

СХЕМА АВТЕНТИФІКАЦІЇ НА ФРАКТАЛЬНИХ МНОЖИНАХ

Для побудови захищених інформаційних ресурсів у відкритих мережах необхідна реалізація засобів автентифікації. Відомі протоколи автентифікації ґрунтуються на перевірці певних таємних знань (ключа чи пароля). Перевага надається схемам перевірки, побудованим на діалозі клієнта та сервера, який здійснюється без передавання секретного знання, навіть у зашифрованій формі, - протоколам з нульовим розголошенням. Як правило, такі протоколи використовують математично складні задачі з невідомим розв'язком зворотної проблеми. Ця невідомість виступає причиною вразливості протоколу – винайдення рішення задачі зведе нанівець надійність протоколу. Запропонована схема автентифікації, побудована на комплексних фрактальних множинах з використанням методів дистанційного оцінювання знань. Фрактальні множини зручні для використання завдяки поєднанню властивостей скінченності та нескінченності. Властивість скінченності дозволяє побудову самої множини, властивість нескінченності гарантує можливість багаторазового використання схеми. На-

ведено алгоритм клієнт-серверної взаємодії. Використання схеми дозволить покращити показників безпеки мережних інформаційних ресурсів.

Ключові слова: автентифікація, протокол з нульовим розголошенням, фрактал, фрактальна множина, мережна безпека.

Samoilenko Denis, PhD, docent of Ship Electrical Equipment and Information Security Department, National University of Shipbuilding after Admiral Makarov. E-mail: denniksam@gmail.com

Самойленко Денис Миколайович, кандидат фізико-математичних наук, доцент, доцент кафедри електрообладнання суден та інформаційної безпеки. Національний університет кораблебудування імені адмірала Макарова.

Самойленко Денис Николаевич, кандидат физико-математических наук, доцент, доцент кафедры электрооборудования суден и информационной безопасности. Национальный университет кораблестроения имени адмирала Макарова.

УДК 621.391:519.7

БЕЗКЛЮЧОВІ ГЕШ-ФУНКЦІЇ РЕГІСТРОВОГО ТИПУ

Антон Олексійчук, Катерина Король

Безключові геш-функції відносяться до найважливіших криптографічних примітивів і застосовуються в сучасних системах шифрування, автентифікації, цифрового підпису, генерації ключів тощо. Незважаючи на помітний прогрес у розробці різноманітних атак на “конкретні” геш-функції, розуміння закономірностей, що лежать в основі зазначених атак, визначення умов їх застосовності та розробка методів оцінювання їх ефективності є предметом активних подальших досліджень. Метою статті є встановлення загальних умов, що визначають практичну стійкість широкого класу геш-функцій, які базуються на реєстрах звуку, відносно атак, спрямованих на побудування колізій їх стискувальних функцій. Показано, що задача побудування колізій зводиться до розв'язання автоматних рівнянь відносно двійкових невідомих, які задовольняють певним обмеженням. При цьому множини всіх розв'язків таких рівнянь (без урахування обмежень) мають простий алгоритмічний опис, що дозволяє перелічувати ці розв'язки в режимі реального часу.

Ключові слова: безключова геш-функція, пошук колізій, скінченний автомат, нелінійний реєстр звуку, система автоматних рівнянь, MDx, SHA.

Вступ. Безключові (криптографічні) геш-функції відносяться до найважливіших криптографічних примітивів. Вони застосовуються в сучасних системах шифрування, автентифікації, цифрового підпису, генерації ключів та звичайно виконують роль своєрідної ланки, що пов'язує окремі частини криптографічної системи (див., наприклад, [4, 5]). З появою у 2004 – 2005 роках потужних атак на окремі функції сім'ї MDx [13 – 16] суттєво підсилюється інтерес фахівців до побудови нових видів геш-функцій, розробки методів їх криптоаналізу та обґрунтування їх стійкості

відносно перспективних атак. Певним підсумком досліджень у цьому напрямі можна вважати прийняття у 2012 році нового стандарту гешування даних – алгоритму Кессак [8].

Незважаючи на помітний прогрес у розробці різноманітних атак на “конкретні” геш-функції, розуміння закономірностей, що лежать в основі зазначених атак, визначення загальних умов їх застосовності та розробка методів оцінювання їх ефективності є предметом подальших досліджень, спрямованих на створення загальної теорії побудови та аналізу геш-функцій. Потреби в та-

кої теорії відчуваються, зокрема, у зв'язку з наявністю великої кількості евристичних припущень та “ad hoc-прийомів”, що використовуються у сучасних атаках, більшість з яких базується, скоріше, на інтуїції розробників, ніж на загальних наукових засадах. Свідченням тому є сперечання та дискусії стосовно реальної ефективності або застосовності окремих атак, спростування чи перегляд раніше отриманих результатів (див., наприклад, [3]). Для розуміння причин, за якими окремі атаки є ефективніше (а окремі геш-функції – вразливіше) в порівнянні з іншими, необхідно проаналізувати властивості математичних об'єктів та конструкцій, на яких базуються сучасні алгоритми гешування. Дослідженню одного з найбільш відомих класів таких алгоритмів присвячено дану роботу.

