ИССЛЕДОВАНИЯ АЛГОРИТМА ГПЧ НА ОСНОВЕ БИЛИНЕЙНОГО СПАРИВАНИЯ НА ТОЧКАХ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

Н.И. Червяков, М.Г. Бабенко, А.С. Назаров, И.С. Крисина
Северо-Кавказский федеральный университет, Ставрополь

Представлен алгоритм ГПЧ на основе билинейного спаривания на точках эллиптической кривой. Проводится исследование данного алгоритма при реализации в нейросетевом базисе.

Современные информационные системы требуют особых подходов к сохранению секрета. Одним из важных криптографических примитивов является генератор псевдослучайных чисел (ГПЧ). В настоящее время особую актуальность приобретают ГПЧ, построенные на точках эллиптической кривой. Это объясняется тем, что они удовлетворяют двум критериям – криптографической и статистической безопасности. Первый критерий получается вследствие того, что эллиптическая кривая позволяет:

- 1) строить криптографические протоколы с меньшей длиной ключа,
- 2) сохранять при этом уровень безопасности разработанного шифра.

Вследствие всего вышесказанного особую актуальность приобретает научная задача: разработка нового алгоритма построения ГПЧ, сочетающего в себе высокое быстродействие, хорошие статистические и криптографические свойства формируемой выходной последовательности.

В генерации и использовании случайных чисел нуждаются:

- механизмы целостности (ISO 8731-2 [7]);
- криптографические механизмы обмена ключами (протокол [8] Diffie-Hellman);
- схемы построения цифровых подписей (схема ElGamal);
- схема цифровой подписи (DSS) [9].

Кроме того, случайные числа используются для генерации псевдонимов, трафика и общения приложений. Это обеспечивает защиту от атак анализа трафика. Такой подход позволяет вычислить устойчивые и эффективные потоковые шифры [9].

Желательны случайные последовательности битов хорошего качества, то есть хорошего поведения в статистическом смысле и смысле непредсказуемости. Иначе, для криптоанализа существовала бы возможность вычислить последующие биты, учитывая сегмент этой битовой последовательности и располагая разумными компьютерными ресурсами [10]. За прошлые два десятилетия была проведена значительная работа по созданию и анализу генераторов псевдослучайных чисел или последовательностей битов [10].

Уровень случайности последовательности может быть определен с помощью статистических тестов. Они эмулируют вычисления, встречаемые на практике. Эти тесты позволяют проверить то, что при исследовании свойства последовательности совпадают с предсказанными, если каждый бит (или число) был взят в соответствии с равномерным распределением вероятности [11]. При разработке безопасные генераторы ключа должны удовлетворять определенным критериям, таким как длительный период, идеальное распределение k -кортежа, большая линейная сложность, хаотичность, рас-

пространение и нелинейность [11]. Большинство из них содержится в предложенной методике тестирования.

Теоретическая статистика предоставляет некоторые количественные меры случайности. Существует буквально бесконечное число критериев проверки случайности последовательности [6].

Тест на случайное блуждание оказывается одним из наиболее мощных и чувствительных тестов на наличие корреляций в ГПЧ. В частности, тест с использованием идеи случайного блуждания был одним из тестов, выявивших корреляции в ГПЧ типа «сдвиговой регистр» [1]. Другой тест на случайное блуждание позволил объяснить природу этих корреляций [3].

Существует несколько вариаций теста на случайное блуждание в различном количестве измерений [2]. Была рассмотрена одномерная модель направленного случайного блуждания [3].

Алгоритм теста.

Шаг 1.

1.1. Однонаправленное блуждание начинается в некотором узле одномерной решетки при дискретных значениях времени i с вероятностью $1 - \mu$.

1.2. Однонаправленное блуждание останавливается с вероятностью μ . Переход на шаг 2.

Шаг 2. В случае 1.2 переход на шаг 1. Начало нового блуждания.

Вероятность блуждания длиной n равна $P(n) = \mu^{n-1} (1 - \mu)$. Средняя длина блуждания равна $\langle n \rangle = \frac{1}{1 - \mu}$. Следует отметить, что рассмотренная модель представляет собой эффективный метод Вольфа для одномерной модели Изинга [3]. Это можно увидеть из того, что средний размер кластера в методе Вольфа равен средней длине блуждания для $\mu = \tanh\left(\frac{J}{k_B T}\right)$, где J – константа связи спинов.

