**DOI:** 10.18372/2225-5036.23.11822

# КРИПТОГРАФІЧНА ФУНКЦІЯ ГЕШУВАННЯ SafeBK


**Каріна Безверха, Василь Кінзерявий, Андрій Гізун**

*Національний авіаційний університет, Україна*

**БЕЗВЕРХА Каріна Сергіївна**

*Рік та місце народження:* 1992 рік, м. Наро-Фомінськ, Росія.
*Освіта:* Національний авіаційний університет, 2014 рік.
*Посада:* аспірант кафедри безпеки інформаційних технологій.
*Наукові інтереси:* інформаційна безпека.
*Публікації:* 10 науковий публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
*E-mail:* karina0kira@ukr.net

**КІНЗЕРЯВИЙ Василь Миколайович,** к.т.н.

*Рік та місце народження*: 1985 рік, м. Кам'янець-Подільський, Україна
*Освіта:* Національний авіаційний університет, 2007рік.
*Посада:* доцент кафедри безпеки інформаційних технологій.
*Наукові інтереси:* інформаційна безпека, криптографія та криптоаналіз.
*Публікації:* більше 90 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, патенти та авторські свідоцтва.
*E-mail:* v.kinzeryavyy@gmail.com

**ГІЗУН Андрій Іванович,** к.т.н.

*Рік та місце народження:* 1987 рік, м. Нетішин, Хмельницька область, Україна.
*Освіта:* Національний авіаційний університет, 2010 рік.
*Посада:* доцент кафедри безпеки інформаційних технологій.
*Наукові інтереси:* інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
*Публікації:* більше 50 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
*E-mail:* andriy.gizun@gmail.com



**Анотація.** *Застосування веб-технологій та форм електронного документообігу в процесі обміну інформацією між користувачами хоча і спрощує даний процес, однак породжує ряд нових загроз конфіденційності, цілісності і доступності інформації та появу раніше невідомих уразливостей. Одним з найпоширеніших методів захисту є використання цифрових сертифікатів, які забезпечують конфіденційний обмін даними між клієнтом та сервером шляхом шифрування та аутентифікації цифрового сертифікату. Цифровий сертифікат являє собою відкритий ключ користувача, завірений ЕЦП сертифікаційного центру. Однак цифровий сертифікат це не лише відкритий ключ з інформацією, а так званий підпис сервера чи веб-ресурсу, який реалізується використовуючи геш-функції. Проте із розвитком інформаційних технологій та появою нових видів атак зростає число недоліків існуючих геш-функцій. Так, в роботі запропоновано нову функцію гешування, що була розроблена на основі геш-функції SHA-2. Вдосконалення стосувалось внесенням ряду змін: збільшено розміру слів та збільшення дайджесту повідомлення; на етапі попередньої обробки вхідне повідомлення доповнюється псевдовипадковою послідовністю; збільшено кількість нелінійних функцій. Запропоновані зміни дозволяють забезпечити зменшення кількості раундів у функції стиснення, що дозволить гарантувати як мінімум аналогічні показники стійкості з одночасним зростанням швидкості обробки даних.*


**Ключові слова:** *захист інформації, криптографія, геш-функції, цифрові сертифікати, SHA-2.*

**Вступ**

На сьогоднішній день інформаційне забезпечення в режимі реального часу займає вагоме місце в діяльності організацій всіх типів господарювання та органів державної влади в тому числі. Через веб-портали організації висвітлюють результати своєї діяльності, надають он-лайн послуги та фінансові послуги, проводять фінансові операції, обмінюються інформацією. Веб-сервери використовуються не тільки для рекламних цілей, а й для поширення програмного забезпечення та електронної комерції, забезпечення віддаленої роботи через захищений канал зв'язку та багато іншого. Органи держаної влади через офіційні веб-портали та загальні реєстри забезпечують виконання вимог законодавства в частині надання адміністративних послуг та звернення громадян. Веб-браузери постійно розширюють свої функціональні можливості та надають користувачам можливість збереження своїх конфіденційних даних, документів, пошти та ін. У зв'язку з цим, забезпечення захищеного доступу до Веб-ресурсів та обмін інформацією між ними займає одне з пріоритетних напрямів в процесі забезпечення захисту інформації та потребує постійного вдосконалення. Одним з найпоширеніших методів захисту є використання криптографічних сертифікатів – цифрових сертифікатів, які забезпечують конфіденційний обмін даними між клієнтом та сервером шляхом шифрування та аутентифікації цифрового сертифікату. Цифровий сертифікат являє собою відкритий ключ користувача, завірений ЕЦП сертифікаційного центру. Однак цифровий сертифікат це не лише відкритий ключ з інформацією, а так званий підпис сервера чи веб-ресурсу, який реалізується використовуючи геш-функції. За останні роки тенденція зростання кількості кібератак збільшується в геометричній прогресії. Так, при збільшення кількості атак, а отже і виявленні нових уразливостей, спостерігається ряд проблем з реалізацією і застосуванням цифрових сертифікатів. Відомі атаки, як DROWN (дозволяє розшифрувати шифротекст без знання закритого ключа) [1], FREAK (дозволяє проникнути у встановлене зашифроване з'єднання та аналізувати трафік) [2], LOGJAM (дозволяє читання та модифікацію даних, що передаються по захищеному каналу зв'язку) [3], завдали великих збитків багатьом власникам веб-ресурсів, в тому числі таким гігантам як Google, Mozilla, Yahoo та ін. та поставили під питання надійність цифрових сертифікатів. Тому підвищення надійності цифрових сертифікатів, як найпоширеніших методів захисту обміну даними через канали зв'язку, є актуальним та потребує вдосконалення.