Метою статті є встановлення загальних умов, що визначають практичну стійкість широкого класу геш-функцій, які базуються на регістрах зсуву, відносно атак, спрямованих на побудування колізій їх стискувальних функцій. Оскільки зазначені (а також багато які інші) геш-функції реалізуються за допомогою скінченних автоматів, виявляється природним використовувати для їх аналізу саме теоретико-автоматні методи.

В п. 1 описано конструкцію Меркля-Дамгорда [7, 9] побудування геш-функцій, стійких до колізій, на основі стискувальних функцій, що володіють аналогічною властивістю. В п. 2 введено до розгляду клас функцій регістрового типу, який включає в себе стискувальні функції окремих алгоритмів сім'ї MDx. Показано, що задача побудування колізій зазначених функцій зводиться до розв'язання автоматних рівнянь відносно двійкових невідомих, які задовольняють певним обмеженням. При цьому множини всіх розв'язків таких рівнянь (без урахування обмежень) мають простий алгоритмічний опис, що дозволяє перелічувати ці розв'язки в режимі реального часу. У висновках стисло сформульовано основні результати статті.

1. Конструкція Меркля-Дамгорда

Для будь-якого натурального l позначимо V_l множини двійкових векторів довжини l , $V_{\leq l} = \bigcup_{i=1}^l V_i$. Далі під (безключовою) геш-функцією розуміється довільне відображення $H: V_{\leq m} \rightarrow V_n$. Якщо це відображення задається за допомогою певного алгоритму, то останній називається *алгоритмом гешування*; він ототожнюється з відображенням H і позначається тим самим символом.

Нехай X, Y – скінченні множини, $h: X \rightarrow Y$ – довільне відображення. Говорять, що впорядкована пара $(x_1, x_2) \in X^2$ є *колізією* функції h (або що повідомлення x_1 і x_2 *утворюють колізію* цієї функції), якщо $x_1 \neq x_2$ та $h(x_1) = h(x_2)$.

Більшість сучасних геш-функцій будується на основі так званої конструкції Меркля-Дамгорда, що запропонована в [9] і незалежно в [7]. Ця конструкція являє собою спосіб побудування геш-функції $H: V_{\leq 2^{l-1}} \rightarrow V_N$ за довільними відображенням $h: V_N \times V_M \rightarrow V_N$, вектором $s^{(0)} \in V_N$ та натуральним числом $L < M$.

Нехай $x \in V_{\leq 2^{l-1}}$ – вхідне повідомлення довжини l . Тоді алгоритм обчислення значення $H(x)$ визначається наступним чином:

1) сформулювати доповнення повідомлення x : $\hat{x} = (x \| 1 \| 0^r \| \bar{l})$, де $\|$ – символ конкатенації, \bar{l} – вектор довжини L , що є двійковим записом числа l , а r дорівнює остачі від ділення числа $-(L+l+1)$ на M (іншими словами, r – найменше невід'ємне ціле число, для якого довжина повідомлення \hat{x} є кратною M);

2) представити \hat{x} у вигляді: $\hat{x} = \hat{x}_0, \dots, \hat{x}_{t-1}$, де $\hat{x}_i \in V_M$ для кожного $i \in \overline{0, t-1}$, обчислити значення

$$s^{(i+1)} = h(s^{(i)}, \hat{x}_i), i \in \overline{0, t-1}, \quad (1)$$

та покласти $H(x) = s^{(t)}$.

Отже, згідно з конструкцією Меркля-Дамгорда, обчислення значень геш-функції H виконується в два етапи. На першому з них здійснюється процедура доповнення (padding), тобто заміна вхідного повідомлення x повідомленням \hat{x} . На другому етапі значення $H(x)$ отримується в результаті виконання ітераційної процедури відповідно до формули (1).

Відображення $h: V_N \times V_M \rightarrow V_N$ називають іноді *стискувальною функцією* алгоритму гешування H . Зауважимо, що це відображення можна розглядати як функцію переходів автомату без виходу з вхідним алфавітом V_M та множиною станів V_N . Тоді значення $H(x)$ співпадає з фінальним станом цього автомату, що відповідає його початковому стану $s^{(0)}$ та вхідній послідовності $\hat{x} = \hat{x}_0, \dots, \hat{x}_{t-1}$.

Приклад 1. Геш-функція SHA-1 (відповідно SHA-256) будується на основі конструкції Меркля-Дамгорда, де $M = 512$, $N = 160$ (відповідно $N = 256$), $L = 64$, а вектор $s^{(0)} \in V_N$ визначається

як певна константа. Стискувальна функція h задається рівністю

$$h(s, x) = s + g(s, x), (s, x) \in V_N \times V_M, \quad (2)$$

де $+$ є символом операції абелевої групи $(\mathbf{Z}_{2^{32}})^5$ (відповідно $(\mathbf{Z}_{2^{32}})^8$), а функція $g: V_N \times V_M \rightarrow V_N$ визначається за допомогою окремого алгоритму; див. нижче п. 2. Подібним чином будуватиметься також геш-функція SHA-512, де $M=1024$, $N=512$, $L=128$, а символ $+$ у формулі (2) позначає операцію абелевої групи $(\mathbf{Z}_{2^{64}})^8$ [10].

