***Клименко Ксенія Вікторівна**, асистент, кафедра землеустрою та кадастру, Південна філія Національного університету біоресурсів і природокористування України «Кримський агротехнологічний університет», Україна.*
***Орлова Тетяна Олександрівна**, кандидат технічних наук, доцент, кафедра землеустрою та кадастру, Південна філія Національного університету біоресурсів і природокористування України «Кримський агротехнологічний університет», Україна.*
***Саломатін Валерій Миколайович**, доктор геолого-мінералогічних наук, професор, кафедра геодезії та геоінфоматики, Південна філія Національного університету біоресурсів і природокористування України «Кримський агротехнологічний університет», Україна.*

***Klimenko Kseniya**, the South Branch of the National University of Life and Environmental Sciences of Ukraine «Crimean Agrotechnological University», Ukraine, **e-mail: mkv_1382@mail.ru**.*
***Orlova Tatiana**, the South Branch of the National University of Life and Environmental Sciences of Ukraine «Crimean Agrotechnological University», Ukraine, **e-mail: to156119@mail.ru**.*
Salomatin Valeriy**, the South Branch of the National University of Life and Environmental Sciences of Ukraine «Crimean Agrotechnological University», Ukraine, **e-mail: maksota@mail.ru

УДК 004.056

Замула А. А.,
Семченко Д. А.

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННЫЕ НА ДИСКРЕТНОМ ЛОГАРИФМЕ

В работе представлена математическая модель генератора псевдослучайных чисел, рассматривается проблематика решения задач дискретного логарифма. Приводится анализ алгоритмов генерации псевдослучайных чисел, основанных на задаче дискретного логарифма. В качестве примера рассматривается генератор Сундарама-Пателя, даются качественные и количественные характеристики стойкости данного генератора к основным видам атак.

Ключевые слова: *генератор, дискретный логарифм, псевдослучайное число, криптостойкость, алгоритм, бит.*

1. Введение

Задача дискретного логарифмирования является одной из ключевых задач криптографии с открытым ключом. Она опирается на высокую вычислительною сложность обращения числовых функций. Операция дискретного логарифмирования является обратной к степенной функции и принадлежит к классу NP задач. Возможность эффективного решения задачи вычисления дискретного логарифма связана с квантовыми вычислениями. Теоретически доказано, что, используя их, дискретный логарифм может быть вычислен за полиномиальное время. Классическими криптографическими схемами, базирующимися на сложности задачи дискретного логарифмирования, являются: схема генерации общего ключа Диффи-Хеллмана, схема электронной подписи Эль-Гамаля, криптосистема Мэсси-Омуры для передачи сообщений.

Целью статьи является анализ существующей реализации генератора псевдослучайных чисел Сундарама-Пателя, основанного на сложности вычисления дискретного логарифма. На основании приведенных результатов строится итеративный генератор. Приводится сравнительный анализ такого генератора с генератором Сундарама-Пателя и генератором Блюма. На основании результатов, полученных при сравнительном анализе, делаются выводы о криптографической стойкости рассмотренных генераторов.

Введем условные обозначения и определения, которые важны для дальнейших рассуждений.

Пусть X_n, Y_n два случайных распределения вероятностей на множестве $\{0,1\}^n$, где $\{0,1\}^n$ множество строк длиной n бит. В дальнейшем будем обозначать $x \leftarrow X_n$ как выбор элемента x из $\{0,1\}^n$ в соответствии с распределением X_n.

Пусть $\Delta(n)$ является ограничением для *статистического расстояния* $\sum_{x\in\{0.1\}^n} \left|\Pr ob_{X_n}[x] - \Pr ob_{Y_n}[x]\right|$ между X_n и Y_n, то есть: $\sum_{x\in\{0.1\}^n} \left|\Pr ob_{X_n}[x] - \Pr ob_{Y_n}[x]\right| \le \Delta(n)$. При этом X_n и Y_n есть *статистически неразличимыми*, если для каждого полинома $P(\cdot)$ и для достаточно большого n будет верно выражение $\Delta(n) \le \frac{1}{P(n)}$.

