



Problem 1. «An ancient civilization»



A long time ago in a galaxy far, far away, on one of the planets, during excavations, a damaged archive of an extinct civilization was found. The archive consisted of seven tablets. After carefully studying, the researchers discovered that each tablet had four lines written on it.

Line 1	Line 2	Line 3	Line 4
0	000000 ... 0000000 (64 zeros)	Lhxvsdsjachmjbby	57606456
1	lost*	aufwhssactatvcgk	4261992
2	lost	bskhvqsoanivylhh	319391
3	lost	ffamnbetiolqsuzv	4507419
4	lost	lignrdirwvwsllbbl	30068739
5	lost	ltyiqezqxofdiilp	15965222
6	lost	vnckgq	3595645

* – the inscription «lost» in a line means that the line is empty.

The archaeologists were also able to restore the inscription on the back of the first tablet: «*The past is the key to the present. The present is the key to the future. Each of the seven sectors of space contains sixty-four stars leading to the first four galaxies.*»

Trying to restore and decipher the archive, the researchers reached a dead end. Now they need your help: find the key and decipher the message of the ancient civilization.



Problem 2. «Cryptanalysis of RSA»

Let (e, n) be an RSA public key. Let M_1, M_2 be unknown messages encrypted via RSA algorithm, i. e., $M_i^e = C_i \pmod n$, for $i = 1, 2$. Here you can see the data that is known.

```
e = 478853242985154664467762146288559833356382026543431035766138282368122190
86062545569,
n = 379703284647896346753254503828009959379851606332716949320398301386171316
966425526386539378800151258587337311995631457605570369065453529230023765
319342285073463098745982365680739537576969325080998775569316149313167427
902779642495446233283994650628144477669265679070784099933877043171457174
6372170728725349558017,
C1 = 163704387214409346643528781190375904112976150163669721461061165362047040
394496554290354079052733090437858753423699103600464494362347753534265372
671255786871274286428662434604838644848585499738163720928489885303745862
212116800137226936723578245872796880460212364775577714268154970592359188
9045263588042807864761,
C2 = 355381281178772898823963559035091503412951744375682488618045656685426084
501262069008603654752644625019016885092765687446916010785494437852619471
924295879928734145229524928856184485139454562589416369897821947694348226
331319814036551968701821651230910791192048120451210023139919338291800636
7533798052415091072350.
```

Find the unknown original messages M_1 and M_2 . The message M_2 was obtained from a text string using the Python function `text_to_number()`. Decode this text using the `number_to_text()` function. The function code is provided below.

```
from binascii import hexlify, unhexlify
def text_to_number(text):
    s = text.encode()
    h = hexlify(s)
    d = int(h, 16)
    return d
def number_to_text(m):
    h2 = hex(m)[2:]
    b = unhexlify(h2)
    res = b.decode()
    return res
```

Remark. With the correct choice of a method, calculations will take less than one minute.



Problem 3. «The BSW Conjecture»

Problem for a special prize!

Notation. Let $\text{GF}(q)$ be the finite field of order q , and $\text{GF}(q)^*$ be the set of its nonzero elements. The quadratic character χ of $\text{GF}(q)$ takes the value 1 for nonzero squares, the value -1 for nonzero nonsquares, and $\chi(0) = 0$.

Conjecture 1. Let $q > 31$ be an odd prime power. Take a map ψ of $\text{GF}(q)^*$ that is an involution, pairs every square with a non-square, and satisfies

$$\chi((x - y)(x - \psi y)(\psi x - y)(\psi x - \psi y)) = -1$$

whenever $y \notin \{x, \psi x\}$. Then $\psi(x) = n/x$ for some non-square n .

The case $q \equiv 1 \pmod{4}$. Blokhuis, Seress and Wilbrink showed¹ the Conjecture for every prime power $q \equiv 1 \pmod{4}$ with $q > 31$. The case $q \equiv 3 \pmod{4}$ is open.

Geometric formulation. Work in $\text{PG}(2, q)$ with q odd, and use the conic

$$C: \quad xy = z^2.$$

Remember, that

- A *tangent* is a line meeting C in exactly one point.
- A *passant* (external line) is a line containing no point of C .
- An *exterior point* is a point off C that lies on a tangent.
- An *interior point* is a point off C that lies on no tangent.