Добре відомо, що конструкція Меркля-Дамгорда дозволяє будувати стійкі до колізій геш-функції на основі стискувальних функцій, які володіють аналогічною властивістю. Для уточнення сенсу цього твердження розглянемо, поряд із зазначеним вище повідомленням x , інше повідомлення $x' \in V_{\leq 2^{l-1}}$ довжини l' . Позначимо $\hat{x}' = \hat{x}'_0, \dots, \hat{x}'_{t'-1}$ його доповнення та покладемо

$$s^{(j+1)} = h(s^{(j)}, \hat{x}'_j), j \in \overline{0, t'-1}. \quad (3)$$

Припустимо, що (x, x') – колізія функції H , причому $l \neq l'$. Тоді $\hat{x}'_{t-1} \neq \hat{x}_{t-1}$ і на підставі рівностей (1), (3) повідомлення $(s^{(t-1)}, \hat{x}_{t-1})$ і $(s'^{(t-1)}, \hat{x}'_{t-1})$ утворюють колізію функції h . Якщо ж $l = l'$, то $t = t'$ і колізію цієї функції можна знайти серед пар $((s^{(i)}, \hat{x}_i), (s'^{(i)}, \hat{x}'_i))$ таких, що $\hat{x}_i \neq \hat{x}'_i, i \in \overline{0, t-1}$.

Отже, в будь-якому випадку за відомою колізією (x, x') функції H можна побудувати колізію її стискувальної функції, використовуючи $O(l(x, x'))$ операцій (звернення до функції h та порівняння на рівність елементів множини V_M), де $l(x, x')$ – максимум довжин слів x та x' .

З іншого боку, як впливає безпосередньо з наведеного опису конструкції Меркля-Дамгорда, якщо повідомлення $(s^{(0)}, x_1)$ та $(s^{(0)}, x_2)$, де $x_1, x_2 \in V_M$, утворюють колізію функції h , то пара (x_1, x_2) є колізією функції H .

Останнє твердження, певною мірою, зводить задачу побудування колізій геш-функції H до знаходження колізій функції $h_{s^{(0)}}(x) = h(s^{(0)}, x)$, $x \in V_M$. Якщо при цьому функція h визначається за формулою (2), то колізії функції $h_{s^{(0)}}$ співпадають з колізіями функції $g_{s^{(0)}}(x) = g(s^{(0)}, x)$, $x \in V_M$.

2. Стискувальні функції, що базуються на регістрах зсуву, та відповідні їм системи автоматних рівнянь

Опишемо загальну схему побудови стискувальних функцій, за якою будуються, зокрема, зазначені функції окремих алгоритмів сім'ї MDx. Спочатку введемо декілька допоміжних позначень.

Зафіксуємо натуральні числа $l, m, n \geq 2$, покладемо $M = ml$, $N = nl$. Позначимо символом $+$ операцію додавання за модулем 2^l двійкових цілих чисел, що відповідають булевим векторам довжини l ; символом $F_{l \times l}$ – множину матриць розміру $l \times l$ над полем $F = \mathbf{GF}(2)$, а символом $GL(l, 2)$ – групу оборотних матриць порядку l над цим полем.

Для будь-яких функції $f: V_l^{n-1} \rightarrow V_l$ та послідовності $A = (A_1, \dots, A_n)$, де $A_1, \dots, A_n \in GL(l, 2)$, позначимо $\mathfrak{R}(f, A)$ регістр зсуву (РЗ) довжини n , що визначається як автомат без виходу з вхідним алфавітом V_l , множиною станів V_l^n та функцією переходів

$$\phi(s, z) = (s_n A_n + z + f(s_1, \dots, s_{n-1}), s_1 A_1, \dots, s_{n-1} A_{n-1}), \quad (4)$$

де $s = (s_1, \dots, s_n) \in V_l^n$, $z \in V_l$ (див. рис. 1, де показана схема регістру, що відповідає послідовності I одиничних матриць A_1, \dots, A_n над полем F).

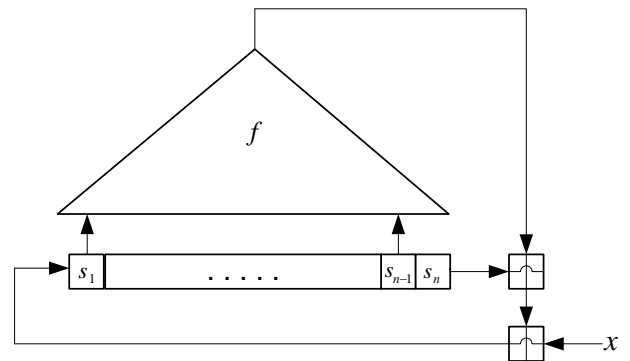


Рис. 1. Регістр зсуву $\mathfrak{R}(f, I)$

Для кожного $z \in R_l$ позначимо ϕ_z часткову функцію переходів РЗ $\mathfrak{R}(f, A)$: $\phi_z(s) = \phi(s, z)$, $s \in V_l^n$. Якщо РЗ знаходиться в початковому стані $s^{(0)}$, а на його вхід подається довільна послідовність z_0, z_1, \dots двійкових векторів довжини l , то стан регістру в j -му такті визначається за формулою $s^{(j)} = (\phi_{z_{j-1}} \circ \dots \circ \phi_{z_0})(s^{(0)})$, $j = 0, 1, \dots$

Зауважимо, що на підставі формули (4) та оборотності матриць A_1, \dots, A_n кожна функція ϕ_z є підстановкою на множині V_l^n , і для будь-яких двох станів $s, s' \in V_l^n$ РЗ $\mathfrak{R}(f, A)$ існує точно одна послідовність $(z_1, \dots, z_n) \in V_l^n$ така, що $s' =$

$(\phi_{z_1} \circ \dots \circ \phi_{z_n})(s)$ (іншими словами, $\mathfrak{R}(f, A)$ є регулярним автоматом, будь-який стан якого є досяжним з будь-якого іншого стану за n кроків, і при тому єдиним способом).