Пусть D — недетерминированная машина Тьюринга [1], тогда обозначим $\Pr ob[x \leftarrow X_n; D(x) = 1]$ как δ_{D,X_n}, и $\Pr ob[y \leftarrow X_y; D(y) = 1]$ как δ_{D,Y_n}. Если для любой недетерминированной D полиномиального времени, для каждого полинома $P(\cdot)$, при достаточно большом n выполняется неравенство $\left|\delta_{D,X_n} - \delta_{D,Y_n}\right| \le \frac{1}{P(n)}$, тогда X_n и Y_n *вычислительно неразличимы.*

Пусть G_n — криптографически стойкий генератор псевдослучайных бит, если функция G_n может быть вычислена за полиномиальное время и два семейства распределения вероятностей X_n и Y_n вычислительно неразличимы, где G_n индуцирует семейство распределений вероятностей X_n.

Инициализирующее значение генератора — определим как seed [1].

Пусть A_n некоторое семейство множеств таких, что для каждого n выполняется условие $2^{n-1} \le |A_n| < 2^n$ (то

есть нам необходимо n бит, чтобы описать элементы из A_n). Обозначим U_n как равномерное распределение над A_n. Также пусть k_n последовательность чисел, таких, что для каждого n, $k_n < n$.

Рассмотрим генератор $AG_n : \{0,1\}^{k_n} \to A_n$ элементов произвольного множества A_n, где AG_n генерирует семейство распределения вероятностей над A_n следующим образом: $\Pr ob_{AG_n}[y] = \Pr ob[y = AG_n(s); s \leftarrow R_{k_n}]$.

Пусть p — простое число. Обозначим n длину двоичного представления числа p. Множество $Z_p^* = \{x : 1 \le x \le p-1\}$ является циклической группой по умножению $\bmod p$. Пусть g генератор элементов из Z_p^*. Таким образом, функция $f : Z_{p-1} \to Z_p^*$, $f(x) = g^x \bmod p$ является перестановкой. Функция, обратная f (функция дискретного логарифма) предположительно трудно вычисляемая. Наиболее известным методом вычисления дискретного логарифма является так называемый метод вычисления индексов [1], вычислительная сложность метода экспоненциально n.

Одной из важных задач вычисления дискретного логарифма является ускорение вычисления функции $f(x) = g^x$. Одним из возможных способов достижения этого, может быть ограничение его входных значений только небольшими величинами x.

Пусть c число, которое зависит от n ($c = c(n)$). Предположим, что даны $y = g^x \bmod p$, где $x \le 2^c$. Вычисление дискретного логарифма от y является сложным даже, если известно, что $x \le 2^c$. Время выполнения, необходимое для вычисления дискретного логарифма, при использовании метода вычисления индексов, зависит только от размера n всей группы. В зависимости от размера c различные методы могут быть более эффективными. Так называемые, baby-step giant-step алгоритма Shanks или ρ-Полларда [2] могут рассчитать дискретный логарифм от y за время $O(2^{c/2})$.

Таким образом, если обозначить $c = \omega(\log n)$, то не существует известных алгоритмов способных вычислить дискретный логарифм от $y = g^x \bmod p$, где $x \le 2^c$, за полиномиальное время. Предположение о том, что такого алгоритма не существует, называется предположением о дискретном логарифме с короткими c бит экспонентами ($c - DLSE$).

$$P_r\begin{bmatrix} p \leftarrow PRIMES(n); \\ x \leftarrow R_c; \\ D(p,g,g^x,c) = x \end{bmatrix} \le \frac{1}{P(n)}. \quad (1)$$

Предположение $c - DLSE$: Пусть $PRIMES(s)$ множество n разрядных простых чисел и пусть величина c, которая растет быстрее, чем величина $\log n$ (т. е. $c = \omega(\log n)$). Для каждой вероятностной машины Тьюринга D полиномиального времени, для любого многочлена $P(\cdot)$ и для достаточно больших n будет верно неравенство (1).

Это предположение поддерживается результатом Шнорра [3], который доказывает, что нет общего алгоритма, способного рассчитать c битные дискретные логарифмы за менее чем $2^{c/2}$ шагов.

