УДК 003.26:004.056.55

А.Ю. Дяченко

Черкаський національний університет імені Богдана Хмельницького, Черкаси

КРИПТОГРАФІЧНЕ ХЕШУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНИХ МОДЕЛЕЙ

Представлений новий метод криптографічно стійкого хешування інформації та основі багатопараметричних моделей. Оскільки розроблена хеш-функція є незворотною і стійкою до колізій першого та другого роду, то вона може бути використана для криптографічного хешування інформації у найрізноманітніших інформаційних системах. Складовою частиною запропонованого методу хешування інформації є генератор псевдовипадкових чисел на базі багато-параметричних моделей. Результати досліджень показують, що генератор є близьким до еталонного. Відповідно обчислювальна складність знаходження колізій близька до $2^{n/2}$, тобто хеш-функція є криптостікою.

Ключові слова: *багатопараметрична модель, криптографічне хешування, криптографічна стійкість, захист інформації.*

Вступ

Постановка проблеми. За останні роки були виявлені недоліки в відомих методах хешування інформації. Наприклад: проблема стійкості мультиколізій (Антоні Жукс) [1], алгоритм пошуку колізій в хеш-функції MD5 (Ван Сяоюнь и Юй Хунбо), атака на SHA-1 (Крістоф де Каньєр, Крістіан Рехберг), можливість генерації підробних цифрових сертифікатів на основі колізій в MD5 (Сотіров Олександр, Марк Стівенс) та ін. Водночас в зв'язку зі стрімким зростанням потужності апаратної складової комп'ютерів стають практично актуальними навіть ті типи криптографічних атак, що відносно нещодавно були неактуальними через занадто великі обсяги обчислень. Тому актуальною є задача розробки нових криптографічних методів хешування інформації.

Аналіз останніх досліджень і публікацій. Хешування інформації застосовується при вирішенні широкого кола різноманітних завдань: в програмуванні при побудові асоціативних масивів, пошуку дублікатів в даних, знаходження контрольної суми при передачі інформації. Серед методів хешування особливий клас складають криптографічно стійкі, що призначені для застосування в системах захисту інформації: при генерації цифрового підпису, для збереження паролів та ін. Найбільш відомими методами криптографічного хешування є MD (5,6), SHA (1,2,3), RIPEMD и HAVAL та ГОСТ Р 34.10-2001 [2].

В останні роки здійснюється багато досліджень по розробці нових та вдосконаленню існуючих методів криптографічного хешування. Наприклад, Лужецький В. А. та Баришев Ю. В. розробили конструкцію багатоканального хешування, що дало можливість узагальнити та удосконалити відомі підходи підвищення стійкості хешування до мультиколізій [3]. Бойко А. О. та Горбенко І. Д. запропонували критерії, показники та методику оцінки функцій хешування з підвищеною швидкодією [4]. При цьому підвищення швидкодії досягається за рахунок розпаралелювання обчислень. Цікавим є різновид каскадно-комбінаційного хешування даних в схемах аутентифікації в Інтернет-платіжних системах під час розрахунків банківською карткою в Інтернеті, що запропонований Клювак О. В [5]. Ще одним напрямком є застосування нейронних мереж для вирішення задач захисту інформації [6], в тому числі для хешування даних.

На сьогодні існуючі методи хешування даних в інформаційних системах поповнились методами хешування на основі багатопараметричних моделей (БМ). Аналіз структури та дослідження функціонування багатопараметричних моделей надає нові можливості для перетворення інформації, що і стало основою нового методу криптографічного хешування.

Формулювання мети статті. Метою роботи є розробка нових методів криптографічно стійкого хешування інформації на основі БМ.

Була сформульована гіпотеза про те, що у хеш-функції можна використовувати числа з криптографічно стійкого генератора псевдовипадкових послідовностей на основі БМ.

Для досягнення поставленої мети послідовно розв'язуються наступні задачі: порівняльний аналіз відомих методів криптографічного хешування; розробка нового алгоритму криптографічно стійкого хешування на основі БМ; дослідження властивостей розробленого алгоритму та реалізація розроблених методів в спеціалізованих програмах.

Виклад основного матеріалу

Хеш-функція H є криптографічно стійкою якщо вона задовольняє наступним трьом основним вимогам:

1. Незворотність або стійкість до відновлення праобразу: для певного значення хеш-функції m

повинно бути обчислювально неможливо знайти блок даних X, для якого H(X) = m.

2. Стійкість до колізій першого роду або відновленню других праобразів: для заданого повідомлення M повинно бути обчислювально неможливо підібрати друге повідомлення N, для якого H(N) = H(M).