Для означення класу стискувальних функцій реєстрового типу введемо одне допоміжне відображення. Зафіксуємо натуральне число $T > m$, матриці $B_1, \dots, B_m \in F_{l \times l}$, комутативну групову операцію $\dot{+}$ на множині V_l та задамо відображення $G: V_l^m \rightarrow V_l^T$, вважаючи

$$G(x_0, \dots, x_{m-1}) = (x_0, \dots, x_{T-1}), (x_0, \dots, x_{m-1}) \in V_l^m, \quad (5)$$

де

$$x_{i+m} = x_i \dot{+} B_1 + x_{i+1} \dot{+} B_2 + \dots + x_{i+m-1} \dot{+} B_m, i \in \overline{0, T-m-1}. \quad (6)$$

Нарешті, зафіксуємо довільну групову операцію $*$ на множині V_N та розглянемо стискувальну функцію

$$h(s, x) = s * g(s, x), (s, x) \in V_N \times V_M, \quad (7)$$

де

$$g(s, x) = (\phi_{x_{T-1}} \circ \dots \circ \phi_{x_0})(s), (s, x) \in V_N \times V_M, \quad (8)$$

а вектор $(x_0, \dots, x_{T-1}) = G(x)$ задається за допомогою співвідношень (5), (6). Обчислення значень функції h відбувається у три етапи. Спочатку за вхідним вектором $x \in V_M$ (або, що те ж саме, за набором $(x_0, \dots, x_{m-1}) \in V_l^m$) формується послідовність x_0, \dots, x_{T-1} . Далі вона подається на вхід реєстру $\mathfrak{R}(f, A)$, переводячи його з початкового стану s у фінальний стан $g(s, x)$. Нарешті, обчислюється значення $h(s, x)$ за формулою (7).

Зауважимо, що за описаною схемою будуть стискувальні функції окремих алгоритмів сім'ї MDx, лише з тією відмінністю, що функція f у виразі підстановки ϕ_{x_j} (див. формули (4), (8)), взагалі кажучи, залежить від номера $j \in \overline{0, T-1}$. Приймаючи це до уваги, сформулюємо таке означення.

Означення. Нехай $M = ml$, $N = nl$, де l, m, n – натуральні числа, більші за 1, $*$ – групову операцію на множині V_N . Тоді відображення h вигляду (7) називається *стискувальною функцією реєстрового типу*, якщо існують натуральне число $T > m$, функції $f_j: V_l^{n-1} \rightarrow V_l$, $j \in \overline{0, T-1}$, і матриці $A_1, \dots, A_n \in GL(l, 2)$, $B_1, \dots, B_m \in F_{l \times l}$ такі, що

$$g(s, x) = (\phi_{x_{T-1}}^{(T-1)} \circ \dots \circ \phi_{x_0}^{(0)})(s), (s, x) \in V_N \times V_M, \quad (9)$$

де вектор $(x_0, \dots, x_{T-1}) = G(x)$ визначається за формулами (5), (6), а

$$\phi_z^{(j)}(s) = (s_n A_n + z + f_j(s_1, \dots, s_{n-1}), s_1 A_1, \dots, s_{n-1} A_{n-1}) \quad (10)$$

для будь-яких $s = (s_1, \dots, s_n) \in V_l^n$, $z \in V_l$, $j \in \overline{0, T-1}$.

Приклад 2. Стискувальна функція алгоритму SHA-1 є функцією реєстрового типу. При цьому $l = 32$, $m = 16$, $n = 5$, $T = 80$, а матриці A_1, \dots, A_5 у формулі (10) визначаються таким чином: $A_1 = A_3 = A_4 = A_5 = I_{32}$, $A_2 = C^{30}$, де I_{32} – одинична матриця порядку 32, C – матриця оператора циклічного зсуву на 1 біт ліворуч. Функція f_j має наступний вигляд:

$f_j(s_2, s_3, s_4) = s_1 C^5 + \tilde{f}_j(s_2, s_3, s_4) + K_j$, $s_1, s_2, s_3, s_4 \in V_{32}$, де $K_j \in V_{32}$ – певна константа,

$$\tilde{f}_j(s_2, s_3, s_4) = \begin{cases} s_2 s_3 \oplus \overline{s_2 s_4}, & 0 \leq j \leq 19; \\ s_2 \oplus s_3 \oplus s_4, & 20 \leq j \leq 39; 60 \leq j \leq 79; \\ s_2 s_3 \oplus s_2 s_4 \oplus s_3 s_4, & 40 \leq j \leq 59, \end{cases}$$

а операції булева множення, додавання та заперечення виконуються над векторами s_2, s_3, s_4 по координатно. Крім того, операція $\dot{+}$ у формулі (6) співпадає з покоординатним булевим додаванням на множині V_l , а відображення G є лінійним над полем F : $G(x_0, \dots, x_{15}) = (x_0, \dots, x_{79})$, де $x_{i+16} = (x_i \oplus x_{i+2} \oplus x_{i+8} \oplus x_{i+13})C$, $i \in \overline{0, 63}$ [10].

