УДК 004.7 **doi: 10.26906/SUNZ.2018.4.139**

В. Я. Певнев, А. В. Фролов, В. В. Фролов

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков, Украина

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ДИНАМИЧНЫМИ ПАРАМЕТРАМИ

В работе представлены результаты экспериментальных исследований усовершенствованных конгруэнтных генераторов и генераторов на основе регистров сдвига с изменяемыми параметрами. Модификация генераторов заключалась в суммировании выходных последовательностей с двух генераторов. Приведены результаты тестирования выработанных псевдослучайных последовательностей генераторами с изменяющимися порождающими полиномами различной длины и начальными состояниями для генераторов на основе регистров сдвига и параметра m для конгруэнтного генератора. В результате было отмечено улучшение статистических свойств сгенерированных псевдослучайных последовательностей и значительное повышение устойчивости к существующим методам криптоанализа.

Ключевые слова: генератор, регистр сдвига, конгруэнтный генератор, криптостойкость, выходная последовательность, криптоанализ.

Введение

Развитие инфокоммуникационных технологий в конце XX - начале XXI столетия привело к бурному росту интереса к вопросам обеспечения безопасности. В информационных технологиях выделяется специальность кибербезопасность (КБ). Кибербезопасность является неотъемлемой частью информационной безопасности в компьютерных системах [1,2]. Основные вопросы, которые решает КБ это обеспечение конфиденциальности, доступности и целостности информации, циркулирующей в системе. Решению этих вопросов посвящены работы многих авторов. Как у всякой развивающейся науки существует достаточно противоречивые взгляды на пути обеспечения данных свойств систем КБ. Наиболее важным, с точки зрения авторов, является проблема доступности. Ее практически полностью отдали на откуп специалистам по надежности, функциональной безопасности, организации и управлению работой компьютерных систем и сетей. Хотя при отсутствии доступа к каким –либо устройствам говорить об обеспечении целостности или конфиденциальности вообще не приходится. Задача обеспечения целостности возникает на каждом временном цикле существования информации. В некоторых случаях методы обеспечения целостности совпадают на различных этапах, в некоторых – они инклюзивные [3].

Наиболее быстро и всесторонне развивается та часть КБ, которая связана с обеспечением конфиденциальности. Это обусловлено тем, что после снятия грифов секретности с криптографических протоколов, в эту область пришло большое количество специалистов с силовых структур, занимавшихся вопросами шифрования, молодежь, которой это было просто интересно. Появилось большое количество разнообразных шифров, среди которых можно выделить AES, Калину, Кузнечик [4-6]. Большинство этих криптографических систем относится к блочным симметричным шифрам. Однако в реальной жизни очень часто приходится использовать поточное шифрование. Эту функцию могут выполнять и большинство симметричных алгоритмов. Вместе с тем задача получения случайной последовательности стоит достаточно остро. Такие последовательности широко используются в моделировании, при разработке разного вида игр. Наилучшими генераторами случайных чисел являются физические датчики, в которых источником случайности являются тепловой шум, дробовой шум, фотоэлектрический эффект и другие физические явления [7,8]. Однако такие последовательности невозможно повторить. Выходом из такого положения является создание псевдослучайных последовательностей (ПСП).

Наиболее распространённые на данный генераторы ПСП являются конгруэнтные генераторы и генераторы на основе регистров сдвига. В основе конгруэнтных генераторов стоят числовые последовательности, в которых каждый член зависит от одного или нескольких предыдущих. В основе генераторов на основе регистров сдвига лежит порождающий полином. Данные генераторы не являются достаточно криптостойкими, так как достаточно легко взламываются, но имеют большое преимущество в простоте и быстроте работы. Одним из вариантов увеличения криптостойкости генерируемых ПСП является использование двух генераторов, в которых результирующая ПСП является суммой двух ПСП. При таком подходе значительно увеличивается период ПСП. В работах [9,10] было предложено использование генераторов ПСП с изменяемыми параметрами, что привело к созданию систем устойчивым к современным методам криптоанализа.

