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. ПУШКАРЬОВ, В.М.КАЗИМИРОВА, Р.І.КІЯНЧУК

ФУНКЦІЯ ҐЕШУВАННЯ „КУПИНА” – НОВИЙ НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Вступ

У якості основної криптографічної функції ґешування в Україні майже двадцять 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 ґеш-функція, що базується на новому блоковому шифрі „Калина” (ДСТУ 7624:2014 [5]). Новий національний стандарт ДСТУ 7564:2014 [6] визначає криптографічну функцію ґешування „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 статті наводиться розгорнутий альтернативний опис функції ґешування „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 ґеш-значення.
Внутрішній стан	– бітова послідовність фіксованої довжини (512 або 1024 біта), що є проміжним значенням на кожній ітерації перетворення функції ґешування, а також вхідним та вихідним значеннями перетворень P і Q; для цих перетворень внутрішній стан подається як матриця розміром $8 \times c$ байт.
Ґеш-значення (ґеш-вектор)	– бітова послідовність фіксованої довжини ($n = 8 \cdot s,\ s \in \{1,2,...,64\}$), що є результатом роботи функції ґешування.
Доповнення	– вставка додаткових біт у кінець повідомлення для отримання кратності довжини бітової послідовності довжині внутрішнього стану функції ґешування.
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 ґешування;
$H(M)$	– результат обчислення функції ґешування для повідомлення M (ґеш-значення);
IV	– вектор ініціалізації;
l	– розмір внутрішнього стану функції ґешування (у бітах), $l \in \{512, 1024\}$;
M	– повідомлення;
m_i	– i-й блок повідомлення M;
n	– довжина обчисленого ґеш-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 ґеш-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 ґешування з усіченням обчисленого ґеш-значення до розміру n біт.

2. Загальні положення

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

ДСТУ 7564:2014 визначає функцію ґешування, яка виконує перетворення «Купина-256» або «Купина-512», що забезпечують обчислення ґеш-значення з довжинами 256 або 512 біт відповідно. Ґеш-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 ґеш-значення довжиною n біт позначається як «Купина- n».

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

3.Структура перетворення

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

При формуванні ґеш-значення повідомлення доповнюється (див. п.5), далі поділяється на l-бітні блоки $m_0,\ldots,m_t$, 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 $i=1,\ldots,t$, а початкове значення $h_0=IV$. Після обробки останнього блоку повідомлення
результуюче ґеш-значення обчислюється як

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

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

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

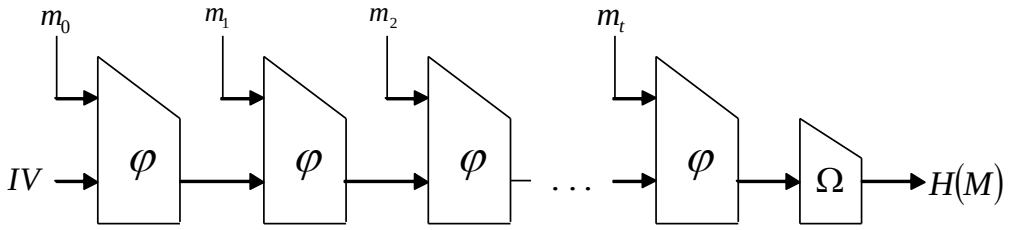


Рис. 1. Загальна структура функції ґешування

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 ґеш-значення n наведено у табл. 1.

Розмір вектору ініціалізації збігається із розміром внутрішнього стану.

Таблиця 1

Залежність параметрів функції ґешування від розміру ґеш-значення

Розмір ґеш-значення n	Розмір внутрішнього стану l	Кількість ітерацій r	Кількість стовпців в матриці c	Вектор ініціалізації (*IV*)
$8\le n\le 256$	512	10	8	0x4000…00
$256<n\le 512$	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.

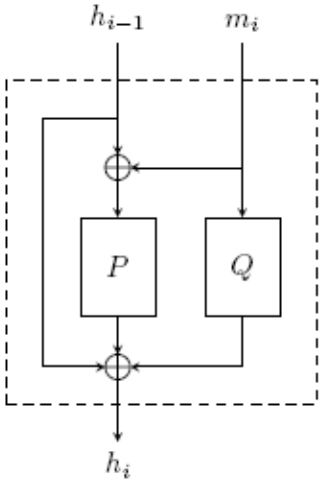


Рис. 2. Схема функції стиснення φ

Завершальне перетворення Ω визначається наступним чином:

$$\Omega(x) = trunc_n(P(x) \oplus x),$$

де $trunc_n(x)$ виконує відсікання всіх біт аргумента x крім останніх (старших) n біт. Завершальне перетворення Ω схематично представлено на рис. 3.