Зауважимо, що для побудови стискувальних функцій можна використовувати реєстри зсуву більш загального вигляду, що визначаються за допомогою довільних відображень множини V_l^{n+1} у множини V_l .

Для будь-якого відображення $F_j: V_l^{n+1} \rightarrow V_l$ та послідовності $\tilde{A} = (A_1, \dots, A_{n-1})$, де $A_1, \dots, A_{n-1} \in GL(l, 2)$, позначимо $\tilde{\mathfrak{R}}(F_j, \tilde{A})$ автомат без виходу з вхідним алфавітом V_l , множиною станів V_l^n та функцією переходів

$$\phi_z^{(j)}(s) = (F_j(z, s_1, \dots, s_n), s_1 A_1, \dots, s_{n-1} A_{n-1}),$$

$$s = (s_1, \dots, s_n) \in V_l^n, z \in V_l, j \in \overline{0, T-1}. \quad (11)$$

Зрозуміло, що зазначений автомат співпадає з означеним вище РЗ $\mathfrak{R}(f_j, A)$ у випадку, коли $A = (\tilde{A}, A_n)$, $F_j(z, s_1, \dots, s_n) = s_n A_n + z + f_j(s_1, \dots, s_{n-1})$ для будь-яких $z, s_1, \dots, s_n \in V_l$, $j \in \overline{0, T-1}$. Отже, замінюючи у формулюванні означення функцій реєстрового типу формулу (10) на формулу (11), отримаємо більш широкий клас стискувальних

функцій, який охоплює майже всі відомі алгоритми гешування сім'ї MDx (при цьому, як правило, відображення $F_j: V_l^{n+1} \rightarrow V_l$, $j \in \overline{0, T-1}$, є бієктивним за кожною змінною z , s_n при будь-яких фіксованих значеннях решти).

Приклад 3. Стискувальна функція алгоритму MD5 будується на основі РЗ $\mathfrak{R}(F_j, \tilde{A})$, де $l=32$, $m=16$, $n=4$, $T=64$, $A_1=A_2=A_3=I_{32}$,

$F_j(z, s_1, s_2, s_3, s_4) = s_1 + (f_j(s_1, s_2, s_3) + s_4 + z + K_j)C^{v_j}$,
 C – матриця оператора циклічного зсуву на 1 біт ліворуч, K_j, v_j – певні константи,

$$f_j(s_1, s_2, s_3) = \begin{cases} s_1 s_2 \oplus \overline{s_1 s_3}, & 0 \leq j \leq 15; \\ s_1 s_3 \oplus \overline{s_3 s_2}, & 16 \leq j \leq 31; \\ s_1 \oplus s_2 \oplus s_3, & 32 \leq j \leq 47; \\ s_2 \oplus (s_1 \vee \overline{s_3}), & 48 \leq j \leq 63. \end{cases}$$

Зауважимо, що відображення F_j , $j \in \overline{0, 63}$, є бієктивним за кожною змінною z , s_4 при фіксованих значеннях решти. При цьому відображення G , що визначає спосіб формування вхідної послідовності x_0, \dots, x_{T-1} за її початковим відрізком $(x_0, \dots, x_{m-1}) \in V_l^m$, має вигляд, відмінний від (6), і задається наступним чином:

$$x_i = \begin{cases} x_{(1+5i) \bmod 16}, & 16 \leq i \leq 31; \\ x_{(5+3i) \bmod 16}, & 32 \leq i \leq 47; \\ x_{(7i) \bmod 16}, & 48 \leq i \leq 63. \end{cases}$$

Розглянемо зараз довільну стискувальну функцію реєстрового типу $h: V_N \times V_M \rightarrow V_N$ і довільний вектор $s^{(0)} \in V_N$. Зрозуміло, що побудування колізій функції $h_{s^{(0)}}$ рівносильно розв'язанню системи рівнянь

$$(\phi_{x_{T-1}}^{(T-1)} \circ \dots \circ \phi_{x_0}^{(0)})(s^{(0)}) = (\phi_{x_{T-1}}^{(T-1)} \circ \dots \circ \phi_{x_0}^{(0)})(s^{(0)}), \quad (12)$$

$$(x_0, \dots, x_{T-1}) = G(x_0, \dots, x_{m-1}),$$

$$(x'_0, \dots, x'_{T-1}) = G(x'_0, \dots, x'_{m-1}) \quad (13)$$

відносно пари різних невідомих $x, x' \in V_M$. Зауважимо, що перше з цих двох рівнянь (відносно довільних наборів невідомих (x_0, \dots, x_{T-1}) , $(x'_0, \dots, x'_{T-1}) \in V_l^T$, без урахування обмеження (13)) розв'язується тривіально. Це випливає з наступного твердження.

