УДК 681.3.06 (0.43)

О.Г. Король[1], Л.Т. Пархуць[2], С.П. Євсеєв[1]
[1]Харьківський національний економічний університет,
[2]Національний університет "Львівська політехніка"

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ МЕТОДУ КАСКАДНОГО ФОРМУВАННЯ MAC З ВИКОРИСТАННЯМ МОДУЛЬНИХ ПЕРЕТВОРЕНЬ

Запропоновано метод каскадного формування MAC-коду з використанням модульних перетворень на основі алгоритмів MASH-1 і MASH-2. Досліджено швидкодію схем ключового гешування для фіксованих показників безпеки, оцінено складність формування MAC запропонованою схемою в кількості S-циклів 32-розрядного процесора на один байт оброблюваних даних.

Ключові слова: схема ключового гешування, модульні перетворення, каскадне формування MAC-коду.

The paper proposes a method for MAC code cascade formation using modular transformations based on algorithms MASH-1 and MASH-2. The performance of the scheme for fixed hash key safety parameters was studied and MAC formation using the proposed scheme in the amount of S-cycles of the 32-bit processor per byte of data being processed was estimated.

Key words: key hashing scheme, modular transformations, cascade formation of the MAC code.

Вступ

Результати проведених досліджень показали, що, застосовуючи багатошарові схеми ключового гешування, можна будувати ефективні механізми контролю цілісності й автентичності інформації в телекомунікаційних системах і мережах [1 – 8; 12]. Однак відомі багатошарові конструкції (наприклад, алгоритм UMAC) поряд з високими показниками швидкодії і криптографічної стійкості за рахунок застосування криптографічного шару перетворення (з використанням блокового симетричного шифру) втрачають властивості універсального гешування, що приводить до погіршення колізійних властивостей формованих кодів автентифікації повідомлень. Тому перспективним напрямом досліджень у цьому аспекті є розроблення й теоретичне обґрунтування нових схем ключового гешування, що дають можливість забезпечити як низькі колізійні властивості універсального гешування, так і високі показники безпеки.

Метою статті є розроблення методу каскадного формування MAC-коду з використанням модульних перетворень на основі алгоритмів MASH-1 і MASH-2, дослідження оцінки швидкодії та складності формування MAC запропонованою схемою в кількості S-циклів 32-розрядного процесора на один байт оброблюваних даних.

Основна частина. Розроблення методу каскадного формування MAC-коду з використанням модульних перетворень. Модульні перетворення поширені під час побудови криптографічних алгоритмів перетворення інформації, зокрема побудови асиметричних засобів захисту інформації й протоколів розповсюдження ключових даних [3; 5; 7; 11], для формування псевдовипадкових послідовностей [11], методів гешування та інших механізмів захисту інформації [3; 5; 7]. Аналіз літературних джерел [9 – 11] показує, що модульні перетворення застосовуються сьогодні для побудови безключових геш-функцій. Так, у четвертій частині міжнародного стандарту ISO/IEC 10118-4 визначено дві безключові функції гешування MASH-1 і MASH-2, які використовують модульну арифметику, а саме модульне зведення в ступінь для побудови геш-коду

[5; 8; 9; 12]. Сама назва функцій MASH-1 і MASH-2 походить від Modular Arithmetic Secure Hash (безпечне гешування на основі модулярної арифметики), що підкреслює застосування модулярних перетворень при формуванні геш-образу.

