УДК 003.26:004.056.55

В.Г. Бабенко[1], С.Г. Козловська[2]

[1] *Черкаський державний технологічний університет, Черкаси*
[2] *Східноєвропейський університет економіки і менеджменту, Черкаси*

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МАТРИЧНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

В статті проведено аналіз властивостей результатів перетворення, здійсненого на основі матричних операцій криптографічного перетворення визначеного фрагменту інформації. Виявлено залежність властивостей результату перетворення від виду інформації, над якою здійснюється дане перетворення. В результаті дослідження встановлено, що технологія використання матричних операцій криптографічного перетворення полягає у виборі виду операнда матричної операції, тобто при використанні інформації в байтовому форматі забезпечується виконання нелінійного перетворення, а при використанні бітового формату представлення даних забезпечується лінійність перетворення.

Ключові слова: *матрична операція, криптографічне перетворення, технологія використання операцій, аналіз, властивість операції, лінійність, нелінійна операція.*

Вступ

Постановка проблеми. Сучасний стан розвитку програмно-технічних засобів обробки інформації вимагає розробки та вдосконалення технологій її захисту. Причому постійне зростання обсягів інформації, що підлягає автоматизованій обробці, зумовлює також і досягнення вимоги збільшення швидкодії систем захисту інформації.

Зважаючи на те, що одним з найпоширеніших способів захисту інформації є перетворення інформації на основі криптоалгоритмів, то актуальною задачею сьогодні можна назвати розробку та вдосконалення швидкодіючих алгоритмів криптографічного захисту. Саме тому на даний час основним питанням, що підлягає вирішенню, є збільшення об'ємів інформації, що може оброблятися функціями криптографічного перетворення. Одним із шляхів вирішення даної проблеми є застосування матричних операцій криптографічного перетворення для розробки криптоалгоритмів. Так як функції криптографічного перетворення, що складають базис криптоалгоритму, обов'язково повинні володіти відповідними властивостями, зокрема бути нелінійними, тоді постає задача комплексного використання лінійних та нелінійних перетворень при обмеженні складності криптографічних алгоритмів.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень особливу увагу привертають публікації [1 – 5], в яких запропоновано застосовувати матричні операції криптографічного перетворення та криптопримітиви, побудовані на основі них, для алгоритмів захисту інформаційних ресурсів. Так в [1 – 3] розроблено методи захисту інформаційних ресурсів на основі матричних та розширених матричних операцій криптографічного перетворення та запропонована структурна схема їх застосування. Суть статті [4] полягає у проведенні оцінки криптостійкості та швидкості реалізації криптографічного захисту інформації на основі операцій матричного та розширеного матричного криптографічного перетворення.

В колективній монографії [5] розроблені методи та засоби криптографічного перетворення, що забезпечують підвищення якості функціонування систем захисту інформаційних ресурсів на основі матричного криптографічного перетворення, а також дають можливість забезпечити необхідні значення швидкості шифрування та криптостійкості за рахунок збільшення апаратної та програмної складності реалізації системи криптографічного захисту інформації. Проте в проаналізованих публікаціях відсутні результати дослідження щодо застосування матричних операцій в якості функцій нелінійного перетворення при розробці криптоалгоритмів.

Формулювання мети статті. Мета роботи – дослідити властивості матричних операцій криптографічного перетворення інформації при їх реалізації в криптографічних алгоритмах.

Основний матеріал

Для досягнення основної поставленої мети даного дослідження, а саме дослідження особливостей використання операцій криптографічного перетворення інформації, в першу чергу необхідно здійснити аналіз способів застосування матричних операцій криптографічного перетворення інформації. Потім виявити закономірності результатів проведеного аналізу та на основі них розробити рекомендації, що складатимуть основу технології використання матричних операцій для побудови криптоалгоритмів.

При перетворенні інформації на основі матричних операцій криптографічного перетворення необхідно забезпечити однозначність перетворення

інформації як при прямому так і зворотному перетворенні.

Всі операції криптоперетворення, побудовані на основі елементарних операцій, забезпечують роботу з бітами. Проте в залежності від виду операнда матричні операції можуть реалізувати перетворення бітів інформації, байтів інформації, слів і т.д.

