction) numbers 31, 331, 3 331, 33 331, 333 331, 3 333 331 and 33 333 331 are prime! But the next number 333 333 331 is composite, since it can be divided by 17.

Let us say that Fermat prime numbers have the *sequence primality parameter* equal to 5, Mersenne prime numbers have it equal to 4, while for the last construction this parameter equals 7. So, the sequence primality parameter stands for the length of the longest subsequence of prime numbers in the sequence of numbers constructed.

Solution

Participants proposed distinct approaches to get new sequences with big SPP (sequence primality parameter). For sure there were many proposals containing the known sequence $n^2 + n + 41$ with SPP = 40. As interesting it is possible to mention also

$6n^2 - 6n + 31$ (SPP=29)

$5n^2 + 5n + 1$ (SPP=9)

$5n^2 + 5n + 13$ (SPP=12)

$1/4|n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316|$ (SPP=57; references to results of Dress and Landreau, 2002, and Gupta, 2006).

$[A^{3^n}]$ for the special Mill's constant (SPP=11)

Some participants analyzed the deep mathematical background for the problem. The others gave Willans formula for primes (1964) but without detailed analysis of it in relation to our problem.

4.12. Problem "Column functions"

Formulation

Problem for a special prize!

Alice wants to construct a super strong symmetric cipher. On this way she solves some hard mathematical problems.

Consider 2^n pairwise distinct vectorial one-to-one functions, $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $i = 1, \ldots, 2^n$. Applying these functions we construct a special binary matrix and then try to determine some its properties.

For $n = 2^m$, $m \geqslant 5$, define a binary matrix M of size $2^n \times n2^n$ as follows. The i-th row, $i = 1, \ldots, 2^n$, is a concatenation of values $G_i(0, 0, \ldots, 0, 0)$, $G_i(0, 0, \ldots, 0, 1)$, …, $G_i(1, 1, \ldots, 1, 1)$. The columns of the matrix M can be interpreted as vectors of values of $n2^n$ Boolean functions in n variables. We call them *column functions*.

Prove or disprove the following **conjecture** for at least one $m \geqslant 5$: for any matrix formed in the way described above there exist $2^{n/2}$ column functions $f_1, \ldots, f_{2^{n/2}}$ such that there is a nonzero Boolean function $f : \mathbb{F}_2^{2^{n/2}} \to \mathbb{F}_2$ satisfying the following conditions:

— for every $x \in \mathbb{F}_2^n$

$$f(f_1(x), f_2(x), \ldots, f_{2^{n/2}}(x)) = 0;$$

— for every $y \in \mathbb{F}_2^{2^{n/2}}$ the value $f(y)$ can be calculated using not more than $2^{n/2}$ addition and multiplication operations modulo 2.

Example. Let $m = 1$, then $n = 2$ and we construct matrix of size 4×8. Consider one-to-one vectorial Boolean functions G_1, G_2, G_3, G_4 from $\mathbb{F}_2^2$ to $\mathbb{F}_2^2$ defined by their vectors of values

$(0,1,2,3)$, $(0,2,1,3)$, $(0,3,1,2)$ and $(3,2,1,0)$ respectively. Then the resulting matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

We need to find $2^{n/2} = 2$ column functions. Let f_1 and f_2 be defined as the first and the second columns of the matrix respectively, and $f(x_1, x_2) = x_1 \oplus x_2$ with the addition modulo 2. Then, $f(f_1(x), f_2(x)) \equiv 0$ since $f_1(x) = f_2(x)$ for any $x \in \mathbb{F}_2^n$.

Also, let f_1 and f_2 be the fifth and the sixth columns of the matrix. Then, giving $f(x_1, x_2) = x_1 x_2$ with the multiplication modulo 2, we obtain $f(f_1(x), f_2(x)) \equiv 0$ since $f_1(x) \neq f_2(x)$ for any $x \in \mathbb{F}_2^n$.

In the both cases the functions f can be calculated using only one operation. Note that the existence of such f implies that f_1 and f_2 are *algebraically dependent*.

Solution

We provide one of the shortest solutions proposed by Robin Jadoul, Jack Pope and Esrever Yievs (Belgium).

Theorem. Let M be a binary matrix of size $2^n \times n \cdot 2^n$. Then for any $n+1$ column functions there is a non-zero function $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$ vanishing on those column functions and using at most $2n+1$ addition and multiplication operations.

