Дослідження примітивів малоресурсної криптографії

В. П. Семеренко
кафедри обчислювальної техніки,
Вінницький національний технічний університет
м. Вінниця, Україна, vpsemerenko@ukr.net

Research of the Primitives in Low Resource Cryptography

V. P. Semerenko
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, 21021, Ukraine,
vpsemerenko@ukr.net

Анотація **– Проведено аналіз криптостійкості стандартних засобів захисту інформації з обмеженими обчислювальними ресурсами. Обгрунтовано умови існування односторонніх функцій з врахуванням симетрії часу за допомогою теорії лінійних послідовнісних машин (ЛПС). Розглянуто функціонування лінійних конгруентних генераторів на основі автоматних моделей в полі Галуа. Запропонована структура малоресурсної односторонньої хеш-функції на основі теоретичного апарату ЛПС.**

Abstract **– The analysis of cryptoresistance of the standard protection with the restricted computable resources is done. The conditions of existence of one-way functions taking into account the time symmetry by help of the theory of linear finite state machine (LFSM) are proved. The functioning of linear congruent generators based on automaton models in Galois field is considered. The structure of the low resource one-way hash-function which based on theory of LFSM are suggested.**

Ключові слова**: малоресурсна криптографія, одностороння функція, хеш-функція, генератор псевдовипадкових чисел, лінійна послідовнісна схема**

Keywords: **low resource cryptography, one-way function, hash function, pseudorandom generator, linear finite state machine**

I. Вступ

Магістральним шляхом розвитку інформаційних технологій в найближчі роки стане Інтернет Речей (Internet of Things, IoT). Цей напрямок характе-ризується об'єднанням в єдину безпровідну мережу різноманітних приладів, сенсорів, давачів (типу міток радіочастотної ідентифікації, REID) [1].

Стрімкий розвиток таких технологій робить дуже актуальними питання, які пов'язані з їх інформаційною безпекою. Основною проблемою є те, що зазначені Інтернет-засоби мають значні обмеження на програмно-апаратні ресурси, що робить неможливим застосування до них відомих стандартних способів захисту інформації.

Ефективним вирішенням проблеми забезпе-чення інформаційної безпеки у світі Інтернету Речей може стати так звана «малоресурсна» (*low resource*) або «легковагова» криптографія (*lightweight cryptography, LWC*) [2].

Задачею проектування засобів малоресурсної криптографії є знаходження компромісу між наявними обмеженнями, ціною та криптостійкістю алгоритмів захисту. Такий компроміс можна шукати як на основі спрощення відомих так і розробці нових криптографічних засобів. Таким чином, сьогодні є актуальними дослідження з позицій малоресурсної криптографії таких базових примітивів як хеш-функції, генератори псевдо-випадкових чисел, блокові та потокові шифри тощо.

II. Односторонні функції

Розглянемо функцію F, яка перетворює двійковий рядок символів довжиною n в двійковий рядок символів довжиною m ($m << n$):

$$F:\{0,1\}^n \to \{0,1\}^m$$

Функція F називається односторонньою (*one-way*), якщо виконуються такі умови [3]:

1. Для детермінованої машини Тьюрінга існує алгоритм, який для будь-якого аргументу x з поліноміальною складністю обчислює $y = F(x)$.

2. Ймовірнісна машина Тьюрінга може по заданому y визначити аргумент x із рівняння $y = F(x)$ з дуже малою ймовірністю:

$$P\{F(T_R(F(x))) = F(x)\} < \frac{1}{p(n)} \qquad (1)$$

де $p(n)$ – деякий поліном розмірності n.

Неформально кажучи, одностороння функція $F(x)$ легко обчислює своє значення для будь-якого аргументу x, однак, дуже важко знайти аргумент функції по її значенню.

Одностороння функція є центральним поняттям в криптографії, багато криптографічних примітивів базується на її основі, але саме існування такої функції до цього часу математично не доведено. Як не доведено та не спростовано збіг класів складності P та NP ($P \neq NP$?).