***Метою*** даної роботи є підвищення ефективності цифрових сертифікатів шляхом розробки нової геш-функції SafeBK.

## Основна частина дослідження

Одними з найпоширеніших криптографічних алгоритмів є геш-функції. Вони необхідні для «стиснення» інформації в образи, які представляють собою бітові комбінації фіксованої довжини. Геш-функції сімейства SHA-2 користуються високою популярністю в додатках, пов'язаних із систематизацією, пошуком і захистом інформації. Цифрові протоколи використовують шифрування з відкритим ключем для аутентифікації клієнта та сервера. На етапі підтвердження підключення узгоджується геш-функція, яка відіграє роль ідентифікаційної відмітки і використовується для забезпечення цілісності передачі даних. Тобто геш-функція повинна унеможливлювати підробку сертифікату, залишаючи при цьому той же підпис засвідчувального центру. До недавнього часу в цифрових сертифікатах використовувалась геш-функція SHA-1. У зв'язку з виявленням численних колізій в SHA-1 [4,5] та в самих цифрових сертифікатах [5-7], організаціями Microsoft, Google та іншими було ініційовано рішення про заміну функції гешування [8]. Починаючи з 2016 року в SSL-сертифікаті використовується геш-функція SHA-2. Однак обчислювальні технології не стоять на місті, потужність техніки збільшується, і вже сьогодні багато робіт присвячено дослідженню криптостійкості геш-функції SHA-2, зокрема в роботах [9-11] було виявлено такі недоліки:

– знаходження колізій для усічених варіантів SHA-512 [10,11];

– знаходження першого та другого прообразу;

– атака дня народження.

У роботі запропоновано нову геш-функцію SafeBK, прототипом якої виступає SHA-512. На нашу думку дана геш-функція може дозволити підвищити ефективність криптографічного захисту цифрових сертифікатів при її застосуванні.

## Опис розробленої геш-функції SafeBK

Запропонована геш-функції SafeBK складається з двох етапів: попередньої обробки (див. формулу (1)) та визначення геш-значення (описується формулами (2)-(3)).

*Етап попередньої обробки*

На етапі попередньої обробки вхідне повідомлення $M$ ($M \in V_N$, $V_N \in \{0,1\}^N$, $N$ - довжина повідомлення $M$ в бітах, $N \in Z$, $N < 2^{128}$) доповнюється додатковою послідовністю $D_l$ (довжина повідомлення $M$) та псевдовипадковою послідовністю $salt$ (визначається на основі $M$), так щоб результуюча довжина повідомлення була кратна довжині блоків даних $L$ ($L = 1024 \cdot t'$ біт, $t' \in N$):

$$M_{rez} = \left( M,\ D_l, salt \right), \qquad (1)$$

де $M_{rez} \in V_{NN}$, $V_{NN} = N + 128 + N_{salt}$, $D_l = H_{Dl}(M)$, $D_l \in V_{128}$, $salt = H_{Gen}(M)$, $salt \in V_{Nsalt}$, $N_{salt} = 2L - ((N+128) \bmod L)$, в якості функції $H_{Gen}$ може виступати будь-яка функція генерування псевдовипадкової послідовності на основі $M$, $H_{Dl}$ − функція визначення довжини $M$. На основі доповненого повідомлення $M_{rez}$ буде визначатись геш-значення повідомлення $M$. Повідомлення $M_{rez}$, $M_{rez} \in V_{NN}$, розбивається на $k$ $L$-бітних блоків: $M_{rez} = (m_1, m_2 .... m_k)$, де $m_i \in V_L$, $i = \left(\overline{1,k}\right)$, $k = (NN)/L$.

