УДК 621. 391:519.2:519.7

МЕТОДИКА І РЕЗУЛЬТАТИ ПОРІВНЯННЯ АЛГОРИТМІВ ГЕШ-ФУНКЦІЙ, ЩО ПРИЙМАЮТЬ УЧАСТЬ У 3-МУ РАУНДІ КОНКУРСУ NIST SHA-3

А.О. БОЙКО, І.Д. ГОРБЕНКО, С.І. ДАЦЕНКО

Запропоновані критерії та показники оцінки перспективних функцій гешування, обгрунтовано та розроблено формальну методику їх порівняння.

Ключові слова: порівняння геш-функцій, формалізована методика порівняння, геш-функція, конкурс NIST SHA-3.

Однією з найважливіших і, в той же час недостатньо вирішених, є задача порівняння різних алгоритмів геш-функцій при різних розмірах параметрів і обмеженнях. Ця задача є актуальною через те, що зараз відбувається третій раунд конкурсу NIST SHA-3 Competition, у якому досліджуються 5 геш-функцій, які є кандидатами на внесення до стандарту США у 2012 році.

Як вже неодноразово зазначалось, український стандарт гешування ГОСТ 34.311-95 є морально застарілим, і на нього знайдено декілька атак [1, 2]. Тому доцільно розглянути, вивчити і порівняти ці 5 геш-функцій, щоб обрати серед них кандидата на гармонізацію в Україні. Переваги такого підходу:

- в ході NIST SHA-3 Competition ці геш-функції були детально проаналізовані світовим криптографічним товариством, що забезпечує високий рівень довіри до них;
- за умовами конкурсу геш-функції не можуть бути обтяжені патентами, а отже можуть бути вільно використані в Україні.

На основі попередніх досліджень [3] можна зробити висновок, що порівняння геш-функцій можна проводити з використанням двох типів критеріїв: безумовних і умовних.

До безумовних критеріїв відносяться ті, виконання яких для геш-функцій є обов'язковим, а саме критерії стійкості до:

знаходження колізії;

знаходження прообразу;

знаходження другого прообразу;

відрізнення геш-функції від випадкової функції;

розкриття змісту повідомлення, що підлягає гешуванню, шляхом аналізу побічних каналів.

Критерію стійкості до знаходження прообразу не відповідає алгоритм JH. Алгоритми Skein, Blake, Keccak, Grostl відповідають вимогам безумовних критеріїв. Саме їх і буде розглянуто далі.

Через те, що безумовним критеріям відповідають усі 4 алгоритми, то неможливо визначити переваги одного з алгоритмів над іншими. Тому далі необхідно керуватись умовними критеріями при виборі.

Для порівняння алгоритмів геш-функцій пропонується використати наступні умовні критерії:

1) швидкодія x86;

2) швидкодія x86_64;

3) швидкодія ARM;

4) швидкодія AVR Atmel;

5) кількість RAM AVR Atmel;

6) кількість ROM AVR Atmel;

7) швидкодія FPFA;

8) розмір FPFA;

9) максимально досяжний коефіцієнт прискорення при використанні паралельних обчислень;

10) відношення максимального числа раундів, на які знайдено атаки коллізії, прообразу, другого прообразу до загального числа раундів;

11) відношення максимального числа раундів, на які знайдено псевдо- і близькі атаки, а також відрізнювачі, до загального числа раундів.

Через те, що в процесі порівняння через останні два показника виникає ситуація ділення на нуль, пропонується замість них використати обернені показники, які обчислюються як $1-\frac{r_{vun}}{r_{all}}$, де r_{vun} – кількість успішно атакованих раундів, r_{all} – загальна кількість раундів. Таким чином, ці два показники показують частку раундів, які ще залишилось пройти криптоаналітикам, щоб зламати геш-функцію. Чим більше це значення, тим кращі перспективи у геш-функції в плані стійкості.

Умовні критерії були розбиті на наступні групи:

- критерії, пов'язані з програмною реалізацією (критерії 1-3);
- критерії пов'язані з програмно-апаратною реалізацією на обчислювальних пристроях з обмеженими ресурсами (критерії 4-6);
- критерії апаратної реалізації (критерії 7,8);
- критерій гнучкості паралельних обчислень (критерій 9);
- критерії для оцінки перспектив збереження стійкості (критерії 10,11).

