

УДК 621.3.06

Р.В. Олійников, д-р техн. наук, І.Д. Горбенко, д-р техн. наук, О.В. Казимиров, канд. техн. наук, В.І. Руженцев, канд. техн. наук, О.О. Кузнєцов, д-р техн. наук, Ю.І. Горбенко, канд. техн. наук, О.В. Дирда, канд. техн. наук, А.О. Бойко, канд. техн. наук, В.І. Долгов, д-р техн. наук, А.І. Пушкаръов, В.М.Казимирова, Р.І.Кіянчук

ФУНКЦІЯ ГЕШУВАННЯ „КУПИНА” – НОВИЙ НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ВСТУП

У якості основної криптографічної функції гешування в Україні майже 20 років використовувався міждержавний стандарт ГОСТ 34.311-95 (російський ГОСТ Р 34.11-94 [1]). Це перетворення ще забезпечує практичну стійкість, водночас, для нього вже відомі ефективні криптоаналітичні атаки [2]. Крім того, з точки зору швидкодії реалізації на програмних платформах загального призначення ГОСТ 34.311-95 суттєво поступається більш сучасним рішенням. Інші країни вже відмовились від використання ГОСТ Р 34.11-94 у якості стандарту: у Білорусії введений в дію СТБ 34.101.31-2011 [3], у РФ – ГОСТ Р 34.11-2012 [4].

В Україні на основі консервативного підходу із залученням відомих і добре досліджених конструкцій була розроблена геш-функція, що базується на новому блоковому шифрі „Калина” (ДСТУ 7624:2014 [5]). Новий національний стандарт ДСТУ 7564:2014 [6] визначає криптографічну функцію гешування „Купина”, додатковий режим її застосування для формування коду автентифікації повідомлення (імітовставки), а також значення для перевірки реалізацій.

Для скорочення обсягу тексту національного стандарту була застосована математична нотація, що дозволяє отримати точний і компактний запис. Водночас, такий підхід може ускладнювати сприйняття сутності алгоритму для фахівців, що не мають фундаментальної криптологічної освіти. У цій статті наводиться розгорнутий альтернативний опис функції гешування „Купина”, із позначеннями, традиційними для галузі комп’ютерних наук.

1. ТЕРМІНОЛОГІЯ ТА ПОЗНАЧЕННЯ

Вектор ініціалізації	бітова послідовність фіксованої довжини (512 або 1024 біта), що використовується як початкове значення при обчисленні геш-значення.
Внутрішній стан	бітова послідовність фіксованої довжини (512 або 1024 біта), що є проміжним значенням на кожній ітерації перетворення функції гешування, а також вхідним та вихідним значенням перетворень P і Q ; для цих перетворень внутрішній стан подається як матриця розміром $8 \times c$ байт.
Геш-значення (геш-вектор)	бітова послідовність фіксованої довжини ($n = 8 \cdot s$, $s \in \{1, 2, \dots, 64\}$), що є результатом роботи функції гешування.
Доповнення	вставка додаткових біт у кінець повідомлення для отримання кратності довжини бітової послідовності довжині внутрішнього стану функції гешування.
Повідомлення	бітова послідовність довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт.

Функція стиснення ітеративне перетворення, що відображає l -бітний блок повідомлення та l -бітне значення, отримане функцією стиснення на попередньому кроці, у нове l -бітне значення.