Целью работы является сравнительный анализ статистические свойств ПСП, вырабатываемых конгруэнтными генераторами и генераторами на основе регистров сдвига, в которых используются динамично изменяемые параметры.

Основная часть

Представленная работа состоит из описания и результатов проведения исследования двух типов генераторов ПСП – конгруэнтного и генератора на основе регистрах сдвига. Главные особенности представленных генераторов - это использование динамично изменяемых параметров. В зависимости от типа исследуемого генератора это могут быть параметры a и c для конгруэнтного генератора и порож-

дающие полиномы для генератора на основе регистрах сдвига. Кроме использования динамичных параметров для повышения криптостойкости выходной последовательности была разработана модификация алгоритма генерации ПСП, состоящая в использовании операции XOR над сгенерированными последовательностями определенной длины, полученными от двух регистров, имеющих различную разрядность. Используемые регистры меняют свои параметры не реже чем через каждые 2*N - 1 битов, где N произведение разрядности двух регистров.

Описание, проведение и результаты эксперимента с конгруэнтными генераторами. Для проведения экспериментальных исследований была взята улучшенная версия классического конгруэнтного генератора, т.к. она имеет лучшие статистические свойства [9]. Алгоритм заключается в следующем:

– берется два классических конгруэнтных генератора;

– генерируются по одной последовательности от каждого генератора;

– производится операция побитового сложения (XOR) между двумя сгенерированными последовательностями.

Для тестирования свойств модификации алгоритма, было проведено сравнительный анализ между 10-ю сгенерированными последовательностями с использованием статических параметров (a, c, m) генератора и 10-ю сгенерированными последовательностями с использованием динамичных параметров (a, c, m). Для статического генератора было использовано пять групп параметров a и c, которые приведены в таблице 1 и параметр m равен 2^{20}-1 для каждой группы. Для динамичного генератора были использованы идентичные группы параметров a и c (табл. 1), которые случайным образом выбирались и подставлялись в генератор при каждой новой генерации. Для рандомизации параметра m, было взято значение 2^{20}-1 и 9 простых чисел наиболее близких по спаданию к 2^{20}-1: 1048423, 1048433, 1048447, 1048507, 1048517, 1048549, 1048559, 1048571, 1048573. Простые числа имеют хорошие статистические свойства, а их приближенность к максимальному модулю (2^{20}-1) обусловлено тем, что они имеют наименьшую разницу в количестве единиц в бинарной форме и не приведет к росту количества нулей в общей статистике. Они также случайным образом выбирались из списка и использовались при новых итерациях.

Таблица 1 – **Перечень используемых параметров *a*, *c***

Группа	1	2	3	4	5
a	84589	36261	17221	2416	4096
c	45989	66037	107839	374441	150889

Перечень проведенных тестов:

– количество нулей и количество единиц;

– количество повторений групп символов;

– предельное (максимальное) количество повторений нулей и единиц.

Приведенные тесты хорошо известны и широко применяются при оценке случайности различных последовательностей [11]. При проведении тестирования генерировались ПСП размером в 10000 элементов. Результаты тестирования ПСП с различными параметрами генераторов (ПГ) представлены в табл. 2.

Таблица 2 – **Результаты тестирования ПСП с различными параметрами конгруэнтных генераторов**