Твердження. Нехай $A_1, \dots, A_n \in GL(l, 2)$, $f_j: V_l^{n+1} \rightarrow V_l$, а функція $\phi_z^{(j)}$ визначається за формулою (10), $z \in V_l$, $j \in \overline{0, T-1}$. Тоді для будь-яких

$s, s' \in V_l^n$, $j_0, \dots, j_{n-1} \in \overline{0, T-1}$ існує точно один вектор $(x_0, \dots, x_{n-1}) \in V_l^n$ такий, що $s' = (\phi_{x_{n-1}}^{(j_{n-1})} \circ \dots \circ \phi_{x_0}^{(j_0)})(s)$.

Доведення. Нехай для простоти позначень $j_i = i$, $i \in \overline{0, n-1}$. Покладемо

$$s^{(i)} = (\phi_{x_{i-1}}^{(i-1)} \circ \dots \circ \phi_{x_0}^{(0)})(s^{(0)}) = (s_1^{(i)}, \dots, s_n^{(i)}), \quad i \in \overline{0, n}. \quad (14)$$

Треба показати, що вектор (x_0, \dots, x_{n-1}) однозначно визначається з системи рівнянь (14) за відомими значеннями $s^{(0)}$ та $s^{(n)}$.

З формул (10) та (14) випливають наступні рівності:

$$s_1^{(i)} = s_n^{(i-1)} A_n + f_{i-1}(s_1^{(i-1)}, \dots, s_{n-1}^{(i-1)}) + x_{i-1},$$

$$s_2^{(i)} = s_1^{(i-1)} A_1, \dots, s_{n-1}^{(i)} = s_{n-2}^{(i-1)} A_{n-2}, s_n^{(i)} = s_{n-1}^{(i-1)} A_{n-1}, \quad i \in \overline{1, n}. \quad (15)$$

Використовуючи формули (15), отримаємо, що $s_n^{(n)} = s_{n-1}^{(n-1)} A_{n-1} = s_{n-2}^{(n-2)} A_{n-2} A_{n-1} = \dots = s_1^{(1)} A_1 \cdots A_{n-1} = (s_n^{(0)} A_n + f_0(s_1^{(0)}, \dots, s_{n-1}^{(0)}) + x_0) A_1 \cdots A_{n-1}$.

З останньої рівності можна однозначно відновити x_0 за відомими $s^{(0)}$ та $s^{(n)}$, а, отже, обчислити $s^{(1)}$ за формулою (14).

Далі, використовуючи формули (15), отримаємо, що $s_{n-1}^{(n)} = s_{n-2}^{(n-1)} A_{n-2} = s_{n-3}^{(n-2)} A_{n-3} A_{n-2} = \dots = s_1^{(2)} A_1 \cdots A_{n-2} = (s_n^{(1)} A_n + f_1(s_1^{(1)}, \dots, s_{n-1}^{(1)}) + x_1) A_1 \cdots A_{n-2}$.

Звідси однозначно відновимо x_1 та обчислимо значення $s^{(2)}$ за формулою (14).

Продовжуючи аналогічні міркування, однозначно відновимо усі координати вектора (x_0, \dots, x_{n-1}) . Твердження доведено.

Наслідок 1. За умовою твердження бінарна операція

$$(s, x) \mapsto (\phi_{x_{n-1}}^{(j_{n-1})} \circ \dots \circ \phi_{x_0}^{(j_0)})(s), \quad s, x = (x_0, \dots, x_{n-1}) \in V_l^n$$

є квазігрупою на множині V_l^n (тобто оборотна за кожним аргументом при фіксованому іншому).

Наслідок 2. Нехай $T = nt$. Тоді для будь-яких $s, s' \in V_l^n$ рівняння

$$(\phi_{x_{T-1}}^{(T-1)} \circ \dots \circ \phi_{x_0}^{(0)})(s) = s'$$

має точно $2^{t(T-n)}$ розв'язків $(x_0, \dots, x_{T-1}) \in V_l^T$, які знаходяться у взаємно однозначній відповідності з наборами $(s^{(n)}, s^{(2n)}, \dots, s^{(t-1)n}) \in V_N^t$.

Зауважимо, що отримане твердження та наслідки з нього залишаються справедливими й у більш загальному випадку, коли функція $\phi_z^{(j)}$ визначаються за формулою (11), а відображення $F_j: V_l^{n+1} \rightarrow V_l$ є бієктивним за кожною змінною z , s_n при будь-яких фіксованих значеннях решти, $j \in \overline{0, T-1}$.

Таким чином, якщо $h: V_N \times V_M \rightarrow V_N$ є функцією реєстрового типу, то для будь-якого вектора $s^{(0)} \in V_N$ множина всіх розв'язків $((x_0, \dots, x_{T-1}), (x'_0, \dots, x'_{T-1})) \in V_l^T \times V_l^T$ рівняння (12) має простий алгоритмічний опис, що дозволяє перелічувати ці розв'язки в режимі реального часу. Тому основна трудність побудування колізій функції $h_{s^{(0)}}$ полягає в знаходженні саме таких розв'язків, які задовольняють додатковому обмеженню (13).