Проведемо аналіз властивостей перетворення інформації, представленої в бітовому та байтовому виді на основі матричних операцій. При проведенні дослідження обмежимося матричними операціями, які в загальному виді представлені операціями криптографічного перетворення, побудованими на основі додавання за модулем два та заданими виразом [5]:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix},$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 ... x_n$ – операнди відповідно; $\oplus$ – операція "сума за модулем 2".

Проведемо перетворення інформації, заданої в бітовому форматі, зокрема чисел від 0 до 255, на основі матричного перетворення, що описується виразом:

$$\vec{F} = \begin{pmatrix} x_1 \oplus x_4 \oplus x_8 \\ x_6 \oplus x_8 \\ x_2 \oplus x_7 \\ x_1 \oplus x_7 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_6 \\ x_1 \\ x_5 \oplus x_7 \\ x_1 \oplus x_4 \oplus x_6 \oplus x_7 \end{pmatrix}. \qquad (1)$$

Результати перетворення числової інформації на основі матричної моделі (1) представлені в табл. 1, де x – початкове значення числа (до здійснення перетворення), y – одержане значення числа (після здійснення перетворення), а «$\rightarrow$» – це матрична операція задана відповідною моделлю.

Аналіз табл. 1 показав, що використання матричних операцій криптографічного перетворення при застосуванні інформації в бітовому форматі забезпечує виконання лінійного перетворення.

Логічно припустити, що властивості перетворення на основі матричної операції, що здійснюється над інформацією в байтовому представленні, також характеризуються лінійністю, адже байт є вісім бітів. Перевіримо дане припущення на прикладі.

Проведемо перетворення числової інформації заданого діапазону в байтовому форматі на основі матричного перетворення, що описується виразом:

$$\vec{F} = \begin{pmatrix} x_4 \oplus x_7 \\ x_2 \oplus x_6 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_5 \oplus x_6 \oplus x_8 \\ x_2 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \end{pmatrix}. \qquad (2)$$

Фрагмент результатів перетворення чисел від 0 до 255 на основі моделі (2) представлені в табл. 2.

Аналіз табл. 2 показав, що використання матричних операцій криптографічного перетворення при застосуванні інформації в байтовому форматі забезпечує виконання нелінійного перетворення.

Таким чином, запропоноване припущення не є істинним, адже очікувані результати не співпали.

Як видно із табл. 1 і табл. 2, властивості результатів перетворення над інформацією в бітовому та байтовому виді різні. Проте результати отримані на основі матричних операцій, що задаються різними виразами, тому вважати закономірністю залежність виявленої властивості результатів перетворення від виду інформації, над якою здійснювалося дане перетворення, хоч інформація вибрана однакова, не коректно. Тому для уточнення та перевірки отриманих результатів проведемо перетворення інформації заданої в байтовому форматі, а саме 256 чисел, на основі матричного перетворення, що описується виразом (1). Результати перетворення числової інформації на основі матричної моделі (1) представлені в табл. 3. Аналіз табл. 3 показав, що отримані результати перетворення на основі матричної операції криптографічного перетворення при застосуванні інформації в байтовому форматі забезпечує виконання нелінійного перетворення.

В результаті обчислювального експерименту отримані дані (табл. 1) показують, що кожне конкретне число перетворюється однозначно в кожне конкретне число, тобто операція є лінійною та реалізує варіант перестановки.

Якщо провести заміну операндів матричної операції – бітів на байти, то матриці прямого та оберненого перетворення будуть однаковими, тобто повністю співпадуть.

Проте вияснилось, що при матричному криптоперетворенні байтів було отримано нелінійне перетворення (табл. 2, 3), отже і матричні моделі прямого та оберненого перетворення повинні відрізнятися. Аналіз табл. 1 – 3 показав, що використання матричних операцій криптографічного перетворення при використанні інформації в байтовому форматі забезпечує виконання нелінійного перетворення, а при використанні бітового формату представлення даних забезпечується лінійність перетворення.