Кол-во нулей	Кол-во единиц	Кол-во повторений групп символов						Предельное кол-во повторений	
		00	11	000	111	0000	1111	Единиц	Нулей
ПГ1: *a*=84589, *c*=45989. ПГ2: *a*=36261, *c*=66037									
4973	5027	1648	1670	689	731	314	333	11	11
ПГ1: *a*=84589, *c*=45989. ПГ2: *a*=17221, *c*=107839									
4959	5041	1655	1699	679	715	316	345	12	12
ПГ1: *a*=84589, *c*=45989. ПГ2: *a*=2416, *c*=374441									
4991	5009	1661	1654	703	741	332	324	14	11
ПГ1: *a*=84589, *c*=45989. ПГ2: *a*=4096, *c*=150889									
4933	5067	1618	1696	713	754	335	351	15	14
ПГ1: *a*=36261, *c*=66037. ПГ2: *a*=17221, *c*=107839									
5016	4984	1686	1642	706	705	336	326	12	14
ПГ1: *a*=36261, *c*=66037. ПГ2: *a*=2416, *c*=374441									
4910	5090	1616	1720	675	736	326	345	11	11
ПГ1: *a*=36261, *c*=66037. ПГ2: *a*=4096, *c*=150889									
5042	4958	1724	1662	727	712	354	318	12	10
ПГ1: *a*=17221, *c*=107839 ПГ2: *a*=2416, *c*=374441									
4992	5008	1640	1681	729	711	348	353	24	12
ПГ1: *a*=17221, *c*=107839. ПГ2: *a*=4096, *c*=150889									
4952	5048	1639	1691	707	740	309	351	24	14
ПГ1: *a*=2416, *c*=374441. ПГ2: *a*=4096, *c*=150889									
4838	5162	1581	1752	697	822	313	395	14	15
Сумма для первого, второго теста и среднее (максимальное) значение для третьего теста									
49606	50394	16468	16878	7025	7478	3283	4552	15(24)	12(15)
Результаты тестирования ПСП с динамическими параметрами.									
49954	50046	16675	16730	7145	7226	3330	3371	16	16

Согласно полученным данным средние значения отклонения от половинного значения для статических параметров составило 0,00394 и для динамических параметров 0,00046. Оба эти результаты удовлетворяют критерию, утвержденному NIST, который составляет 0,01 [11].

При рассмотрении количества повторений групп символов следует отметить, что результаты появления пар символов незначительно отличаются, при этом составляют менее одного процента. Появления по три и четыре символа имеет значительное отличие при использовании генераторов с фиксированными параметрами, в то время, как у генераторов с динамичными параметрами расхождения были меньшими. Предельное количество повторений нулей и единиц для генераторов с фиксированными параметрами менялось от 11 до 24 для единиц, и от 10 до 15 для нулей. При этом среднее значение данного теста составило 15 и 12 символов соответственно. У генераторов с динамичными параметрами для единиц и нулей это значение составило 16 знаков. Таким образом, можно сделать вывод о том, что использование динамично изменяемых параметров позволяет получить более случайные последовательности, способные противостоять известным методам криптоанализа.

Описание, проведение и результаты эксперимента с генераторами на основе регистров сдвига. Для решения поставленной задачи был разработан ряд экспериментов, конечной целью которых было проведение:

– анализа влияния начальных состояний регистра на статистические свойства результирующей последовательности;

– анализа влияния используемого полинома на статистические свойства генератора;

– анализа среднего отклонения символов в результирующей последовательности.

Исследование проводилось на последовательности в 3100 битов, на которой выполнялись 3 статистических теста: частотный, на группы битов и на максимальное количество подряд идущих одинаковых битов. Тестирование проводилось на группах из 30 и 100 последовательностях.

Всего было произведено 24 эксперимента на различных комбинациях полиномов, по 12 на приводимых полиномах и 12 неприводимых. Кроме этого, было произведено 10 экспериментов при различных начальных состояниях регистров, половина из которых - на случайных состояниях, остальные - на специально подобранных. Вычисление среднего отклонения осуществлялось на результатах, полученных при исследовании неприводимых полиномов. Для проверки неприводимых полиномов были выбраны все неприводимые полиномы разрядностью 17 и 31 (17, 3, 0), (17, 5, 0), (17, 6, 0), (31, 3, 0), (31, 6, 0), (31, 7, 0), (31, 13, 0). Данные полиномы были взяты из [12]. В качестве составных полиномов были подобраны максимально различные случаи, также часть полиномов было сгенерировано случайным образом, используя сторонний генератор.