Proof. Let $f_1, \ldots, f_{n+1}$ be the column functions. Let

$$S = \{(f_1(x), f_2(x), \ldots, f_{n+1}(x)) \ : \ x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+1}$$

be the set of tuples formed by the column functions. Since $|S| < |\mathbb{F}_2^{n+1}|$, we can pick $z = (z_1, \ldots, z_{n+1}) \in \mathbb{F}_2^{n+1} \setminus S$. Now we define f as

$$f(x_1, \ldots, x_{n+1}) = (x_1 \oplus (z_1 \oplus 1)) \cdot (x_2 \oplus (z_2 \oplus 1)) \cdot \ldots \cdot (x_{n+1} \oplus (z_{n+1} \oplus 1)).$$

It is clear that $f(y) = 1$, where $y \in \mathbb{F}_2^{n+1}$ if and only if $y = z$. Thus, $f(y) = 0$ for any $y \in S$.

Let us calculate the number of operations. The values $z_1 \oplus 1, \ldots, z_{n+1} \oplus 1$ are some known constants at the stage of calculating f. Depending on the value of z, there are at most $n+1$ additions and exactly n multplications. Hence, the total number of operations is at most $2n+1$. ■

Corollary. The conjecture is true for $m \geqslant 4$.

Proof. We just need to bound the number of column functions and the number of operations for f provided by the theorem. For the number of column functions, the bound is $n+1 \leqslant 2^{\frac{n}{2}}$. For the number of operations, the bound is $2n+1 \leqslant 2^{\frac{n}{2}}$. Both of them are satisfied for $n \geqslant 9$. Hence, the bounds are satisfied for $m \geqslant 4$. ■

The problem was solved by the following teams: Robin Jadoul, Jack Pope and Esrever Yievs (Belgium), Sergey Makogon, Semyon Kochetkov, Kirill Tretyakov (Russia), Bach Pham Cong (Vietnam), Mikhail Kudinov, Denis Nabokov, Alexey Zelenetskiy (Sweden & Russia), Victoria Vysotskaya, Kirill Tsaregorodtsev, Anastasiia Chichaeva (Russia), Xuefeng Xu, Jiafu Liu, Renzhang Liu (China), Rinchin Zapanov, Alexander Bakharev, Sergei Zinchenko (Russia).

4.13. Problem "A unique decoding"

Formulation

Problem for a special prize!

Consider a binary error-correcting code C of length n. Recall that it is just a subset of $\mathbb{F}_2^n$ and we transmit only elements of C over a noisy communication channel. Sending $x \in C$, some bits of x can be inverted in the channel. Getting $y \in \mathbb{F}_2^n$, a receiver decodes it into the nearest by Hamming metrics element of C. The Hamming weight $wt(x \oplus y)$ of $x \oplus y$ which is equal to the number of ones in $x \oplus y$ is the exact number of errors. Here $\oplus$ states for XORing. Error-correcting codes are of great interest in communication theory and post-quantum cryptography.

Consider the principle of the maximum-likelihood decoding. Obtaining some $y \in \mathbb{F}_2^n$, we suppose that the number of errors happened, say d_y, is minimal possible, i.e.

$$d_y = \min_{x \in C} wt(x \oplus y).$$

Next, let $\mathcal{D}(y) = \{x \in C : wt(x \oplus y) = d_y\}$. Finally, we decode y into any $x \in \mathcal{D}(y)$.

We are interested in all cases of codes for which $|\mathcal{D}(y)| = 1$ for all $y \in \mathbb{F}_2^n$. In other words for such code every binary vector $y \in \mathbb{F}_2^n$ can be decoded in the unique way.

Q1 What codes C can provide this property?

Q2 What codes C that are linear subspaces of $\mathbb{F}_2^n$ can provide this property?

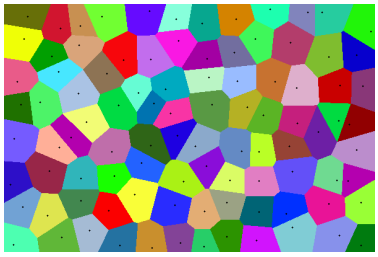
Remarks.