Порівняння алгоритмів проводитимемо методом визначення вагових коефіцієнтів на основі функції втрати ефективності систем. Цей метод вже був успішно використаний пр порівнянні ЕЦП [4]. Всі відомі попередні методи порівняння геш-функцій базувались на основі експертних оцінок. Це вносило певний елемент суб'єктивності в результати оцінювання. Тому в цій роботі зап-

ропоновано використовувати метод порівняння, який не використовує експертних оцінок в якості вхідних даних, а замість них використовує лише числові показники алгоритмів геш-функцій. Таким чином, значно підвищується точність отриманих на виході результатів.

Далі наведено опис метода визначення вагових коефіцієнтів на основі функції втрати ефективності систем, як запропоновано у [5].

Нехай існує K систем $S^{(1)},S^{(2)},...,S^{(k)}$, які необхідно порівняти. Кожна з цих систем може бути охарактеризована певним набором параметрів $A=\{\alpha_1,\alpha_2,...,\alpha_n\}$. Для кожної з систем кожний з параметрів $\alpha_i, i=\overline{1,n}$ та $\alpha_i \in A$ може приймати певне значення, тобто:

$$S^{(1)} \to A^{(1)} = \left\{\alpha_{1}^{(1)},\alpha_{1}^{(1)}_{2},...,\alpha_{n}^{(1)}\right\}$$

.

.

$$S^{(k)} \to A^{(k)} = \left\{\alpha_{1}^{(k)},\alpha_{1}^{(k)}_{2},...,\alpha_{n}^{(k)}\right\}$$

Порівняння систем здійснюється шляхом розрахунку і подальшого порівняння часткових і загальносистемних показників.

Часткові показники характеризують ефективність системи з точки зору деякої функціональної задачі. Частковий показник має вигляд

$$\gamma_j = \sum_{i=1}^{l_j} \rho_{ij}\eta_{ij}^{(k)}, \qquad (1)$$

де ρ_{ij} – ваговий коефіцієнт параметра в групі параметрів, які характеризують j – у функціональну задачу; $\eta_{ij}^{(k)}$ – формування значення параметра k-ої системи.

Узагальнена оцінка системи визначається як

$$\Gamma^{(k)} = \sum_{i=1}^{l_j} \beta_j\gamma_j^{(k)}, \qquad (2)$$

де β_j – ваговий коефіцієнт часткового показника (по суті функціональної задачі); $\gamma_j^{(k)}$ – значення часткового показника для k-ої системи.

Розглянутий метод дозволяє визначити:

– нормовані значення параметрів системи η_{ij};

– вагові коефіцієнти параметрів ρ_{ij};

– вагові коефіцієнти функціональних задач β_j без залучення експертів і, в результаті, обчислити узагальнений системний показник.

Отже, розглянемо порядок розрахунків вагових коефіцієнтів і узагальненого системного показника.

1. Вихідна множина параметрів A підлягає аналізу і розбивається на групи, які характеризують виконання окремих функціональних задач. Для проведення аналізу можна використати різні методи декомпозиції. За результатами аналізу отримаємо наступну таблицю (табл. 1):

Таким чином вихідна множина розбита на j груп і в кожній групі є по i параметрів.

Таблиця 1

Групи параметрів

№ групи j	№ параметра в групі i	$\alpha_{ij}^{(1)}$	$\alpha_{ij}^{(2)}$	...	$\alpha_{ij}^{(k)}$	$\alpha_{ij\max}$	$\alpha_{ij\min}$
1	1	$\alpha_{11}^{(1)}$	$\alpha_{11}^{(2)}$	...	$\alpha_{11}^{(k)}$	$\max\limits_k \alpha_{11}^{(k)}$	$\min\limits_k \alpha_{11}^{(k)}$
	2	$\alpha_{21}^{(1)}$	$\alpha_{21}^{(2)}$	...	$\alpha_{21}^{(k)}$	$\max\limits_k \alpha_{21}^{(k)}$	$\min\limits_k \alpha_{21}^{(k)}$
	3	$\alpha_{31}^{(1)}$	$\alpha_{31}^{(2)}$	...	$\alpha_{31}^{(k)}$	$\max\limits_k \alpha_{31}^{(k)}$	$\min\limits_k \alpha_{31}^{(k)}$
2	1	$\alpha_{12}^{(1)}$	$\alpha_{12}^{(2)}$	...	$\alpha_{12}^{(k)}$	$\max\limits_k \alpha_{12}^{(k)}$	$\min\limits_k \alpha_{12}^{(k)}$
	2	$\alpha_{22}^{(1)}$	$\alpha_{22}^{(2)}$	...	$\alpha_{22}^{(k)}$	$\max\limits_k \alpha_{22}^{(k)}$	$\min\limits_k \alpha_{22}^{(k)}$
	...	...	...	...	...	...	...
	I_j	$\alpha_{I_j2}^{(1)}$	$\alpha_{I_j2}^{(2)}$	...	$\alpha_{I_j2}^{(k)}$	$\max\limits_k \alpha_{I_j2}^{(k)}$	$\min\limits_k \alpha_{I_j2}^{(k)}$
...	...	...	...	...	...	...	...
J	1	$\alpha_{1J}^{(1)}$	$\alpha_{1J}^{(2)}$	...	$\alpha_{1J}^{(k)}$	$\max\limits_k \alpha_{1J}^{(k)}$	$\min\limits_k \alpha_{1J}^{(k)}$
	2	$\alpha_{2J}^{(1)}$	$\alpha_{2J}^{(2)}$	...	$\alpha_{2J}^{(k)}$	$\max\limits_k \alpha_{2J}^{(k)}$	$\min\limits_k \alpha_{2J}^{(k)}$

