соціальному середовищі в значній мірі визначає можливість управління відповідним середовищем.

1. *Гуц А.К., Фролов Ю.В.* Математические методы в социологии. М.: ЛИБРОКОМ. 2008, -235 с.
2. *Редько В.Г.* Эволюция, нейронные сети, интеллект. Модели и концепции эволюционной кибернетики. Москва: ЛИБРОКОМ. 2009, - 224 с.
3. *Акофор Р., Эммери Ф.* О целеустремлённых системах. М.: Мир, 1999. – 233 с.
4. Социальная информатика: основания, методы, перспективы. / Под ред. Н.И. Лапина. М.: Книжный дом. 1998. -321 с.
5. *Белотелов Н.В., Бродский Ю.И., Павловский Ю.К.* Математическое моделирование и гуманитарный анализ. Москва: ЛИБРОКОМ. 2000, -345 с.

Поступила 23.10.2013р.

УДК 681.142.2; 622.02.658.284; 621. 325

М. Б. Ступень, аспірант кафедри АСУ, НУ “Львівська політехніка”

ПІДВИЩЕННЯ КРИПТОЛОГІЧНОЇ СТІЙКОСТІ ШИФРУВАННЯ З ВИКОРИСТАННЯМ ДРОБОВО-ЛІНІЙНИХ ПЕРЕТВОРЕНЬ

У статті описано методи підвищення криптологічної стійкості системи шифрування. Описано математичне доведення підходу підвищення стійкості шифрування при використанні дробово-лінійних перетворень, зокрема з використанням кватернарних дробово-лінійних перетворень.

*Ключові слова***:** стійкість, шифрування, зображення, кватернарна форма.

This article describes methods for improving the stability of cryptology encryption. A mathematical proof approach increased resistance encryption using fractional-linear transformations is described, in particular using quaternary fractional linear transformations.

Keywords: resistance, encryption, image, quaternary form

В статье описаны методы повышения криптологической устойчивости системы шифрования. Описано математическое доказательство подхода повышения устойчивости шифрования при использовании дробно-линейных преобразований, в частности с использованием четвертичных дробно-линейных преобразований.

Ключевые слова: устойчивость, шифрование, изображения, четвертичная форма.

Вступ. Проблема стійкості криптографічної системи.

Проблема обгрунтування стійкості криптографічної системи зводиться до доведення відсутності поліноміального алгоритму, який розв'язує задачу зламування системи. Однак тут виникає ще одна й дуже серйозна перешкода:

сучасний стан теорії складності обчислень не дає змоги визначити для конкретних задач певного класу нижніх оцінок складності, вищих від поліноміальні. З цього випливає, що нині стійкість криптографічних систем можна визначати лише із залученням певних гіпотез. Тому головний напрям досліджень полягає в пошуку найслабших достатніх умов існування стійких систем певних класів.

Центральним поняттям у теорії асиметричних криптографічних систем є поняття односторонньої функції [1, 2]. Неформально під односторонньою функцією розуміють ефективно обчислювану функцію, для обернення якої (тобто для пошуку хоча б одного значення аргументу за заданим значенням функції) не існує ефективних алгоритмів.

Усі практичні криптосистеми з відкритим ключем грунтуються на функціях, які вважають односторонніми, хоча ця властивість не була доведена для жодної з них. Це означає, що теоретично є можливим створення односторонньої функції, котра дасть змогу конструювати алгоритми, які неможливо буде „зламати".

Слід зазначити, що існує два підходи до побудови практично стійких шифрів. У першому випадку будується криптосистема, і потім показується, що її розкол є складною задачею. У другому випадку вибирається деяка складна математична задача, і потім будується відповідна криптосистема, якої розкол еквівалентний рішенню цієї задачі.