В основу запропонованого методу ключового універсального гешування доказової стійкості покладено використання модульних перетворень, що забезпечують розв'язання завдання знаходження прообразу або секретного ключа у схемі гешування до однієї з відомих теоретико-складних задач, наприклад, до завдання факторизації, дискретного логарифмування або завдання RSA, при цьому пропонується використовувати ітеративні циклові функції алгоритмів MASH-1 і MASH-2:

$$f(x_i, H_{i-1}) = \left(\left(\left((x_i \oplus H_{i-1}) \vee A\right)^2 \bmod N\right) \perp n\right) \oplus H_{i-1} \tag{1}$$

і

$$f(x_i, H_{i-1}) = \left(\left(\left((x_i \oplus H_{i-1}) \vee A\right)^{2^8+1} \bmod N\right) \perp n\right) \oplus H_{i-1}. \tag{2}$$

Запропонований метод універсального гешування основується на ітеративній схемі формування геш-коду із цикловою функцією, побудованою з використанням модульних перетворень. Для забезпечення низьких колізійних властивостей універсального гешування запропонована циклова функція повинна бути реалізована з використанням виразів (1) або (2) з відповідними обмеженнями на модульні перетворення [5; 8; 12]. Результати аналізу показують, що найвитратнішою з обчислювального погляду операцією при реалізації циклових функцій (1) і (2) є операція модульного піднесення до степеня. За безпосереднього піднесення до степеня через ланцюжок операцій множень обчислювальна складність реалізації таких циклових функцій зросте пропорційне показнику степеня, тобто для піднесення числа x до степеня n. Для зниження обчислювальної складності реалізації схем гешування з використанням циклових функцій (1) і (2) пропонується використовувати алгоритм швидкого піднесення до степеня, в основу якого покладено подання числа x^n у такому вигляді:

$$x^n = x^{((...((m_k \cdot 2 + m_{k-1}) \cdot 2 + m_{k-2}) \cdot 2 + ...) \cdot 2 + m_1) \cdot 2 + m_0} = ((...(((x^{m_k})^2 \cdot x^{m_{k-1}})^2 ...)^2 \cdot x^{m_1})^2 \cdot x^{m_0}, \tag{3}$$

де $(m_k, m_{k-1}, ..., m_0)$ – двійкове подання числа n, тобто $m_i \in \{0,1\}$ й

$$n = m_k \cdot 2^k + m_{k-1} \cdot 2^{k-1} + ... + m_1 \cdot 2 + m_0. \tag{4}$$

Перегрупувавши співмножники у поданні числа x^n, одержимо такий вираз:

$$x^n = x^{m_0} \cdot (x^2)^{m_1} \cdot (x^{2^2})^{m_2} \cdot (x^{2^3})^{m_3} \cdot ... \cdot (x^{2^k})^{m_k},$$

звідки випливає, що для піднесення числа x до степеня n потрібно реалізувати не більш ніж k операцій піднесення до квадрата і не більше ніж k операцій множення, де $k+1$ – кількість елементів у двійковому записі числа n, тобто $k = (\log_2 n) - 1$. Отже, асимптотичну обчислювальну складність обчислення x^n можна оцінити як $O(\log_2 n)$.

У табл. 1 наведено залежності складності реалізації операції піднесення до степеня через ланцюжок множень і через вирази (3), (4) із зазначенням порядку модуля перетворення, мінімально потрібного для забезпечення необхідного рівня безпеки.

Таблиця 1

Оцінки обчислювальної складності реалізації операції піднесення до степеня різними методами

Метод піднесення до степеня	Порядок модуля перетворень / еквівалентна довжина ключа симетричного криптоалгоритму		
	1024 / 80	3072 / 128	15360 / 256
Через ланцюжок добутків	10308	10924	104623
Швидкий алгоритм піднесення до степеня	2046	6142	30718

Аналіз даних табл. 1 показує, що реалізація запропонованого методу універсального гешування через традиційний алгоритм піднесення до степеня обчислювально недосяжна. Кількість

множень, які потрібно виконати для обчислення одного значення циклової функції навіть за мінімального рівня безпеки (потужність множини ключових даних блокового симетричного шифру дорівнює 2^{80}), перевищує можливості найсучасніших обчислювальних систем.

