УДК 681.324.067

Ю.І. ГОРБЕНКО, канд. техн. наук

МЕТОДИ ОЦІНКИ НЕОБОРОТНОСТІ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ БАГАТОМОДУЛЬНИХ ПЕРЕТВОРЕНЬ В СКІНЧЕННИХ ПОЛЯХ

Вступ

В [1, 2] запропоновано методи та досліджено властивості псевдовипадкових послідовностей, які будуються на основі використання багатомодульних перетворень в простих та розширеннях скінченних полів Галуа. Визначено необхідні та достатні умови існування ПВП з рівноймовірним розподілом символів довільного алфавіту m, заданим періодом повторення та існуванням ізоморфізмів. Запропоновано спосіб введення ключа генератора ПВП. Разом з тим, залишились не дослідженими властивості необоротності такого генератора щодо складності компрометації ключа генератора на основі здійснення криптоаналізу. В [2] запропоновано достатньо грубий метод оцінки складності криптоаналізу такого генератора, який зводиться до розв'язку дискретного логарифмічного рівняння в скінченному полі Галуа.

Мета цієї статі – теоретична та практична оцінка складності здійснення криптоаналізу генератора ПВП на основі трьох- та багатомодульних перетворень в скінченних полях Галуа.

1. Сутність методу генерування ПВП

Розглядається метод генерування ПВП з певним алфавітом символів, наприклад m, на основі багатомодульних перетворень в скінченному полі Галуа $GF(p^n)$, $n \geq 1$. Вважається, що здійснюється k перетворень елементів розширення поля Галуа $GF(p^n)$, відповідно за модулями $(f(X), f_1(X)), (f_1(X), f_2(X)), \ldots, (f_{k-2}(X), f_{k-1}(X))$ та останнім модулем m. Загальними параметрами є кортеж $(f(X), p, n, \theta_j)$, де $f(X)$ – незвідний поліном ступеня n над полем $GF(p)$, а θ_j – первісний елемент, вибраний із множини $\{\theta\}$ порядку $\varphi(p^n - 1)$, де $\varphi(\,)$ – функція Ейлера [3]. Для даного випадку генерування (формування) елементів поля здійснюється за правилом

$$a_i = (\theta_j)^i (\mathrm{mod}(f(X), p, n)). \tag{1}$$

Метод (1) породжує скінченне поле Галуа з періодом повторення $p^n - 1$. Нехай $(f_s(X), p_s, n_s)$ будуть кортежами загальних параметрів, наприклад поліномів (в тому числі незвідних) $f_s(X)$. $s = (1, k-1)$, а n_s – їх ступені, причому згідно [1]

$$n_1 > n_2,\ n_2 > n_3,\ \ldots,\ n_{k-2} > n_{k-1}, \tag{2}$$

а також виконуються нерівності

$$p^{n_1} >> p^{n_2},\ p^{n_2} >> p^{n_3},\ \ldots,\ p^{n_{k-2}} >> p^{n_{k-1}},\ p^{n_{k-1}} >> m. \tag{3}$$

Розглядається генератор ПВП, що функціонує згідно з багатомодульним перетворенням

$$b_i = \left((\theta_j)^i (\mathrm{mod}(f(X), p, n), (f_1(X), p_1, n_1), (f_2(X), p_2, n_2), \ldots \right.$$
$$\left. \ldots, (f_{k-1}(X), p_{k-1}, n_{k-1}), (f_m(X), \mathrm{m})\right), \tag{4}$$

де

$$(f_s(X), p_s, n_s) \tag{5}$$

кортежі загальних параметрів, m – певне натуральне число, k – ступінь багатомодульності, p_m (не обов'язково просте), m – ціле натуральне, $n \geq 1$.

Справедливим є твердження 1.

Твердження 1. Детермінований генератор ПВП, що функціонує згідно з алгоритмом багатомодульного перетворення

$$b_i = \left((\theta_j)^{K_0+i}(\mathrm{mod}(f(X),p,n),(f_1(X),p_1,n_1),(f_2(X),p_2,n_2),\ldots \right.$$
$$\left. \ldots,(f_{k-1}(X),p_{k-1},n_{k-1}),\left(f_m(X),\tilde{m}\right)\right), \qquad (6)$$

де K_0+i – плинний ключ генератора, причому K_0 є початковим ключем, а i – ключем сеансу, є необоротним з експоненційною складністю атаки «повне розкриття».