Цілком можливо, що розв'язання цієї проблеми не існує в рамках існуючої парадигми обчислень.

Тому спробуємо проаналізувати проблему існування односторонньої функції з іншого боку.

В сучасних моделях обчислювальних процесів використовується лінійна структура часу, яка направлена від минулого до майбутнього. Однак в фундаментальних законах фізики від класичної ньютонівської динаміки до теорії відносності та квантової динаміки категорія часу не містить в собі відмінності між минулим і майбутнім [4]. Це означає, що теореми, які вірні при зміні часу від "теперішнього" до "майбутнього", будуть також вірними при зміні часу від "теперішнього" до "минулого".

Відразу введемо необхідні уточнення.

По-перше, ми маємо на увазі не фізичну категорію часу, а лише математичну.

По-друге, будемо розглядати лише динамічні системи (ДС), які характеризуються множинами станів, входів і виходів, а також двома функціями: переходів і виходів. Обмежимось тільки інтегрованими ДС з одним ступенем свободи, для яких послідовність змін станів в часі утворює в просторі станів системи замкнуту фазову траєкторію у вигляді кола [5].

Найбільш розповсюдженим представником зазначених ДС є автономні кінцеві автомати, зокрема, автономні лінійні автомати. Саме такі автомати і використовуються в сучасній криптографії.

III. Автоматні представлення криптографічних функцій

Багатообіцяючим підходом в криптографії є використання теоретико-автоматних моделей.

Розглянемо криптографічні примітиви на основі теорії лінійних послідовнісних схем (ЛПС) [6].

ОЗНАЧЕННЯ 1. ЛПС з r елементами пам'яті, l входами і m виходами є кінцевим автоматом лінійного типу (лінійним автоматом), який над полем Галуа $GF(q)$ описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2) \qquad (1)$$

і функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2) \qquad (2)$$

де t – дискретний час, $A = \|a_{ij}\|_{r \times r}$; $B = \|b_{ij}\|_{r \times l}$; $C = \|c_{ij}\|_{m \times r}$; $D = \|d_{ij}\|_{m \times l}$ – характеристичні матриці; $S(t) = \|s_i\|_r$; $U(t) = \|u_i\|_l$; $Y(t) = \|y_i\|_m$ – відповідно слово стану, вхідне і вихідне.

Елементи матриці A в (1) визначаються коефіцієнтами породжувального полінома, що свідчить про тісний зв'язок автоматного і поліноміального представлень в полях Галуа.

Найпростішою апаратною реалізацією ЛПС є загальновідомий регістр зсуву з лінійним оберненим зв'язком (РЗЛОЗ).

ОЗНАЧЕННЯ 2. Автономною ЛПС Λ_{fst} над полем $GF(2)$ називається така ЛПС, функціонування якої не залежить від вхідних сигналів і описується функцією станів (переходів)

$$S(t+1) = A \times S(t), \quad GF(2) \qquad (3)$$

Апаратною реалізацією автономної ЛПС є РЗЛОЗ, який після запуску далі функціонує у вільному режимі згідно (3). При виборі матриці A в (3) на основі примітивного породжувального поліному r-вимірна ЛПС буде генерувати М-послі-довність періоду $2^r - 1$, яка при великих r практично не відрізняється від випадкової послідовності. Тобто, така ЛПС буде псевдовипадковим генератором чисел (ПВГЧ) в полі. $GF(2)$

Такий ПВГЧ (назвемо його прямим) функціонує по шкалі часу від "теперішнього" до "майбутнього".

