Моделі псевдонедетермінованих криптографічних перетворень

Баришев Ю. В.

к. т. н., старший викладач кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, yuriy.baryshev@gmail.com

***Анотація* — Визначено актуальність досліджень, пов'язаних з розробкою методів, які породжують для зловмисників невизначеність під час криптоаналізу перетворень. Наведено підхід, який визначає шлях зміни класичних криптографічних перетворень на псевдонедетерміновані. На прикладі шифрування та гешування наведено зразок використання даного підходу для формалізації методів у вигляді математичних моделей цифрових автоматів.**

Ключові слова: автомат, псевдонедетрмінованість, шифрування, гешування, загальні атаки.

Models of Pseudononderterministic Cryptographic Transformations

Baryshev Y. V.

PhD (ukr), Senior Lecturer, Information Protection Department, Vinnytsia National Technical University,
Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com

***Abstract* — The importance of research concerned development of methods, those allow to increase intruder uncertainness at the transformation cryptanalysis process, is defined. The approach, which determines the way of classic cryptographic transformations upgrading to the pseudononderterministic ones, is presented. The approach usage is shown using ciphering and hashing as examples for the methods formalization as mathematical models of a digital automata.**

Keywords: automata, pseudononderterministic, ciphering, hashing, generic attacks.

I. Вступ

Сучасна парадигма розвитку криптографії передбачає відкритість її алгоритмів для дослідження громадськістю. Це дозволяє говорити про "практичну" стійкість цих алгоритмів, тобто за відсутності теоретичного обґрунтування криптографічної стійкості алгоритму його його валідація відбувається завдяки тому, що результати практичних спроб зламу не виявили вразливих місць [1-3]. Такий підхід дозволяє широко використовувати криптографічні алгоритми в комп'ютерних системах без втрати їх комерційної привабливості. Останнє пояснюється тим, що відомі алгоритми, які мають теоретичне доведення своєї стійкості базуються на криптографічних примітивах, реалізація яких є неприродною для універсальних процесорів. Як наслідок, використання таких алгоритмів спричиняє потребу в істотній кількості додаткового процесорного часу [2, 3]. Водночас практично стійкі криптографічні алгоритми будуються на криптографічних примітивах, реалізація яких природна для універсальних процесорів, а тому програмне забезпечення, яке використовує ці алгоритми, не забирає багато процесорного часу для свого виконання.

Відкритість криптографічних алгоритмів разом з цією очевидною перевагою також породила й недолік – можливість дослідження алгоритмів зловмисником [1, 4]. Останнє породило низку небезпек для інформації, яка захищається такими алгоритмами. Одними з найяскравіших представників є загальні атаки на алгоритми гешування, які, зокрема, надають зловмиснику можливість попередньої підготовки до атак [4-8]. Саме тому дослідження, покликані закрити від зловмисника алгоритм, залишаючи при цьому його відкритим для досліджень з боку громадськості, є актуальними.

Метою даного дослідження є покращення криптографічної стійкості алгоритмів шляхом приховування від зловмисника криптографічних перетворень, які виконуються для захисту конкретної інформації.

Для досягнення мети необхідно розв'язати низку задач, однією з яких є задача розробки математичних моделей цих криптографічних алгоритмів. Розв'язанню цієї задачі присвячена дана робота.

II. Поняття псевдонедетермінованості криптографічного перетворення

Концепція псевдонедетермінованих криптографічних алгоритмів на прикладі псевдонедетермінованого гешування розглянута в роботі [9]. Відповідно до даного підходу криптографічні перетворення розглядається з точки зору автоматів, які можуть їх реалізовувати.

Відомо, що детермінованим автоматом називається такий автомат, який в будь-якому стані і для будь-якого значення з алфавіту, яке подається на автомат для читання, переходить один і тільки один стан [10]. Детермінований автомат представляється у вигляді п'ятірки $\{\mathbf{S}, \mathbf{A}, \delta, s_0, \mathbf{D}\}$, де $\mathbf{S}$ – множина станів автомата; $\mathbf{A}$ – вхідний алфавіт; δ – однозначне відображення $\mathbf{S} \times \mathbf{A} \to \mathbf{S}$, s_0 – виокремлений стан автомата, що називається початковим ($s_0 \in \mathbf{S}$); $\mathbf{D}$ –

підмножина в $\mathbf{S}$, що називається множиною завершальних станів [11].

Недетермінованим вважається такий автомат, в якого правила переходу не обов'язково є функцією. Тобто, з одного початкового стану s_0 при реакції на одні й ті самі вхідні дані автомат може перейти в декілька різних станів [10]. Нехай ε – порожнє повідомлення, тоді недетермінований автомат описується у вигляді п'ятірки $\{\mathbf{S},\mathbf{A},\delta',s_0,\mathbf{D}\}$, де δ' – відображення $\mathbf{S}\times(\mathbf{A}\cup\{\varepsilon\})\to\mathbf{S}$ [11].

Таким чином, поняття псевдонедетермінованого криптографічного перетворення, аналогічно до поняття псевдовипадкових чисел, передбачає, що дане перетворення для стороннього спостерігача (зловмисника) має такий вигляд, наче воно виконується недетермінованим автоматом. Однак для спостерігача, який знає правило-ключ дане перетворення виглядає, як таке, що виконується детермінованим автоматом. З наведених вище визначень випливає, що дана задача розв'язується шляхом заміни відображення δ, яке є однозначним, тобто δ – функція, на відображення δ', яке не обов'язково є однозначним.