Будемо розглядати також частковий випадок твердження 1 для трьохмодульного перетворення. В даному випадку елементи розширення поля Галуа також генеруються згідно (1). Але (2) – (6) приймають наступний вигляд

$$n_1 > m, \qquad (7)$$

$$p^{n_1} >> p^m, \qquad (8)$$

$$b_i = \left((\theta_j)^{K_0+i}\left(\mathrm{mod}(f(X),p),(f_1(X),p_1,n_1),\left(f_m(X),\tilde{m}\right)\right)\right). \qquad (9)$$

Де, як в (4), K_0+i – плинний ключ генератора, K_0 початковий, а i – ключ сеансу.

2. Оцінка складності обернення генератора ПВП

Проведемо оцінку складності дискретного логарифмування для трьох- та багатомодульного перетворень.

У випадку для скінченного поля Галуа $GF(p)$ маємо

$$b_i = \left((\theta_j)^X(\mathrm{mod}(P),(P_1),(m))\right), \qquad (10)$$

де $X = K_0 + i$ належить визначенню, за умови, що відомою є деяка послідовність символів b_i, первісний елемент θ_j та кортеж параметрів (P, P_1, m).

При здійсненні атаки «груба сила» можуть бути застосовані такі основні методи – перебирання ключів, таблична атака та атака зі словником [5].

При застосуванні атаки «груба сила» вважається, що довжина ключа k не більш ніж довжина генерованої ПВП і порушник, перебираючи ключ X, робить спробу отримати значення

$$b_i^* = b_i. \qquad (11)$$

При виконанні умови (11) буде визначено ключ генератора.

Для оцінки можливостей реалізації атаки «груба сила» можуть бути використані такі показники як N_k – число ключів, безпечний час $t_б$, P_p – ймовірність успішного криптоаналізу тощо [2, 5]. Значення $t_б$ можна обчислити [5]:

$$t_б = \frac{N_k}{\gamma K} P_p, \qquad (12)$$

де γ – потужність криптоаналітичної системи, K =3,15 10^7 – число секунд у році.

Таблична атака та атака зі словником ґрунтуються на використанні математичного апарату «парадоксу про день народження» – методом створення колізій [5]. Для даного методу параметри ймовірність колізій P_k, число спроб криптоаналітика k та повна множина можливих вихідних значень n пов'язані між собою параметричним рівнянням [5]

$$1 - P_k = e^{-(k(k-1))/2n}, \qquad (13)$$

або в кінцевому вигляді

$$k^2 - k + 2n\ln(1 - P_з) = 0. \qquad (14)$$

Співвідношення (14) дозволяє оцінити число експериментів, які необхідно виконати для здійснення колізії з застосуванням математичного апарату «парадоксу про день народження».

В ряду випадків пару «ключ генератора – вихідний блок ПВП» можна отримати методом словника. В цьому випадку генеруються або збираються пари «ключ генератора – вихідний блок ПВП» в спеціальному словнику. А пошук ключа здійснюється засобом знаходження реалізації ПВП, що співпадає з виходом генератора по словнику.

Проведемо аналіз можливостей та умов реалізації атаки типу «груба сила», яка проводиться відносно (10) з метою визначення елемента поля $(\theta_j)^X (\mathrm{mod}\, p)$. Розглянемо модель відображення m-ічного символу в p-ічний. Нехай довжини символів в двійковому поданні будуть l_p, l_{p_1} та l_m відповідно для модулів p, p_1 та m. Визначимо ймовірність угадування по b_i символу p-ічного символу, а по суті визначення $\theta_j^{K_0+i}$.

Теорема 1. Для умов (11) ймовірність правильного відображення (вгадування) $P_{\text{ПВ}}$ m-ічного b_i символу в p-ічний $\theta_j^{K_0+i}$ визначається співвідношенням

$$P_{\text{пв}} = 2^{l_m - l_p}, \tag{15}$$

де l_p та l_m – двійкове подання довжин символів p та m.