Учитывая современные вычислительные мощности, а также алгоритмы расчета дискретного логарифма, оказывается достаточным установить $n = 1024$, а $c = 160$, то есть, понадобится не менее 2^{80} шагов для расчета такого дискретного логарифма.

Рассмотрим функцию $f(x) = g^x \bmod p$ как однонаправленную. При этом легко прогнозировать последний значащий бит из $x \in Z_{p-1}$ посредством проверки: является ли y квадратичным вычетом или нет на множестве Z_p^* (существует тест полиномиальной сложности).

Булевой предикат Π называется «трудным» [4] для односторонней функции f, если любой алгоритм A, который при данной функции $y = f(x)$ прогнозирует $\Pi(x)$ с вероятностью существенно выше, чем $\frac{1}{2}$ и может быть использован для создания нового алгоритма A', который на входе y вычисляет x с непренебрежимой вероятностью.

$$\Pi : Z_{p-1} \to \{0,1\}, \quad (2)$$

$$\Pi(x) = \left(x \le \frac{p-1}{2}\right). \quad (3)$$

В [4] показано, что предикат (2), (3) является «трудным», для функции дискретного логарифма, а в [5] доказано, что каждый бит двоичного представления числа x (за исключением наименьшего значащего) является «трудным» для функции дискретного логарифма.

2. Генератор Сундарама-Пателя

Пусть p будет n-битное простое число, такое что $p \equiv 3 \bmod 4$ и g генератор множества Z_p^*. Обозначим c как величину, которая растет быстрее чем $\log n$, то есть $c = \omega(\log n)$.

В [6] показано, что при $c - DLSE$ предположении, биты $x_2, x_3, ..., x_{n-c}$ все одновременно «трудные» для функции $f(x) = g^x \bmod p$.

Теорема 1. Для достаточной большого n, если p есть n-битное простое число, такое что $p \equiv 3 \bmod 4$ и если предположение $c - DLSE$ верно, то для каждого числа j, которое удовлетворяет условию $2 \le j \le n - c$, для каждой машины Тьюринга D полиномиального времени, для каждого многочлена $P(\cdot)$ и для достаточно большого n верно выражение (4) [6]

$$\left|\Pr ob[x \leftarrow Z_{p-1}; D(g^x, x_2, ..., x_{j-1}) = x_j] - \frac{1}{2}\right| \le \frac{1}{P(n)}. \quad (4)$$

Рассмотрим генератор Сундарама-Пателя. Пусть p будет n битным простым числом, таким что $p \equiv 3 \bmod 4$ и $c = \omega(\log n)$. Рассмотрим следующую функцию, которую определим как PSG. (генератор Сундарама-Пателя) (5), (6):

$$PSG_{n,c} : Z_{p-1} \to Z_p^* \times \{0,1\}^{n-c-1}, \quad (5)$$

$$PSG_{n,c}(x) = (g^x \bmod p, x_2, ..., x_{n-c}). \quad (6)$$

Таким образом, подавая на вход случайный seed $x \in Z_{p-1}$, генератор формирует g^x и $n-c-1$ последовательных бит числа x, начиная со второго наименее значащего бита.

При условии верности гипотезы $c - DLSE$, $PSG_{n,c}$ является генератором, обладающим высокой криптографической стойкостью на множестве $Z_p^* \times \{0,1\}^{n-c-1}$ [7]. Если U_n равномерное распределение на множестве Z_p^*, тогда распределение индуцированное $PSG_{n,c}$ над множеством $Z_p^* \times \{0,1\}^{n-c-1}$, вычислительно неразличимо от распределе-

ния $U_n \times R_{n-c-1}$. Другими словами, для вероятностной машины Тьюринга D полиномиального времени, возможно определить $\delta_{D,URn} = \Pr ob[y \leftarrow Z_p^*; r \leftarrow R_{n-c-1}; D(y,r) = 1]$ и $\delta_{D,PSG_{n,c}} = \Pr ob[x \leftarrow Z_{p-1}; D(PSG_{n,c}(x)) = 1]$.