Conjecture 2. Let $q \equiv 3 \pmod{4}$ and $q > 31$. Let S be a set of $(q + 1)/2$ exterior points of C such that every line through two distinct points of S is a passant. Then S is exactly the set of exterior points on some passant.

Note that Conjectures 1 and 2 are equivalent.

The problem. Please, prove the Conjecture 1 for an arbitrary q (general problem). Prove it for an infinite class of prime power q 's or for finitely many values of q .

¹See A. Blokhuis, Á. Seress, and H. A. Wilbrink, Characterization of complete exterior sets of conics, *Combinatorica* **12** (1992), no. 2, 143–147. DOI 10.1007/BF01204717.



Problem 4. «Secret coding»

There are 12 known vectors $a_i \in \mathbb{Z}^6$ and numbers b_i . All of them are given in the table below.

i	a_{i1}	a_{i2}	a_{i3}	a_{i4}	a_{i5}	a_{i6}	b_i
1	−5	−8	0	−1	−1	−4	−18
2	−5	−6	5	−7	−8	−6	−1
3	−2	−1	8	−8	−2	5	83
4	−1	6	0	−8	−3	5	37
5	2	0	−4	−2	2	−5	−8
6	−6	4	−5	3	3	0	−85
7	34	−8	−9	12	12	−8	156
8	30	−8	−1	16	39	2	231
9	9	5	29	−11	−9	−7	142
10	−37	−3	−58	12	−4	32	−340
11	4	−30	−12	6	35	−10	96
12	−30	22	−56	0	−42	25	−426

There exists an unknown vector

$$s = (s_1, \dots, s_6), \quad |s_j| \leq 10,$$

and unknown numbers $e_i \in \{-1, 0, 1\}$, such that for each $i = 1, \dots, 12$ it holds

$$b_i = a_i s + e_i.$$

Please find the vector s and all values of errors e_i .



Problem 5. «Grandchildren»

Three children — Asya, Vanya, and Sonya — live in one house. Interestingly, the number of the house they live in is divisible by each of the children's ages. Their grandmother lives in another house on the same street, and the number of her house is formed by writing the ages of Asya and Vanya side by side. Here is one more interesting fact: when Sonya walks from her house to her grandmother's, she passes exactly 6 times as many houses as her own age in years. And this journey takes her 25 minutes. That is exactly the amount of time it takes Vanya to complete his math homework.

The question is: how old are Asya, Vanya, and Sonya?
By the way, this is the digital key to Grandma's house.





Problem 6. «Alice in the Tweedleworld»

Tweedledum and Tweedledee lived on opposite sides of the city and were very lonely; they often sent each other letters and postcards, and wished each other happy holidays. Alice worked as a postman, and she was lonely as well, so she secretly read those postcards.



Quite recently, Tweedledum and Tweedledee started to encrypt their messages. Alice could not figure out what was written there and decided to find a way to read them. Alice asked the Cheshire Cat to turn invisible and spy on what Tweedledee was writing to Tweedledum. One day he succeeded!

Cheshire Cat said that the text written by Tweedledee was the following:

How can I prove to you that I know secret word, without ever whispering a single syllable of the word itself?

After encryption Tweedledee obtained:

H I o p k w r o v u t c a n o w h e n s a l t o t e s p c d e e , v r r w i t e r e t i n g w h w o o a h r u t i d f s y i l t t i l a b h e n g l s e l w l e f e ? o s o r

This message was delivered by Alice to Tweedledum. After some time Tweedledum answered to Tweedledee with the ciphertext:

B o d l m e e n y l y a s t h a a t k r t i i h e n g d s r n s d w k e e e c e p c r e r , f o u i t l o d n g w o a r m a s t i s y o w I k u t h a y t l o n s u o d h o w u t e ! s

Please, help Alice to read what Tweedledum wrote and explain the encryption method.

[illegible]

00000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb0000000000000000
0046a02ff01d00700000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bd0070000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbd00700000
0000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb0000000000000000046
a02ff03e80300000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa8
8acd0070000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbd007000
000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb000000000000000000
46a02ff03d0070000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbd
0070000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbd0070000000
00000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb0000000000000000046a0
2ff03e80300000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa88a
cd0070000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbe80300000
00000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa88ac0000000000000
000046a02ff03e8030000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaa88acd007000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbe
80300000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa88ace8030
000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa88ac000000000
0000000046a02ff04d007000000000000160014bbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbe80300000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa8
8ace80300000000000001976a914aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa88ac0
0000000000000000046a02ff0300000000

At the bottom of the page there was a hint:

«We say nothing as we come in, but when leaving, each of us follows
after the Return.»

