УДК 004.056.55

М.О. ПОЛУЯНЕНКО, О.В. ПОТІЙ, д-р техн. наук

ДОСЛІДЖЕННЯ РЕГІСТРІВ ЗСУВУ З НЕЛІНІЙНИМИ ЗВОРОТНИМИ ЗВ'ЯЗКАМИ В ЯКОСТІ КОМБІНУЮЧИХ ТА ФІЛЬТРУЮЧИХ ФУНКЦІЙ

Вступ

Розглянемо загальну структуру схему комбінуючого генератора (рис. 1, *а*) та фільтруючого генератора (рис. 1, *б*) ПВП із застосуванням декількох регістрів зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) або регістрів зсуву з нелінійними зворотними зв'язками (РЗНЗЗ) – $РЗ_i\ (i=1,\ldots,L)$. В даному випадку f розглядається як комбінуюча або фільтруюча функція від L змінних.

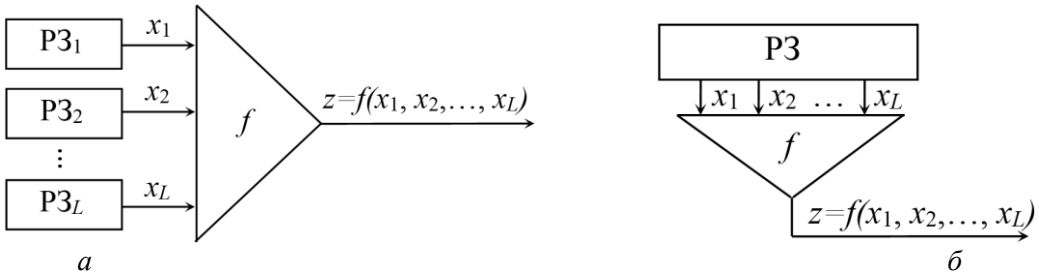

Рис. 1. Структурна схема комбінуючого (*а*) та фільтруючого (*б*) генератора ПВП

Булевою функцією, що відповідає РЗНЗЗ, в загальному виді називається булеве відображення виду $f: GF_2^L \to GF_2$. Булеві функції будемо представляти у вигляді многочленів (поліном Жегалкіна або алгебраїчна нормальна форма – АНФ) над полем $GF(2)$:

$$f(x_1, x_2, \ldots, x_L) = a_0 + \sum_{i=1}^{L} a_i x_i + \sum_{i=1}^{L-1} \sum_{j=i+1}^{L} a_{ij} x_i x_j + \sum_{i=1}^{L-2} \sum_{j=i+1}^{L-1} \sum_{m=j+1}^{L} a_{ijm} x_i x_j x_m + \ldots .$$

Алгебраїчним степенем $def(f)$ функції f називається кількість змінних у самому довгому доданку АНФ, при якому коефіцієнт не дорівнює нулю. Функція степеню не вище 1 є *афінною функцією*. Випадку, коли у афінної функції $a_0 = 0$, відповідає *лінійна функція*. Множина афінних булевих функцій від L змінних позначається як A_L.

В даній роботі розглядаються РЗНЗЗ другого порядку, тобто ті, алгебраїчний степінь яких дорівнює $def(f) = 2$. Крім того, будемо досліджувати лише ті РЗНЗЗ другого порядку, які формують послідовність максимального періоду, тобто М-послідовність. Позначимо такі нелінійні регістри як М-РЗНЗЗ.

Постановка задачі

Розглянемо деякі з основних, у даному випадку, показників оцінки криптографічної стійкості:

– *Збалансованість*.

Булева функція f від L змінних називається збалансованою, якщо функція приймає значення 0 та 1 однаково часто. Це одне з найбільш природних необхідних властивостей, що накладаються на булеві функції, що використовуються в поточних шифрах [0].

Якщо булева функція збалансована, то ймовірність того, що вона прийме значення 0 або 1, однакова та дорівнює $1/2$. Це дозволяє послабити статистичні залежності між входом

функції та її виходом. В іншому випадку у криптоаналитика є можливість, використовуючи розподіл усіх співвідношень, провести криптоаналіз шифру.