Далі використовуються наступні позначення:

\oplus	– додавання за модулем 2 (XOR);
$0x$	– префікс числа, що записане у шістнадцятковій системі числення;
$a \bmod b$	– ціле невід’ємне число, що дорівнює залишку від ділення цілого числа a на натуральне число b ;
B_i	– i -й байт вхідної послідовності;
C^i	– константа перетворення XORRoundKey або Add64RoundKey для i -го циклу;
c	– кількість стовпців внутрішнього стану в матричному поданні;
φ	– функція стиснення;
H	– визначена у стандарті функція гешування;
$H(M)$	– результат обчислення функції гешування для повідомлення M (геш-значення);
IV	– вектор ініціалізації;
l	– розмір внутрішнього стану функції гешування (у бітах), $l \in \{512, 1024\}$;
M	– повідомлення;
m_i	– i -й блок повідомлення M ;
n	– довжина обчисленого геш-значення;
N	– довжина повідомлення M без доповнення;
P, Q	– складові перетворення функції стиснення;
P_{512}	– перетворення P для 512-бітного внутрішнього стану;
P_{1024}	– перетворення P для 1024-бітного внутрішнього стану;
Q_{512}	– перетворення Q для 512-бітного внутрішнього стану;
Q_{1024}	– перетворення Q для 1024-бітного внутрішнього стану;
r	– кількість ітерацій у перетвореннях P і Q ($r = t$ в ДСТУ 7564:2014);
S	– внутрішній стан геш-функції;
t	– кількість блоків m , з яких складається повідомлення M , включаючи доповнення;
v_i	– i -й біт вхідної послідовності;
Ω	– завершальне перетворення;
Купина- n	– режим використання функції гешування з усіченням обчисленого геш-значення до розміру n біт.

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Під функцією гешування H розуміється залежне від вектора ініціалізації IV відображення послідовності біт M у геш-значення $H(M)$ фіксованої довжини n .

ДСТУ 7564:2014 визначає функцію гешування, яка виконує перетворення «Купина-256» або «Купина-512», що забезпечують обчислення геш-значення з довжинами 256 або 512 біт відповідно. Геш-значення довжиною 256 бітів додатково може бути усічено до бітової послідовності довжиною від 8 до 248 біт з кроком у 8 біт, 512 бітів може бути усічене до бітової послідовності довжиною від 264 до 504 біт з кроком у 8 біт. Режим роботи для формування геш-значення довжиною n біт позначається як «Купина- n ».

Основними режимами роботи функції гешування, що рекомендуються до застосування, є «Купина-256», «Купина-384» і «Купина-512».

3 СТРУКТУРА ПЕРЕТВОРЕННЯ

Функція гешування, визначена в ДСТУ 7564:2014, формує геш-значення для повідомлення, що складається з бітової послідовності довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт.

При формуванні геш-значення повідомлення доповнюється (див. п.5), далі поділяється на l -бітні блоки m_0, \dots, m_t , після чого виконується обробка кожного блоку шляхом ітеративного виконання функції стиснення φ . При цьому формуються значення $h_i = \varphi(h_{i-1}, m_i)$, де $i = 1, \dots, t$, а початкове значення $h_0 = IV$. Після обробки останнього блоку повідомлення результуюче геш-значення обчислюється як

$$H(M) = \Omega(h_t),$$

де Ω – завершальне перетворення, що повертає n -бітне значення, кратне 8 ($0 < n \leq \frac{l}{2}$). Опис завершального перетворення Ω наведено у п.5.

На рис. 1 схематично представлено структуру перетворення повідомлення $M (m_0, \dots, m_t)$ при обчисленні геш-значення $H(M)$.

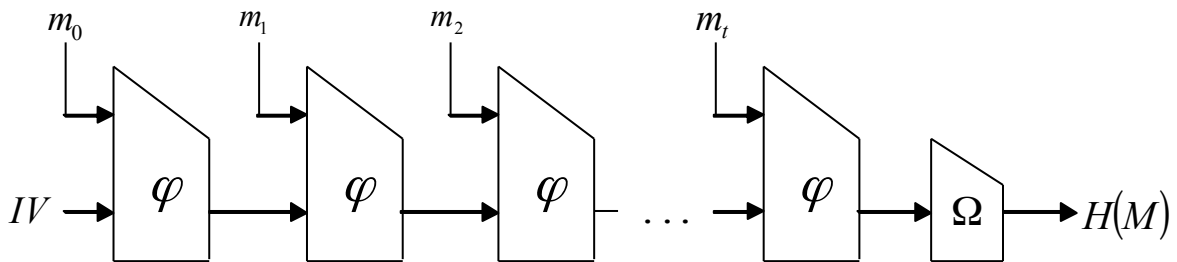


Рисунок 1 – Загальна структура функції гешування

4 ПАРАМЕТРИ АЛГОРИТМУ

Допустимі значення розміру l внутрішнього стану становлять 512 або 1024 біт відповідно для режимів функціонування «Купина-256» і «Купина-512».