III. Математичні моделі псевдонедетермінованого шифрування та гешування

Автомат, який реалізує детерміноване зашифрування повідомлення $\mathbf{M}=\{m_1,m_2,\ldots,m_l\}$, ($l\in\mathbf{N}$) формалізується так $\{\{e_k(m_l)\},\{m_i\},e_k(\cdot),k,e_k(m_l)\}$, де $\{e_k(m_l)\}$ – множина шифротекстів; $\{m_i\}$ – множина блоків даних, які можливі на i-й ітерації $i=\overline{1,l}$; $e_k(\cdot)$ – функція зашифрування, k – ключ шифрування (у випадку блокового шифрування) або початковий стан генератора гами (у випадку потокового). Відповідно пропонується такий автомат, який реалізує псевдонедетерміноване зашифрування описується таким чином $\{\{e_k(m_l)\},\{m_i\},\mathbf{E},k,e_{(v_l)k}(m_l),\mathbf{V}\}$, де $\mathbf{E}$ – множина функцій зашифрування, $\mathbf{V}$ – вектор керування, значення якого на кожній з ітерацій належить до секретної інформації та обумовлює вибір функції з множини $\mathbf{E}$. З даних описів видно, що для стороннього спостерігача псевдонедетерміноване шифрування має вигляд недетермінованого автомата $\{\{e_k(m_l)\},\{m_i\},\mathbf{E},k,e_{(v_l)k}(m_l)\}$.

Класичне гешування описується автоматом $\{\mathbf{H},\{m_i\},f(\cdot),k,h_l\}$, де $\mathbf{H}=\{h_1,h_2,\ldots,h_l\}$ – множина проміжних геш-значень, $f(\cdot)$ – функція незворотного ущільнення [9]. Для реалізації псевдонедетермінованого гешування пропонується такий автомат $\{\mathbf{H},\{m_i\},\mathbf{F},k,h_l,\mathbf{V}\}$, де $\mathbf{F}$ – множина функцій ущільнення, вибір однієї з яких залежить від значення вектора керування v_i, передбаченого для обробки i-го блока даних. Для стороннього спостерігача процес гешування виглядатиме так, наче він реалізується недетермінованим автоматом $\{\mathbf{H},\{m_i\},\mathbf{F},k,h_l\}$.

Аналогічно до розглянутих криптографічних перетворень описуються й інші криптографічні перетворення.

Запропонований підхід псевдонедетермінованих криптографічних перетворень відрізняється від відомого раніше підходу до керованих криптографічних перетворень [8, 12] тим, що керований підхід передбачає вибір однієї з множини функцій на кожній ітерації при цьому залишаючи сталість її аргументів, а псевдонедетермінований підхід є узагальненням керованого і для нього ця сталість необов'язкова, а з точки зору криптографічної стійкості – небажана.

IV. Висновки

Запропонований в даній роботі підхід до побудови псевдонедетермінованих криптографічних перетворень дозволяє виконувати математичний опис автоматів, які реалізують ці перетворення. Основною перевагою псевдонедетермінованого підходу при розробці криптографічних перетворень є збільшення їх практичної стійкості при лінійному зростанні часу їх реалізації.

[1] C. Blondeau, G. Leander, K. Nyberg. Differential-Linear Cryptanalysis Revisited, 2014, p. 20, http://users.ics.aalto.fi/~blondeau/PDF/FSE2014.pdf

[2] A. Petrov, *The computer secutity. Cryptographic proctection methods*. Moscow: DMK, 2000, p. 448 (in Russian)

[3] С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security, Бином-Пресс, Москва, 2002, с. 384.

[4] B. Preneel. Analysis and design of cryptographic hash functions. Katholieke Universiteit Leuven, 1993, p. 323 http://homes.esat.kuleuven.be/ ~preneel/phd_preneel_feb1993.pdf

[5] P. Gauravaram, J. Kelsey. "Cryptanalysis of a class of cryptographic hash functions", *Cryptology ePrint Archive*, 2007, p. 30. http://eprint.iacr.org/2007/277.pdf

[6] J.Kelsey, T. Kohno. Herding hash functions and the Nostradamus attack, 2005, p. 18. http://archives.scovetta.com/pub/crypto/Nostradamus%20Attack.pdf

[7] J. J.Hoch, A. Shamir Breaking the ICE – Finding Multicollisions in Iterative Concatenated and Expanded (ICE) Hash Functions, 2006, p. 13. http://www.wisdom.weizmann.ac.il/~yaakovh/papers/hashpaper_submission.pdf.

[8] J-P. Aumasson, O. Dunkelman, S. Indesteege and B. Preneel. Cryptanalysis of Dynamic SHA(2). COmputer Security and Industrial Cryptography publications, 2009, p. 18. https://www.cosic.esat.kuleuven.be/ publications/article-1277.pdf

[9] В. А. Лужецький, Ю. В. Баришев. Концепція псевдонедетермінованого гешування. Системи управління, навігації та зв'язку, 3, 2010, с. 94-98.

[10] Д. А. Андерсон. Дискретная математика и комбинаторика : пер. с англ. М. М. Беловой. Издательский дом "Вильямс", Москва, 2004, с. 960.

[11] А. Ахо, Дж Хопкрофт, Дж. Ульман. Построение и анализ вычислительных алгоритмов. Мир, Москва, 1979, с. 536.

[12] Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. Криптография: от примитивов к синтезу алгоритмовСПб.:, 2004. – 448 с.