Отже, в RSA стійкість визначається як складність знаходження функції, оберненої до односторонньої функції $\boldsymbol{F(x) = x^y (\mathrm{mod}\ N)}$, яка залежить від складності розвинення на множники модуля $\boldsymbol{N}$ (факторизація), хоча строгих доведень даного факту не існує. Стійкість алгоритму RSA може бути суттєво знижена через некоректний вибір параметрів алгоритму. Спочатку автори RSA пропонували випадково вибирати прості числа $\boldsymbol{P}$ і $\boldsymbol{Q}$, по 50 десяткових знаків кожне. Вважалося, що такі великі прості числа важко розвинути на прості множники при криптоаналізі.

Другою вадою RSA є наявність так називаних нешифровних блоків повідомлення, тобто таких $\boldsymbol{M}$, для яких виконується рівність $\boldsymbol{M^e (\mathrm{mod}\ N) \equiv 1}$. Наприклад, $\boldsymbol{M = 1,2, \ldots N - 1}$ завжди є нешифровними блоками.

Ця особливість встановлює певні вимоги на вибір параметрів алгоритму. Для знаходження простих чисел використовуються різні способи. Наприклад, мала теорема Ферма: якщо $\boldsymbol{N}$, то $\boldsymbol{i^{N-1} (\mathrm{mod}\ N) \equiv 1}$, для всіх $\boldsymbol{i}$, $\boldsymbol{1 \le i \le N - 1}$.

Відомості з теорії чисел.

Нехай $\boldsymbol{m}$ – ціле додатнє число, a – ціле число, взаємно просте з m, $\boldsymbol{\varphi(m)}$ - функція Ейлера [3]. Для такого числа a справедлива, як відомо, теорема Ейлера:

$$a^{\varphi(m)} \equiv 1 \ (\mathrm{mod}\ m). \qquad (1)$$

З конгруенції (1) випливає, що існує таке найменше ціле ціле додатнє

число δ, для якого також виконується конгруенція $a^{\varphi(m)} \equiv 1 \pmod{m}$. Таке число δ називають показником числа а по модулю m.

Властивості показника δ числа a по модулю m [3 – 6].

Властивість 1. Якщо $a_1 \equiv a_2 \pmod{m}$, то числа a_1 і a_2 належать до одного показника по модулю m.

Властивість 2. Якщо a належить до показника δ по модулю m, то в послідовності степенів

$$a^0 = 1, a, a^2, a^3, ..., a^{\delta-1}, \tag{2}$$

всі числа не порівнювані між собою по модулю m.

Властивість 3. Якщо a належить до показника δ по модулю m, то конгруенція

$$a^{\alpha} \equiv a^{\beta} \pmod{m}, \tag{3}$$

де α і β - деякі цілі додатні числа, існує тоді і тільки тоді, коли

$$\alpha \equiv \beta \pmod{\delta}. \tag{4}$$

Підвищення криптографічної стійкості шифрування з використанням дробово-лінійних перетворень.

Нехай P, Q - довільні прості числа. Нехай у відповідності до алгоритму RSA виконуються наступні співвідношення

$$n = PQ,\ \varphi(n) = (P-1)(Q-1), ed \equiv 1 \pmod{\varphi(n)}, e < \varphi(n), d < \varphi(n). \tag{5}$$

Нехай A – ціле невід'ємне число. Виконаємо дробово-лінійне перетворення

$$\begin{cases} u = \dfrac{\alpha e + \beta}{\beta e + \gamma} \\ v = \dfrac{\alpha d + \beta}{\beta d + \gamma} \end{cases} \tag{6}$$

з виконанням умов: $(\beta,\ \alpha) \neq 1$, $\beta^2 - \alpha\gamma = 0$ і

$$de \equiv 1 \pmod{\varphi(n)}, \tag{7}$$

де $e < \varphi(n)$, $d < \varphi(n)$. Натуральні e, d в (7) завжди існують, наприклад, $e = \varphi(n) - 1, d = \varphi(n) - 1$.