*Етап визначення геш-значення*

Обчислення дайджесту повідомлення проходить ітеративно, обробляючи кожен $m_i$ блок повідомлення $M_{rez}$, $m_i \in V_L$, $i = \left(\overline{1,k}\right)$ функцією стиснення $F_g$, щоб отримати результуюче геш-значення:

$$h_i = F_g(h_{i-1}, m_i),\ i = \overline{(1,k)}, \quad (2)$$

$$H(IV, M_{rez}) = h_k, \quad (3)$$

де $h_0 = IV$, $IV$ - вектор ініціалізації, $IV \in V_{L/2}$, $h_i$ - проміжні значення дайджесту повідомлення $h_i \in V_{L/2}, i = \overline{(1,k)}$; $H$ - результуюче значення дайджесту, $H \in V_{L/2}$; $F_g$ - функція стиснення, що використовується в геш-функції.

Функція стиснення $F_g$ виконується в три етапи: розбиття блоків на слова (описується формулами (4)-(5)), ініціалізація змінних (див. формулу (6)), безпосереднє стиснення (описується формулами (7)-(20)).

*Етап 1 функції стиснення* $F_g$. Кожен $m_i$ блок повідомлення $M_{rez}$, $m_i \in V_L$, $i = \overline{(1,k)}$, розкладається на 16 слів:

$$m_i = (W_0^i, ..., W_{15}^i), \quad (4)$$

де $W_j^i \in V_{L/16}$, $j = \overline{0,15}$.

На основі отриманих слів $W_j^i$, $j = \overline{0,15}$, розраховуються слова $W_u^i$ (5), $W_u^i \in V_{L/16}$, $u = \overline{16,63}$:

$$W_u = W_{u-16} + Delta0(W_{u-15}) + W_{u-7} + Delta1(W_{u-2}), \quad (5)$$

де $Delta0(W_u) = Rotr(W_u,1) \oplus Rotr(W_u,8) \oplus SHR(W_u,7)$, $Delta1(W_u) = Rotr(W_u,19) \oplus Rotr(W_u,61) \oplus SHR(W_u,6)$, $Rotr(x,l)$ − правий побітовий циклічний зсув аргументу $x$ на $l$ − біт; $SHR(x,l)$ − лівий зсув аргументу $x$ на $l$ − біт.

*Етап 2 функції стиснення* $F_g$. Виконується переініціалізація векторів внутрішнього стану $T$,

$$T = (T_1, ..., T_8),\ T_z \in V_{L/16},\ z = \overline{1,8}:\ T_z = h_{i-1}^z, \quad (6)$$

де $h_{i-1} = (h_{i-1}^1, ..., h_{i-1}^8)$, $h_{i-1}$ − попереднє значення дайджесту, що подається на вхід функції $F_g$, $h_{i-1}^z \in V_{L/16}$, $z = \overline{1,8}$.

*Етап 3 функції стиснення* $F_g$. На даному етапі відбувається безпосереднє стиснення блоку даних $m_i \in V_L$, $i = \overline{1,k}$, $k = NN / L$, при цьому у кожному із 64 раундів буде змінюватись значення векторів внутрішнього стану $T = (T_1, ..., T_8)$, $T_z \in V_{L/16}$, $z = \overline{1,8}$, за допомогою їх перемішування із векторами $W_j$ та константами $K_j$, $j = \overline{0,63}$.

Для кожного $j$-го раунду виконуються наступні дії:

$$j = \overline{0,63}:\ F_{g_1} = T_8 \oplus Sigma1(T_5) \oplus Ch(T_5,T_6,T_7) + W_j + K_j, \quad (7)$$

$$F_{g_2} = Sigma0(T_1) \oplus Maj(T_1,T_2,T_3), \quad (8)$$

$$F_{g3} = JQ(T_3,T_6) \oplus Maj(T_2,T_3), \quad (9)$$

$$F_{g_4} = SH(T_8,T_7) \oplus Sigma(T_8), \quad (10)$$

$$T_8 = T_7 + F_{g_4};\ T_7 = T_6;\ T_6 = T_5;$$

$$T_5 = T_4 + F_{g_1};\ T_4 = T_3;\ T_3 = T_2 + F_{g_3};\ T_2 = T_1;\ T_1 = F_{g_1} + F_{g_2}, \quad (11)$$