Тогда, для любого полинома $P(\cdot)$ и для достаточно большого n справедливо неравенство (7):

$$\left|\delta_{D,UR_n} - \delta_{D,PSG_{n,c}}\right| \le \frac{1}{P(n)}. \quad (7)$$

Указанное позволяет получить генератор, обладающий высокой криптографической стойкостью.

Далее предположим, что p является n битным простым числом, таким что $p \equiv 3 \bmod 4$ и $c = \omega(\log n)$ [8]. Пусть g генератор на множестве Z_p^*, а $g^{2^{n-c}} \bmod p$ обозначим как $\hat{g}$. Если s является целым числом, то i-тый бит его двоичного представления обозначим s_i.

Рассмотрим следующую функцию: $RG_{n,c}$: $Z_{p-1} \to Z_p^*$, $RG_{n,c}(g) = \hat{g}^{(sdiv 2^{n-c})} g^{s_1} \bmod p$. Таким образом, рассматриваем возведение в степень по модулю на множестве Z_p^* с базой g, но только после обнуления битов входного значения s в позициях $2,...,n-c$.

Функция RG генерирует распределение на множестве Z_p^*. Распределение вероятности на множестве Z_p^* имеет вид (8):

$$\Pr ob_{RG_{n,c}}[y] = \Pr ob[y = RG_{n,c}(s); s \leftarrow Z_{p-1}]. \quad (8)$$

Приводимая ниже лемма показывает, что распределение $RG_{n,c}$ является вычислительно неразличимым от равномерного распределения на множестве Z_p^* если $c-DLSE$ предположение верно.

Лемма 1. Пусть p n-битное простое такое что $p \equiv 3 \bmod 4$ и пусть U_n равномерное распределение на множестве Z_p^*. Если $c-DLSE$ предположение верно, тогда два распределения U_n и $RG_{n,c}$ являются вычислительно неразличимы.

Доказательство леммы 1 осуществляется от противного. Если $RG_{n,c}$ можно отличить от U_n, тогда модифицированный генератор Сундарама-Пателя PSG не является безопасным. Любой значимый отличительный признак между $RG_{n,c}$ и равномерным распределением на множестве Z_p^* может быть преобразован в отличительный признак для $PSG_{n,c}$. Что противоречит $c-DLSE$ предположению.

Предположим, что существует D машина Тьюринга («отличитель»), которая способна различить распределения и многочлен $P(\cdot)$ такой, что для бесконечно больших n, имеем (9):

$$\delta_{D,U_n} - \delta_{D,RG_{n,c}} \ge \frac{1}{P(n)}, \quad (9)$$

где

$$\delta_{D,U_n} = \Pr ob[x \leftarrow Z_p^*; D(p,g,x,c) = 1],$$

$$\delta_{D,RG_{n,c}} = \Pr ob\left[s \leftarrow Z_{p-1}; D(p,g,RG_{n,c}(s),c) = 1\right].$$

Пусть $\widehat{D}$ машина Тьюринга («отличитель»), которая имеет возможность провести успешный криптоанализ PSG.

Для того чтобы провести успешный криптоанализ $PSG_{n,c}$ на основании входных данных (p,g,y,r,c) таких, что $y \in Z_p^*$ и $r \in \{0,1\}^{n-c-1}$ следует определить, соответствуют ли эти данные распределению $U_n \times R_{n-c-1}$ или $PSG_{n,c}$ выходов генератора $PSG_{n,c}$.

Предположим, что (y,r) был составлен в соответствии с $PSG_{n,c}(x)$ для некоторого случайного $x \in Z_{p-1}$. Тогда $w = g^u$ где $u = 2^{n-c}(xdiv 2^{n-c}) + x_1 \bmod (p-1)$ [9]. То есть, дискретный логарифм от w по основанию g имеет $n-c-1$ бит в позициях $2,...,n-c$ равные 0.

Таким образом, как только установим, что $\hat{g} = g^{2^{n-c}}$, получим $w = \hat{g}^{xdiv 2^{n-c}} g^{x_1} \bmod p$, т. е. $w = RG_{n,c}(x)$. Тогда, если (y,r) составлен согласно PSG_n, то w имеет такое же распределение что и RG_n.