3. Стійкість до колізій другого роду: повинно бути обчислювально неможливо підібрати пару повідомлень (M, MI), що мають однаковий хеш [7].

Не доведено існування необернених хеш-функцій, для яких обчислення будь-якого праобразу певного значення хеш-функції теоретично неможливо. Тому знаходження оберненого значення є лише обчислювально важкою задачею.

Також для криптографічних хеш-функцій важливо, щоб при незначній зміні аргументу значення функції суттєво змінювалось. Така властивість називається «лавинним ефектом». У [8] показано, що БМ можуть використовуватися в якості генератора псевдовипадкових послідовностей (ГПП). Для дослідження розробленого ГПП на основі багатопараметричних моделей було проведено серію експериментів з використанням комп'ютерної програми RandomTest, що спеціально розроблена для дослідження псевдовипадкових послідовностей.

Узагальнені результати експериментів наведено у табл. 1 (кількість елементів послідовності - 10000000).

Таблиця 1

Результат дослідження генератора псевдовипадкової послідовності

Предметна область	Математичне сподівання	Дисперсія	Середньо-квадратичне відхилення	Частотний тест, %	«хі-квадрат», %	Коеф. Монте-Карло, %	Коеф. кореляції
1. Серцево-судинні захворювання	0,499997	0,083336	0,288745	57,6514	51,6276	0,0534	0,000178
2. Економіка США	0,499999	0,083378	0,288748	57,6537	51,6292	0,0567	0,000175
3. Забрудненість атмосфери	0,499999	0,083371	0,288719	57,6572	51,6245	0,0573	0,000176
4. Функції математичної логіки	0,499997	0,083363	0,288742	57,6563	51,6247	0,0593	0,000178
5. Захворювання на рак	0,499998	0,083335	0,288744	57,6511	51,6225	0,0562	0,000175
6. Соціологічні опитування	0,499999	0,083338	0,288748	57,6565	51,6244	0,0552	0,000177

Порівнюючи результати експериментів з вимогами до еталонних ГПП можна зробити висновок, що розроблений ГПП дуже близький до еталонного. Крім того отримані елементи ПП мають такі особливості: рівноймовірний розподіл усіх символів використовуваного алфавіту, при зміні початкового значення ГПП суттєво відрізняються від попередніх, не містять періодичних, кореляційних та інших залежностей. Тобто псевдовипадкова послідовність (ПП) є достатньо якісною для криптографічних методів. В запропонованому алгоритмі хешування на основі БМ спочатку здійснюється розбиття вхідної інформації на блоки певного розміру. В загальному випадку розмір блоку може бути довільним, але для забезпечення достатнього рівня криптостійкості рекомендується обирати розмір блоку не менше 128 біт. Далі над блоком виконуються операції XOR (виключне АБО), циклічного побітового зсуву, інверсії (логічне NOT). При цьому числа з ГПП використовуються як параметри операцій над блоками двійкових даних.

Очевидно, що для знаходження колізій в даному методі необхідно розробити алгоритм, що дозволяє прогнозувати ГПП. Оскільки ГПП є дуже близьким до еталонного, то спрогнозувати його практично неможливо. Отже, запропонована хеш-фукнція є практично незворотною та стійкою до колізій першого та другого роду, і, відповідно, криптографічно стійкою.

Дослідження даного методу здійснювалось шляхом знаходження хешів для всіх слів з словників англійської (483524 слів), російської (162164 слів) та української (105872 слів) мов. Додатково використовувався об'єднаний словник зі слів усіх трьох мов. Хеш знаходився не тільки для кожного слова з словника, а і для декількох модифікацій даного слова. Модифікація здійснювалась шляхом випадкової заміни 1-3 літер в слові. Наприклад, для слова «молоко» можливі такі модифікації: «нолоко», «молока», «молоно» та ін. В результаті досліджень однакових хешів для різних слів не виявлено. Приклади хешування наведено у табл. 2.

Таблиця 2

Приклади хешування даних

Початкове значення	Результат хешування (хеш)
молоко	273D97E472B3178C9949A3F026EE444F
Молоко	F7DB5B78B3C2BE403CE8070CA981A99A
нолоко	B168A306BBD1CE0D58F57F9ED57712D5
молОко	072FB7A671E50703EAB7924BEF1695DD
молоКо	D3E39DEA9433C024CF1A9DF7904B4B18
омлоко	24E0139A18FA20933213D6868F88063D
молоно	431CA0F8163682FC84C86A80740B7060
молака	9996161B3A51AF3EF54E0459C059D302
молока	93B6B3BB7892776826FB47A2B7A336B6
молоко1	AC01328E6A6097E78994754AA781FF8E
молоко11	A1F8B2E8BE3829DCF5DD1FCA92DE9D92
молоко2	6E446BE5DF3B94CE2D9F9520E9B89FDE
1молоко	8C64D4FE388C453245D0468BED6AA859

Як видно з табл. 2 при незначній зміні початкового значення хеш суттєво змінюється. Тобто запропонований метод забезпечує «лавинний ефект», що дозволяє уникнути витоку інформації навіть про окремі біти початкового значення.