Для построения схемы разделения секрета введем операцию спаривания на эллиптической кривой, аналогичную рассмотренной в работе [4]. Для любой точки $P \in E(F_{p^k})$ выполняется равенство $(n+1)P = O$, где O – точка в бесконечности. Обозначим $E(F_{p^k})$ множество точек эллиптической кривой, которая задана уравнением $y^2 = x^3 + ax + b$, над полями F_{p^k} . Для построения спаривания важно знать структуру группы точек эллиптической кривой. Ниже приведена теорема, описывающая структуру группы, когда эллиптическая кривая задана над полем F_{p^k} , где p – простое число, $k \geq 1$ и порядок группы точек эллиптической кривой выражается формулой $E(F_{p^k}) = p^k + 1 - t$.

Теорема 1 [5]. Если $t^2 = p^k, 2p^k, 3p^k$, то группа – циклическая. Если $t^2 = 4p^k$, то группа изоморфна $Z_{\sqrt{p^k-1}} \oplus Z_{\sqrt{p^k-1}}$ в случае $t = 2\sqrt{p^k}$, или изоморфна $Z_{\sqrt{p^k+1}} \oplus Z_{\sqrt{p^k+1}}$ в случае $t = -2\sqrt{p^k}$.

Если $t = 0, p^k \not\equiv 3 \pmod{4}$, то группа циклическая. Если $t = 0, p^k \equiv 3 \pmod{4}$, то группа или циклическая или изоморфна $Z_{\frac{p^k+1}{2}} \oplus Z_2$.

Из теоремы 1 следует, что в случае, если $t^2 = 4p^k$ и r – четное число, группа точек $E(F_{p^k})$ представляется в виде прямой суммы $Z_{\sqrt{p^k-1}} \oplus Z_{\sqrt{p^k-1}}$ или $Z_{\sqrt{p^k+1}} \oplus Z_{\sqrt{p^k+1}}$. Обозначим эти группы $E[l]$, где $l = \sqrt{p^k-1}$ или $l = \sqrt{p^k+1}$.

Так как $E[l]$ представляется в виде прямой суммы циклических групп, то можно зафиксировать некоторую образующую пару точек G и H таким образом, чтобы любую точку в $E[l]$ можно представить с их помощью. Рассмотрим точки $P = a_1G + b_1H$ и $Q = a_2G + b_2H$, принадлежащие $E[l]$, где $a_1, a_2, b_1, b_2 \in [0, l-1]$. Для некоторых зафиксированных целых $\alpha, \beta \in [0, l-1]$ определим функцию следующим образом:

$$L_{\alpha, \beta} : E[l] \times E[l] \rightarrow E[l] \text{ и } L_{\alpha, \beta}(P, Q) = (a_1, b_1 - a_2, b_2)(\alpha G + \beta H)$$

исключая тривиальный случай, когда α и β одновременно равны нулю.

Пусть G_1, G_2 и G_3 – три абелевы группы. Билинейное спаривание является отображением $e : G_1 \times G_2 \rightarrow G_3$ среди этих трех групп. Это отображение должно удовлетворять свойству билинейности: для $\alpha, \beta \in G_1, \gamma, \delta \in G_2$ справедливо $e(\alpha + \beta, \gamma) = e(\alpha, \gamma) + e(\beta, \gamma), e(\alpha, \gamma + \delta) = e(\alpha, \gamma) + e(\alpha, \delta)$.

Следующая теорема показывает, что функция $L_{\alpha, \beta}$ задает билинейное спаривание.

Теорема 2 [4]. Функция $L_{\alpha, \beta}$ обладает следующими свойствами:

1. Тожественность.

Для всех $P \in E[l], L_{\alpha, \beta}(P, P) = O$.

2. Билинейность.

Для всех $P, Q, R \in E[l]$

$$L_{\alpha, \beta}(P + Q, R) = L_{\alpha, \beta}(P, R) + L_{\alpha, \beta}(Q, R) \\ \text{и } L_{\alpha, \beta}(P, Q + R) = L_{\alpha, \beta}(P, Q) + L_{\alpha, \beta}(P, R).$$

3. Ассиметричность.

Для всех $P, Q \in E[l]$

$$L_{\alpha, \beta}(P, Q) = -L_{\alpha, \beta}(Q, P).$$

4. Невырожденность.

Для всех $P \in E[l]$

$$L_{\alpha, \beta}(P, O) = O.$$

Кроме того, если $L_{\alpha, \beta}(P, Q) = O$ для всех $Q \in E[l]$, тогда $P = O$.

Функция $L_{\alpha, \beta}$ называется спариванием, поскольку она отображает $E[l] \times E[l] \rightarrow E[l]$ (аналогично традиционным спариваниям Вейля и Тейта).