Позначимо початковий стан ЛПС як $S(0)$, а кінцевий стан через тактів роботи прямого ПВГЧ як $S(n)$. Тоді послідовність обчислень згідно (3) можна компактно записати так:

$$S(n) = F_{fst}(S(0)) \quad (4)$$

ОЗНАЧЕННЯ 3. Оберненою автономною ЛПС Λ_{inv} над полем $GF(2)$ називається така ЛПС, функціонування якої не залежить від вхідних сигналів і описується функцією станів (переходів)

$$S(t) = A_{inv} \times S(t+1), \quad GF(2) \quad (5)$$

Апаратною реалізацією оберненої автономної ЛПС є ПВГЧ (назвемо його оберненим), який функціонує по шкалі часу від "теперішнього" до "минулого".

Обернений ПВГЧ генерує елементи в полі Галуа в оберненому порядку в порівнянні з прямим ПВГЧ. Якщо обернений ПВГЧ почне працювати після прямого ПВГЧ, тоді можна зі стану $S(n)$ знову повернутись в стан $S(0)$:

$$S(0) = F_{inv}(S(n)) \quad (6)$$

Не важко зрозуміти, що повернутись в стан $S(0)$ іншим способом, наприклад, за допомогою функції переходів (3), «дуже важко». Таким чином, функція переходів (3), чи функція F_{fst} в (4), є односторонньою для прямого ПВГЧ.

Аналогічно, для оберненого ПВГЧ одно-сторонньою функцією є функція станів (5) чи функція F_{inv} в (6).

Цікаво проаналізувати зв'язок між функціями F_{fst} і F_{inv} з позицій складності обчислень. Як видно з (3) та (6) ці функції в математичному сенсі відрізняються своїми характеристичними матрицями.

Матриці A та A_{inv} є взаємно оберненими, тобто їх добуток дорівнює одиничній матриці I:

$$A \times A_{inv} = I$$

Як відомо, послідовний алгоритм знаходження оберненої матриці в найгіршому випадку має часову складність $O(n^3)$ [7]. На практиці використовуються матриці A дуже простої структури, і фактично перехід від одної матриці до іншої вимагає лише двох циклічних операцій зсуву рядків і стовпців матриць [8].

Таким чином, задача переходу від F_{fst} до F_{inv} і навпаки має поліноміальну складність і належить до класу складності P. А самі обчислення за формулами (3) та (5) мають лінійну складність $O(n)$.

По суті функції F_{fst} та F_{inv} є дзеркальним відображенням одна одної і їх можна розглядати як дві сторони однієї інтегрованої функції F. І ця функція вже не є односторонньою при роботі з різними шкалами часу.

В [9] отримано фундаментальний результат, який коротко формулюється у вигляді такої теореми: «псевдовипадкові генератори існують тоді і лише тоді, коли існують односторонні функції».

Як показують вищенаведені розрахунки зазначена теорема буде справедливою при використанні лише одного часового напрямку.

IV. Лінійний конгруентний генератор

Лінійний конгруентний генератор (ЛКГ) належить до найвідоміших генераторів псевдовипадкових чисел. Зважаючи на простоту реалізації та швидкість роботи його цілком можна віднести до засобів малоресурсної криптографії. Незважаючи на низьку криптостійкість, ЛКГ має дуже широку сферу застосування, зокрема, в компіляторах багатьох мов програмування.

ЛКГ формує псевдовипадкове число x_i згідно формули

$$x_i = (a \times x_{i-1} + c) \bmod m \quad (7)$$

де a, c, m - цілочислові константи ($i = 1, 2, 3, \ldots$),

x_0 - початкове значення (зародок, *seed*).

Неважко помітити аналогію між ЛКГ та ЛПС.

Формули (3) і (7) реалізують примітивно-рекурсивну функцію з одним змінним параметром: час t для ЛПС і x_i для ЛКГ. Обчислення за модулем m в (7) аналогічне обчисленню в полі Галуа в (3). При правильному виборі констант в (7) ЛКГ буде генерувати достатньо довгу і статистично хорошу послідовність чисел, аналогічну М-послідовності для ЛПС.