Висновки

В результаті досліджень було виявлено, що запропонований новий хешування інформації на основі багатопараметричних моделей є криптографічно стійким. Використання принципу роботи багатопараметричних моделей та специфіка процесу генерації псевдовипадкових чисел забезпечує методу необхідну криптостійкість та універсальність, що виступає суттєвою перевагою при його впровадженні для криптографічного захисту інформаційних систем. Слід виділити перспективи досліджень в галузі застосування багатопараметричних моделей для задач хешування інформації: підвищення швидкодії за рахунок розпаралелювання процесу хешування; виявлення типів та параметрів БМ, що найбільш придатні для задач хешування; розробка нових та вдосконалення існуючих систем цифрового підпису на основі хешування з використанням БМ.

Список літератури

1. Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions / Antoine Joux // Lecture Notes in Computer Science. – 2004. – № 3152. – С. 306-316.

2. Шнайер Б. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Вильямс, 2005. – 425 с.

3. Лужецький В.А. Конструкції хешування стійкі до мультиколізій / В.А.Лужецький, Ю.В. Баришев // Збірник «Наукові праці ВНТУ». - Вінниця, 2010. — Т. 1. — С. 5- 13.

4. Бойко А.О. Обґрунтування архітектури функції хешування з використанням паралельних обчислень / А.О. Бойко, І.Д. Горбенко // Збірник «Вісник Харківського національного університету». – Х., 2010. — № 810. — С. 29- 36.

5. Клювак О.В. Механізм безпечної передачі аутентифікаційних даних в Інтернет платіжних системах / О.В. Клювак // Збірник «Фінансово-кредитна діяльність: проблеми теорії та практики». – К., 2012. – Т. 1. — С. 123- 136.

6. Томашевський О.М. Криптографічний захист інформаційних систем на базі штучної нейронної мережі / О.М. Томашевський // Збірник «Труды Одесского политехнического университета».– Одеса, 2001. — Т. 4(16).– С. 74–77.

7. Halunen K. An Automata-Theoretic Interpretation of Iterated Hash Functions – Application to Multicollisions / Kimmo Halunen, Juha Kortelainen, Tuomas Kortelainen // Cryptology ePrint Archive. – 2009. – 13 с.

8. Дяченко А.Ю. Генератор псевдовипадкових послідовностей на основі індуктивних моделей / А.Ю. Дяченко, С.В. Голуб, В.В. Квасніков // Вісник Інженерної академії України. – К., 2009. — Т.2. — С. 87- 89.

Надійшла до редколегії 2.04.2015

Рецензент: д-р техн. наук, проф. С.В. Голуб, Черкаський національний університет імені Богдана Хмельницького, МОН України, Черкаси.

КРИПТОГРАФИЧЕСКИЕ ХЕШИРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ МНОГОПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ

А.Ю. Дяченко

Представлен новый метод криптографически стойкого хеширования информации на основе многопараметрических моделей. Поскольку разработанная хеш-функция является необратимой и стойкой к коллизиям первого и второго рода, то она может быть использована для криптографического хеширования информации в разнообразных информационных системах. Составной частью предложенного метода хеширования информации является генератор псевдослучайных чисел на основе многопараметрических моделей. Результаты исследований показывают, что генератор является близким к эталонному. Соответственно, вычислительная сложность нахождения коллизий близка к $2^{n/2}$, то есть хеш-функция является криптостойкой.

Ключевые слова: *многопараметрическая модель, криптографическое хеширование, криптографическая стойкость, защита информации.*

CRYPTOGRAPHIC HASHING OF INFORMATION BASED ON MULTIVARIATE MODELS

A.Yu. Dyachenko

This article presents a new method of cryptographically resistant hashing information based on multivariate models. Since developed hash function is irreversible and resistant to collisions of the first and second kind, it could be used for cryptographic hashing of information in various data systems. Part of the proposed method hashing information is pseudorandom number generator based on multivariable models. The results show that the generator is close to the ideal. Accordingly, the computational complexity of finding collision close to $2^{n/2}$ and the hash function is cryptographically strong.

Ключевые слова: *multivariate models, cryptographic hashing, cryptographic resistance, protection of information.*