2. В кожній групі параметрів визначається підвищуючі і понижуючі параметри.

Підвищуючім параметром $\alpha_{ij\max}$ називається параметр? підвищення значення якого призводить до підвищення ефективності системи (чим більше, тим краще). Понижуючим називається параметр $\alpha_{ij\min}$, підвищення значення якого погіршує властивості системи.

Для кожного підвищуючого параметра обчислюється

$$\alpha_{ij\max} = \max_k \alpha_{ij}^{(k)}. \qquad (3)$$

Аналогічно для понижуючих параметрів

$$\alpha_{ij\min} = \min_k \alpha_{ij}^{(k)}. \qquad (4)$$

Отримані дані заносяться в останній стовпчик таблиці 1.

3. Визначаються нормовані значення параметрів. Як видно з виразу (1) для визначення часткового показника необхідно згорнути всі значення параметрів. Однак в явному вигляді цього робити неможна, тому що параметри мають різний фізичний зміст і розмірність. Частковий показник γ_j величина безрозмірна. Саме по цій величині проводиться нормування параметрів.

Нормування параметрів виконується у відповідності з виразом:

$$\eta_{ij}^{(k)} = \begin{cases} \dfrac{\alpha_{ij}^{(k)}}{\alpha_{ij\max}} \text{ для підвищуючих,} \\ \dfrac{\alpha_{ij\min}}{\alpha_{ij}^{(k)}} \text{ для понижуючих.} \end{cases} \qquad (5)$$

Результати нормування заносяться в табл. 2.

Таблиця 2

Результати нормування параметрів

№ групи (j)	№ параметра (i)	$\eta_{ij}^{(1)}$	$\eta_{ij}^{(2)}$	$\eta_{ij}^{(3)}$	$\overline{\eta}_{ij}$	$\Delta\overline{\eta}_{ij}$	d_{ij}	ρ_{ij}
1	1	...	...	...	...	…	…	…
	2	...	...	...	...	…	…	…
2	1	...	...	...	...	…	…	…
	2	...	...	...	...	…	…	…
	...	...	...	...	...	…	…	…
	I_j	...	...	...	...	…	…	…
...	...	...	...	...	...	…	…	…
J	1	...	...	...	...	…	…	…
	2	...	...	...	...	…	…	…

Далі необхідно виконати обробку значень, наведених в таблиці 2.

4. Визначається середнє значення кожного з нормованих параметрів:

$$\overline{\overline{\eta_{ij}}} = \frac{1}{m}\sum_{k=1}^{m}\eta_{ij}^{(k)}, \qquad (6)$$

де m – кількість порівнюваних систем $k = \overline{1,m}$.

5. Розраховується середнє значення розбіжності кожного нормованого параметра

$$\Delta\overline{\eta_{ij}} = \frac{1}{m}\sum_{k=1}^{m}|\eta_{ij}^{(k)} - \overline{\eta_{ij}}|. \qquad (7)$$

Величина (7) характеризує відхилення параметрів систем от від середнього значення.

6. Розраховується нормоване значення розбіжності

$$d_{ij} = \frac{\Delta\overline{\eta_{ij}}}{\overline{\overline{\eta_{ij}}}}. \qquad (8)$$

7. Розраховується нормоване значення вагових коефіцієнтів по кожній групі параметрів

$$\rho_{ij} = \frac{d_{ij}}{\sum_{i=1}^{l_j} d_{ij}}, \qquad (9)$$

де l_j – кількість параметрів в j-тій групі.