Залежність розміру внутрішнього стану (l), кількості ітерацій (r), кількості стовпців внутрішнього стану (c) у матричному поданні та значення векторів ініціалізації від розміру геш-значення (n) наведено у таблиці 1.

Розмір вектору ініціалізації збігається із розміром внутрішнього стану.

Таблиця 1 – Залежність параметрів функції гешування від розміру геш-значення

Розмір геш-значення (n)	Розмір внутрішнього стану (l)	Кількість ітерацій (r)	Кількість стовпців в матриці (c)	Вектор ініціалізації (IV)
$8 \leq n \leq 256$	512	10	8	0x4000...00
$256 < n \leq 512$	1024	14	16	0x8000...00

5 ОСНОВНІ ПЕРЕТВОРЕННЯ

Функція стиснення φ складається з перетворень l -бітного блока P і Q та визначається наступним чином:

$$\varphi(h, m) = P(h \oplus m) \oplus Q(m) \oplus h.$$

Функцію стиснення φ наведено на рис. 2. Перетворення P і Q (відповідно, T_l^{\oplus} та T_l^+ в ДСТУ 7564:2014) описані у п.6.

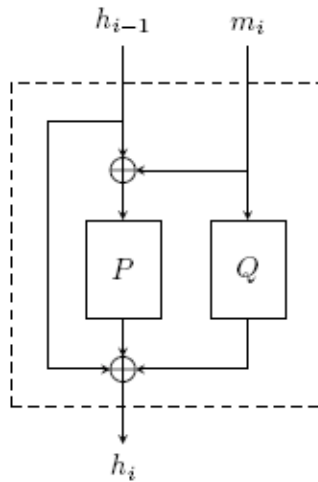


Рисунок 2 – Схема функції стиснення φ

Завершальне перетворення Ω визначається наступним чином:

$$\Omega(x) = \text{trunc}_n(P(x) \oplus x),$$

де $\text{trunc}_n(x)$ виконує відсікання всіх біт аргумента x крім останніх (старших) n біт. Завершальне перетворення Ω схематично представлено на рис. 3.

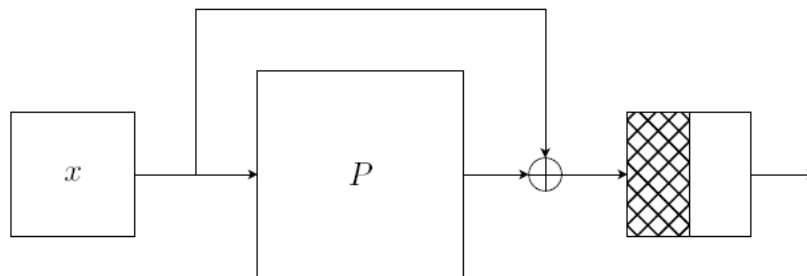


Рисунок 3 – Завершальне перетворення Ω

Доповнення повідомлення здійснюється наступним чином: на вхід функції гешування подається повідомлення (бітова послідовність) M довільної довжини N ($N < 2^{96}$), що задана у бітах. Кожне повідомлення доповнюється, незалежно від його довжини. У кінець повідомлення додається допоміжна інформація, яка містить одиничний біт, необхідну кількість нульових бітів (див. далі) та довжину повідомлення на вході функції гешування, таким чином, щоб доповнена бітова послідовність мала довжину, кратну розміру внутрішнього стану l .