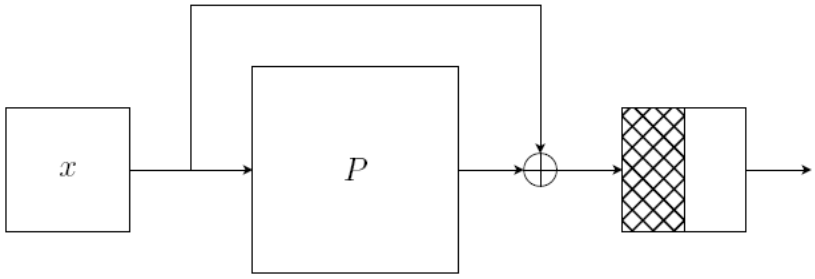


Рис. 3. Завершальне перетворення Ω

Доповнення повідомлення здійснюється наступним чином: на вхід функції ґешування 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 ґешування, 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 ґешування 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 ґеш-значення.

У режимі ґешування «Купина-256» вхідна послідовність байт позначається як $in_0, in_1, \ldots, in_{63}$. Результуюча послідовність байт після оброблення позначається як $out_0, out_1, \ldots, out_{63}$. Процес заповнення внутрішнього 512-бітного стану S функції ґешування, 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 ґешування є аналогічним.

Вхідна послідовність							
in_0	in_8	in_{16}	in_{24}	in_{32}	in_{40}	in_{48}	in_{56}
in_1	in_9	in_{17}	in_{25}	in_{33}	in_{41}	in_{49}	in_{57}
in_2	in_{10}	in_{18}	in_{26}	in_{34}	in_{42}	in_{50}	in_{58}
in_3	in_{11}	in_{19}	in_{27}	in_{35}	in_{43}	in_{51}	in_{59}
in_4	in_{12}	in_{20}	in_{28}	in_{36}	in_{44}	in_{52}	in_{60}
in_5	in_{13}	in_{21}	in_{29}	in_{37}	in_{45}	in_{53}	in_{61}
in_6	in_{14}	in_{22}	in_{30}	in_{38}	in_{46}	in_{54}	in_{62}
in_7	in_{15}	in_{23}	in_{31}	in_{39}	in_{47}	in_{55}	in_{63}

↓

Внутрішній стан функції ґешування							
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$	$s_{0,4}$	$s_{0,5}$	$s_{0,6}$	$s_{0,7}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,4}$	$s_{1,5}$	$s_{1,6}$	$s_{1,7}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$	$s_{2,4}$	$s_{2,5}$	$s_{2,6}$	$s_{2,7}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$	$s_{3,4}$	$s_{3,5}$	$s_{3,6}$	$s_{3,7}$
$s_{4,0}$	$s_{4,1}$	$s_{4,2}$	$s_{4,3}$	$s_{4,4}$	$s_{4,5}$	$s_{4,6}$	$s_{4,7}$
$s_{5,0}$	$s_{5,1}$	$s_{5,2}$	$s_{5,3}$	$s_{5,4}$	$s_{5,5}$	$s_{5,6}$	$s_{5,7}$
$s_{6,0}$	$s_{6,1}$	$s_{6,2}$	$s_{6,3}$	$s_{6,4}$	$s_{6,5}$	$s_{6,6}$	$s_{6,7}$
$s_{7,0}$	$s_{7,1}$	$s_{7,2}$	$s_{7,3}$	$s_{7,4}$	$s_{7,5}$	$s_{7,6}$	$s_{7,7}$

↓

Результуюча послідовність							
out_0	out_8	out_{16}	out_{24}	out_{32}	out_{40}	out_{48}	out_{56}
out_1	out_9	out_{17}	out_{25}	out_{33}	out_{41}	out_{49}	out_{57}
out_2	out_{10}	out_{18}	out_{26}	out_{34}	out_{42}	out_{50}	out_{58}
out_3	out_{11}	out_{19}	out_{27}	out_{35}	out_{43}	out_{51}	out_{59}
out_4	out_{12}	out_{20}	out_{28}	out_{36}	out_{44}	out_{52}	out_{60}
out_5	out_{13}	out_{21}	out_{29}	out_{37}	out_{45}	out_{53}	out_{61}
out_6	out_{14}	out_{22}	out_{30}	out_{38}	out_{46}	out_{54}	out_{62}
out_7	out_{15}	out_{23}	out_{31}	out_{39}	out_{47}	out_{55}	out_{63}