Таким чином, ми визначили вагові коефіцієнти параметрів. Фізичний зміст коефіцієнта полягає в тому, що його значення залежить від розбіжності параметрів. Тобто, якщо значення одного і того ж параметра для різних систем має значну розбіжність, тоді цей параметр отримує більшу вагу при порівнянні систем. Навпаки, якщо значення параметра для усіх систем однакове, то цей параметр отримує нульову вагу, оскільки для порівняння систем він не важливий.

8. Розраховується значення часткових показників ефективності по кожній групі параметрів

$$\gamma_j^{(k)} = \sum_{i=1}^{l_j}\rho_{ij}\eta_{ij}^{(k)}.$$

Отримані результати можна звести до табл. 3

Таблиця 3

Часткові показники порівнюваних систем

№ групи	№ порівнюваної системи			
	$S^{(1)}$	$S^{(2)}$	...	$S^{(k)}$
1	$\gamma_1^{(1)}$	$\gamma_1^{(2)}$	...	$\gamma_1^{(k)}$
2	$\gamma_2^{(1)}$	$\gamma_2^{(2)}$	...	$\gamma_2^{(k)}$
...	...	...	...	...
j	$\gamma_j^{(1)}$	$\gamma_j^{(2)}$	...	$\gamma_j^{(k)}$

Таким чином, ми отримали часткові показники ефективності.

Повернемося до виразу (2). Для розрахунку загальносистемного показника необхідно розрахувати вагові коефіцієнти β_j кожної функціональної задачі, яка характеризується певним власним набором параметрів.

Для кількісної оцінки умов порівняння систем введемо функцію втрат ефективності k-тої системи

$$\theta^{(k)} = 1 - \frac{\Gamma^{(k)}}{\max_{\beta}\Gamma^{(k)}}. \qquad (10)$$

функція (10) характеризує ступінь наближення ефективності системи даних β до максимально можливої при любих значеннях β.

Шляхом обчислення розбіжності функцій втрат ефективності можна проводити дослідження допустимих областей значень вагових коефіцієнтів на основі функції (10). Для цього для кожної фіксованої сукупності значень вагових коефіцієнтів можна знайти максимальне та мінімальне значення функції втрат ефективності і побудована функція $\rho(B)$ вигляду

$$\rho(B) = \max_k\theta^{(k)} - \min_k\theta^{(k)}, \qquad (11)$$

причому $B_j = \{\beta\}\setminus\beta_j$.

Функція (11) характеризує величину максимальної розбіжності. З (11) можна визначити діапазон вагових коефіцієнтів, при якому розбіжність втрат ефективності систем (або розбіжність загальносистемних показників) не перевищуватиме деякої величини або прийме мінімальне значення.

Розглянемо методику розрахунку вагових коефіцієнтів.

Нехай маємо j груп параметрів. Розрахуємо вагові коефіцієнти для кожної групи параметрів, за умови наявності значень γ_j.

Обчислимо вагові коефіцієнти для першої групи параметрів. Для цього β_1 змінюватимемо з деяким кроком в межах від 0,1 до 0,9 при дотриманні умови нормування

$$\sum_{i=1}^{l}\beta_i = 1. \qquad (12)$$

де l – число груп параметрів.

Для кожного набору β визначимо значення

загальносистемних показників усіх систем відповідно до виразу

$$\Gamma^{(k)} = \sum_{j=1}^{l} \beta_j \gamma_j^{(k)} . \qquad (13)$$

Після цього розрахуємо значення $\theta^{(k)}$ за формулою (10) та значення $\rho(B_j)$, за формулою (11). Побудуємо графіки розбіжності значень $\rho(B_j)$

Знайдемо значення β_1, при якому функція $\rho(B_1)$ приймає мінімальне значення. Отримане значення β_1 приймається в якості вагового коефіцієнта. Аналогічно поступимо для $\beta_2,...,\beta_j$.

Для остаточного визначення коефіцієнтів слід їх пронормувати, щоб вони задовольняли умові (12). Для цього обчислимо

$$\hat{\beta}_j = \frac{\beta_j}{\sum_{j=1}^{l} \beta_j} . \qquad (14)$$

Значення загальносистемних показників визначаються як

$$\hat{\Gamma}^{(k)} = \sum_{j=1}^{l} \hat{\beta}_j \gamma_j^{(k)} . \qquad (15)$$

Найкращою вважається система, для якої

$$\Gamma_{opt} = \max_k \hat{\Gamma}^{(k)} . \qquad (16)$$

Вихідні дані для порівняння зібрані з сайтів [7-11], присвячений проекту NIST SHA-3 Competition.