Для розв'язання систем рівнянь (12), (13), в принципі, можуть бути застосовані відомі загальні методи, зокрема, ймовірнісний метод [2] або метод статистичних наближень скінченних автоматів [1, 6]. Зауважимо, що ідеї, на яких базуються останні два методи, використовуються при побудові так званих різнецевих атак на стискувальні функції алгоритмів гешування сім'ї MDx [6, 11–16].

Висновки. Стискувальні функції майже усіх сучасних алгоритмів гешування сім'ї MDx будуються на основі певних реєстрів зсуву над алфавітом потужності 2^l , де, як правило, $l=32$. Задача побудування колізій стискувальних функцій реєстрового типу рівносильна розв'язанню систем автоматних рівнянь вигляду (12) при обмеженнях (13), причому множини всіх розв'язків таких рівнянь (без урахування обмежень) мають простий алгоритмічний опис, що дозволяє перелічувати ці розв'язки в режимі реального часу. Отже, стійкість зазначених геш-функцій відносно атак, спрямованих на побудування колізій, базується на складності знаходження хоча б одного елемента перетину двох скінченних множин, кожна з яких задається за допомогою простих алгоритмічних процедур. Фактичне значення стійкості кожного окремого алгоритму гешування з означеного класу залежить від властивостей функції зворотного зв'язку (вигляду (10) або (11)) відповідного реєстру зсуву та відображення G вигляду (5).

Однією з задач подальших досліджень є побудова систем автоматних рівнянь, що описують стискувальні функції більш складних алгоритмів гешування, подібних SHA-256 та SHA-512. Зокрема, викликає інтерес відповідь на запитання про справедливість для зазначених алгоритмів аналогу твердження, доведеного у даній статті.

ЛІТЕРАТУРА

- [1]. Бабаш А.В. Решение автоматных уравнений с искажениями в функции перехода автомата // Проблемы передачи информации. – 2002. – Т. 38. – Вып. 3. – С. 62-71.
- [2]. Балакин Г.В. О вероятностном подходе к решению систем уравнений с целочисленными неиз-

вестными // Дискретная математика. – 1995. – Т. 7. – Вып. 1. – С. 88-98.

- [3]. Карпунин Г.А., Ермолаева Е.З. Оценки сложности поиска коллизий для хэш-функции RIPEMD // Прикладная дискретная математика. Приложение. – 2012. – № 5. – С. 43-44.
- [4]. Фергюссон Н., Шнайер Б. Практическая криптография: Пер. с англ. – М.: “Вильямс”, 2005. – 424 с.
- [5]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.
- [6]. Chabaud F., Joux A. Differential collision search attack on SHA-0 // Advances in Cryptology – CRYPTO'98, Proceedings. – Springer-Verlag, 1998. – P. 56-71.
- [7]. Damgård I.B. A design principle for hash function // Advances in Cryptology – CRYPTO'89, Proceedings. – Springer-Verlag, 1990. – P. 416-427.
- [8]. ECRYPT II: Final hash function status report / <http://www.ecrypt.eu.org/documents/D.SYM.11>, 31 Jan., 2013.
- [9]. Merkle R.C. On way hash function and DES // Advances in Cryptology – CRYPTO'89, Proceedings. – Springer-Verlag, 1990. – P. 428-436.
- [10]. National Institute of Standards and Technology (NIST). FIPS-180-2: Secure Hash Standard, <http://www.itl.nist.gov/fipspubs>.
- [11]. Pramstaller N., Rechberger C., Rijmen V. Exploiting coding theory for collision attacks on SHA-1 // Cryptography and Coding 2005, Proceedings. – Springer-Verlag, 2005. – P. 78-95.
- [12]. Rijmen V., Oswald E. Update on SHA-1 // Topics in Cryptology. – CT-RSA, Proceedings. – Springer-Verlag, 2005. – P. 58-71.
- [13]. Wang X., Lai X., Feng D., Chen H., Yu X. Cryptanalysis of the hash functions MD4 and RIPEMD // Advances in Cryptology – EUROCRYPT'2005, Proceedings. – Springer-Verlag, 2005. – P. 1-18.
- [14]. Wang X., Yu H. How to break MD5 and other hash functions // Advances in Cryptology – EUROCRYPT'2005, Proceedings. – Springer-Verlag, 2005. – P. 19-35.
- [15]. Wang X., Yu H., Yin Y.L. Efficient collisions search attacks on SHA-0 // Advances in Cryptology – CRYPTO'2005, Proceedings. – Springer-Verlag, 2005. – P. 1-16.
- [16]. Wang X., Yu H., Yin Y.L. Finding collisions in the full SHA-1 // Advances in Cryptology – CRYPTO'2005, Proceedings. – Springer-Verlag, 2005. – P. 17-36.

REFERENCES

- [1]. Babash A. V. Solving automaton equations with distortions in the automaton transition function. Problems of Information Transmission, 2002, vol. 38(3), pp. 218-226.
- [2]. Balakin G. V. On a probabilistic approach to solving systems of equations with integer-valued unknowns, Discrete Mathematics and Applications, 1995, vol. 5(1), pp. 43-51.