– *Наявність заборон.*

В разі аналізу ПВП, що генерується за допомогою фільтруючого генератору, виникає ще одне поняття – заборона булевої функції, тобто наявність комбінацій вихідної послідовності, яка не може мати місце не за яких комбінацій вхідної послідовності.

Інтуїтивно зрозуміло, що наявність заборони у фільтруючої функції генератора робить її «слабкіше», ця заборона ніколи не з'явитися у вихідній послідовності генератора, що погіршує його статистичні властивості.

– *Кореляційна імунність.*

Вимога кореляційної імунної функції пов'язана з протистоянням кореляційній атаці, ідея якої полягає в наступному [10]. Розглянемо комбінуючий генератор ПВП (рис. 1, *а*). Ключем генератора є початковий стан всіх регістрів. Обсяг ключа дорівнює $2^{l_1+\ldots+l_L}$, де l_i – довжина РЗ_i для $i=1,\ldots,L$.

Кожний з РЗ_i генерує послідовність $x_i = x_i^1 x_i^2 \ldots$, як правило, близьку за своїми властивостями до випадкової. Зокрема, при досить великій довжині послідовності для випадково вибраного її біта x_i^j має місце ймовірність випадкової події $x_i^j = 0$: $\text{P}[x_i^j = 0] \approx 1/2$. Отже, якщо $y = y^1 y^2 \ldots$ – довільна послідовність, яка не залежить від x_i, то

$$\text{P}[x_i^j = y^j] = \text{P}[x_i^j = 0]\cdot \text{P}[y^j = 0] + \text{P}[x_i^j = 1]\cdot \text{P}[y^j = 1] \approx \frac{1}{2}\left(\text{P}[y^j = 0] + \text{P}[y^j = 1]\right) = \frac{1}{2}.$$

Припустимо, що $\text{P}[f = x_1] \neq 1/2$ (у цьому випадку говорять, що *функція* f *корелює зі змінною* x_1). За допомогою кореляційної атаки знайдемо початковий стан s_1 РЗ_1. Для цього будемо перебирати всі можливі 2^{l_1} станів РЗ_1, для кожного з них будуємо послідовність $z' = z'_1 z'_2 \ldots$ та підраховуємо кількість збігів з ПВП $z'_i = z_i$. Для всіх послідовностей, крім однієї (що генерується s_1), частка збігів буде $\approx 1/2$. Тим самим визначимо, що частина ключа – стан s_1. Якщо функція f має кореляцію з усіма своїми змінними (або з усіма, крім однієї – тоді стан регістра, відповідного цієї змінної, знайдемо останнім, знаючи стан всіх інших регістрів), то знайдемо ключ генератора за $2^{l_1} + \ldots + 2^{l_L}$ випробувань, що набагато менше складності атаки грубої сили.

– *Нелінійність.*

Практика показує [10], що криптографічні перетворення, які мають властивості, близькі до властивостей лінійних функцій, в багатьох випадках призводять до істотного зниження стійкості шифрів. З цієї причини в криптографії важливе значення мають функції, властивості яких виключають слабкості, властиві функціям, близьким до лінійних. Таким чином, бажаною якістю функції є її нелінійність, що розуміється в широкому сенсі: як заперечення лінійності. У блокових та потокових шифрах застосування функції з високою нелінійністю сприяє підвищенню стійкості шифрів к лінійному та диференціальному методам криптоаналізу.

У літературі мало описується зв'язок між різними криптографічними властивостями. Практика показує [10], що в якості компонент шифру необхідно вибирати «хороші з усіх боків» функції, що є насправді дуже непростим завданням, оскільки багато властивостей суперечать одна одній. Хоча теоретичні результати показують, що у випадкової функції багато криптографічних параметрів, близьких до оптимальних. Питання в тому, як її вибрати, випадкову?

Отримані результати

Введемо деякі визначення, що будемо використовувати у подальшому [0].