На базе выше изложенного спаривания предложим алгоритм построения ГПЧ.

Алгоритм ГПЧ.

Вход: p – простое число, $a, b, \alpha, a_1, b_1 \in F_p$, где α – квадратичный невычет в F_p^*

Выход: ГПЧ

1. Для $i = 1$ до $n-1$ выполнять: $(a_{i+1}, b_{i+1}) = (a_1, \alpha b_1)(a_i, b_i)$.

2. Вывод $a_n G + b_n H_n$.

3. Конец.

Условием для того, чтобы этот алгоритм мог построить последовательность максимального периода $p^2 - 1$, является $ord\{a_1x + b_1\} = p^2 - 1$ в поле $F_{p^2}^* = \{ax + b \mid x^2 = \alpha, \alpha, a, b \in F_p^*\}$, где α - квадратичный невычет в F_p^* .

Рассмотренный выше алгоритм построения ГПЧ был реализован в среде программирования Microsoft Visual Studio 2010 на языке программирования C++. Затем над построенным ГПЧ был проведен тест на наличие корреляций «Критерий направленного случайного блуждания». Алгоритм теста был описан выше.

Было произведено 20 χ^2 -проверок по критерию направленного случайного блуждания с $\mu = \frac{1}{2}$. Был применен «Алгоритм Р» случайного блуждания:

1. При $r < \mu$ совершается шаг вправо.
2. При $r \geq \mu$ остановка (где r – случайное число, порожденное генератором).

Таким образом, $\mu = \frac{1}{2}$ означает, что в проверках участвует один бит генератора. В результате проведения теста корреляции направленного блуждания были получены результаты для генератора, построенного на основе билинейного спаривания точек эллиптической кривой. Распределение выходных величин незначительно отличается от χ^2 -распределения. Каждый из двадцати тестов пройден в том смысле, что получены вполне приемлемые результаты построенного генератора псевдослучайных чисел.

Из всего вышесказанного можно сделать вывод, что предложенный ГПЧ обладает большим периодом. Проведенные тесты показали, что построенный ГПЧ обладает хорошими статистическими свойствами.

В работе [12] представлены новые методики, основанные на использовании искусственных нейросетевых архитектур для улучшения традиционных генераторов, таких как ANSI X.9, базовых для DES и IDEA. Также в этой работе предлагается методика тестирования с использованием нейронных сетей, разработанная для оценки свойства непредсказуемости. Этот тест непредсказуемости, наряду с обычно используемыми статистическими тестами и тестами нелинейности, предложен как методология оценки устойчивости генераторов псевдослучайных чисел. Посредством этой методологии оценены классические и предложенные генераторы. Показано, что предложенные генераторы ведут себя значительно лучше, чем традиционные, в частности в терминах непредсказуемости [13].

По результатам применения методики тестирования данного ГПЧ показано, что разработанный генератор псевдослучайных чисел обладает хорошими статистическими свойствами.

Литература

1. Vattulainen I., Ala-Nissila T., Kankaala K // Phys. Rev. Lett. 73, 2513, 1997.
2. Binder K., Heermann D.W. Monte Carlo simulation in statistical physics. Springer-Verlag, Berlin, 1992.
3. Shchur L.N., Heringa J.R., Blöte H.W // Physica A241, 1997. P. 579.
4. Lee H.-S. A self-pairing map and its applications to cryptography // Applied Mathematics and Computation. 2004. Vol. 151. P. 671–678.
5. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Алгоритмические основы эллиптической криптографии. М.: Изд-во МЭИ, 2004. 499 с.
6. Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. – М.: Издательский дом «Вильямс», 2001. 832 с.

7. ISO 8731-2, «Approved Algorithms for Message Authentication, Part 2: Message Authenticator Algorithm (MAA)».
8. Diffie W., Hellman M.E. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22, No 6. P. 644-654.
9. Schneier B. Applied Cryptography. J. Willey & Sons, second edition, 1996.
10. Zeng K., Yang C.-H., Wei D.-Y., Rao T.R.N. Pseudo random bit generators in stream cipher cryptography // IEEE Computer, 1991. P. 8-17.
11. Simmons G. J. (editor). Contemporary Cryptology. The Science of Information Integrity // IEEE Press, 1992.
12. Червяков Н.И. и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.
13. Karras D.A., Zorkadis V. Improving pseudorandom bit sequence generation and evaluation for secure internet communications using neural network techniques // IEEE, 2003. P. 1367–1372.