Розглянемо доведення теореми. При довжині m-ічного b_i символу в двійковому поданні l_m число можливих його станів визначається як 2^{l_m}. При перетворенні за модулем p_1 довжина символу в двійковому поданні буде l_{p_1}, а число можливих станів визначається як $2^{l_{p_1}}$. При цьому степінь розширення алфавіту можна оцінити як

$$\mu_2 = 2^{l_{p_1}} \Big/ 2^{l_m} = 2^{l_{p_1} - l_m}.$$

При перетворенні за модулем p довжина символу в двійковому поданні буде l_p, а число можливих станів визначається як 2^{l_p}. Ступінь розширення алфавіту при переході до перетворення за модулем p

$$\mu_1 = 2^{l_p} \Big/ 2^{l_{p_1}} = 2^{l_p - l_{p_1}}.$$

Відповідно ймовірність вгадування символу алфавіту за модулем p_1 визначається як

$$P_{p_1} = 1 \Big/ \mu_2 = 2^{l_m - l_{p_1}}. \tag{16}$$

Ймовірності вгадування символу алфавіту за модулем p визначається як

$$P_p = 1 \Big/ \mu_1 = 2^{l_{p_1} - l_p}. \tag{17}$$

Таким чином теорема доведена.

Загальна ймовірність вгадування символу алфавіту $P_{\text{в}}$ за модулем p при переході від m-ічного джерела до p-ічного буде визначатись перемноженням подій P_{p_1} та P_p, тобто

$$P_{\text{в}} = P_{p_1} \cdot P_p = 2^{l_m - l_{p_1}} \cdot 2^{l_{p_1} - l_p} = 2^{l_m - l_p}. \tag{18}$$

Використовуючи (18), можна також визначити складність $I_{\text{в}}$ вгадування одного символу алфавіту за модулем p при переході від m-ічного джерела до p-ічного, як

$$I_{\text{в}} = 1 \Big/ P_{\text{в}} = 2^{l_p - l_m}. \tag{19}$$

Таким чином, при застосуванні схеми генератора без гешування складність $I_{ВІ}$ відновлення ключа $X = K_0 + i$ визначається

$$I_{ВД} = I_{В} \cdot I_{ДЛ} = 2^{l_p - l_m} \cdot \exp\left(\varepsilon \ln(p)^{\nu} \ln\ln(p)^{(1-\nu)}\right). \quad (20)$$

Для випадку застосування схеми генератора з вгадуванням елемента поля, розв'язком дискретного логарифму та гешуванням складність $I_{ВДГ}$ відновлення ключа $X = K_0 + i$ визначається

$$I_{ВДГ} = I_{В} \cdot I_{ДЛ} \cdot I_{Г} = 2^{l_p - l_m} \cdot \exp\left(\varepsilon \ln(p)^{\nu} \ln\ln(p)^{(1-\nu)}\right) \cdot 2^{n/2} \quad (21)$$

Необхідно відмітити, що вирази (20) та (21) отримані для випадку, коли ПВП виробляється засобом використання тільки одного m-ічного символу. Якщо для вироблення ПВП використовується μ m-ічних символи, а значення i збільшується за відомим правилом, то (20) та (21) можна використовувати для оцінки криптографічної стійкості генератора ПВП, що пропонується. Якщо i збільшується за невідомим правилом, то необхідно вирішувати додатково ще і задачу визначення правила його зміни. Але, так як правило зміни i будемо вважати відомим криптоаналітику, то (20) та (21) рекомендується для оцінки складності обернення генераторів ПВП типу (20) та (21).

В таблиці наведено оцінки складності обернення генератора ПВП згідно (20) та (21). Аналіз даних таблиці дозволяє зробити висновок про те, що складність обернення генератора носить експоненційний характер і є більшою за складність методу «груба сила».

0

p, p_1, m Метод		$2^{256}, 2^{28}, 2^{8}$	$2^{256}, 2^{128}, 2^{64}$	$2^{512}, 2^{256}, 2^{8}$	$2^{1024}, 2^{512}, 2^{256}$	$2^{2048}, 2^{1024}, 2^{512}$
$I_{ВД}$		$5.0543 \cdot 10^{089}$	$7.0143 \cdot 10^{072}$	$2.1618 \cdot 10^{172}$	$1.4827 \cdot 10^{259}$	$1.1867 \cdot 10^{300}$
$I_{ВДГ}$	n	$6.1103 \cdot 10^{113}$	$8.4798 \cdot 10^{096}$	$2.6135 \cdot 10^{196}$	$1.7925 \cdot 10^{283}$	$1.4346 \cdot 10^{524}$
	160					
	256	$1.7199 \cdot 10^{128}$	$2.3868 \cdot 10^{111}$	$7.3562 \cdot 10^{210}$	$5.0453 \cdot 10^{297}$	$4.0381 \cdot 10^{538}$
	384	$3.1726 \cdot 10^{147}$	$4.4029 \cdot 10^{130}$	$1.3570 \cdot 10^{230}$	$9.3071 \cdot 10^{316}$	$7.4490 \cdot 10^{557}$
	512	$5.8524 \cdot 10^{166}$	$8.1219 \cdot 10^{149}$	$2.5031 \cdot 10^{249}$	$1.7168 \cdot 10^{336}$	$1.3741 \cdot 10^{577}$