При доповненні спочатку у кінець повідомлення додається одиничний біт «1», потім додаються w нульових бітів, де $w = (-N - 97) \bmod l$. Після цього додаються ще 96 біт, в яких записано значення N (найменш значущі байти мають менший номер, тобто використовується формат little endian; послідовність бітів усередині байту задається

відповідно до п.8.1, табл.2. Максимальна довжина повідомлення, що може бути оброблено, становить $2^{96} - 1$ біт.

6 ПЕРЕТВОРЕННЯ P ТА Q

Перед виконанням перетворень P і Q вхідна послідовність представляється як внутрішній стан функції гешування довжиною l біт ($l = 512$ або $l = 1024$ в залежності від розміру внутрішнього стану). Після завершення виконання перетворень P і Q внутрішній стан знову трансформується у послідовність байт, яка подається на вхід наступної ітерації функції стиснення φ або на завершальне перетворення для формування результуючого геш-значення.

У режимі гешування «Купина-256» вхідна послідовність байт позначається як $in_0, in_1, \dots, in_{63}$. Результуюча послідовність байт після оброблення позначається як $out_0, out_1, \dots, out_{63}$. Процес заповнення внутрішнього 512-бітного стану S функції гешування, перед початком перетворень та зворотній процес після їх завершення, наведено на рис. 4. Відображення 1024-бітної вхідної послідовності для режиму «Купина-512» у внутрішній стан функції гешування є аналогічним.