1) An example. There are so-called perfect codes C that allow to divide $\mathbb{F}_2^n$ into non-intersecting balls $B_r(x) = \{y \in \mathbb{F}_2^n : wt(x \oplus y) \leqslant r\}$ of some radius r centered in all $x \in C$. In other words, C is *perfect* if for some r it holds

$$\bigcup_{x \in C} B_r(x) = \mathbb{F}_2^n \text{ and } B_r(x) \cap B_r(x') = \varnothing \text{ for } x \neq x', \text{ where } x, x' \in C.$$

It is not difficult to see that any such code provides $|\mathcal{D}(y)| = 1$ for all $y \in \mathbb{F}_2^n$. But what else?

2) Some notions related to *Voronoi diagrams* can be helpful, see general mathematical definitions at `https://en.wikipedia.org/wiki/Voronoi_diagram`. In our problem we are looking for codes with non-intersecting discrete Voronoi cells for all $x \in C$.



Solution

Several teams proposed some interesting ideas. First of all, many of them found out that parameter

$$\delta(x) = \min_{y \in C, y \neq x} wt(x \oplus y)$$

should be odd for any $x \in C$ if C is unique decodable. Unfortunately, this condition is not sufficient. In addition, if $wt(x \oplus y)$ is odd for any $x, y \in C$, $x \neq y$, then the code has a unique decoding. However, this is true only if $|C| \leqslant 2$ since the perimeter of any triangle is even. Thus, the first construction is

1. $C = \{x, y\}$, where $x, y \in \mathbb{F}_2^n$ and $wt(x \oplus y)$ is odd.

Also, faces satisfy this property. They are the sets of the following form:

2. $\Gamma^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} = \{x \in \mathbb{F}_2^n : x_{i_1} = a_1, \ldots, x_{i_k} = a_k\}$, where $0 \leqslant k \leqslant n$, $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$ and $a_1, \ldots, a_k \in \mathbb{F}_2$. This construction includes trivial $C = \mathbb{F}_2^n$ and $|C| = 1$.

Note that these constructions provide the codes of the form $C = a \oplus U$, where $a \in \mathbb{F}_2^n$ and $U \subseteq \mathbb{F}_2^n$ is linear. Hence, C is a linear code if and only if $0 \in C$. Among $2^{n-1}(2^n - 1)$ codes of the first type and 3^n codes of the second type, there are $2^n - 1$ and 2^n linear codes.

The third construction is the direct product of codes.

3. Let C_1 and C_2 be unique decodable. Then $C_1 \times C_2 = \{(x, y) : x \in C_1, y \in C_2\}$ is unique decodable as well.

It is clear that $C_1 \times C_2$ is linear if and only if both C_1 and C_2 are linear codes. It is also clear that any isometric mapping preserves the property.

4. Let $C \subseteq \mathbb{F}_2^n$ be unique decodable. Then $\pi(C) \oplus a = \{\pi(x) \oplus a : x \in C\}$, where $a \in \mathbb{F}_2^n$ and π permutes the coordinates $x_1, \ldots, x_n$ of x.

The most interesting conjecture related to the constructions 3 and 4 was proposed by Robin Jadoul, Jack Pope and Esrever Yievs (Belgium).

Conjecture. Any unique decodable code can be defined recursively:

— Any perfect code is unique decodable.
— The direct product of two unique decodable codes is unique decodable, see construction 3.
— A permutation $\pi(C)$ of a unique decodable C is unique decodable, see construction 4.

The team proposed some idea that would be a base of its proof (but not a complete proof). Note that the conjecture is satisfied for all considered examples of unique decodable codes.

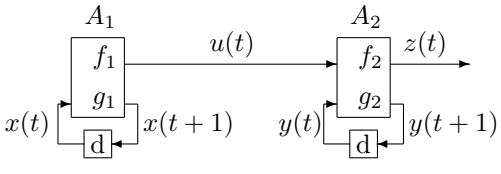
4.14. Problem "Finite-state machines"

Formulation

Problem for a special prize!

Alice decided to invent some generator that produces a sequence of maximal possible period relatively to its state size. Since she knows about finite-state machine, her generator G is constructed using two such machines A_1 and A_2:

— $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ with the state-transition function $g_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and the output function $f_1 : \mathbb{F}_2^n \to \mathbb{F}_2$, $n \geqslant 1$;
— $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$ with the state-transition function $g_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ and the output function $f_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2$, $m \geqslant 1$.