Розглянемо ще один підхід до вирішення задачі обернення генераторів ПВП виду (10), що ґрунтується на классах лишків. Для цього подамо (10) у такому вигляді:

$$\begin{gathered} b_i = \Theta^{x_i} (\bmod P)(\bmod P_1)(\bmod m), \\ \Theta^{x_i} (\bmod P)(\bmod P_1) = q_i \cdot m + b_i, \\ 0 \le q_i \cdot m + b_i < P_1, \\ \Theta^{x_i} (\bmod P) = l_i \cdot P_1 + q_i \cdot m + b_i, \quad 0 \le l_i \cdot P_1 + q_i \cdot m + b_i < P, \\ \Theta^{x_i} (\bmod P) = l_i \cdot P_1 + q_i \cdot m + b_i (\bmod P). \end{gathered} \quad (22)$$

Аналіз (22) показує, що x_i, l_i, q_i є невідомими та належать визначенню. Тепер врахуємо, що правило зміни x_i є відомим. На основі (22) можна скласти систему рівнянь виду

$$\begin{cases} \Theta^{x_i} (\bmod P) = l_i \cdot P_1 + q_i \cdot m + b_i (\bmod P); \\ \Theta^{x_{i+1}} (\bmod P) = l_{i+1} \cdot P_1 + q_{i+1} \cdot m + b_{i+1} (\bmod P); \\ \ldots\ldots\ldots \\ \Theta^{x_{i+k}} (\bmod P) = l_{i+k} \cdot P_1 + q_{i+k} \cdot m + b_{i+k} (\bmod P). \end{cases} \quad (23)$$

Аналіз системи рівнянь (22) показує, що кожне нове рівняння в системі добавляє два невідомих, але при цьому існує лінійна залежність між x_i та x_{i+1} тощо. В цілому в системі k-го порядку буде $2k+1$ невідомих, якщо навіть вважати що тільки x_i є невідомим.

Таким чином, система рівнянь виду (23) з $2k+1$ невідомими розв'язку не має. Також необхідно відмітити, що по аналогії з трьохмодульним перетворенням, при багатомодульному перетворенні кожне додаткове модульне перетворення добавляє два невідомих.

Висновки та рекомендації

Властивості необоротності генератора ПВП по суті пов'язані з розв'язком дискретних логарифмічних рівнянь, наприклад для трьохмодульним перетворенням виду (9) та (10) відносно i та K_0+i.

Для успішного криптоаналізу генератора необхідно спочатку вирішити дискретне логарифмічне рівняння та знайти елемент – прообраз. В цьому випадку спочатку необхідно знайти прообраз відповідного елемента поля A_i, а потім вирішити дискретне логарифмічне рівняння зі складністю $I_{\text{дл}}$.

Для умови (13) ймовірність правильного відображення (вгадування) $P_{\text{ПВ}}$ m-ічного b_i символу в p-ічний $\theta_j^{K_0+i}$ визначається співвідношенням (18).

Аналіз системи рівнянь (22) показує, що кожне нове рівняння в системі добавляє два невідомих, причому існує лінійна залежність між x_i та x_{i+1} тощо. В системі k-го порядку буде $2k+1$ невідомих. Тому система рівнянь виду (23) з $2k+1$ невідомими розв'язку не має.

Список літератури. 1. *Потий А.В.* Метод многомодульного преобразования чисел // Обработка информации и обеспечение надежности систем управления : сб. науч. тр. – Харьков: НАНУ, ПАНИ, ХВУ, 1997. – С. 63-68. 2. Гріненко Т.О., Горбенко Ю.І. Метод генерування псевдовипадкових послідовностей на основі багатомодульних перетворень в скінченних полях. 3. *Андерсон, Джеймс А.* Дискретная математика и комбинаторика : пер. с англ. – М. : Изд. дом «Вильямс», 2003 – 960 с. 4. *ISO/IEC 18031* Information technology – Security techniques –Random bit generation. 2005. 5. *Горбенко Ю.І., Горбенко І.Д.* Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. – Харків : Форт, 2010. – 593с.

Харківський національний університет радіоелектроніки

Надійшла до редколегії 17.03.2011