Вагою булевої функції або *вагою Хеммінга* називається кількість одиниць у векторі та позначається як $wt(f)$ або $wt(x)$.

Відстанню Хемінга між булевими функціями f та g є відстань Хеммінга між векторами їх значень $dist(f,g)=wt(f\oplus g)$.

Твердження та теореми з метою скорочення обсягу роботи надано без доведення. Доведення є загальнодоступними та наведені, наприклад, у [1 – 8]. Всі значення експериментально перевірені на всій множині РЗНЗЗ (РЗЛЗЗ як окремий випадок) для розмірів з $L=4$ до 9 комірок включно.

Збалансованість

М-РЗНЗЗ, як і М-РЗЛЗЗ, генерують модифіковану послідовність де Брейна і якщо додати до розгляду стан заповнення усіх комірок нульовими значеннями, то отримана функція буде збалансованою. При рівноімовірному і незалежному виборі аргументів булевої функції f, імовірності її значень відповідно $P(1)=wt(f)/2^L$ $P(0)=1-wt(f)/2^L$.

Наявність заборон

М-РЗНЗЗ є функціями, які не мають заборон. Це випливає з того, що РЗНЗЗ формують послідовність де Брейна, яка за визначенням має всі можливі комбінації послідовності.

Однак слід бути обережними, оскільки цілком збалансована фільтруюча функція в тому чи іншому вигляді переносить властивості вхідної послідовності до властивості послідовності, що генерується [10]. Наприклад, в роботі [0] встановлено новий критерій, який ідейно говорить наступне: «фільтруюча функція зберігає заборони (у відповідному сенсі) тоді і тільки тоді, коли вона цілком збалансована». Відповідно, якщо на вхід функції надходить «далека» від випадкової послідовність, то й на виході її статистичні властивості будуть погані.

Кореляційна імунність

Наявність кореляційно імунної функції степеня m означає, що значення функції $Z=f(X)$ статистично незалежні від будь-якого набору з не більше ніж m компонентів довільного вектора-аргументу $X=GF(2)^L$. Це рівнозначно умові, що на вихід перетворення не «просочується» інформація про вектори, що надходять на вхід перетворення і мають вагу Хеммінга не більше m.

Булева функція f називається *кореляційно імунною порядку* m, $1\le m\le L$, якщо для будь-якої сукупності номерів m змінних $1\le i_1<i_2<\ldots<i_m\le L$ випадкові величини $X=(x_{i_1},x_{i_2},\ldots,x_{i_m})$ та $Y=f(x_1,x_2,\ldots,x_L)$ є незалежними.

Можна довести, що кореляційно імунна порядку m функція від L змінних є кореляційно імунною довільного меншого порядку. Таким чином, булевій функції f відповідає деякий максимальний порядок її кореляційної імунності $m_{\max}$, який позначається через $cor(f)$.

Випадок, коли $m=L$, має місце лише коли $f=const$. Максимального кореляційного імунітету степеня $m=L-1$ досягають тільки афінні функції, тобто криптографічно слабкі. Крім того, якщо f збалансована та $cor(f)=L-2$, то функція f також афінна. Таким чином, є сенс розглядати порядок кореляційної імунності m лише у діапазоні $1\le m\le L-3$.

Збалансована кореляційно-імунна функція порядку m називається *m-стійкою функцією*. Формально будь-яку збалансовану булеву функцію можна розглядати як 0-стійку і

довільну булеву функцію як (-1) стійку. За аналогією з $cor(f)$ вводиться позначення для *максимального порядку стійкості*:

$$sut(f)=\begin{cases}-1, & \text{якщо } f \text{ не збалансована},\\ cor(f), & \text{якщо } f \text{ збалансована}.\end{cases}$$

Таблиця 1

Розподіл кількості регістрів в залежності від максимальної стійкості для М-РЗЛЗЗ та М-РЗНЗЗ другого порядку