For any $t = 1, 2, \ldots$, let

1) $x(t)$ and $y(t)$ be the states of A_1 and A_2 respectively, $x(1)$ and $y(1)$ be the initial states;
2) $x(t+1) = g_1(x(t))$ be the next state of A_1 and $u(t) = f_1(x(t))$ be the output bit of A_1;
3) $y(t+1) = g_2(u(t), y(t))$ be the next state of A_2 and $z(t) = f_2(u(t), y(t))$ be the output bit of A_2.

The sequence $z(1), z(2), z(3), \ldots$ is the output of the generator G. It is not difficult to see that it is eventually periodic whose the smallest period does not exceed 2^{n+m}.

Due to experiments, Alice noticed that the least period of the output sequence of G is less than 2^{n+m} if the Hamming weight of f_1 is even. Help Alice to prove or disprove this conjecture.

Remark. Recall that the Hamming weight of a Boolean function is the number of arguments on which it takes the value one.

Solution

By contradiction: we assume that the least period of G is 2^{m+n}. Then the least period of $u(t)$ is 2^n. Indeed, for some $t_1 \geqslant 2^n$ (to be inside the cycle) there exists $t_2 = t_1 + t \cdot i$, where t is the least period of $u(t)$ and $i \in \{1, \ldots, 2^m\}$, such that

$$(u(t_1), y(t_1)) = (u(t_2), y(t_2)),$$

i. e. the least period of $z(t)$ does not exceed $t \cdot 2^m$.

Thus, $\{x(t), t = 1, \ldots, 2^n\} = \mathbb{F}_2^n$ and the Hamming weight $\mathrm{wt}(f_1)$ is the number of 1's in the cycle $u(1), \ldots, u(2^n)$. Let us introduce

$$g_2^0 : y \mapsto g_2(0, y) \text{ and } g_2^1 : y \mapsto g_2(1, y), y \in \mathbb{F}_2^m.$$

If the least period of $z(t)$ is 2^{m+n}, then

$$\begin{array}{ccccccc}
x(0 \cdot 2^n + 1), y(0 \cdot 2^n + 1) & \to & \ldots & \to & x(1 \cdot 2^n), y(1 \cdot 2^n) & \to \\
x(1 \cdot 2^n + 1), y(1 \cdot 2^n + 1) & \to & \ldots & \to & x(2 \cdot 2^n), y(2 \cdot 2^n) & \to \\
 & & \ldots & & & \\
x((2^m - 1) \cdot 2^n + 1), y(2^m - 1) \cdot 2^n + 1) & \to & \ldots & \to & x(2^m \cdot 2^n), y(2^m \cdot 2^n) &
\end{array}$$

must be all 2^{n+m} distinct values of $\mathbb{F}_2^{n+m}$. Hence, all of $y(1), y(2^n+1), \ldots, y((2^m-1)\cdot 2^n+1)$ are different since $x(1) = x(2^n + 1) = \ldots = x((2^m - 1) \cdot 2^n + 1)$. Thus, the transformation $g : y(i \cdot 2^n + 1) \mapsto y((i + 1) \cdot 2^n + 1)$, where i is any nonnegative integer, that is equal to

$$g_2^{u(i \cdot 2^n + 1)} \circ \ldots \circ g_2^{u(i \cdot 2^n + 2^n)} = g_2^{u(1)} \circ \ldots \circ g_2^{u(2^n)},$$

is a full-cycle permutation. Since the cycle length is 2^m, its sign is negative, i.e. $\mathrm{sign}(g) = -1$. But

$$\mathrm{sign}(g) = \mathrm{sign}(g_2^{u(1)}) \cdot \ldots \cdot \mathrm{sign}(g_2^{u(2^n)}) = \mathrm{sign}(g_2^0)^{2^n - \mathrm{wt}(f_1)} \cdot \mathrm{sign}(g_2^1)^{\mathrm{wt}(f_1)} = 1,$$

since $\mathrm{wt}(f_1)$ is even. This is a contradiction. The solution is completed.