С другой стороны если (y,r) был составлен из y случайно выбранного из Z_p^* и r случайно выбранного из $\{0,1\}^{n-c-1}$, то w является случайным элементом на множестве Z_p^*.

Таким образом, $\widehat{D}$ будет угадывать правильное распределение с такой же точностью, как D. Указанное противоречит безопасности PSG генератора.

3. Итеративный генератор

Пусть итеративный генератор получает в качестве инициализирующего значения случайный элемент s из множества Z_{p-1} и после этого многократно применяет функцию RG к нему. Псевдослучайные биты, выводимые генератором, это те биты которые проигнорированы функцией RG. Результат функции RG будет служить новым входным значением для следующей итерации.

Алгоритм $IRG_{n,c}$ (*итеративный RG генератор*) работает следующим образом. Начиная с $x^{(0)} \in_R Z_{p-1}$ устанавливает $x^{(i)}$ равным RGn,c ($x^{(i-1)}$). Обозначим $r^{(i)}$ как $x_2^{(i)}, x_3^{(i)}, ..., x_{n-c}^{(i)}$. Выход генератора будет $r^{(0)}, r^{(1)}, ..., r^{(k)}$, где k это количество итераций, выбранное таким образом, что $k = poly(n)$ и $k(n-c-1) > n$.

Теорема 2. При условии $c-DLSE$ предположении, $IRG_{n,c}$ является безопасным генератором псевдослучайных бит.

Доказательство. Сначала отметим, что для достаточно большого n, $r^{(0)}$ является практически равномерно распределенной $(n-c-1)$ битной строкой, так как $r^{(0)}$ составлена из битов в позициях $2,3,...,n-c$ случайного элемента из множества Z_{p-1} и соответственно их отклонение ограничено значением 2^{-c} (то есть статистическое расстояние между распределением $r^{(0)}$ и равномерным распределением на множестве $\{0,1\}^{n-c-1}$ ограничено 2^{-c}) [10].

Из **леммы 1** известно, что все значения $x^{(i)}$ следуют распределению, которое вычислительно неразличимо от равномерного на множестве Z_p^*. Согласно приведенному выше аргументу следует, что все $r^{(i)}$ должны следовать распределению, которое вычислительно неразличимо от R_{n-c-1}.

Более формально, доказательство следует из комбинированного аргумента. Если есть «отличитель» D между распределением, сгенерированным $IRG_{n,c}$ и распределением $R_{k(n-c-1)}$, то для определенного индекса i должен быть отличитель D_1 между распределением, которому следует $r^{(i)}$ и равномерному распределению R_{n-c-1}. Из этого следует, что возможно различить распределение которому следует $x^{(i)}$ и равномерное распределение на множестве Z_p^*. Это противоречит **лемме 1** и, особенно, предположению $c-DLSE$.

4. Анализ эффективности итеративного генератора

Итеративный генератор формирует $n-c-1$ псевдослучайные биты за счет возведения в степень по модулю со случайной c -битной экспонентой или осуществляет примерно $1{,}5\,c$ умножений по модулю на множестве Z_p^*. В сравнении с генератором Сундарама-Пателя, где такое же количество псевдослучайных бит потребовало бы $1{,}5\,n$ умножений по модулю.

Если предположим что **Теорема 1** не верна, то есть для некоторых j таких что $2 \le j \le n-c$ существует алгоритм A , который выполняется за время $T(n)$, и многочлен $P(\cdot)$ такой что (10):

$$\Pr ob[x \leftarrow Z_{p-1}; \mathrm{A}(g^x, x_2, ..., x_{j-1}) = x_j] > \frac{1}{2} + \frac{1}{P(n)}, \qquad (10)$$

тогда имеем алгоритм I^{A} позволяющий опровергнуть $c-DLSE$, который выполняется за время $O((n-c)cP^2(n)T(n))$, если $2 \le j < n-c-\log P(n)$ и за время $O((n-c)cP^3(n)T(n)$, если $n-c-\log P(n) \le j \le n-c$.