Для аналізу криптостійкості ЛКГ розглянемо процедуру генерації чисел в (7) з позицій складності обчислень. Якщо зародок x_0 є секретним для супротивника, тоді формула (7) відповідає вимогам одностороньої функції.

Чи можна організувати генерацію чисел за допомогою ЛКГ в оберненому порядку?

Розглянемо спочатку найпростіший варіант ЛКГ, коли $c = 0$:

$$x_i = (a \times x_{i-1}) \bmod m \quad (8)$$

Інтерпретуючи ЛКГ як кінцевий автомат в полі Галуа $GF(m)$ неважко вивести формулу генерації псевдовипадкових чисел в оберненому порядку:

$$x_{i-1} = (a_{inv} \times x_i) \bmod m \quad (9)$$

де a_{inv} – константа, обернена до константи a.

Формули (8) і (9) є повними аналогами відповідних формул (3) і (5) для ЛПС. В загальному випадку, коли $c \neq 0$:

$$x_{i-1} = ((x_i + c) \times a_{inv} + c + w) \bmod m \qquad (10)$$

де $w = 1$ або $w = -1$ в залежності від співвідношення між константами a, c, m.

Величину a_{inv} в (9) і (10) можна розглядати, як обернений елемент поля Галуа відносно величини a, тобто співвідношення між вказаними числами таке:

$$a \times a_{inv} = 1 \bmod m$$

Отже, до аналізу ЛКГ можна застосувати всі основні теоретичні положення ЛПС відносно односторонніх функцій, які були розглянуті вище.

V. Малоресурсні хеш-функції

Перспективним напрямком в сфері мініатюри-зації обчислювальних пристроїв є розвиток RFID-технологій [1,2]. Ці технології базуються на автома-тичній ідентифікації об'єктів, коли інформація передається за допомогою радіосигналів і зберігається в спеціальних RFID-мітках. Основними проблемами тут є забезпечення правильності передачі та збереження конфіденційності інформації, записаної в мітки.

Для перевірки цілісності та аутентичності повідомлень можна використати хешування, тобто ущільнення початкової послідовності X символів довільної довжини n в послідовність Y символів фіксованої довжини r $(r << n)$. З-за суттєвих обмежень на часові та апаратні ресурси для RFID-технологій можна використовувати лише максимально «полегшені» хеш-алгоритми.

Для аналізу хеш-функцій також часто використовується автоматний підхід [10]. Розглянемо процедуру хешування на основі теоретичного апарату ЛПС [6]. В цьому випадку послідовність X можна інтерпретувати як вхідну послідовність символів, під дією якого ЛПС з деякого початкового стану $S(0)$ перейде в стан $S(n)$. Математичні перетворення в процесі ітеративних обчислень здійснюються згідно формули (1). Обчислений стан $S(n)$ і буде значенням функції хешування $H(X)$:

$$H(X) = S(n)$$

Така хеш-функція $H(X)$ буде придатною тільки для перевірки відсутності ненавмисних спотворень переданих повідомлень, тобто для перевірки цілісності даних.

Проаналізуємо детальніше умови криптостій-кості зазначеної хеш-функції $H(X)$. Найважливі-шою властивістю криптографічної хеш-функції в термінах теорії ЛПС є таке: легкість обчислення стану $S(n)$ по заданному початковому стану $S(0)$ і практичну неможливість (окрім повного перебору) знаходження стану $S(0)$ по відомому стану $S(n)$. Передбачається, що супротивнику можуть бути відомі характеристичні матриці ЛПС (структура обернених зв'язків при реалізації у вигляді РЗЛОЗ). Іншими словами, хеш-функція $H(X)$ має бути односторонньою функцією F_{fst}.

Однак така одностороння функція має підказку («потаємний вхід» – *trapdoorfunction*): початкове значення (*seed*) ПВГЧ, тобто початковий стан $S(0)$ ЛПС. Завдяки знанню $S(0)$ отримувач даних може згенерувати свою хеш-функцію $H''(X)$ і порівняти її з переданою хеш-функцією $H(X)$.