Для проверки начальных состояний было взято 5 случайных шестнадцатеричных чисел. Специальные числа были вычислены так, чтобы они отображали наиболее редкие и сложные для генератора случаи.

Для эксперимента по определению среднего отклонения количества единиц в последовательностях от половинного значения (1550), для удобства анализа, была выбрана группа из 100 последовательностей.

Для проверки начальных состояний было взято 5 случайных шестнадцатеричных чисел: 5F2348EC, 8EA5E59A, C6E79B0F, 2C5AA385, 6924226A. Подобранные числа были вычислены так, чтобы они отображали наиболее редкие и сложные для генератора случаи: AAAAAAAA, 11111111, FFFFFFFF, 88888888, A1A1A1A1. Для обоих регистров использовались одинаковые начальные состояния. Результаты эксперимента в процентах представлены в табл. 3.

Таблица 3 – **Таблица состояний**

	1	2	3	4	5
Случайные	50,02	50,11	49,89	49,89	49,82
Подобранные	49,89	49,89	49,89	50,08	49,89

В результате проведения проверки различных начальнх состояний регистров, было опредлено, что влияниние на статистические свойства регистров, на последовательности 3100 битов, начальные состояние практически не оказывают. Могут попадаться такие состояния, когда статистика резко ухудшаеться, однако их не много и с увеличением длины последовательности их влияние минимизируется.

В ходе тестирования приводимых полиномов использовались случайно подобранные полиномы, так как проверить все не представляется возможным, исследованы наиболее различные друг от друга полиномы.

В табл. 4 представлены обработанные результаты проведенного эксперимента - средние значения отклонения от половинного значения в процентах при генерации ПСП, используя 12 приводимых и 12 неприводимых полиномов.

Как видно из табл.4, первых два результата для приводимых полиномов являются аномальными и не отражают закономерность. Причина такой ситуации заключается в том, что количество отводов регистра было минимально (только крайние разряды заполнены единицами) и максимальное количество (все разряды заполнены единицами).

Операция XOR минимизирует влияние статистических свойств составных полиномов. Также следует отметить, что далеко не все составные полиномы генерирует гамму с плохими статическими свойствами. На статистику больше влияет количество отводов регистра и где они расположены, чем неприводимость полинома. Однако все неприводимые полиномы дают практически полностью случайную последовательность.

Для измерение среднего отклонения был проведен анализ 100 последовательностях на полино-

мах 17,5,0 и 31,3,0 при различных значениях на начальных состояниях. Результаты эксперимента представлены в табл. 5, где знак минус означает, что количество нулей превышает количество единиц.

Таблица 4 – **Средние значения отклонения от половинного значения**

	1	2	3	4	5	6	7	8	9	10	11	12
Приводимые	47,21	0	50,15	49,85	49,76	50,02	50,37	49,69	49,89	49,73	50,02	49,92
Неприводимые	49,76	50,15	50,21	49,98	50,15	49,95	49,98	49,98	50,18	49,98	49,82	50,08

Таблица 5 – **Исходные значения отклонения**

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	-56	-26	-10	-92	50	-30	44	36	-22	-14	-18	20	140	-10	-78	-68	124	28	-60	-56
N	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
	-54	-4	30	-32	-50	-46	-2	-48	14	-66	-88	26	22	-72	92	-64	-56	-22	34	32
N	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
	-64	100	28	8	36	4	-26	-22	-50	24	-92	-28	56	-6	78	-44	68	10	-30	-8
N	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
	100	8	-86	88	36	22	80	48	-40	10	28	104	-84	108	-44	-20	10	82	-118	-72
N	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
	42	4	-44	-44	156	44	-44	-14	58	0	72	0	12	-2	-14	86	-8	12	-66	-2

В табл.6 указано, в каких пределах (в процентах) находится отклонение, и соответствующее этим пределам количество реализаций. Если подсчитать среднее отклонение в процентах, то оно составляет менее 0,032%.