Останній рядок табл. 1 є фактично оцінкою обчислювальної складності пропонованої схеми гешування. Так, за мінімального рівня стійкості (потужність множини ключових даних блокового симетричного шифру дорівнює 2^{80}) для обчислення одного значення циклової функції буде потрібно не більше ніж 2 046 операцій множень. Для достатнього рівня стійкості (потужність множини ключових даних БСШ дорівнює 2^{128}), що відповідає національному стандарту шифрування США FIPS-197 (AES), для обчислення значення циклової функції буде потрібно виконати не більше за 6142 операцій множення. Для високого рівня стійкості (потужність множини ключових даних БСШ дорівнює 2^{256}), що відповідає чинному вітчизняному стандарту симетричного криптоперетворення ГОСТ-28147-89, для обчислення значення циклової функції буде необхідно виконати не більше за 30 718 операцій множення.

Для порівняння з іншими схемами ключового гешування за показниками стійкості й швидкодії приймемо такі допущення. Нехай одна операція множення над числами порядку 2^m вимагає $\left\lceil \frac{m}{L} \right\rceil$ операцій порозрядного додавання за модулем два (XOR), де L – розрядність процесора використовуваної обчислювальної системи; $\lceil x \rceil$ – округлене до більшого цілого число x. Таке допущення найчастіше застосовують для оцінювання складності реалізації криптоалгоритмів. У цьому випадку оцінка $\left\lceil \frac{m}{L} \right\rceil$ дає приблизну кількість циклів L-розрядного процесора, необхідних для реалізації одного множення над числами, бітова довжина яких не перевищує m. Водночас при гешуванні з використанням модулярних перетворень обробляється відразу $m/8$ байтів інформаційних даних.

У табл. 2 наведено результати порівняльних досліджень швидкодії схем ключового гешування для фіксованих показників безпеки. Показник швидкодії виражений у кількості S циклів 32-розрядного процесора, необхідних для формування одного байта вихідних даних. Показник безпеки фіксувався через довжину секретного ключа, який необхідно зламати зловмисникові. Для схем модулярною арифметикою наведено еквівалентну довжину ключа блокового симетричного криптоалгоритму (див. табл. 1).

Таблиця 2

Оцінка складності алгоритмів гешування в кількості S-циклів 32-розрядного процесора на один байт оброблюваних даних

Функція гешування	Рівень стійкості (довжина ключа)	Кількість циклів S
SHA-2 (512)	512	80
SHA-2 (256)	256	64
SHA-1	160	80
RIPEMD-160	160	160
MD5	128	64
Гешування модулярною арифметикою	80	512
	128	1536
	256	7680

Наведені дані в табл. 2 свідчать, що використання модульних перетворень для розв'язання завдань ключового гешування значно підвищує складність обчислень, швидкодія алгоритмів знижується на 1 – 2 порядки. Водночас пропоновані схеми ключового гешування підтверджене стійким рівнем безпеки (завдання знаходження ключа гешування або прообразу зводиться до розв'язання відомої теоретико-складної задачі). Крім того, вище було показано, що такі схеми

автентифікації задовольняють властивості універсального гешування, чим забезпечуються високі колізійні характеристики формованих MAC.

У цій роботі пропонується модель каскадного формування кодів контролю цілісності й автентичності даних (MAC) з використанням модулярних перетворень. В основу пропонованої моделі покладено багатошарову схему універсального гешування з використанням на останньому етапі модульних перетворень.

Формально запропоновану схему каскадного формування кодів контролю цілісності й автентичності даних наведено на рисунку.

Основна частина інформаційних даних обробляється першими шарами універсального гешування. Формований у результаті такого перетворення геш-код на кінцевому, заключному етапі обробляється криптографічно сильною функцією суворо універсального гешування на основі модулярних перетворень.