Таблиця 1

Результати перетворення чисел заданого діапазону в бітовому форматі на основі виразу (1)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	0	32	16	64	20	96	4	128	185	160	169	192	173	224	189
1	11	33	27	65	31	97	15	129	178	161	162	193	166	225	182
2	204	34	220	66	216	98	200	130	117	162	101	194	97	226	113
3	199	35	215	67	211	99	195	131	126	163	110	195	106	227	122
4	146	36	130	68	134	100	150	132	43	164	59	196	63	228	47
5	153	37	137	69	141	101	157	133	32	165	48	197	52	229	36
6	94	38	78	70	74	102	90	134	231	166	247	198	243	230	227
7	85	39	69	71	65	103	81	135	236	167	252	199	248	231	232
8	64	40	80	72	84	104	68	136	249	168	233	200	237	232	253
9	75	41	91	73	95	105	79	137	242	169	226	201	230	233	246
10	140	42	156	74	152	106	136	138	53	170	37	202	33	234	49
11	135	43	151	75	147	107	131	139	62	171	46	203	42	235	58
12	210	44	194	76	198	108	214	140	107	172	123	204	127	236	111
13	217	45	201	77	205	109	221	141	96	173	112	205	116	237	100
14	30	46	14	78	10	110	26	142	167	174	183	206	179	238	163
15	21	47	5	79	1	111	17	143	172	175	188	207	184	239	168
16	129	48	145	80	149	112	133	144	56	176	40	208	44	240	60
17	138	49	154	81	158	113	142	145	51	177	35	209	39	241	55
18	77	50	93	82	89	114	73	146	244	178	228	210	224	242	240
19	70	51	86	83	82	115	66	147	255	179	239	211	235	243	251
20	19	52	3	84	7	116	23	148	170	180	186	212	190	244	174
21	24	53	8	85	12	117	28	149	161	181	177	213	181	245	165
22	223	54	207	86	203	118	219	150	102	182	118	214	114	246	98
23	212	55	196	87	192	119	208	151	109	183	125	215	121	247	105
24	193	56	209	88	213	120	197	152	120	184	104	216	108	248	124
25	202	57	218	89	222	121	206	153	115	185	99	217	103	249	119
26	13	58	29	90	25	122	9	154	180	186	164	218	160	250	176
27	6	59	22	91	18	123	2	155	191	187	175	219	171	251	187
28	83	60	67	92	71	124	87	156	234	188	250	220	254	252	238
29	88	61	72	93	76	125	92	157	225	189	241	221	245	253	229
30	159	62	143	94	139	126	155	158	38	190	54	222	50	254	34
31	148	63	132	95	128	127	144	159	45	191	61	223	57	255	41

Таблиця 2

Фрагмент результатів перетворення чисел заданого діапазону в байтовому форматі на основі виразу (2)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	5	32	5	64	5	96	5	128	5	160	5	192	5	224	5
1	4	33	36	65	68	97	100	129	132	161	164	193	196	225	228
2	4	34	36	66	68	98	100	130	132	162	164	194	196	226	228
3	7	35	39	67	71	99	103	131	135	163	167	195	199	227	231
4	1	36	1	68	1	100	1	132	1	164	1	196	1	228	1
5	0	37	0	69	0	101	0	133	0	165	0	197	0	229	0
6	7	38	7	70	7	102	7	134	7	166	7	198	7	230	7
7	6	39	38	71	70	103	102	135	134	167	166	199	198	231	230
8	5	40	5	72	5	104	5	136	5	168	5	200	5	232	5
9	12	41	44	73	76	105	108	137	140	169	172	201	204	233	236
10	12	42	44	74	76	106	108	138	140	170	172	202	204	234	236
11	15	43	47	75	79	107	111	139	143	171	175	203	207	235	239
12	1	44	1	76	1	108	1	140	1	172	1	204	1	236	1
13	0	45	0	77	0	109	0	141	0	173	0	205	0	237	0
14	7	46	7	78	7	110	7	142	7	174	7	206	7	238	7
15	14	47	46	79	78	111	110	143	142	175	174	207	206	239	238

Таблиця 3

Результати перетворення чисел заданого діапазону в байтовому форматі на основі виразу (1)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	3	32	35	64	67	96	99	128	131	160	163	192	195	224	227
1	2	33	2	65	2	97	2	129	2	161	2	193	2	225	2
2	7	34	7	66	7	98	7	130	7	162	7	194	7	226	7
3	6	35	38	67	70	99	102	131	134	163	166	195	198	227	230
4	6	36	6	68	6	100	6	132	6	164	6	196	6	228	6
5	7	37	39	69	71	101	103	133	135	165	167	197	199	229	231
6	2	38	2	70	2	102	2	134	2	166	2	198	2	230	2
7	0	39	0	71	0	103	0	135	0	167	0	199	0	231	0