Таблица 6 – **Пределы отклонения**

k=0	0<k<1	1<k<2	2<k<3	3<k<4	4<k<5	k>5
2	41	28	21	5	2	1

ПСП, полученная с помощью генератора на регистрах сдвига с динамичными параметрами, была подвергнута криптоанализу. Для этого по полученной ПСП были проведены попытки получить структуру регистра. В результате был сделан вывод о невозможности восстановить структуру регистра, подтвердивший теоретические предсказания [10].

Преимущества данной модификации заключается в следующем:

– вследствие использования операции сложения по модулю 2, длина получаемой последовательности становится равна: 2^{n*m} - 1, где n, m – разрядности используемых регистров [10]. Изменение параметров регистров позволяет получить длины получаемой последовательности примерно $2^{k1*n*k2*m}$ – 1; где $k1$, $k2$ – размер массива изменяемых параметров соответствующих регистров, n, m – средняя разрядность этих регистров;

– ввиду изменения параметров регистров, становится практически невозможным криптоанализ генератора;

– использование предложенных регистров делает практически невозможным восстановление ПСП без знания соответствующих ключей.

Выводы

В представленной работе было предложено результаты исследований улучшенных генераторов ПСП. За счет использования динамичных параметров было достигнуто улучшение статистических свойств генератора по сравнению с соответствующими генераторами с постоянными параметрами. При сравнении статистических характеристиках на полученных ПСП на конгруэнтных генераторах и генераторах на регистрах сдвига было установлено, что второй тип генераторов имеет несколько лучшие характеристики сгенерированных ПСП. Следует отметить, что оба типа генераторов удовлетворяют требования NIST, превышая их более чем на два порядка. Оба типа генераторов, использующие динамично изменяемые параметры обладают значительной устойчивостью к известным криптоатакам, что позволяет их применение в современных криптосистемах. С точки зрения быстродействия генераторы, использующие регистры сдвига в аппаратном исполнении обладают лучшими параметрами, но более сложны в реализации.

СПИСОК ЛИТЕРАТУРЫ

1. Певнев В.Я. Эффективность информационной безопасности замкнутых систем / В. Я. Певнев // Радіоелектронні і комп'ютерні системи. - 2009. - № 5. - С. 82–85.
2. Певнев В.Я. Математическая модель информационной безопасности / В. Я. Певнев, М. В. Цуранов// Системи обробки інформації. – 2010.-№3. - С. 62-64.

3. Певнев В.Я. Методы обеспечения целостности информации в инфокоммуникационных системах / В.Я. Певнев // Вісник Національного технічного університету ХПІ. Серія: Техніка та електрофізика високих напруг. – 2015. - № 51. – С. 74-77
4. Federal Information Processing Standards Publication 197 November 26, 2001 Specification for the ADVANCED ENCRYPTION STANDARD (AES)
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.
6. ГОСТ Р 34.12-2015Информационная технология. Криптографическая защита информации. Блочные шифры.- Введ. 01-01-2016.- М.: Стандартинфо, 2016
7. Li, Pu; Wang, Yun-Cai; Zhang, Jian-Zhong (2010-09-13). "All-optical fast random number generator". *Optics Express*. 18 (19): 20360–20369. doi:10.1364/OE.18.020360. ISSN 1094-4087.
8. Подорожный И. В. Обзор аппаратных генераторов случайных чисел // Молодой ученый. — 2016. — №1. — С. 190-194. — URL https://moluch.ru/archive/105/24688/ (дата обращения: 28.05.2018).
9. Фролов, А.В. Анализ модификации конгруэнтного генератора псевдослучайных чисел / А.В. Фролов, В.Я. Певнев // Материалы I МНТК Проблемы научно-технического и правового обеспечения кибербезопасности в современном мире. – Х., 2016 – С. 33.
10. Фролов, В.В. Исследование генератора псевдослучайных чисел на регистрах сдвига с обратной связью / В.В. Фролов, В.Я. Певнев //Материалы I МНКТ Проблемы научно-технического и правового обеспечения кибербезопасности в современном мире. - Х., 2016 – С. 32-33.
11. Soto, J. Statistical Testing of Random Number Generators/ J. Soto – National Institute of Standards & Technology, 2009. – pp. 3.
12. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер — Второе издание Триумф, 2013. — 816 с.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет "Харківський політехнічний інститут", Харків
Received (Надійшла) 19.06.2018
Accepted for publication (Прийнята до друку) 22.08.2018