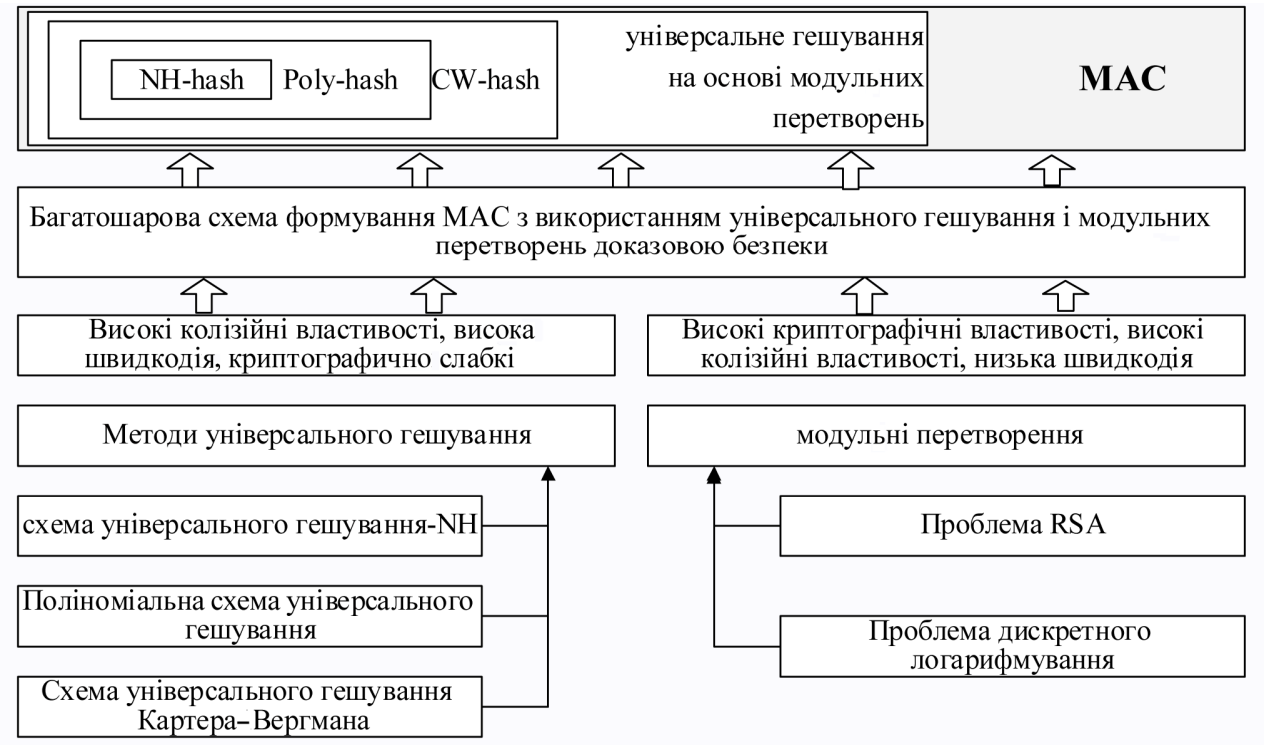

Схема каскадного формування кодів контролю цілісності й автентичності даних з використанням модульних перетворень

Отже, в основу схеми формування MAC із використанням модульних перетворень покладено використання:

– на перших шарах – високошвидкісних методів універсального гешування (Nh-гешування, поліноміальне гешування, гешування Картера – Вергмана);

– на останньому шарі – безпечного суворо універсального гешування на основі модульних перетворень (з використанням циклових функцій (1) і/або (2)).

Запропоноване розв'язання гарантує низькі колізійні властивості сформованих кодів контролю цілісності й автентичності даних, зберегти властивості універсального гешування та забезпечує високі показники безпеки на рівні сучасних засобів криптографічного захисту доказової стійкості. Застосування багатошарової конструкції також істотно знижує обчислювальні витрати на формування кодів контролю цілісності й автентичності більших масивів даних.