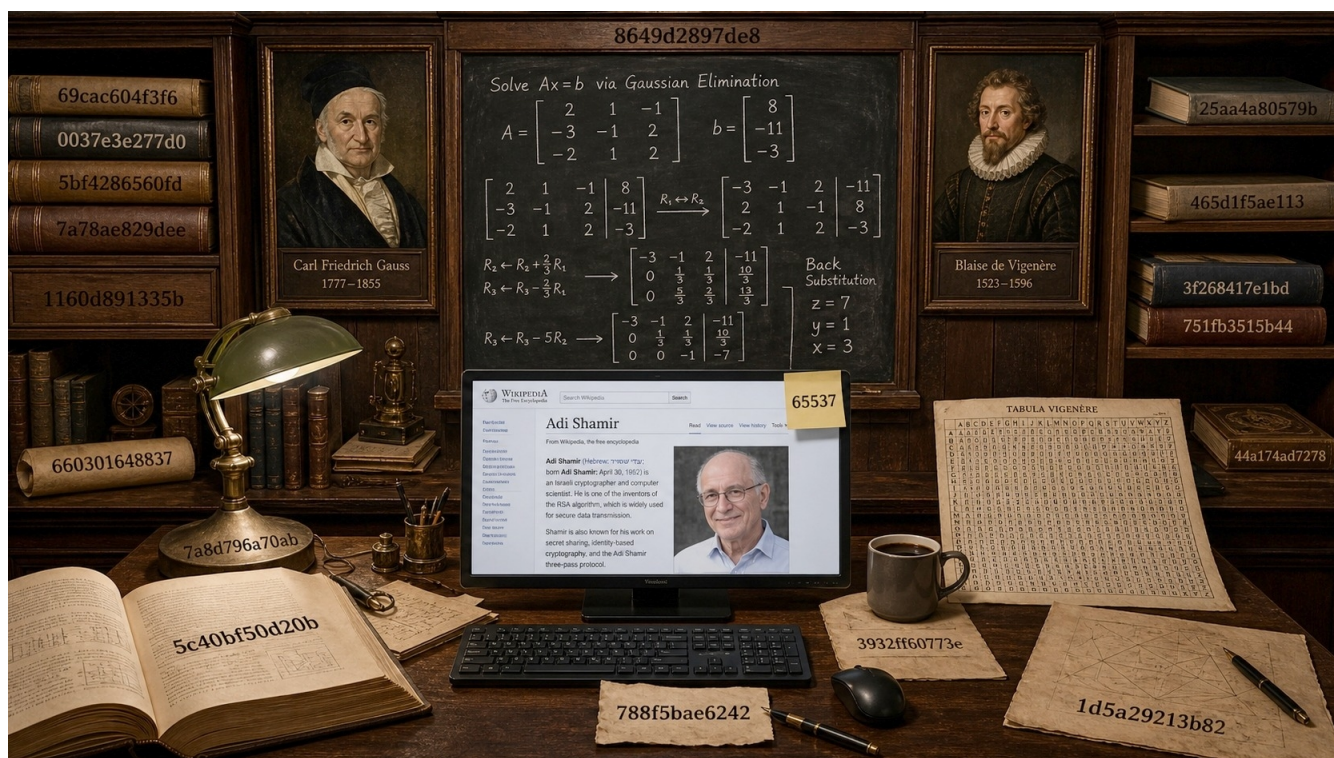
Help Sherlock Holmes to find the access code to the safe-deposit box.





Problem 8. «Crypto room»

Read the words of one of the greatest cryptographers of our time.





Problem 9. «Vector LRS»

Problem for a special prize!