Рис. 4. Відповідність між послідовністю байт та внутрішнім станом функції ґешування

Під час обчислення ґеш-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
}
```

Рис. 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 $\varsigma_j^{(v)}$ з ДСТУ 7564:2014) залежно від номеру циклу перетворення round (i) та розміру внутрішнього стану (l) мають таке подання (у шістнадцятковому вигляді):

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

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

$$P_{1024}:\quad C^i=\begin{bmatrix} 00\oplus i & 10\oplus i & 20\oplus i & 30\oplus i & 40\oplus i & 50\oplus i & \ldots & \mathrm{f}0\oplus i \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & \ldots & 00 \end{bmatrix};$$

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

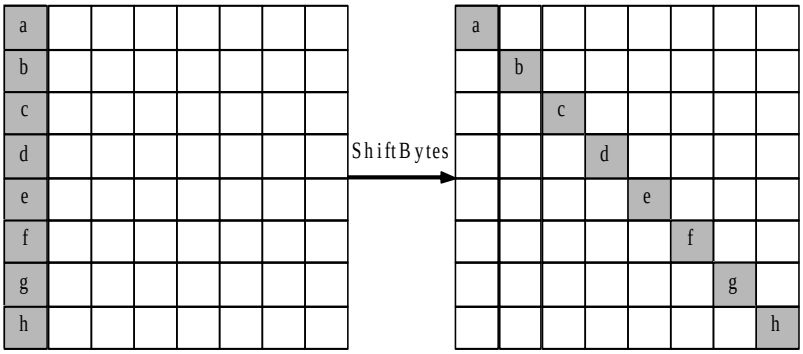
Перетворення `KupynaShiftRows` (функція $\tau^{(l)}$ в ДСТУ 7564:2014) виконує розподілення байтів кожного 64-бітного стовбця серед інших стовпців шляхом циклічного зсуву рядків внутрішнього стану вправо на різну кількість байт. Значення зсувів залежать від розміру внутрішнього стану функції гешування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

Таблиця 2

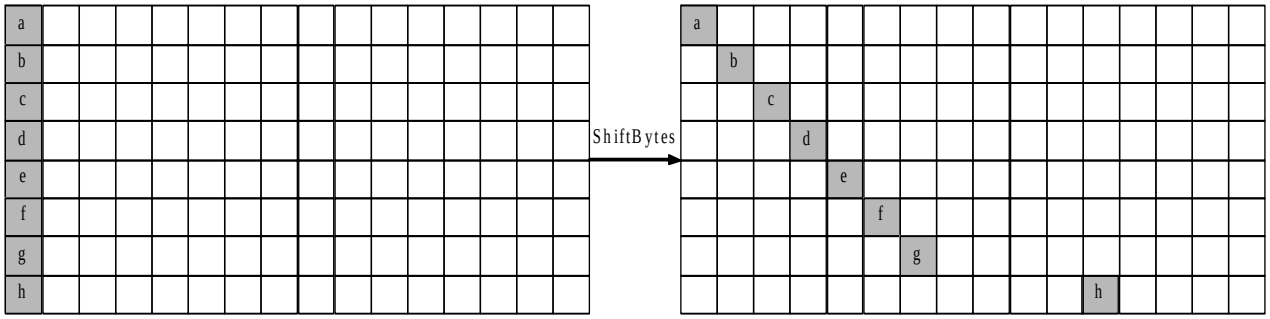
Значення циклічних зсувів рядків залежно від розміру внутрішнього стану

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

Рис. 6. Порядок розподілення байт першого стовбця під час виконання `KupynaShiftRows`

Висновки

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

Ґеш-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 ґешування „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. – 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. – 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. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015. 6. *ДСТУ 7564:2014*. Інформаційні технології. Криптографічний захист інформації. Функція ґешування. – Введ. 01–04–2015. – К. : Мінекономрозвитку України, 2015.

Харківський національний