	Усього	$sut(f)$							
		$m=0$	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$
$L=4$									
М-РЗЛЗЗ	2	0	2	0	–	–	–	–	–
М-РЗНЗЗ 2-го порядку	14	4	10 *m-опт*	–	–	–	–	–	–
$L=5$									
М-РЗЛЗЗ	6	0	2	0	4 *m-опт*	–	–	–	–
М-РЗНЗЗ 2-го порядку	122	64	52	6 *m-опт*	–	–	–	–	–
$L=6$									
М-РЗЛЗЗ	6	0	2	0	4	0	–	–	–
М-РЗНЗЗ 2-го порядку	1 946	788	1 044	76	38 *m-опт*	–	–	–	–
$L=7$									
М-РЗЛЗЗ	18	0	4	0	10	0	4 *m-опт*	–	–
М-РЗНЗЗ 2-го порядку	64 038	33 988	25 578	4 090	378	4 *m-опт*	–	–	–
$L=8$									
М-РЗЛЗЗ	16	0	0	0	12	0	4	0	–
М-РЗНЗЗ 2-го порядку	4 017 982	1 686 218	2 120 124	194 798	16 612	188	42 *m-опт*	–	–
$L=9$									
М-РЗЛЗЗ	48	0	2	0	16	0	28	0	2 *m-опт*
М-РЗНЗЗ 2-го порядку	519 239 746	284 956 836	208 843 948	24 325 344	1091568	21 192	848	10 *m-опт*	–

Нерівність Зігенталера. Якщо f – кореляційно-імунна порядку m функція на $GF(2)^L$, то:

1) $def(f)\le L-m$;

2) якщо f є збалансованою та $sut(f)=m\le L-2$, то $def(f)+sut(f)\le L-1$.

Нерівність Зігенталєра є одним з багатьох протиріч криптографічних властивостей функцій один одному: високий порядок кореляційної імунної функції тягне її низьку алгебраїчну степінь і навпаки.

Якщо функція f є збалансована, $sut(f)=m\le L-2$ та $def(f)=L-m-1$, то f називається m*-оптимальною*.

Звідки маємо m-оптимальні f для РЗЛЗЗ $m=L-1-def(f)=L-2$ та для РЗНЗЗ другого порядку $m=L-1-def(f)=L-3$. Таким чином, ми визначили верхню межу значень для m-стійких функцій. У роботі було досліджено кореляційну імунність усієї множини М-РЗЛЗЗ та М-РЗНЗЗ другого порядку розмірністю $L=4,\ldots,9$. Результати наведені у таблиці 1.

Як бачимо з табл. 1, М-РЗНЗЗ другого порядку досягають значення для m-оптимальних функцій (у таблиці позначені як «m*-опт*») при всіх досліджених L. Однак, є дуже велика частка (приблизно половина усієї множини М-РЗНЗЗ другого порядку), яка не має кореляційної імунності.

Нелінійність

Нелінійністю функції f називається відстань від f до класу афінних функцій. Будемо позначати нелінійність функції f через N_f:

$$N_f = dist(f, A_L) = \min_{g\in A_L} dist(f, g).$$

У випадку парного L максимально можливе значення нелінійності дорівнює $2^{L-1}-2^{(L/2)-1}$, функції, які мають таку нелінійність, виділені в окремий клас – «бент-функції». У разі непарного L точне значення максимальної нелінійності невідомо і представляє складне комбінаторне завдання [10]. Разом з тим, всі бент-функції не збалансовані (на відміну від М-РЗНЗЗ), що робить їх уразливими до статистичного аналізу.

Наступні твердження показують, що чим вище порядок кореляційної імунної функції, тим нижче верхня межа її нелінійності.

Якщо f збалансована і m-стійка, $m\le L-2$. Тоді $N_f \le 2^{L-1}-2^{m+1}$.

За аналогією з поняттям m-оптимальної функції вводиться спеціальна назва для m-стійкої функції максимально можливої нелінійності.

Якщо функція f з $GF(2)^L$ збалансована, $sut(f)=m\le L-2$ і $N_f = 2^{L-1}-2^{m+1}$, то f називається m*-насиченою*.