Звичайно, значення $S(0)$ має бути закритим для супротивника, тобто має стати r-розрядним секретним ключем K, який відомий лише передавачу та отримувачу даних. Таким чином, хеш-функція $H(X)$ має обов'язково бути ключовою. Окрім підвищення криптостійкості секретний ключ забезпечить також імітозахист в протоколах аутентифікації повідомлень.

Всі наведені вище міркування будуть справедливими лише при роботі в одному часовому напрямку, наприклад, від «теперішнього» до «майбутнього». Але, з однаковим успіхом можна працювати і в протилежному часовому напрямку: від «теперішнього» до «минулого». Тоді всі математичні докази стануть дзеркально протилежними і хеш-функція $H(X)$ має бути односторонньою функцією F_{inv}.

Одностороння функція F_{inv} також має підказку: останній стан $S(n)$ ЛПС, тобто саме значення хеш-функції $H(X)$. Засекретити значення $H(X)$ неможливо, але його можна захистити за допомогою r-розрядного секретного ключа, який має передаватись після основного повідомлення.

І на завершення розглянемо найбільш повний сценарій захисту даних за допомогою хеш-функції, коли можна почергово працювати в обох часових напрямках.

Тоді послідовність хешування даних буде такою: спочатку хешується секретний ключ K, далі – основне повідомлення, і на завершення знову хешується секретний ключ K.

В результаті матимемо односторонню хеш-функцію з одним закритим симетричним ключем, та з відкритими початковим станом (нульовим) і останнім станом ЛПС, тобто $H(X)$.

VI. Висновки

Багато обчислювальних пристроїв не мають змоги повноцінно реалізувати складні сучасні засоби захисту,

що потребує розробки криптозасобів з врахуванням обмежених ресурсів. Для ефективного вирішення зазначеної проблеми в роботі проведено дослідження криптостійкості для найпростіших генераторів псевдовипадкових чисел та хеш-функцій на основі автоматних моделей. Варто відзначити, що теоретичні результати, зокрема, про односторонні функції з врахуванням різних часових шкал, можуть бути використані при проектуванні систем будь-якої складності.

Література References

[1] Zhou H., The Internet of Things in the Cloud: A Middleware Perspective. – CRC Press, 2012.

[2] Жуков А. Е. Легковесная криптография [Текст] / А. Е. Жуков // Вопросы кибербезопасности . – 2015. – № 1(9). – С. 26–43.

[3] Введение в криптографию [Текст] / Под общ. ред. В. В. Ященко. – 4-е изд., доп. – М.: МЦНМО, 2012. – 348 с.

[4] Хокинг С. Краткая история времени: От Большого взрыва до черных дыр. – СПб.: Амфора, 2008. – 231 с.

[5] Семеренко, В. П. Темпоральные модели параллельных вычислений [Текст] / В. П. Семеренко // *Austrian Journal of Technical and Natural Sciences. – 2014. – Vol. 1. – P. 13–25.*

[6] Гилл, А. Линейные последовательностные машины [Текст] / А. Гилл; пер. с англ. – М.: Наука, 1974. – 288 с.

[7] Миллер Р. Последовательные и параллельные алгоритмы: Общий подход / Р. Миллер, Л. Боксер. пер. с англ. – М.: БИНОМ. Лаборатория знаний, 2006. – 406 с.

[8] Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія [Текст] / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

[9] Hastad J. A pseudorandom generator from any one-way function / J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby // SIAM Journal of Computing. – 1999. – 29(4). – P. 1364-1396.

[10] Jeon J. C. Analysis of Hash Functions and Cellular Automata Based Schemes [Text] / J. C. Jeon // International Journal of Security and Its Applications. – 2013. – Vol. 7. – No. 3, May. – P. 303-316.