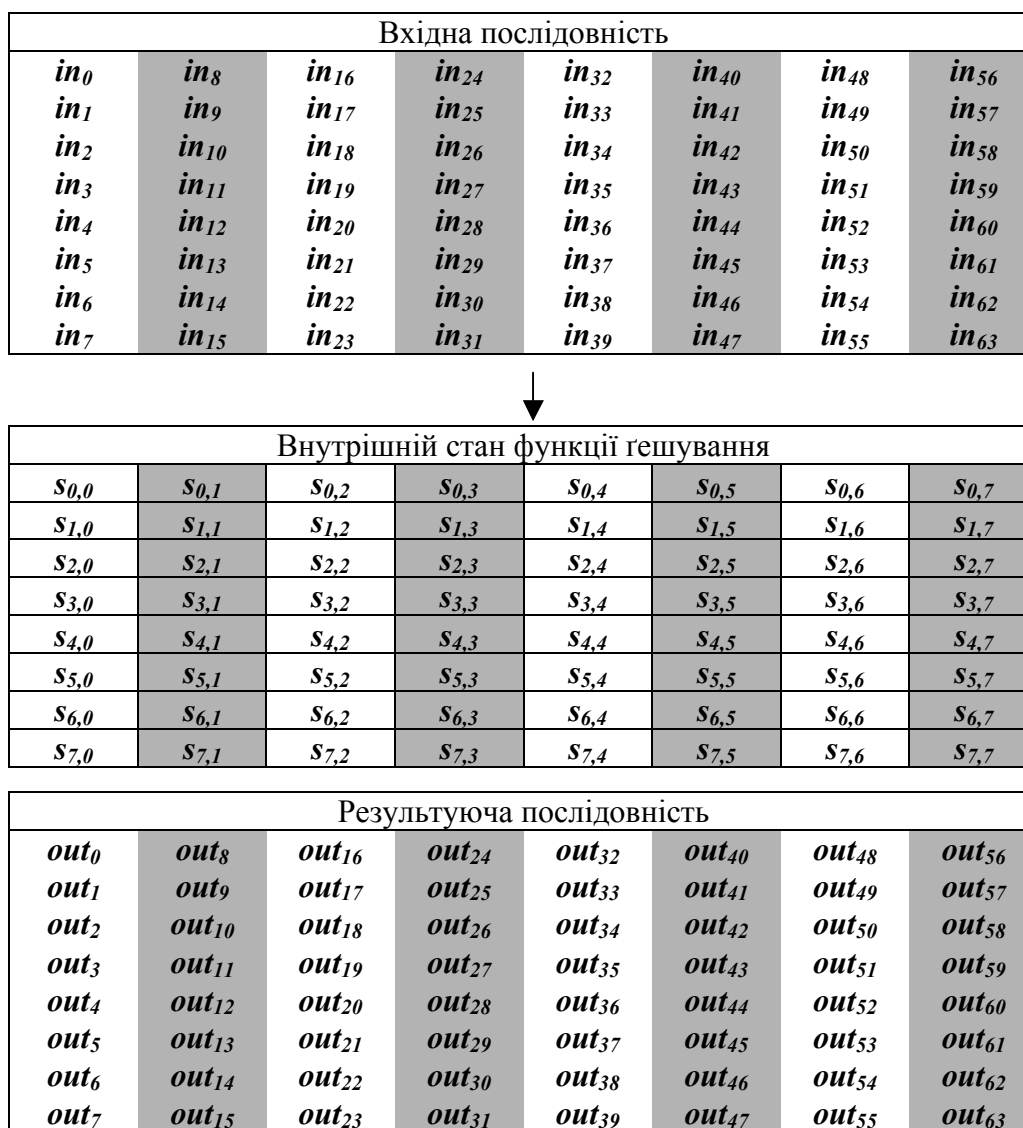


Рисунок 4 – Відповідність між послідовністю байт та внутрішнім станом функції гешування

Під час обчислення геш-значення внутрішній стан функції стиснення має розмір 512 або 1024 бітів. Для кожного варіанта розміру внутрішнього стану використовується власна пара перетворень: P_{512} , Q_{512} або P_{1024} , Q_{1024} .

Перетворення P і Q є варіантами блокового шифру, в яких замість циклових ключів використовуються визначені константи (див. нижче). Кількість циклів (r) залежить від розміру внутрішнього стану та визначена у п.4.

Перетворення P і Q задані наступним чином:

```
void P_Hash(byte in[ 8 * c ], byte out[ 8 * c ] ) {
    byte state[ 8, c ] = in

    for(round = 0 to r-1 step 1) {
        XORRoundKey( state, roundconstP[ round ] )
        Kalyna_S_boxes( state )
        KupynaShiftRows( state )
        MixColumns( state )
    }

    out = state
}

void Q_Hash(byte in[ 8 * c ], byte out[ 8 * c ] ) {
    byte state[ 8, c ] = in

    for(round = 0 to r-1 step 1) {
        Add64RoundKey( state, roundconstQ[ round ] )
        Kalyna_S_boxes( state )
        KupynaShiftRows( state )
        MixColumns( state )
    }

    out = state
}
```

Рисунок 5 – Перетворення P і Q

Операції XORRoundKey, Add64RoundKey, Kalyna_S_boxes, MixColumns співпадають із тими, що використовуються в блоковому шифрі „Калина” і визначені в ДСТУ 7624:2014 (відповідно як $\kappa_l^{(K_v)}$, $\eta_l^{(K_v)}$, π_l' і ψ_l).

Циклові константи roundconstP[round] і roundconstQ[round] (що формуються на основі значень $\omega_j^{(v)}$ та $\zeta_j^{(v)}$ з ДСТУ 7564:2014) залежно від номеру циклу перетворення round (i) та розміру внутрішнього стану (l) мають таке подання (у шістнадцятковому вигляді):

$$P_{512} : C^i = \begin{bmatrix} 00 \oplus i & 10 \oplus i & 20 \oplus i & 30 \oplus i & 40 \oplus i & 50 \oplus i & 60 \oplus i & 70 \oplus i \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{bmatrix} ;$$

$$Q_{512} : C^i = \begin{bmatrix} f3 & f3 & f3 & f3 & f3 & f3 & f3 & f3 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & f0 & f0 \\ 70 \oplus i & 60 \oplus i & 50 \oplus i & 40 \oplus i & 30 \oplus i & 20 \oplus i & 10 \oplus i & 00 \oplus i \end{bmatrix} ;$$