У табл. 2 наведено розраховані значення за вищенаведеними формулами максимально можливої нелінійності збалансованої функції в залежності від її стійкості.

Таблиця 2

Значення нелінійності m-насичених функцій в залежності від їх максимальної стійкості

		$sut(f)$					
		1	**2**	**3**	**4**	**5**	**6**
N_f	$L=4$	4	0	–	–	–	–
	$L=5$	12	8	0	–	–	–
	$L=6$	28	24	16	0	–	–
	$L=7$	60	56	48	32	0	–
	$L=8$	124	120	112	96	64	0
	$L=9$	252	248	240	224	192	128

Значення нелінійності, наведені у табл. 2, не обов'язково досяжні. Позначимо через $N_{f\max}(L,m)$ *максимально можливу нелінійність* m-стійкої булевої функції, заданої на $GF(2)^L$, та наведемо верхню оцінку для нелінійності m-стійких функцій.

З наведеного випливає, що $N_{f\max}(L,-1)=2^{L-1}-2^{L/2-1}$, це значення може досягатися тільки для парних L. Якщо f є збалансованою функцією та L парне значення, справедливо $N_{f\max}(L,m)=2^{L-1}-2^{L/2-1}-2^{m+1}$ [2].

Таблиця 3

Розподіл кількості регістрів в залежності від нелінійності та максимальної стійкості для М-РЗН33 другого порядку

N_f	$sut(f)$						
	$m=0$	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$
$L=4$							
4	4[1)]	m -нас 10	–	–	–	–	–
0	0	0	0	–	–	–	–
$L=5$							
12	56[1)]	0	–	–	–	–	–
8	8	52	m -нас 6	–	–	–	–
0	0	0	0	0	–	–	–
$L=6$							
24	740	856[1)]	0	–	–	–	–
16	48	188	76	m -нас 38	–	–	–
0	0	0	0	0	0	–	–
$L=7$							
56	26 324[1)]	0	0	–	–	–	–
48	7 624	24 862	3 596	0	–	–	–
32	40	716	494	378	m -нас 4	–	–
0	0	0	0	0	0	0	–
$L=8$							
112	1 620 992	1 737 690	0	0	–	–	–
96	65 078	380 856	192 572	14 270	0	–	–
64	148	1 578	2 226	2 342	188	m -нас 42	–
0	0	0	0	0	0	0	0
$L=9$							
240	216 743 896	0	0	0	–	–	–
224	67 714 544	203 967 024	19 364 756	0	0	–	–
192	498 196	4 872 526	4 953 980	1 079 370	18 642	0	–
128	200	4398	6 608	12 198	2 550	848	m -нас 10
0	0	0	0	0	0	0	0

[1)] – значення N_f є максимальними для даних m, L та відповідають $N_{f\max}(L,m)$, які зазначені у [11].

У [11] вказується, що для непарних L та $L\le 7$, $N_{f\max}(L,-1)=2^{L-1}-2^{(L-1)/2}$, але для непарних L та $L\ge 15$ справедлива нерівність $N_{f\max}(L,-1)>2^{L-1}-2^{(L-1)/2}$.

При $m\ge L-2$, за нерівністю Зігенталєра $def(f)\le 1$, звідки $N_{f\max}(L,m)=0$. Також у [11] є посилання на доведену нерівність $N_{f\max}(L,L-3)=2^{L-2}$ та гіпотезу, що $N_{f\max}(L,L-4)=2^{L-1}-2^{L-3}$. Крім того, наведено деякі точні значення $N_{f\max}(L,m)$ для малих L та m:

$N_{f\max}(4,0)=4$;

$N_{f\max}(5,-1)=N_{f\max}(5,0)=N_{f\max}(5,1)=12$;

$N_{f\max}(6,0) = 26$; $N_{f\max}(6,1) = N_{f\max}(6,2) = 24$;

$N_{f\max}(7,-1) = N_{f\max}(7,0) = N_{f\max}(7,1) = 56$.