Результуюча складність як кількість циклів процесора на один оброблюваний байт даних є усередненою оцінкою за всіма шарами перетворення в каскадній конструкції обчислення кодів контролю цілісності й автентичності даних. Оскільки основна частина оброблюваних даних

надходить тільки на перші шари перетворення (див. модель на рис. 1), а останній, криптографічний шар з модулярними перетвореннями застосовується лише один раз для обробки результату гешування попередніми шарами схеми, оцінка складності для більших обсягів оброблюваних даних прагнутиме до оцінки складності схеми UMAC.

Для підтвердження наведених міркувань у табл. 3 подано приблизну оцінку складності формування кодів контролю цілісності й автентичності даних запропонованою схемою з використанням модульних перетворень (див. рис. 1).

Дані, зазначені в табл. 3, отримано розрахунковим шляхом за допомогою усереднення верхньої оцінки складності універсального гешування на перших шарах перетворень (6 циклів на один байт) і оцінки складності модулярних перетворень (з використанням циклових функцій (1) і/або (2)) з табл. 2. Прочерками в табл. 3 проставлені місця, у яких гешування на модулярних перетвореннях (криптографічний шар) не може бути виконане.

Таблиця 3

Оцінка складності формування MAC запропонованою схемою в кількості S-циклів 32-розрядного процесора на один байт оброблюваних даних

Рівень стійкості (еквівалентна довжина ключа, бітів)	Довжина вхідних даних, байтів									
	128	256	512	1024	2048	4096	8192	16384	32768	65536
80	518	262	134	70	38	22	14	10	8	7
128	–	–	1158	582	294	150	78	42	24	15
256	–	–	–	–	7206	3606	1806	906	456	231

Аналіз даних табл. 3 підтверджує наведені вище міркування про зниження питомої складності перетворення (кількості циклів процесора на один байт вхідних даних) із збільшенням довжини оброблюваних інформаційних даних. Практично це означає, що із зростанням довжини блоків даних запропонована схема формування кодів контролю цілісності й автентичності щодо обчислювальної складності стає еквівалентною застосовуваним сьогодні у протоколах мережної безпеки (зокрема в протоколах IPSec) алгоритмам MD-5 і SHA-1, а також алгоритмам SHA-2, CBC MAC-RIJNDAEL і ін. У табл. 4 порівняно обчислювальну складність деяких функцій гешування. Дані щодо швидкодії для пропонованої схеми MAC із модульними перетвореннями наведені для мінімального рівня стійкості (потужність множини ключових даних блокового симетричного шифру дорівнює 2^{80}) і достатнього рівня стійкості (для модульних перетворень еквівалентна довжина ключа блокового симетричного шифру дорівнює 128 бітів). Довжина формованого при цьому MAC дорівнює 80 і 128 бітів відповідно.

Таблиця 4

Оцінка складності формування MAC різними схемами

Алгоритм	Довжина вхідних даних, байтів					
	2048	4096	8192	16384	32768	65536
HMAC-MD5 (128 бітів)	9	9	9	9	9	9
HMAC-RIPE-MD (160 бітів)	27	27	27	27	27	27
HMAC-SHA-1 (160 бітів)	25	25	25	25	25	25
HMAC-SHA-2 (512бітів)	84	84	84	84	84	84
CBC Mac-rijndael (128 бітів)	26	26	26	26	26	26
CBC MAC-DES (64 біти)	62	62	62	62	62	62
Пропонована схема MAC із модульними перетвореннями (80 бітів)	38	22	14	10	8	7
Пропонована схема MAC із модульними перетвореннями (128 бітів)	294	150	78	42	24	15

Для всіх функцій, наведених у табл. 4 (крім запропонованих, з використанням модулярних перетворень), питома складність формування кодів контролю цілісності й автентичності даних не залежить від обсягу оброблюваних даних. Для пропонованої моделі з використанням модульних перетворень питома складність зі зростанням довжини оброблюваних даних знижується. Так, для високого рівня стійкості (еквівалентна довжина ключа блокового симетричного шифру дорівнює 128 бітів) уже для блоків даних з 32 768 байтів порівнянна з відомими й застосовуваними в протоколах мережної безпеки алгоритмами формування MAC. Для мінімального рівня стійкості (потужність множини ключових даних блокового симетричного шифру дорівнює 2^{80}) пропонована схема каскадного формування кодів контролю цілісності й автентичності даних з використанням модулярних перетворень уже для пакетів даних з 2 048 байтів практично не поступається за швидкодією застосовуваним сьогодні алгоритмам формування MAC у протоколах мережної безпеки, зокрема в протоколах IPSec.