де $T_z$ − вектори внутрішнього стану, $T_z \in V_{L/16}$, $z = \overline{1,8}$; $W_j$ − слова, на які розбивається кожен $m_i$ блок; $K_j$ − наперед визначені константи (при необхідності можуть змінюватись), $K_j \in V_{L/16}$; $Ch(x,y,z)$, $Maj(x,y,z)$, $Sigma0(x)$, $Sigma1(x)$, $Delta0(x)$, $Delta1(x)$, $JQ(x,y)$ та $SH(x,y)$ – нелінійні функції, які описані у формулах (12)-(19):

$$Sigma0(x) = Rotr(x,28) \oplus Rotr(x,34) \oplus Rotr(x,39), \quad (12)$$

$$Sigma1(x) = Rotr(x,14) \oplus Rotr(x,18) \oplus Rotr(x,41), \quad (13)$$

$$Ch(x,y,z) = (x+y) \oplus (\bar{x}+z), \quad (14)$$

$$Maj(x,y,z) = (x+y) \oplus (x+z) \oplus (y+z), \quad (15)$$

$$Delta0(x) = Rotr(x,1) \oplus Rotr(x,8) \oplus SHR(x,7), \quad (16)$$

$$Delta1(x) = Rotr(x,19) \oplus Rotr(x,61) \oplus SHR(x,6), \quad (17)$$

$$JQ(x,y) = (\bar{x}+y) \oplus Rotr(x,13) \oplus SHR(\bar{y},17), \quad (18)$$

$$SH(x,y) = SHR(x,7) \oplus Rotr(y,8) \oplus Rotr(\bar{x},y), \quad (19)$$

$F_g$ - проміжні значення функції стиснення, $F_{g_o} \in V_{L/16}$, $o = \overline{1,4}$. $Ch(x,y,z)$, $Maj(x,y,z)$, $Sigma0(x)$, $Sigma1(x)$, $Delta0(x)$, $Delta1(x)$, нелінійні функції, що використовувались в оригінальному SHA-2. $JQ(x,y)$ та $SH(x,y)$ - нові нелінійні функції, що були запропоновані в даній геш-функції.

Після виконання останнього раунду значення векторів внутрішнього стану $T = (T_1, ..., T_8)$, $T_z \in V_{L/16}$, $z = \overline{1,8}$, остаточно змінюються наступним чином:

$$T_z = T_z \oplus h_{i-1}^z, \quad (20)$$

де $h_{i-1}$ − попереднє значення дайджесту, що подається на вхід функції $F_g$ $h_{i-1} = (h_{i-1}^1, ..., h_{i-1}^8)$, $h_{i-1}^z \in V_{L/16}$, $z = \overline{1,8}$. Виходом функції будуть дані кінцеві значення векторів внутрішнього стану.

На нашу думку, геш-функція SafeBK за рахунок додавання псевдовипадкової послідовності *salt* до вхідного повідомлення на етапі попередньої обробки та нелінійних операцій $JQ(x,y)$ та $SH(x,y)$ на етапі визначення геш-значення дозволяють зменшити загальну кількість раундів у функції стиснення при забезпечені аналогічних або і кращих показників швидкодії та захищеності даних, в аспекті стійкості до різноманітних атак та нейтралізації відомих уразливостей порівняно із геш-функцією SHA-2. Для перевірки даного твердження у наступних роботах будуть проведені як теоретичні так і експериментальні дослідження.

## Висновки

У роботі запропоновано нову геш-функцію SafeBK, яка в майбутньому може бути використана для підвищення ефективності криптографічного захисту цифрових сертифікатів, що забезпечить більш надійний обмін конфіденційною інформацією в мережі. Геш-функція SafeBK потребує подальших досліджень для перевірки її швидкодії на різних платформах, стійкості до поширених методів криптоаналізу. В наступних роботах планується провести вищезазначені дослідження та порівняти з показниками геш-функцій серії SHA-2.

### Література


[1] N. Aviram, S. Schinzel, Ju. Somorovsky, «DROWN: Breaking TLS using SSLv2», *Proceedings of the 25th USENIX Security Symposium*, P.18, 2016.

[2] M. Green, «Attack of the week: FREAK (or «factoring the NSA for fun and profit»)», *A Few Thoughts on Cryptographic Engineering*. [Online]. Available at: https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/.

[3] B. Duncan, «Weak Diffie-Hellman and the Logjam Attack». [Online]. Available at: https://weakdh.og.