Definitions. Let $R = GF(2)$, $n \in \mathbb{N}$. We call subsequence of columns $v : \mathbb{N}_0 \rightarrow R^{(n)}$ *vector linear recurrent sequence* (LRS) of order m , if there exist matrices $A_0, \dots, A_{m-1} \in R_{n,n}$, such that for all $i \in \mathbb{N}_0$ it holds

$$v(i+m) = A_{m-1}v(i+m-1) + \dots + A_1v(i+1) + A_0v(i). \quad (1)$$

If there exists $T \in \mathbb{N}$, such that $v(i+T) = v(i)$ for all $i \in \mathbb{N}_0$, then the least such T is called *the period* of the sequence v and is denoted as $T(v)$. Considering the set of m -element items $\{(v(0), \dots, v(m-1)), (v(1), \dots, v(m)), \dots\}$, it is not difficult to show that the period of a vector LRS of order m does not exceed $\tau = 2^{mn} - 1$. In the case when $T(v) = \tau$, we will call the vector LRS v of order m a *vector LRS of maximum period*.

An example. Let $n = 2$, $m = 3$,

$$A_2 = A_1 = A_0 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

and initial columns are $v(0) = v(1) = (0, 0)^T$, $v(2) = (1, 0)^T$. Then it holds $v(3) = (0, 1)^T$, $v(4) = (1, 0)^T$, $v(5) = (1, 1)^T, \dots$. It is not difficult to check that v is a vector linear recurrent sequence of the maximum period $2^6 - 1 = 63$.

The problem. Let v be such a vector LRS of maximum period $\tau = 2^{mn} - 1$ of order m with the recursion law (1), such that for all $d \in \mathbb{N}$ coprime to τ , the sequence $w(i) = v(di)$ is also a vector LRS of maximum period of order m . Is it true that $A_k A_j = A_j A_k$ for all $k, j \in \{0, m-1\}$?



Problem 10.«Bent decompositions»

Problem for a special prize!

Boolean bent functions are studied since 60-s of XX century in connection to cryptographic applications of them and their generalizations, [1].

We invite you to study the following open problem: is it true that an arbitrary Boolean function in n variables (n is even, $n \geq 2$) of degree not more than $n/2$ can be represented as the sum of two bent functions in n variables?

This question was raised in 2011 in close connection with the problem of the asymptotic value of the number of all bent functions in n variables. There is a hypothesis that the answer is «yes». For now all known facts confirm the hypothesis. The hypothesis was checked for $n = 2, 4, 6$ and for some special classes of Boolean functions.

Could you obtain new results in connection to this hypothesis?

More details. A Boolean function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ in an even number of variables n is called a *bent function* if it is at the maximum Hamming distance from the set of all affine Boolean functions in n variables. Equivalently, the Walsh–Hadamard transform of f ,

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \quad y \in \mathbb{Z}_2^n,$$

takes only the values $\pm 2^{n/2}$. The set of all bent functions in n variables is denoted by $\mathcal{B}_n$.

Hypothesis. Let n be an even positive integer. Then every Boolean function in n variables of degree at most $n/2$ can be represented as the sum of two bent functions in n variables. In other words, for every Boolean function f in n variables with $\deg f \leq n/2$, there exist bent functions $g, h \in \mathcal{B}_n$ such that $f = g \oplus h$.

The hypothesis was stated in [2] and verified by computer for $n \leq 6$ in [2; 3].

Known results.

- It is proved in [4] that every Boolean function in n variables of degree d , where $d \leq n/2$ and n is even, can be represented as the sum of a constant number of bent functions in n variables. The constant depends on d and n .
- Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions in 8 variables, see [4].
- A bent function is decomposable into the sum of two bent functions if and only if its dual bent function is also decomposable, see [5].
- It is proved in [6] that the hypothesis holds for $n \leq 6$; every quadratic Boolean function in n variables is the sum of two bent functions. It is shown that every Maiorana–MacFarland bent function and every partial spread function for an arbitrary n are also decomposable.

• It is proved in [7] that every bent function in 8 variables of degree at most 3 can be represented as the sum of two bent functions in 8 variables; every quadratic Boolean function in an even number of variables $n \geq 4$ can be represented as the sum of two bent functions of a special form.

The problem. Please, try to prove or disprove the hypothesis. You can consider some partial subclasses of Boolean functions for the investigation. Here are variations of classes:

- All Boolean functions of degree 4 in 8 variables.
- All cubic Boolean functions for all even n .
- All Boolean functions of degree $\leq n/2$ that depend essentially on at most $n/2 + c$ variables, where $c \geq 2$.
- Decomposition to sum of a constant number of bent functions, where the constant does not depend on n .