The problem was solved by the following teams: Sergey Makogon, Semyon Kochetkov, Kirill Tretyakov (Russia), Kristina Geut, Sergey Titov, Dmitry Ananichev (Russia), Aloysius Ng Yangyi, Xu Chen Tan, David Toh (USA), Victoria Vysotskaya, Kirill Tsaregorodtsev, Anastasiia Chichaeva (Russia), Xuefeng Xu, Jiafu Liu, Renzhang Liu (China), Mikhail Kudinov, Denis Nabokov, Alexey Zelenetskiy (Sweden & Russia). Note that the team of Rinchin Zapanov, Alexander Bakharev, Sergei Zinchenko (Russia) showed even more: they proved that for any f_1 of odd weight there exist g_1, g_2 and f_2 such that the least period of $z(t)$ is 2^{n+m}.

5. Acknowledgement

The authors are very grateful to I. Khilchuk, V. Kochetkova, D. Gerasimov, Yu. Maksimlyuk for their helpful ideas, comments and proposals.

REFERENCES

1. Biere A., Järvisalo M., Kiesl B. Preprocessing in SAT Solving. In Handbook of Satisfiability - Second Edition. IOS Press. 2021. pp. 391–435.
2. Boneh D., Gentry C., Shacham H., and Lynn B. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. // In proceedings of Eurocrypt 2003, LNCS 2656, pp. 416-432, 2003. `https://crypto.stanford.edu/ dabo/pubs/abstracts/aggreg.html`
3. Khaburzaniya I., Chalkias K., Lewi K., Malvai H. Aggregating and thresholdizing hash-based signatures using STARKs. // Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security.
4. Hsiang J.H., Fu S., Kuo P.C., Cheng C.M. PQScale: A post-quantum signature aggregation algorithm // 2023, `https://btq.com/blog/introducing-pqscale-a-scaling-solution-for-post-quantum-signatures`.
5. Kirshanova E. A., Kolesnikov N. S., Malygina E. S., Novoselov S. A. Project of standartization of postquantum digital signature // Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics). Supplemet. 2020, N 13, 44-–51. SibeCrypt'20. (in Russian)
6. *Agievich S., Gorodilova A., Idrisova V., Kolomeec N., Shushuev G., Tokareva N.* Mathematical problems of the second international student's Olympiad in cryptography, Cryptologia, **41**:6 (2017), 534–565.
7. *Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V.* Problems, solutions and experience of the first international student's Olympiad in cryptography, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 3 (2015), 41–62.
8. *Anatoly S., Emil F, Olha L.* Three-Pass Cryptographic Protocol Based on Permutations, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 281-284, doi: 10.1109/ATIT50783.2020.9349343.
9. *Ayat S. M., Ghahramani M.* A recursive algorithm for solving "a secret sharing" problem", Cryptologia, **43**:6 (2019), 497–503.
10. *Geut K., Kirienko K., Sadkov P., Taskin R., Titov S.* On explicit constructions for solving the problem "A secret sharing", Prikladnaya Diskretnaya Matematika. Prilozhenie, 10 (2017), 68–70 (in Russian).
11. *Geut K. L., Titov S. S.* On the blocking of two-dimensional affine varieties, Prikladnaya Diskretnaya Matematika. Prilozhenie, 12 (2019), 7–10 (in Russian).
12. *Gorodilova A., Agievich S., Carlet C., Gorkunov E., Idrisova V., Kolomeec N., Kutsenko A., Nikova S., Oblaukhov A., Picek S., Preneel B., Rijmen V., Tokareva N.* Problems and solutions of the Fourth International Students' Olympiad in Cryptography (NSUCRYPTO), Cryptologia, **43**:2 (2019), 138–174.
13. *Gorodilova A., Agievich S., Carlet C., Hou X., Idrisova V., Kolomeec N., Kutsenko A., Mariot L., Oblaukhov A., Picek S., Preneel B., Rosie R., Tokareva N.* The Fifth International Students' Olympiad in Cryptography — NSUCRYPTO: problems and their solutions, Cryptologia, **44**:3 (2020), 223–256.
14. *Gorodilova A., Tokareva N., Agievich S., Carlet C., Gorkunov E., Idrisova V., Kolomeec N., Kutsenko A., Lebedev R., Nikova S., Oblaukhov A., Pankratova I., Pudovkina M., Rijmen V., Udovenko A.* On the Sixth International Olympiad in Cryptography NSUCRYPTO, Journal of Applied and Industrial Mathematics, **14**:4 (2020), 623–647.
15. *Gorodilova A. A., Tokareva N. N., Agievich S. V., Carlet C., Idrisova V. A., Kalgin K. V., Kolegov D. N., Kutsenko A. V., Mouha N., Pudovkina M. A., Udovenko A. N.* The Seventh International Olympiad in Cryptography: problems and solutions, Siberian Electronic Mathematical Reports, **18**:2 (2021), A4–A29.

