



УКРАЇНА

(19) UA (11) 18373 (13) U  
(51) МПК (2006)  
G09C 1/00

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під  
відповідальність  
власника  
патенту

### (54) СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

1

2

(21) u200603798

(22) 06.04.2006

(24) 15.11.2006

(46) 15.11.2006, Бюл. № 11, 2006 р.

(72) Білецький Анатолій Якович, Білецький Олександр Анатолійович, Кузнецов Олександр Олександрович, Юкальчук Андрій Анатолійович

(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ (НАУ)

(57) Спосіб криптографічного перетворення інформації, який полягає в тому, що інформаційну послідовність подають у вигляді 128 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців (блоків

MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв, який **відрізняється** тим, що як S-блок виступає змінна матриця підстановок, що будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення

$y = M \cdot x^{-1} + \beta$  над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як матрицю  $M$  афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа.

Запропонована корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах шифрування у системах обробки інформації для розширення їх можливостей.

Відомий спосіб криптографічного перетворення [1], який ґрунтується на тому, що інформаційна послідовність подається у вигляді 64 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: перестановка (permutation) - за допомогою блоків перестановок (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв. Ітеративна обробка полягає у багатократному виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою P-блоків) та перемішування (за допомогою S-блоків) інформаційних даних.

Недоліком цього способу є те, що для криптографічного перетворення інформації у якості S-блоку виступає фіксована матриця підстановок, що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Найбільш близьким, до запропонованого тех-

нічним рішенням, обраним як прототип, є удосконалений спосіб криптографічного перетворення [2], який ґрунтується на тому, що інформаційна послідовність подається у вигляді 128 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців (блоків MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв.

Ітеративна обробка полягає у багатократному виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою блоків MixColumn) та перемішування (за допомогою S-блоків) інформаційних даних. Підстановка

$$x = \{x_0, x_1, \dots, x_7\} \rightarrow y = \{y_0, y_1, \dots, y_7\}$$

представляє собою нелінійну заміну байт, яка виконується незалежно для кожного вхідного байта  $x = \{x_0, x_1, \dots, x_7\}$ . Матриці підстановки, за допомогою яких будуються S-блоки є інвертуємими матрицями, що утворюються із використанням композиції двох перетворень:

1. Отримання мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$ , яке будується за кільцем многочленів з

(19) UA (11) 18373 (13) U

операціями по модулю незвідного многочлену

$$g(x)=x^8+x^4+x^3+x+1;$$

При цьому приймається, що якщо  $x=0$ , то  $x^{-1}=0$ .

2. Виконання афінного перетворення над примітивним двійковим полем Галуа  $GF(2)$ , яке задається виразом:

$$y=M \cdot x^{-1} + \beta, \quad (1)$$

де  $M$  - фіксована матриця восьмого порядку, симетрична відносно допоміжної діагоналі:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix};$$

$\beta$  - фіксований восьмиразрядний вектор-стовпець:

$$\beta = |11000110|^T.$$

Матриця підстановки, що утворена із використанням композиції двох вказаних перетворень, має вигляд таблиці 1, де вхідний байт  $x=\{x_0, x_1, \dots, x_7\}$  представлено у вигляді двох напівбайтів

$$x=\{a_1, a_2\},$$

а власні значення осередків таблиці відповідають елементам вихідного байта  $y=\{y_0, y_1, \dots, y_7\}$ , так само представленого у вигляді напівбайтів  $y=\{b_1, b_2\}$ .

Таблиця 1

		$a_2$															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$a_1$	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	DO	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Недоліком способу-прототипу є те, що для криптографічного перетворення інформації у якості S-блоку виступає фіксована матриця підстановок, що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

В основу корисної моделі поставлена задача створити спосіб криптографічного перетворення інформації який, за рахунок використання у якості S-блоку динамічно змінюємих матриць підстановки дасть змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Поставлена задача вирішується за рахунок використання у якості симетричної матриці  $M$  афінного перетворення (1) змінних обернених симетричних матриць які обираються відповідно до значення циклового ключа.

Технічний результат, який може бути отриманий при здійсненні корисної моделі полягає в отриманні можливості гнучко змінювати параметри криптографічної обробки та динамічно керувати

процесом перемішування інформаційних даних.