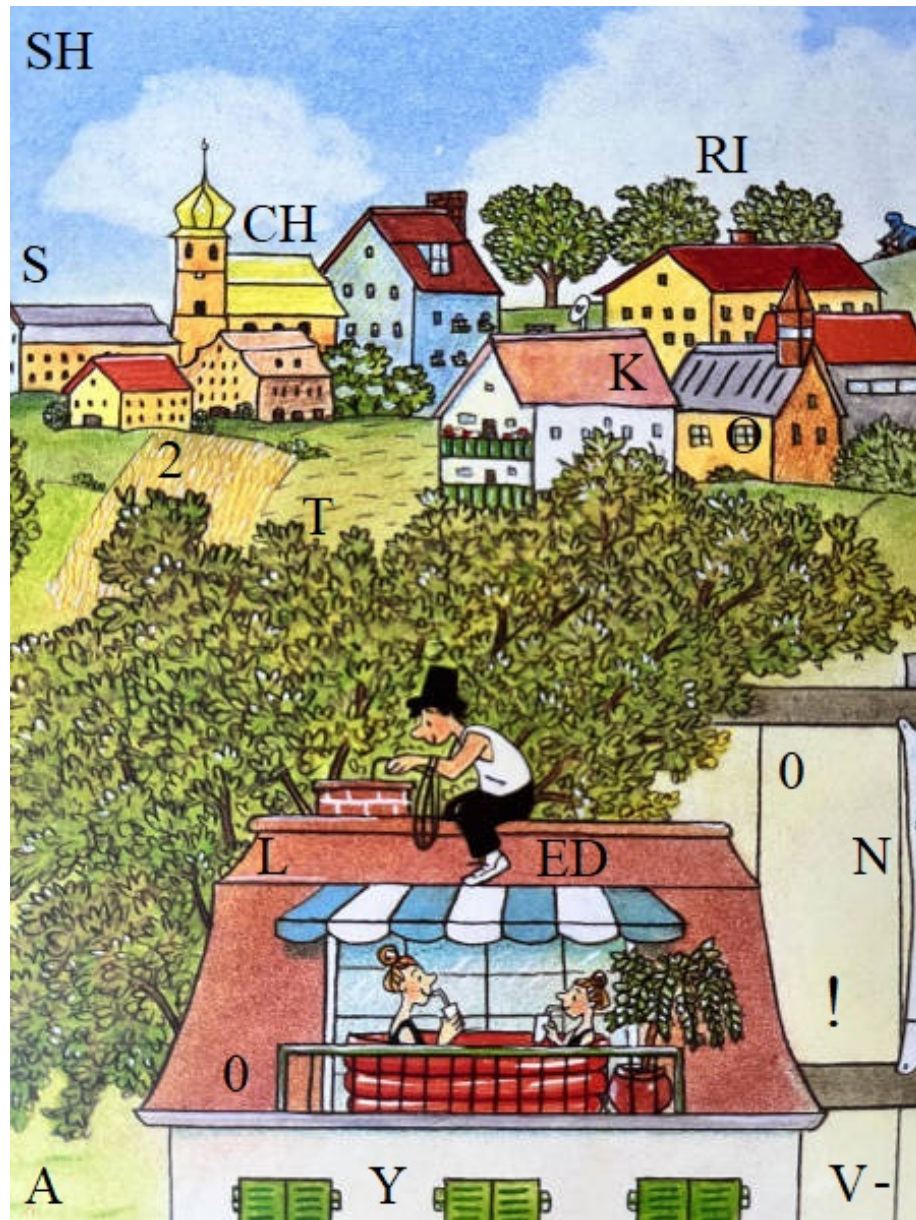
References

- [1] O. S. Rothaus. On bent functions // J. Combin. Theory Ser. A, 1976. V. 20. N 3 P. 300–305.
- [2] N. Tokareva. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Mathematics of Communications, 2011, V 5. N 4. P. 609–621.
- [3] Qu L. and Li C. New results on the Boolean functions that can be expressed as the sum of two bent functions // IEICE Trans. Fund. Elect. Commun. Comput. Sci. 2016. V. 99-A. N 8. P. 1584–1590.
- [4] N. N. Tokareva. On decomposition of a Boolean function into sum of bent functions // Siberian Electronic Mathematical Reports, 2014. V 11. P. 745–751.
- [5] N. Tokareva. Bent functions: results and applications to cryptography // Acad. Press. Elsevier, 2015. 220 pages.
- [6] L. Qu, S. Fu, Q. Dai, C. Li. When a Boolean Function can be Expressed as the Sum of two Bent Functions // IACR Cryptology ePrint Archive, Report 2014/048, 2014.
- [7] A. S. Shaporenko. Derivatives of bent functions in connection with the bent sum decomposition problem. Designs, Codes and Cryptography, 2023. V. 91. N 5. P. 1607–1625.



Problem 11. «Who is here?»

Please, read and explain the message.





Problem 12. «A quantum cipher»

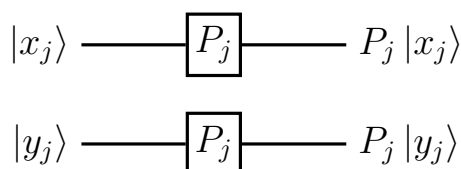
Alice invented the following quantum symmetric cipher. The plaintext is encoded into the sequence of n pairs of qubit states $|x_1\rangle|y_1\rangle, |x_2\rangle|y_2\rangle, \dots, |x_n\rangle|y_n\rangle$, where $|x_j\rangle, |y_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, $j = 1, 2, \dots, n$. Here $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are Hadamard states. The secret key k is a random vector from the set $\{0, 1, 2, 3\}^n$. On iteration j , depending on the value k_j , some Pauli gate $P_j \in \{I, X, Y, Z\}$ is chosen:

k_j	P_j
0	I
1	X
2	Y
3	Z

Note that any quantum gate is a unitary operator that acts on the space of the states of the corresponding quantum system. The used Pauli gates together with identical one are

Identity gate I	$ x\rangle \xrightarrow{I} x\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli X gate	$ x\rangle \xrightarrow{X} x \oplus 1\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli Y gate	$ x\rangle \xrightarrow{Y} i(-1)^x 1-x\rangle$	acts on a single qubit in the state $ x\rangle$