Вказані результати не суперечать результатам, отриманим в даній роботі і наведеним нижче.

У табл. 3 зведено отриманий розподіл за нелінійністю усієї множини М-РЗНЗЗ розмірністю $L = 4,\ldots,9$ в залежності від розміру РЗНЗЗ та кореляційної імунності.

Як бачимо з наведених результатів, М-РЗНЗЗ другого порядку одночасно досягають максимально можливої стійкості та максимальної нелінійності. Причому, всі m-оптимальні функції також є і m-насиченими (у табл. 3 позначені як «m-нас»). Крім того, багато М-РЗНЗЗ, які не є m-насиченими функціями за визначенням, досягають максимально можливого результату для $N_{f\max}(L,m)$ наведеного вище.

В якості прикладу наведемо М-РЗНЗЗ другого порядку розмірністю $L = 9$, що відповідають m-насіченим функціям (з нелінійністю $N_f = 128$ та максимальною стійкістю $sut(f) = 6$):

$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_9 + x_2 \cdot x_5 + x_2 \cdot x_8$$
$$f(x_1, x_2, \ldots, x_9) = x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_7 + x_4 \cdot x_7$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_4 + x_5 + x_7 + x_8 + x_9 + x_4 \cdot x_6 + x_4 \cdot x_8$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_5 + x_3 \cdot x_5$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_5 + x_3 \cdot x_6$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_6 + x_4 \cdot x_6$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_1 \cdot x_6 + x_5 \cdot x_6$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_3 \cdot x_4 + x_3 \cdot x_8$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9 + x_2 \cdot x_7 + x_5 \cdot x_7$$
$$f(x_1, x_2, \ldots, x_9) = x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_8 + x_9 + x_2 \cdot x_4 + x_2 \cdot x_7$$

Аналізуючи отримані результати, бачимо, що симетричні М-РЗНЗЗ мають однакові показники $sut(f)$ та N_f. Всі М-РЗНЗЗ, що досліджувались, мають $N_f \geq 2^{L-2}$.

Висновки

Булеві функції, які відповідають М-РЗНЗЗ, є збалансованими, не мають заборон.

Близько половини булевих функцій, що відповідають М-РЗНЗЗ, є кореляційно імунними функціями, деякі з яких досягають максимальної можливої стійкості та є m-оптимальними функціями.

Всі булеві функції, що відповідають М-РЗНЗЗ другого порядку, за виключенням М-РЗЛЗЗ, мають нелінійність $N_f \geq 2^{L-2}$ та деякі досягають максимального значення, тобто є m-насиченими функціями.

Список літератури:

1. Городилова А.А. От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3(33). С.16–44.

2. Панкратова И.А. Булевы функции в криптографии : учеб. пособие. Томск : Изд. Дом Томск. Гос. ун-та. 2014. 88 с.

3. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К. : ООО «Полиграф-Консалтинг». 2005. 215 с.

4. Токарева Н.Н. Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. 2010. Т. 17, №1. С.33-62.

5. Токарева Н.Н. Нелинейные булевы функции: бент-функции и их обобщения. Изд-во LAP LAMBERT Academic Publishing (Saarbrucken, Germany). 2011. 180 с.

6. Агафонова И.В. Криптографические свойства нелинейных булевых функций // Семинар по дискрет. гармон. анализу и геометр. моделированию. СПб. : DHA & CAGD, 2007. С. 1–24.

7. Шевелев Ю.П. Дискретная математика. Ч. 1: Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ») : учеб. пособие. Томск. гос. ун-т систем управления и радиоэлектроники, 2003. 118 с.

8. Молдовян А.А. Криптография. Скоростные шифры. БХВ-Петербург, 2002. 496 с.

9. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии. 2-е изд. Москва : МЦНМО, 2012. 584с.

10. Смышляев С.В. О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. № 1. С. 5–15.

11. Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Физматлит, 2002. Вып. 11. С. 91–148.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 11.02.2018