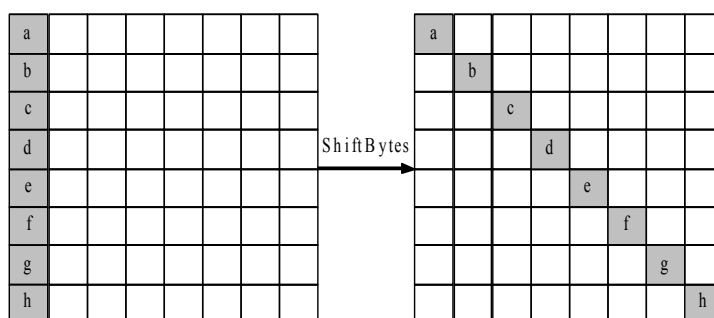
$$P_{1024} : C^i = \begin{bmatrix} 00 \oplus i & 10 \oplus i & 20 \oplus i & 30 \oplus i & 40 \oplus i & 50 \oplus i & \dots & f0 \oplus i \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \dots & 00 \end{bmatrix} ;$$

$$Q_{1024} : C^i = \begin{bmatrix} f3 & f3 & f3 & f3 & f3 & f3 & \dots & f3 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 & f0 & f0 & f0 & f0 & f0 & \dots & f0 \\ f0 \oplus i & e0 \oplus i & d0 \oplus i & c0 \oplus i & b0 \oplus i & a0 \oplus i & \dots & 00 \oplus i \end{bmatrix} .$$

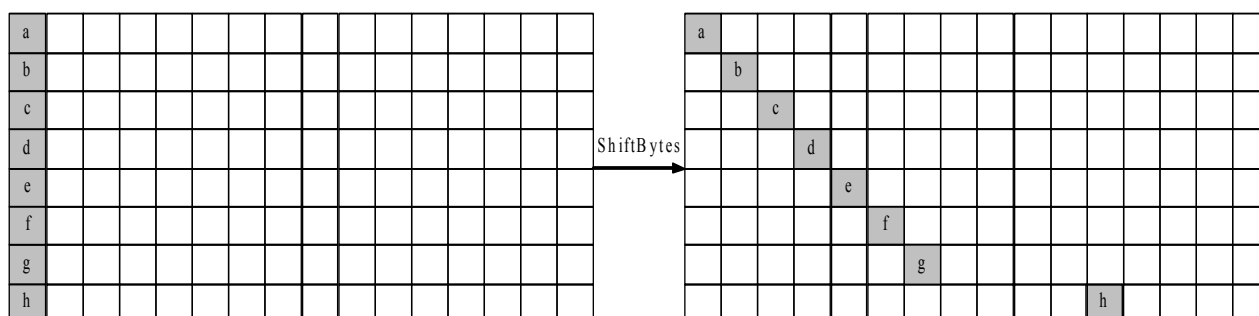
Перетворення `КурнаShiftRows` (функція $\tau^{(l)}$ в ДСТУ 7564:2014) виконує розподілення байтів кожного 64-бітного стовбця серед інших стовпців шляхом циклічного зсуву рядків внутрішнього стану вправо на різну кількість байт. Значення зсувів залежать від розміру внутрішнього стану функції гешування та представлені у табл. 2. Схему перетворення `КурнаShiftRows` для різних розмірів внутрішнього стану представлено на рис. 6.