Знайдемо такі α і β, щоб виконувалася конгруенція

$$(A^u)^v \equiv A^1 \pmod{n}. \tag{8}$$

Тоді за властивістю 3 виконується конгруенція

$$\frac{\alpha e + \beta}{\beta e + \gamma} \cdot \frac{\alpha d + \beta}{\beta d + \gamma} \equiv 1 \pmod{\varphi(n)}, \tag{9}$$

або еквівалентна до неї

$$ed\alpha^2 + (1 - ed)\beta^2 - \gamma^2 + (e + d)\alpha\beta - (e + d)\beta\gamma \equiv 0 \pmod{\varphi(n)}. \tag{10}$$

Відомо [7, 8], що тернарна квадратична форма (10) має хоча б один

розв'язок в цілих числах відносно змінних α, β, γ. Для точнішої оцінки числа розв'язків форми (10) використаємо наступну теорему.

Теорема I [9]. Нехай задана невизначена тернарна квадратична форма

$$f(x, y, z) = ax^2 + a'y^2 + a''z^2 + 2b''xy + 2b'xz + 2byz \tag{11}$$

з визначником

$$\Delta = \begin{vmatrix} a & b'' & b' \\ b'' & a' & b \\ b' & b & a'' \end{vmatrix} > 0 \tag{12}$$

з довільними дійсними коефіцієнтами. Тоді існують такі значення змінних x, y, z, $xyz \neq 0$, при яких

$$\left| f(x, y, z) \right| < \sqrt[3]{\frac{2}{9}\Delta}\,. \tag{13}$$

В силу (13) число розв'язків конгруенції (13) не перевищує $\left[\sqrt[3]{\frac{2}{9}\Delta}\right]$, тобто не перевищує цілої частини $\sqrt[3]{\frac{2}{9}\Delta}$.

Отже, конгруенція (10), лівою частиною якої є тернарна квадратична форма, в силу теореми I в загальному випадку має $\wp(n) \le \left[\sqrt[3]{\frac{2}{9}\Delta}\right]$ розв'язків в цілих числах.

Нехай $\alpha = k\beta$. В силу умови $\beta^2 - \alpha\gamma = 0$ маємо, що $\beta = k\gamma$. Тоді (10) набуде вигляду

$$edk^3 + (e+d)k^2 + (1-ed)k - (e+d) \equiv 1 (\mathrm{mod}\, \varphi(n))\ . \tag{14}$$

Кубічна конгруенція (14) завжди має хоч би один розв'язок [4, 10].

Розглянемо наступні дві послідовності

$$u_0 = e, u_1, u_2, \ldots, u_m, \ldots, \tag{15}$$

$$v_0 = d, v_1, v_2, \ldots, v_m, \ldots, \tag{16}$$

елементи яких будуються по рекурентних співвідношеннях

$$\begin{cases} u_{i+1} = \dfrac{\alpha_i u_i + \beta_i}{\beta_i u_i + \gamma_i} \\ v_{i+1} = \dfrac{\alpha_i v_i + \beta_i}{\beta_i v_i + \gamma_i} \end{cases} \tag{17}$$

В силу побудови чисел в послідовностях (15) і (16) для кожного $k \ge 0$: $u_k v_k \equiv 1 (\mathrm{mod}\, \varphi(n))$ і для кожного натурального A виконується конгруенція

$$A^{u_k v_k} \equiv A^1 (\mathrm{mod}\ \varphi(n))\,. \tag{18}$$

Взявши до уваги (18) можна модифікувати алгоритм шифрування RSA, наступним чином:

таємний ключ вибирати таким, який складається з двох чисел – попереднього таємного ключа *d* і номера *k* пари двох чисел u_k, v_k , для яких виконується (18).

Застосовуючи описану дробово-лінійну модифікацію системи RSA, можливо для різних користувачів надати зашифроване по-різному вхідне зображення, вибравши з послідовностей (15) - (16) для кожного користувача тільки йому задані номери k пари чисел u_k, v_k.