Сутність запропонованого способу криптографічного перетворення інформації полягає в тому, що інформаційна послідовність подається у вигляді 128 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців (блоків MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв. У якості S-блоку виступає змінна матриця підстановок, що будується отриманням мультиплікативно зворотнього елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення (1) над примітивним двійковим полем Галуа  $GF(2)$ , при цьому у якості симетричної матриці  $M$  афінного перетворення використовуються змінні обернені симетричні матриці які обираються відповідно до значення циклового ключа.

Цикловий ключ виробляється із ключа шифру-

вання за допомогою алгоритму вироблення ключів. Довжина циклового ключа дорівнює довжині блоку. Циклові ключі генеруються із ключа шифрування за допомогою розширення ключа. Розширений ключ являє собою лінійний масив 4-х байтових слів. Тобто на кожній ітерації криптографічного перетворення використовується відповідна симетрична матриця  $M$ , яка за допомогою циклового 4 байтового ключа може обиратися із великої множини обернених матриць. Це надає змогу у процесі криптографічного перетворення гнучко змінювати матрицю підстановки та, відповідно, динамічно керувати процесом перемішування інформаційних даних. Так, наприклад, при виборі симетричної матриці

$$M = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

відповідна матриця підстановки має вигляд таблиці 2.

Таблица 2

		$a_2$															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$a_1$	0	63	34	78	71	5E	6D	6A	3F	4D	A8	64	1D	57	A0	FD	B9
	1	74	0A	36	F5	50	CA	5C	DD	79	E2	32	FA	9C	B6	BE	F9
	2	E8	15	D7	D5	C9	06	98	F0	4A	77	07	1C	FC	EB	8C	B3
	3	6E	BC	13	BB	7B	11	AF	18	2C	F6	89	42	8D	14	2E	FB
	4	A6	CB	58	F8	39	AB	88	B1	86	01	61	EF	9E	83	1A	8E
	5	47	24	69	09	51	D4	6C	49	AC	B5	27	82	94	10	0B	B2
	6	E5	8A	3C	91	5B	D1	0F	4F	DF	12	EA	76	05	44	DE	BF
	7	C4	F3	19	C2	16	5D	43	1B	A4	29	68	90	75	96	9F	66
	8	31	60	37	C8	4E	D0	1E	30	FE	F4	B7	85	26	CD	BA	7F
	9	21	48	52	EC	D2	DC	95	87	9D	4B	A3	72	6F	8F	25	A9
	A	C1	CE	C0	E4	D6	ED	56	0C	7A	A7	B8	A2	54	53	C6	F2
	B	84	F7	08	E9	41	23	93	7E	28	81	DA	4C	E7	B0	3B	67
	C	20	33	97	DB	7C	35	AA	7D	CF	2D	3A	3E	55	65	C5	04
	D	3D	C7	6B	A5	17	2B	59	E3	E0	8B	40	62	0D	38	BD	1F
	E	00	D3	9B	B4	EE	2A	03	92	D9	FF	CC	0E	73	C3	5F	AE
	F	80	70	46	A1	E6	45	9A	2F	D8	5A	99	22	AD	02	E1	F1

Головний показник ефективності блоків підстановок - показник нелінійності криптографічного перетворення є інваріантним до лінійного перетворення. Множення на обернену матрицю  $M$  є лінійне перетворення. Отже показник нелінійності перетворення, що виконується за допомогою таблиці 1 дорівнює показникам нелінійності відповідних перетворень, що виконуються за допомогою таблиці 2 та іншими відповідними таблицями (при іншому виборі матриці  $M$ ). Одтак запропоноване технічне рішення дозволяє виконувати криптографічне перетворення даних гнучко змінюючи таблиці перестановки із фіксованим показником нелінійності та динамічно керувати ітеративною обробкою інформаційних даних.

Таким чином, за рахунок використання змінних обернених симетричних матриць вдається на кожній ітерації криптографічного перетворення інфо-

рмації застосовувати у якості S-блоку динамічно змінюємі матриці підстановки, що дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Джерела інформації

1. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at <http://csrc.nist.gov/publications/fips/>  
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

2. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at <http://csrc.nist.gov/publications/fips/>  
<http://csrc.nist.gov/publications/fips/fips197/fips197.pdf>