Результати досліджень генераторів псевдовипадкових послідовностей з динамічними параметрами

В. Я. Пєвнєв, О. В. Фролов, В. В. Фролов

В роботі представлені результати експериментальних досліджень удосконалених модифікованих конгруентних генераторів і генераторів на основі регістрів зсуву із змінними параметрами. Модифікація генераторів полягала в використанні вихідних послідовностей з двох генераторів з різними параметрами шляхом їх бінарного додавання. Наведено результати тестування вироблених псевдовипадкових послідовностей генераторами на основі регістрів зсуву, за рахунок зміни вихідного стану та використання поліномів, які породжують, різної довжини, і параметра m для конгруентного генератора. В результаті було відзначено поліпшення статистичних властивостей генерованих псевдовипадкових послідовностей і значне підвищення стійкості до існуючих методів криптоаналізу.

Ключові слова: генератор, регістр зсуву, конгруентний генератор, криптостійкость, вихідна послідовність, криптоаналіз.

Results of research of generators of pseudo-random sequences with dynamic parameters

V. Pevnev, A. Frolov, V. Frolov

This work consists of a description and the results of the study of two types of PRS generators - congruent and generator based on shift registers. The main features of the presented generators are the use of dynamically changing parameters. These can be parameters a and c for a congruent generator and generating polynomials for a generator based on shift registers. In addition to using dynamic parameters to increase the cryptostability of the output sequence, a modification of the algorithm for generating of PRS has been developed, consisting in using the XOR operation between the generated sequences of a certain length obtained from two registers having different bits. To test the properties of a congruent generator, a comparative analysis has been performed between 10 generated sequences using the generator's static parameters (a, c, m) and 10 generated sequences using dynamic parameters (a, c, m). For the static generator, five groups of parameters a, c and parameter m with value 220-1 for each group have been used. For the dynamic generator, identical groups of parameters a and c have been used, which were randomly selected and insert into the generator for each new iteration. It should be noted that the results of the appearance of pairs of symbols are slightly different, with less than one percent. Appearances of three and four groups of characters have a significant difference when using generators with fixed parameters, while for generators with dynamic parameters the discrepancies were smaller. As a result of the conducted researches conclusions are drawn that the use of dynamically changing parameters allows to obtain more random sequences capable of resisting the known methods of cryptanalysis. In the study of generators based on shift registers, a series of experiments have been developed whose ultimate goal was to analyze the effect of the initial states of the register on the statistical properties of the resulting sequence, analysis of the influence of the polynomial that was used on the statistical properties of the generator and analysis of the average deviation of symbols in the resulting sequence. Based on the results of the experiments, conclusions are drawn that using the new generator configuration significantly increases period of PRS, making it impossible to restore the generator structure. When comparing the statistical characteristics of the obtained PRS on the congruent generators and the generators on shift registers it has been found that the second type of generator has slightly better characteristics of the generated PRS. It should be stressed that both types of generators satisfy NIST requirements, exceeding them by more than two orders of magnitude. Both types of generators using dynamically changing parameters have considerable resistance to known crypto attacks, which allows their use in modern cryptosystems.

Keywords: generator, shift register, congruent generator, cryptostability, output sequence, cryptanalysis.