Дані зібрані для варіантів з довжиною геш-значення 256 бітів. Геш-функція JH не відповідає безумовним критеріям, тому у табл. 4 не представлена.

Для аналізу обрано саме 256-бітні варіанти, тому що головною метою порівняння було визначити потенційну заміну для ГОСТ 34.311-95.

Результати порівняння за описаним вище методом наведені у табл. 5.

Перевагу Skein забезпечила наявність режиму паралельних обчислень. По іншим параметрам він був приблизно на одному рівні із Blake, а по деяким помітно поступався.

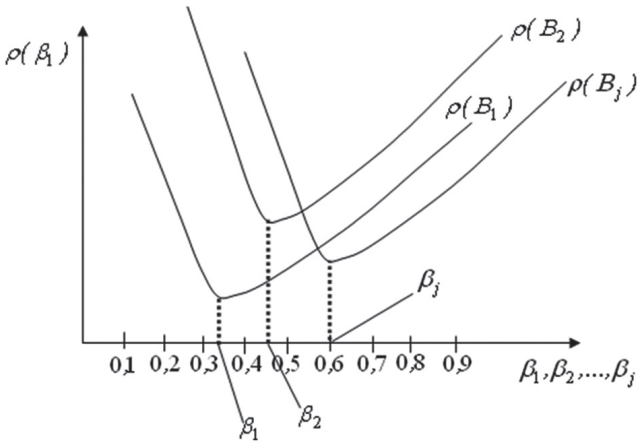

Рис. 1. Графіки функцій $\rho(B_j)$

Таблиця 5

Геш-функція	Значення узагальненого показника (більше-краще)
Skein	3,65
Blake	3,23
Keccak	3,00
Grшstl	2,94

Дані зібрані для варіантів з довжиною геш-значення 512 бітів. Геш-функція JH не відповідає безумовним критеріям, тому у таблиці 6 не представлена.

Результати порівняння 512-бітних варіантів представлені у табл. 7.

Як видно, порядок геш-функцій не змінився, лише зменшились розриви між ними.

Отже, за результатами досліджень доцільно приділити найбільшу увагу вивченню криптографічних властивостей геш-функцій Skein і Blake, які зайняли перше і друге місця відповідно в 256- і 512-бітному варіантах. Зважаючи на особливості швидкодії на при програмній реалізації на різних процесорах, а також наявність режиму з використанням паралельних обчислень у Skein, доцільно розглянути варіант гармонізації обох геш-функцій: Blake-256 для базового рівня стійкості і

Таблиця 4

Группа	Показник	Підв./ пониж.	Blake	Grøstl	Keccak	Skein
1	швидкодія x86, тактів на байт [6]	-	9.21	23.1	31	21.6
	швидкодія x86_64, тактів на байт [6]	-	8.19	22.2	10	7.6
	швидкодія ARM Cortex M3, тактів на байт [7]	-	40.84	272.42	103.19	141.99
2	швидкодія AVR Atmel (atmega1281_16mhz) [8]	-	884	1309	3089	1204
	кількість RAM AVR Atmel (atmega1281, 16mhz) (min)[8]	-	279	487	766	268
	кількість ROM AVR Atmel (atmega1281, 16mhz) (min)[8]	-	3752	3048	4402	2398
3	швидкодія FPFA Xilinx Virtex 5, Mbit/s [9]	+	3143	10276	12393	3178
	кількість слоїв (slices) FPFA Xilinx Virtex 5 [9]	-	1523	1276	1117	1621
4	максимально досяжний коефіцієнт прискорення при використанні паралельних обчислень	+	1	2	1	2^{256}
5	відношення $1 - \frac{\text{максимальне число успішно атакованих раундів}}{\text{загальне число раундів}}$ для атак прообразу, другого прообразу, колізії, [10]	+	0,83	0.66	1	1
	відношення $1 - \frac{\text{максимальне число успішно атакованих раундів}}{\text{загальне число раундів}}$ для псевдо- і близьких атак, а також відрізнювачів, [10]	+	0,64	0	0	0,21