Нехай $\psi(n)$ – найменше спільне кратне чисел $P - 1$ і $Q - 1$, K – максимальне число елементів в послідовностях (15) - (16), $\wp(n) \geq 1$ – число розв'язків конгруенції (14). Виберемо з кожної послідовності підмножину з $m \geq 1$ елементів. Підмножину з m елементів з множини, яка містить K елементів, можна вибрати C_K^m способами. Це означає, що за $\wp(n) \cdot C_K^m \cdot (\varphi(\psi(n)) - 1)$ ітерацій можна розкрити зашифроване повідомлення дробово-лінійним модифікованим методом, що значно більше, ніж в стандартному варіанті RSA.

Підвищення криптографічної стійкості шифрування з використанням кватернарних дробово-лінійних перетворень.

При виконанні співвідношення (5) і (7)

$n = PQ, \varphi(n) = (P-1)(Q-1), ed \equiv 1 (\mathrm{mod}\, \varphi(n)), e < \varphi(n), d < \varphi(n), de \equiv 1 (\mathrm{mod}\, \varphi(n))$

виконаємо кватернарне дробово-лінійне перетворення

$$\begin{cases} u = \dfrac{ax + by + fz + gm + \delta}{cx + hy + lz + km + \Delta} \\ v = \dfrac{bx + fy + gz + am + \delta}{hx + ly + kz + cm + \Delta} \\ s = \dfrac{fx + gy + az + bm + \delta}{lx + ky + cz + hm + \Delta} \\ t = \dfrac{gx + ay + bz + fm + \delta}{kx + cy + hz + lm + \Delta} \end{cases} \qquad (19)$$

Розглянемо наступні послідовності

$$\begin{cases} u_0 = e, u_1, u_2, \ldots, u_m, \ldots, \\ v_0 = e, v_1, v_2, \ldots, v_m, \ldots, \\ s_0 = P, s_1, s_2, \ldots, s_m, \ldots, \\ t_0 = Q, t_1, t_2, \ldots, t_m, \ldots, \end{cases} \qquad (20)$$

елементи яких будуються за рекурентними співвідношеннями

$$\begin{cases} u_{i+1} = \dfrac{\alpha_i u_i + \beta_i v_i + \gamma_i s_i + \delta_i t_i + \Omega}{\alpha_i u_i + \beta_i v_i + \gamma_i s_i + \delta_i t_i + \Delta} \\ v_{i+1} = \dfrac{\beta_i u_i + \gamma_i v_i + \delta_i s_i + \alpha_i t_i + \Omega}{\beta_i u_i + \gamma_i v_i + \delta_i s_i + \alpha_i t_i + \Delta} \\ s_{i+1} = \dfrac{\gamma_i u_i + \delta_i v_i + \alpha_i s_i + \beta_i t_i + \Omega}{\gamma_i u_i + \delta_i v_i + \alpha_i s_i + \beta_i t_i + \Delta} \\ t_{i+1} = \dfrac{\delta_i u_i + \alpha_i v_i + \beta_i s_i + \gamma_i t_i + \Omega}{\delta_i u_i + \alpha_i v_i + \beta_i s_i + \gamma_i t_i + \Delta} \end{cases} \quad (21)$$

Числа в послідовностях (20) для кожного $k \geq 0$ вибираються так, щоб виконувалася конгруенція $U_k V_k \equiv 1(\mathrm{mod}\,\varphi(n))$, де числа U_k, V_k - пара чисел з (21), а для кожного натурального A виконується конгруенція

$$A^{U_k V_k} \equiv A^1(\mathrm{mod}\ \varphi(n)). \quad (22)$$

Криптографічна стійкість методів шифрування, побудованих з використанням кватернарних дробово-лінійних перетворень, є вищою, ніж при використанні звичайних дробово-лінійних перетворень.

Висновки

1. Запропонований метод підвищення стійкості модифікованих алгоритмів дає можливість застосовувати невеликі значення ключів при шифруванні із збереженням якісних характеристик вихідного зображення (чи зображень).

2. Мінімальна стійкість до несанкціонованого дешифрування запропонованою модифікацією забезпечується класичним алгоритмом RSA.

3. Реалізація описаного стійкого модифікованого криптографічного алгоритму з одночасним забезпеченням якості зображення не вимагає значних обчислювальних ресурсів.