Генератор Блюма осуществляет операции многократного возведения в степень по модулю N случайного seed на множестве Z_N^*, где N — есть целое число Блюма ($N = PQ$ с P, Q простыми числами одного размера и сравнимыми с $3 \bmod 4$). На каждой итерации генератор выдает наименьший значащий бит текущего значения. Скорость такого генератора 1 бит за одно возведение в квадрат.

5. Выводы

Задачи дискретного логарифма относятся к классу трудно вычисляемых задач даже при небольших показателях экспоненты. Существуют другие криптографические примитивы, которые могут выиграть в эффективности и стойкости, например,: построение псевдослучайных функций, основанных на DDH проблеме (также еще известны проблемы: CDH, XLP, $DDLP$, $DLP(Inn(G))$, и др.). Наряду с использованным в статье $c-DLSE$ предположением существует ряд других, таких как: TDH, $DLSE$ и д.р. Предположение $c-DLSE$ не исследовано в достаточной степени, чтобы можно было на его основе приводить неопровержимые доказательства криптографической стойкости генератора.

Литература

1. Blum, L. A Simple Unpredictable Pseudo-Random Number Generator [Text] / L. Blum, M. Blum and M. Shub // SIAM J. Computing. — May 1986. — № 15(2).
2. Шнаер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С [Текст] / Б. Шнаер. — 2-е изд. — 610 с.
3. Schnorr, C. Security of Allmost ALL Discrete Log Bits [Electronic recource] / C. Schnorr // Electronic Colloquium on Computational Complexity. Report TR98-033. — Available at http://www.eccc.uni-trier.de/eccc/.
4. Blum, M. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits [Text] / M. Blum and S. Micali // SIAM J.Computing. — November 1984. — № 13(4).
5. Hastad, J. The Security of Individual RSA Bits [Text] / J. Hastad and M. NÄaslund // IEEE FOCS, 1998.
6. Patel, S. An Efficient Discrete Log Pseudo Random Generator [Text] / S. Patel and G. Sundaram // CRYPTO'98, LNCS 1462. — 1998.
7. Hastad, J. The Discrete Logarithm Modulo a Composite Hides O(n) Bits [Text] / J. Hastad, A. Schrift and A. Shamir // JCSS. — 1993. — № 47.
8. Long, D. The Discrete Log Hides O(log n) Bits [Text] / D. Long and A. Wigderson // SIAM J. Computing. —1988. — № 17.
9. Pollard, J. Monte-Carlo Methods for Index Computation (mod p) [Text] / J. Pollard // Mathematics of Computation. — 1978. — № 32(143).
10. Yao, A. Theory and Applications of Trapdoor Functions [Text] / A. Yao // IEEE FOCS, 1982.

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ЩО БАЗУЮТЬСЯ НА ДИСКРЕТНОМУ ЛОГАРИФМУ

В роботі представлена математична модель генератора псевдовипадкових чисел, розглядається проблематика вирішення задач дискретного логарифмування. Наведений аналіз алгоритмів генерації псевдовипадкових чисел, що базуються на вирішенні задачі дискретного логарифму. В якості прикладу розглядається генератор Сундарама-Пателя, наводяться якісні та кількісні характеристики стійкості даного генератора до основних видів атак.

Ключові слова: генератор, дискретний логарифм, псевдовипадкове число, крипостійкість, алгоритм, біт.

Замула Александр Андреевич, *кандидат технических наук, доцент, профессор кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: bit@kture.kharkov.ua***.

Семченко Денис Александрович, *аспирант, кафедра безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: bit@kture.kharkov.ua***.

Замула Олександр Андрійович, *кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій, Харківський національний університет радиоелектроніки, Україна.*

Семченко Денис Олександрович, *аспірант, кафедра безпеки інформаційних технологій, Харківський національний університет радиоелектроніки, Україна.*

Zamula Alexandr, *Kharkov National University of Radio Electronics, Ukraine,* ***e-mail: bit@kture.kharkov.ua***.

Semchenko Denis, *Kharkov National University of Radio Electronics, Ukraine,* ***e-mail: bit@kture.kharkov.ua***