Закінчення табл. 3

8	11	40	43	72	75	104	107	136	139	168	171	200	203	232	235
9	2	41	2	73	2	105	2	137	2	169	2	201	2	233	2
10	7	42	7	74	7	106	7	138	7	170	7	202	7	234	7
11	14	43	46	75	78	107	110	139	142	171	174	203	206	235	238
12	6	44	6	76	6	108	6	140	6	172	6	204	6	236	6
13	15	45	47	77	79	109	111	141	143	173	175	205	207	237	239
14	2	46	2	78	2	110	2	142	2	174	2	206	2	238	2
15	0	47	0	79	0	111	0	143	0	175	0	207	0	239	0
16	19	48	51	80	83	112	115	144	147	176	179	208	211	240	243
17	2	49	2	81	2	113	2	145	2	177	2	209	2	241	2
18	7	50	7	82	7	114	7	146	7	178	7	210	7	242	7
19	22	51	54	83	86	115	118	147	150	179	182	211	214	243	246
20	6	52	6	84	6	116	6	148	6	180	6	212	6	244	6
21	23	53	55	85	87	117	119	149	151	181	183	213	215	245	247
22	2	54	2	86	2	118	2	150	2	182	2	214	2	246	2
23	0	55	0	87	0	119	0	151	0	183	0	215	0	247	0
24	27	56	59	88	91	120	123	152	155	184	187	216	219	248	251
25	2	57	2	89	2	121	2	153	2	185	2	217	2	249	2
26	7	58	7	90	7	122	7	154	7	186	7	218	7	250	7
27	30	59	62	91	94	123	126	155	158	187	190	219	222	251	254
28	6	60	6	92	6	124	6	156	6	188	6	220	6	252	6
29	31	61	63	93	95	125	127	157	159	189	191	221	223	253	255
30	2	62	2	94	2	126	2	158	2	190	2	222	2	254	2
31	0	63	0	95	0	127	0	159	0	191	0	223	0	255	0

Висновки

Виходячи з наведених результатів, можна стверджувати, що одна і та ж сама матрична операція криптографічного перетворення може бути використана для реалізації як лінійного так і нелінійного перетворення, що забезпечує спрощення алгоритму шифрування за рахунок зменшення кількості використовуваних операцій для шифрування та розшифрування інформації, а також ускладнює криптоаналіз результатів перетворення.

Список літератури

1. Бабенко В.Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 9 (107). – С. 163-168.

2. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 9 (107). – С. 145-147.

3. Мельник Р.П. Методи та засоби синтезу операцій розширеного матричного криптографічного перетворення: дис. канд. техн. наук / Мельник Р.П. – Черкаси, 2013. – 178 с.

4. Бабенко В.Г. Оцінка ефективності використання операцій криптографічного перетворення / В.Г. Бабенко, Р.П. Мельник, С.В. Гончар // Вісник інженерної академії України. – 2014. – Вип. 2. – С. 39-41.

5. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: колл. моногр. / Под ред. В.М. Безрука, В.В. Баранника. – Х.: СМИТ, 2013. – 398 с.

Надійшла до редколегії 28.01.2014

Рецензент: д-р техн. наук, проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ МАТРИЧНЫХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Г. Бабенко, С.Г. Козловская

В статье проведен анализ свойств результатов преобразования осуществленного на основе матричных операций криптографического преобразования определенного фрагмента информации. Выявлена зависимость свойств результата преобразования от вида информации, над которой осуществляется данное преобразование. В результате исследования установлено, что технология использования матричных операций криптографического преобразования заключается в выборе вида операнда матричной операции, то есть при использовании информации в байтовом формате обеспечивается выполнение нелинейного преобразования, а при использовании битового формата представления данных обеспечивается линейность преобразования.

Ключевые слова: *матричная операция, криптографическое преобразование, технология использования операций, анализ, свойство операции, линейность, нелинейная операция.*

ESPECIALLY THE USE OF MATRIX OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATIONS

V.G. Babenko, S.G. Kozlovska

The article analyzes the properties of the transformation results carried out on the basis of matrix operations for cryptographic transformation of a particular piece of information. The dependence of the properties of the result of the conversion of the type of information on which this conversion is performed. The study found that the use of the technology matrix operations cryptographic transformation is to select the type of the operand matrix operation, that is, by using the information in byte format ensures compliance with the non-linear transformation, and the use of the bit size of data provides a linear transformation.

Keywords: *matrix operation, a cryptographic transformation, technology use operations, analysis, properties of operations, linear, nonlinear operation.*