Таблиця 6

Группа	Показник		Blake	Grøstl	Keccak	Skein
1	швидкодія x86, тактів на байт [6]	-	12.53	36.7	62	20.1
	швидкодія x86_64, тактів на байт [6]	-	9.29	30.5	20	6.1
	швидкодія ARM Cortex M3, тактів на байт [7]	-	143.03	396.07	175.69	178.24
2	швидкодія AVR Atmel (atmega1281_16mhz) [8]	-	3795	3317	3127	1443
	кількість RAM AVR Atmel (atmega1281_16mhz) (min),[8]	-	541	819	670	429
	кількість ROM AVR Atmel (atmega1281_16mhz) (min), [8]	-	6834	3818	3928	2500
3	швидкодія FPFA Xilinx Virtex 5, Mbit/s, [9]	+	3520	15395	8518	3535
	кількість слоїв (slices) FPFA Xilinx Virtex 5, [9]	-	1718	3138	1117	1632
4	максимально досяжний коефіцієнт прискорення при використанні паралельних обчислень	+	1	2	1	2^{256}
5	відношення $1 - \frac{\text{максимальне число успішно атакованих раундів}}{\text{загальне число раундів}}$ для атак прообразу, другого прообразу, коллізії [10]	+	0,84	0,79	0,66	0
	відношення $1 - \frac{\text{максимальне число успішно атакованих раундів}}{\text{загальне число раундів}}$ для псевдо- і близьких атак, а також відрізнювачів, [10]	+	0,625	0	0	0,21

Skein-512 для застосувань з підвищеними вимогами до стійкості і швидкодії відповідно. До того ж такий підхід дозволить перестрахуватись на випадок, якщо одна з геш-функцій буде зламана.

Література

[1] *Florian Mendel, Norbert Pramstaller, Christian Rechberger, Marcin Kontak, and Janusz Szmidt.* Cryptanalysis of the GOST Hash Function. Режим доступу: http://wiki.uni.lu/esc/docs/mendel_gost.pdf

[2] *І.Д.Горбенко , А.О. Бойко, А. М. Герцог.* Стан створення та напрями досліджень і розробок зі створення перспективних стандартів гешування. Радіоелектронні і комп'ютерні системи № 5(46), Харків, 2010, ст. 67-74

[3] *І.Д.Горбенко , А.О. Бойко, А. М. Герцог.* Порівняння перспективних швидкодіючих функцій гешування. Прикладна радіоелектроніка. Харків 2009, С. 321-326

[4] *Горбенко Ю. І, Горбенко І. Д.* Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія і практика: монографія. – Харків: Видавництво "Форт", 2010. ст. 116-122.

[5] *Окунев Ю. Б., Плотников В. Г.* Принципы системного подхода к проектированию в технике связи. М., "Связь", 1976

[7] Режим доступу: http://www.skein-hash.info/sha3-engineering

[8] Режим доступу: http://bench.cr.yp.to/results-sha3.html

[9] Режим доступу: http://xbx.das-labor.org/

[10] Режим доступу: http://ehash.iaik.tugraz.at/wiki/SHA3_Hardware_Implementations

[11] Режим доступу: http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

Надійшла до редколегії 19.04.2011

Бойко Артем Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: принципи побудування геш-функцій та використання їх у засобах захисту інформації.

Таблиця 7

Геш-функція	Значення узагальненого показника (більше-краще)
Skein	2.5
Blake	2.25
Keccak	2.18
Grшstl	1.75

Даценко Сергій Ігоревич, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: принципи побудування геш-функцій та використання їх у засобах захисту інформації.

УДК 621. 391:519.2:519.7

Методика и результаты сравнения алгоритмов хеш-функций, принимающих участие в 3-м раунде конкурса NIST SHA-3 / А.А. Бойко, И.Д. Горбенко, С. И. Даценко// Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 171–175.

В статье предложен наиболее полный набор критериев оценки перспективных хеш-функций, разработана и обоснована формализованная методика их сравнения. Приведены результаты сравнения финалистов конкурса NIST SHA-3, и сделаны соответствующие рекомендации.

Ключевые слова: сравнение хеш-функций, формализованная методика сравнения, хеш-функция, конкурс NIST SHA-3.

Табл. 07. Ил.01. Библиогр.:11 назв.

UDC 621. 391:519.2:519.7

Techniques and results of comparing hash functions algorithms taking part in the 3rd round of the NIST SHA-3 Competition / A.O. Boiko, I. D. Gorbenko, S.I. Datsenko // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 171–175.

The most complete set of criteria and new formal comparison techniques are considered. Results of comparing the NIST SHA-3 Competition final participants are given and relevant recommendations are provided.

Keywords: hash functions comparison, formalized comparison technique, hash function, NIST SHA-3 Competition.

Tab. 07. Fig. 01. Ref.: 11 items.