[4] P. Karpman, T. Peyrin, M. Stevens, «Practical Free-Start Collision Attacks on 76-step SHA-1». [Online]. Available at: https://eprint.iacr.org/2015/530.

[5] SHA-1 Certificates in Chrome. [Online]. Available at: https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html.

[6] F. Kohlar, S. Schage, «On the Security of TLS-DH and TLS-RSA in the Standard Model1», p. 50, 2013.

[7] Ch. Meyer, J. Schwenk, «Horst Gortz Institute for IT-Security», *Chair for Network and Data Security Ruhr-University Bochum. Lessons Learned From Previous SSL/TLS Attacks A Brief Chronology Of Attacks And Weaknesses*, p. 15.

[8] C. Castelluccia, E. Mykletun, G. Tsudik, «Improving Secure Server Performance by Re-balancing SSL/TLS Handshakes», *Proceedings of ACM Symposium on Information, computer and communications security*, p. 26-34, 2006.

[9] S. Kumar Sanadhya, P. Sarkar, «22-Step Collisions for SHA-2». [Online]. Available at:: http://arxiv.org/abs/0803.1220.

[10] «Improving Local Collisions: New Attacks on Reduced SHA-256». [Online]. Available at: https://eprint .iacr.org/2015/350.pdf )

[11] Ch. Dobraunig, M. Eichlseder, F. Mendel, «Analysis of SHA-512/224 and SHA-512/256». [Online]. Available at: https://eprint.iacr.org/2016/374.pdf



**УДК 004.056.55 (045)**



***Безверхая К.С., Кинзерявый В.Н., Гизун А.И. Криптографическая функция хеширования SafeBK***
***Аннотация.*** *Применение веб-технологий и форм электронного документооборота в процессе обмена информацией между пользователями хотя и упрощает данный процесс, однако порождает ряд новых угроз конфиденциальности, целостности и доступности информации и появление ранее неизвестных уязвимостей. Одним из самых распространенных методов защиты является использование цифровых сертификатов, которые обеспечивают конфиденциальный обмен данными между клиентом и сервером путем шифрования и аутентификации цифрового сертификата. Цифровой сертификат представляет собой открытый ключ пользователя, заверенный ЭЦП сертификационного центра. Однако цифровой сертификат это не только открытый ключ с информацией, а так называемый подпись сервера или веб-ресурса, который реализуется используя хеш-функции. Однако с развитием информационных технологий и появлением новых видов атак, приводит к росту числа недостатков существующих хеш-функций. Так, в работе предложена новая функция хеширования, которая была разработана на основе хеш-функции SHA-2. Совершенствование касалось внесением ряда изменений: увеличено размера слов и увеличение дайджеста сообщения; на этапе предварительной обработки входящее сообщение дополняется псевдослучайной последовательностью; увеличено количество нелинейных функций. Предложенные изменения позволяют обеспечить уменьшение количества раундов в функции сжатия, позволит гарантировать как минимум аналогичные показатели устойчивости с одновременным ростом скорости обработки данных.*
***Ключевые слова:*** *защита информации, криптография, хеш-функции, цифровые сертификаты, SHA-2.*

***Bezverkha K., Kinzeryavyy V., Gizun A. Cryptographic hash function SafeBK***
***Abstract.*** *The application of web technologies and forms of electronic document circulation in the process of information exchange between users though simplifies this process, however, generates a number of new threats to the confidentiality, integrity and availability of information and the appearance of previously unknown vulnerabilities. One of the most common methods of protection is the use of digital certificates that ensure the confidential exchange of data between a client and a server by encrypting and authenticating a digital certificate. A digital certificate is a public key, certified by the EDS of the certification center. However, a digital certificate is not just a public key with information, but a so-called signature of a server or web resource that is implemented using the hex functions. However, with the development of information technology and the emergence of new types of attacks, leads to an increase in the number of disadvantages of existing gash functions. Thus, in the paper a new heaching function was proposed, which was developed on the basis of the SHA-2 hex function. Improvements involved the introduction of a number of changes: increased the size of words and an increase in the message digest; At the pre-processing stage, the incoming message is supplemented by a pseudo-random sequence; the number of nonlinear functions is increased. The proposed changes allow to reduce the number of rounds in the compression function, which will guarantee at least similar stability indicators with simultaneous increase in data processing speed.*
***Key words:*** *information security, cryptography, hash functions, digital certificates, SHA-2.*



Отримано 22 *червня 2017 року*, затверджено редколегією 14 *липня 2017 року*