16. *Gorodilova A. A., Tokareva N. N., Agievich S. V., Beterov I.I., Beyne T., Budaghyan L., Carlet, C., Dhooghe S., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Malygina E.S., Mouha N., Pudovkina M.A., Sica F., Udovenko A.N.* An overview of the Eight International Olympiad in Cryptography "Non-Stop University CRYPTO", Siberian Electronic Mathematical Reports, **19**:1 (2022), A9–A37.
17. *Idrisova V.A., Tokareva N.N., A. A. Gorodilova, I. I. Beterov, T. A. Bonich, E. A. Ishchukova, N. A. Kolomeec, A. V. Kutsenko, E. S. Malygina, I. A. Pankratova, M. A. Pudovkina, A. N. Udovenko* // Mathematical problems and solutions of the Ninth International Olympiad in cryptography NSUCRYPTO // Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics). 2023, No. 4, P. 29-54.
18. *Kapalova N., Dyusenbayev. D., Sakan K.* A new hashing algorithm - HAS01: development, cryptographic properties and inclusion in graduate studies, Global Journal of Engineering Education, **24**:2 (2022), 155–164.
19. *Kiss R., Nagy G. P.* On the nonexistence of certain orthogonal arrays of strength four, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 52 (2021), 65–68.
20. *Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography, Prikladnaya Diskretnaya Matematika (Applied Discrete Mathematics), 40 (2018), 34–58.
21. `https://algassert.com/quirk`
22. `https://nsucrypto.nsu.ru/`
23. `https://nsucrypto.nsu.ru/outline/`
24. `https://nsucrypto.nsu.ru/archive/2021/total_results/#data`
25. `https://nsucrypto.nsu.ru/unsolved-problems/`
26. `https://nsucrypto.nsu.ru/media/MediaFile/data_round2.txt`
27. `https://nsucrypto.nsu.ru/media/MediaFile/test_vector.txt`
28. `https://nsucrypto.nsu.ru/media/MediaFile/test_vector2.txt`

Tokareva Natalia Nikolaevna — Ph.D, associate professor, Novosibirsk State University, Novosibirsk. E-mail: **crypto1127@mail.ru**

Zaikin Oleg Sergeevich — Ph.D, senior lecturer, Matrosov Institute for System Dynamics and Control Theory, Irkutsk, Irkutsk. E-mail: **zaikin.icc@gmail.com**

Idrisova Valeriya Aleksandrovna — Ph.D, assistant, Novosibirsk State University, Novosibirsk. E-mail: **vvitkup@yandex.ru**

Ishchukova Evgeniya Alexandrovna — Ph.D, position, Institute of Computer Technologies and Information Security, Southern Federal University, Rostov-on-Don. E-mail: **uaishukova@sfedu.ru**

Kalgin Konstantin Viktorovich — Ph.D, senior lecturer, Novosibirsk State University, Novosibirsk. E-mail: **kalginkv@gmail.com**

Kolomeec Nikolay Aleksandrovich — Ph.D, senior lecturer, Novosibirsk State University, Novosibirsk. E-mail: **kolomeec@math.nsc.ru**

Kutsenko Aleksandr Vladimirovich — Ph.D, senior lecturer, Novosibirsk State University, Novosibirsk. E-mail: **alexandrkutsenko@bk.ru**

Kyazhin Sergey Nikolaevich — CryptoPro, Moscow. E-mail: **s.kyazhin@kaf42.ru**

Malygina Ekaterina Sergeevna — Ph.D, position, Immanuel Kant Baltic Federal University, Kaliningrad. E-mail: **EMalygina@kantiana.ru**

Pankratova Irina Anatol'evna — Ph.D, position, Tomsk State University, Tomsk. E-mail: **pank@mail.tsu.ru**