Pauli Z gate	$ x\rangle \xrightarrow{Z} (-1)^x x\rangle$	acts on a single qubit in the state $ x\rangle$

Here $x \in \{0, 1\}$. The chosen gate acts on every qubit from the corresponding pair: $|x_j\rangle \otimes |y_j\rangle \rightarrow (P_j |x_j\rangle) \otimes (P_j |y_j\rangle)$. The state $(P_j |x_j\rangle) \otimes (P_j |y_j\rangle)$ is the result of the encryption of j -th pair $|x_j\rangle|y_j\rangle$, this process can be described by the quantum circuit Q :



Assume that the same key $(k_1, k_2, \dots, k_n)$ can be used for more than one encryption. Describe in details possible vulnerabilities of the cipher that Eve could use in order to obtain information about the key or the plaintext qubit states.

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 orthonormal 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 $|\psi\rangle$ in a basis $\{|0\rangle, |1\rangle\}$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$. One can also write $|\psi\rangle = \alpha'_0|+\rangle + \alpha'_1|-\rangle$, where amplitudes α'_0, α'_1 possess the same norm condition and characterize the probabilities of observing the system in the states $|+\rangle$ and $|-\rangle$.

In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \rightarrow |x\rangle \otimes |y\rangle$ 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 unentangled (separable) 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 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. For brevity one can write $|a\rangle \otimes |b\rangle \equiv |ab\rangle$.

In fact the state can also be written in other orthonormal basis, for example one can consider four Bell states

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned}$$

or

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle), & |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle), \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle), & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle). \end{aligned}$$

Then for the state of the system of two qubits we have $|\psi\rangle = \alpha_{\Phi^+} |\Phi^+\rangle + \alpha_{\Phi^-} |\Phi^-\rangle + \alpha_{\Psi^+} |\Psi^+\rangle + \alpha_{\Psi^-} |\Psi^-\rangle$. The physical meaning of amplitudes $\alpha_{\Phi^+}, \alpha_{\Phi^-}, \alpha_{\Psi^+}, \alpha_{\Psi^-}$ is the same as before.