Таблиця 2 – Значення циклічних зсувів рядків залежно від розміру внутрішнього стану

Номер рядка	Значення зсуву байт	
	Внутрішній стан 512 біт	Внутрішній стан 1024 біти
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	11



а) 512-бітний внутрішній стан



б) 1024-бітний внутрішній стан

Рисунок 6 – Порядок розподілення байт першого стовбця під час виконання `CurynaShiftRows`

ВИСНОВКИ

„Купина” є криптографічною функцією гешування, що визначена у національному стандарті України ДСТУ 7564:2014. Перетворення підтримує обчислення геш-значення з довжинами від 8 до 512 біт із кроком 8 біт. Основними режимами роботи функції гешування, що рекомендуються до застосування, є «Купина-256», «Купина-384» і «Купина-512».

Геш-функція базується на новому блоковому шифрі „Калина” (ДСТУ 7624:2014) і розроблена на основі консервативного підходу із залученням відомих і добре досліджених конструкцій.

Розгорнутий альтернативний опис функції гешування „Купина”, наведений у статті, відповідає визначеному в ДСТУ 7564:2014, але використовує інші позначення, традиційні для галузі комп’ютерних наук.

Список літератури: 1. ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хэширования. – Введ. 01–01–1995. – М., 1994. – 20 с. 2. Mendel Florian, Pramstaller Norbert, Rechberger Christian, et.al. Cryptanalysis of GOST hash function. Advances in Cryptology – CRYPTO 2008. Springer, 2008: 162-178. 3. СТБ 34.101.31–2011. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности [Текст]. – Взамен СТБ П 34.101.31–2007 ; введ. 31–01–2011. – Минск, 2011. – 35 с. 4. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Текст]. – Взамен ГОСТ Р 34.11–94 ; введ. 01–01–2013. – М.: Стандартинформ, 2012. 5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015. 6. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. [Текст]. – Введ. 01–04–2015. – К. : Мінекономрозвитку України, 2015.

Харьковский национальный университет радиоэлектроники

Поступило в редколлегию

УДК 621.3.06

Функция хэширования «Купина» – новый национальный стандарт Украины / *Р.В. Олейников, И.Д. Горбенко, А.В. Казимиров, В.И. Руженцев, А.А. Кузнецов, Ю.И. Горбенко, О.В. Дырда, А.А. Бойко, В.И. Долгов, А.И. Пушкарёв, В.Н. Казиминова, Р.И. Киянчук*

В статье приведено развернутое альтернативное описание криптографической функции хэширования «Купина» из нового национального стандарта Украины ДСТУ 7564:2014. Используемые в описании обозначения, традиционные для компьютерных наук, упрощают восприятие сущности криптографического преобразования для широкого круга специалистов в области информационных технологий.

Табл. 2. Рис. 6. Библиогр.: 6 назв.

УДК 621.3.06

Функція гешування „Купина” – новий національний стандарт України / *Р.В. Олійников, І.Д. Горбенко, О.В. Казимиров, В.І. Руженцев, О.О. Кузнєцов, Ю.І. Горбенко, О.В. Дирда, А.О. Бойко, В.І. Долгов, А.І. Пушкарёв, В.М. Казимирова, Р.І. Кіянкчук*

У статті наведений розгорнутий альтернативний опис криптографічної функції гешування „Купина” із нового національного стандарту України ДСТУ 7564:2014. Позначення, застосовані в описі, традиційні для комп’ютерних наук, спрощують сприйняття сутності криптографічного перетворення для широкого кола фахівців у галузі інформаційних технологій.

Табл. 2. Рис. 6. Бібліогр.: 6 назв.

UDC 621.3.06

The “Kupyna” hash function – the new Ukrainian national standard / *R. Oliyynkov, I. Gorbenko, O. Kazymyrov, V. Ruzhentzev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, A. Boiko, V. Dolgov, A. Pushkaryov, V. Kazymyrova, R. Kiyanchuk*

A detailed alternative description of the Kupyna hash function specified in the new Ukrainian national standard DSTU 7564:2014 is given in the article. Notations used in the description are traditional for computer science and simplify understanding of the cryptographic transformation for IT-specialists.

2 Tab. 6 Fig. Ref.: 6 items.