4.Стійкість захисту від несанкціонованого дешифрування може здійснюватися «прив'язкою» програмного забезпечення до дистрибутивного носія (комп'ютера), або до розміщення елементів топології.

Теоретична стійкість визначається за умови, що не існує часових обмежень на несанкціоноване дешифрування, і, отже, це є відповіддю на питання, що криптосистема не може бути розкрита в принципі. Їх можна побудувати за допомогою випадкового рівноймовірного ключа шифрування, довжина якого не менше довжини відкритого тексту. Зовсім стійкі системи надзвичайно дорогі в реалізації. Тому на практиці використовують системи, які в принципі можна розкрити, але за неприйнятний час.

Для будь-якої криптосистеми існує відповідність між її вартістю й часом її «зламу». Зашифровані дані, крім того, мають цінність, що звичайно знижується згодом. Це дає певну відповідність між цінністю й часом зберігання інформації.

Оскільки, однією із основних проблем поза забезпечення відповідної стійкості алгоритму RSA вибором коректних параметрів є низька швидкість проведення обчислень і операцій шифрування/дешифрування (RSA

приблизно в 1000 разів працює повільніше, ніж DES), то для довгих текстових повідомлень його використання стає неефективним. Ефективність алгоритму RSA проявляється при шифруванні/дешифруванні зображень, особливо зображень, в яких є чітко виділені контури.

1. *Вербіцький О. В.* Вступ до криптології. //Видавницгво науково-технічної літератури. – Львів 1998. – 247 с.
2. *Ємець В., Мельник А., Попович Р.* Сучасна криптографія. Основні поняття.// «БАК», Львів, 2003. – 144 с.
3. *Виноградов И.М.* Основы теории чисел.// Изд. 2, переработ., М. – Л., ОНТИ, 1938. – с.88.
4. *Бородін О.І.* Теорія чисел. // «Вища школа», – Київ,1970, – с.277.
5. *Курант Рихард, Роббинс Герберт*. Что такое математика?// Научно-издательский центр «Регулярная и хаотическая динамика», Ижевск, 2000, 592 с.
6. *Нильс Фергюсон, Брюс Шнайер*. Практическая криптография// Изд. Вильямс, 2005, 416 с.
7. Г*олубева Е. П.* , "Представление больших чисел тернарными квадратичными формами", Матем. сб., 129(171) : 1 (1986), 40–54 с.
8. *Пачев У. М.* , "Представление целых чисел изотропными тернарными квадратичными формами", //Изв. РАН. Сер. матем., 70:3 (2006), 167–184.
9. *Венков Б.А*. Исследования по теории чисел.// «Наука», Ленинград, 1981, 448с.
10. *Карл Фридрих Гаусс*. Труды по теории чисел. Общая ред. академика Виноградова И.М. Москва, 1959. – 469 с.

Поступила 7.10.2013р.

УДК 621.391

Б.В. Дурняк, Р.Б.Стахів, УАД, м.Львів

РОЗРОБКА ОСНОВНИХ КОМПОНЕНТ ТЕХНОЛОГІЇ ФОРМУВАННЯ ЗАСОБІВ ЗАХИСТУ НА ОСНОВІ ВИКОРИСТАННЯ ЕТИКЕТОК

Однією з компонент технології формування засобів захисту є інформаційна модель $IM^E = F^I[I^D, I^C, I^R, I^Z, I^N, I^O]$, де I^D – текстові дані з документів на продукт, I^C - текстові дані для споживача, I^Z- текстові дані засобів захисту, I^R- текстові дані реклами, I^N - надмірна інформація, I^O – інформація про опакування. Використання будь якої моделі полягає у тому, що остання може використовуватися для проведення аналізу обєкту, що моделюється, який може полягати у визначенні значень деяких параметрів обєкту. Тому, F^I є функція, що описує взаємозвязки між компонентами моделі. Оскільки окремі компоненти представляють собою текстові форми, то ця форма є основою для інших компонент, наприклад, I^Z може представляти