- [3]. Kapurnin G. A., Ermolaeva E. Z. Estimates of collision resistance complexity for the hash function RIPEMD. *Discrete Applied Mathematics. Application.* 2012, № 5, pp. 43- 44.
- [4]. Ferguson N., Schneier B. *Practical cryptography.* John Wiley & Sons, 2003, 432 p.
- [5]. Schneier B. *Applied cryptography: Protocols, algorithms, and source code in C, 2nd Edition.* John Wiley & Sons, 1995, 784 p.
- [6]. Chabaud F., Joux A. Differential collision search attack on SHA-0. *Advances in Cryptology – CRYPTO’98, Springer-Verlag, 1998, pp. 56-71.*
- [7]. Damgård I. B. A design principle for hash function. *Advances in Cryptology – CRYPTO’89, Springer-Verlag, 1990, pp. 416-427.*
- [8]. ECRYPT II: Final hash function status report. <http://www.ecrypt.eu.org/documents/D.SYM.11>, 31 Jan., 2013.
- [9]. Merkle R.C. On way hash function and DES. *Advances in Cryptology – CRYPTO’89., Springer-Verlag, 1990, pp. 428-436.*
- [10]. National Institute of Standards and Technology (NIST). FIPS-180-2: Secure Hash Standard, <http://www.itl.nist.gov/fipspubs>.
- [11]. Pramstaller N., Rechberger C., Rijmen V. Exploiting coding theory for collision attacks on SHA-1. *Cryptography and Coding 2005, Springer-Verlag, 2005, pp. 78-95.*
- [12]. Rijmen V., Oswald E. Update on SHA-1. *Topics in Cryptology. CT-RSA, Springer-Verlag, 2005, pp. 58-71.*
- [13]. Wang X., Lai X., Feng D., Chen H., Yu X. Cryptanalysis of the hash functions MD4 and RIPEMD. *Advances in Cryptology – EUROCRYPT’2005, Springer-Verlag, 2005, pp. 1-18.*
- [14]. Wang X., Yu H. How to break MD5 and other hash functions. *Advances in Cryptology – EUROCRYPT’2005, Springer-Verlag, 2005, pp. 19-35.*
- [15]. Wang X., Yu H., Yin Y.L. Efficient collisions search attacks on SHA-0. *Advances in Cryptology – CRYPTO’2005, Springer-Verlag, 2005, pp. 1-16.*
- [16]. Wang X., Yu H., Yin Y.L. Finding collisions in the full SHA-1. *Advances in Cryptology – CRYPTO’2005, Springer-Verlag, 2005, pp. 17-36.*

БЕЗКЛЮЧЕВЫЕ ХЭШ-ФУНКЦИИ РЕГИСТРОВОГО ТИПА

Безключевые хэш-функции относятся к наиболее важным криптографическим примитивам и применяются в современных системах шифрования, аутентификации, цифровой подписи, генерации ключей и т.д. Несмотря на заметный процесс в разработке различных атак на “конкретные” хэш-функции, понимание закономерностей, лежащих в основе указанных атак, нахождение условий их применимости и разработка методов оценивания их эффективности являются предметом активных дальнейших исследований. Цель статьи состоит в установлении общих условий, определяющих практическую стойкость широкого

класса хэш-функций, основанных на регистрах сдвига, относительно атак, направленных на построение коллизий их сжимающих функций. Показано, что задача построения коллизий сводится к решению автоматных уравнений относительно двоичных неизвестных, удовлетворяющих определенным ограничениям. При этом множества всех решений таких уравнений (без учета ограничений) имеют простое алгоритмическое описание, что позволяет перечислять эти решения в режиме реального времени.

Ключевые слова: безключевая хэш-функция, поиск коллизий, конечный автомат, нелинейный регистр сдвига, система автоматных уравнений, MDx, SHA.

KEYLESS HASH FUNCTIONS OF SHIFT REGISTERS TYPE

Keyless hash functions are one of the most important cryptographic primitives and are used in modern encryption, authentication, digital signature, keys generation systems, etc. Although conspicuous progress in developing of various attacks on "specific" hash functions, understanding of the principles underlying these attacks, determining the conditions of their applicability, and development of methods for their performance estimating is an active subject of further research. The goal of this paper is to establish the general conditions of practical security for a broad class of hash functions based on shift registers against collision search attacks on their compression functions. It is shown that the problem of building of collisions can be reduced to solving some automaton equations with binary unknowns satisfying certain constraints. Then the set of all solutions of these equations (without constraints) have simple algorithmic description that allows to enumerate these solutions in the real time-mode.

Index Terms: keyless hash function, collision search attacks, finite state automaton, nonlinear shift register, system of automaton equations, MDx, SHA.

Олексійчук Антон Миколайович, доктор технічних наук, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».

E-mail: alex-crypto@mail.ru

Алексейчук Антон Николаевич, доктор технических наук, профессор Института специальной связи и защиты информации НТУУ «КПИ».

Alekseychuk Anton, Doctor of Technical Science, Professor of Institute of Special Communication and Information Security of NTUU «KPI».

Король Катерина Вікторівна, аспірантка Донецького національного університету.

E-mail: kate.lorok@gmail.com

Король Екатерина Викторовна, аспирантка Донецького національного університету.

Korol Kate, post-graduate student of Donetsk National University.