Висновки

Отже, результати досліджень показують, що розроблена схема формування кодів контролю цілісності й автентичності даних з використанням модульних перетворень дає змогу забезпечити високі колізійні властивості безпечного гешування. Крім того, внаслідок багатошарової конструкції обчислення геш-коду вдається суттєво скоротити обчислювальну складність гешування й підвищити, швидкість обробки інформаційних повідомлень.

1. Король О. Г. Исследование коллизионных свойств кодов аутентификации сообщений UMAC / О. Г. Король, А. А. Кузнецов, С. П. Евсеев // Прикладная радиоэлектроника. – Х. : Изд-во ХНУР, 2012. – Т. 11, № 2. – С. 171–183. 2. Король О. Г. Исследование методов обеспечения аутентичности и целостности данных на основе односторонних хэш-функций / О. Г. Король, С. П. Евсеев // Захист інформації : науково-технічний журнал. Спецвипуск (40). – 2008. – С. 50–55. 3. Король О. Г. Исследование свойств модулярных преобразований и методов хеширования информации на их основе / О. Г. Король, Л. Т. Пархуць, С. П. Евсеев // Системи обробки інформації. – 2013. – № 4(111). – С. 106–110. 4. Король О. Г. Исследование статистических коллизионных свойств MAC-кодов аутентичности данных и обоснование предложений по их совершенствованию / О. Г. Король, С. П. Евсеев, Д. С. Захаров // Системи обробки інформації. – 2012. – № 8(106). – С. 94–102. 5. Король О. Г. Метод универсального хеширования на основе модулярних преобразований / О. Г. Король, С. П. Евсеев // Системи обробки інформації. Інформаційні технології та комп'ютерна інженерія. – 2011. – № 7(97). – С. 131–132. 6. Король О. Г. Механизмы и протоколы защиты информации в компьютерных сетях и системах / О. Г. Король, С. П. Евсеев, А. В. Дорохов // Научный журнал Министерства обороны республики Сербия. Военно-технический вестник, Белград, 2011. – Вып. 4. – С. 15–30 7. Король О. Г. Обоснование выбора цикловой функции для итеративного хеширования информации / О. Г. Король, Л. Т. Пархуць, С. П. Евсеев // Системи обробки інформації. – 2013. – № 6(113). – С. 115– 119. 8. Король О. Г. Разработка модели и метода каскадного формирования MAC с использованием модулярных преобразований // Захист інформації: науково-технічний журнал. – 2013. – Т. 15, № 3. – С. 186. 9. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебное пособие/ А. В. Потий. – Х. : ХНУРЭ, 2002. – 80 с. 10. Писаренко И. И. Оценка рисков информационной безопасности в банковской сфере [Электронный ресурс] / И. И. Писаренко. – Режим доступа : http://www.itsec.ru. 11. Столлингс В. Криптография и защита сетей: принципы и практика В. Столлингс ; пер. с англ. – 2-е изд. – М. : ИД "Вильямс", 2001. – 672 с. 12. Korol O. G. Development of the Model and Method of Integrity Control and Data Authenticity Codes Generation Based On Modular Transformations / O. G. Korol // Перспективні технології і методи проектування МЕМС : матеріали IX міжнародної конференції MEMSTECH 2013. – Львів : Видавництво Львівської політехніки, 2013. – С. 79–83.